O COSO *ENTERPRISE RISK MANAGEMENT* E O *BUSINESS PROCESS MANAGEMENT* NO GERENCIAMENTO DE RISCOS DOS ÓRGÃOS E ENTIDADES DO PODER EXECUTIVO FEDERAL

THE COSO ENTERPRISE RISK MANAGEMENT AND BUSINESS PROCESS MANAGEMENT IN THE MANAGEMENT OF RISKS OF THE ORGANS AND ENTITIES OF THE FEDERAL EXECUTIVE BRANCH

Alexandre Borba de Oliveira, UFSM, alexandre03@gmail.com; Fernando do Nascimento Lock, UFSM, fernandolock@hotmail.com; Alejandra Palazuelos Pereira, UFSM, alepereirapalazuelos@gmail.com.

RESUMO

O objetivo deste estudo é analisar a possibilidade de integração entre o COSO *Enterprise Risk Management* e o *Business Process Management*, no processo de gestão de riscos dos órgãos e entidades do Poder Executivo Federal. A pesquisa é de caráter exploratório, de abordagem qualitativa e quanto aos procedimentos, caracterizada como bibliográfica e documental. Foram analisados conceitos e fundamentos de instrumentos capazes de contribuir no processo de gestão de riscos das organizações públicas. As análises realizadas evidenciaram que essa integração pode auxiliar no processo de gestão de riscos, através de atividades organizadas e integradas, a fim de que os riscos possam ser gerenciados de forma otimizada, através de uma análise horizontal dos processos envolvidos. Entretanto, existem limitações relacionadas a cultura organizacional, entre outras, que podem comprometer essa integração.

Palavras-chave: Gestão de Riscos; COSO *Enterprise Risk Management*; *Business Process Management*.

ABSTRACT

The objective of this study is to analyze the possibility of integration between COSO Enterprise Risk Management and Business Process Management in the risk management process of the organs and entities of the Federal Executive Branch. The research is exploratory, with a qualitative and procedural approach, characterized as bibliographic and documentary. Were analyzed concepts and fundamentals of tools capable of contributing to the risk management process of public organizations.The analysis showed that this integration can help in the process of risk management, through organized and integrated activities, so that risks can be optimally managed, through a horizontal analysis of the processes involved. However, there are limitations related to organizational culture, among others, that may compromise this integration.

Keywords: *Risk Management; COSO Enterprise Risk Management; Business Process Management.*

1. Introdução

A Controladoria-Geral da União e o Ministério do Planejamento, Orçamento e Gestão determinaram, por meio da Instrução Normativa Conjunta MP/CGU n° 01/2016, a adoção de uma série de medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos e à governança, aos órgãos e entidades do Poder Executivo Federal. Estes deverão instituir Política de Gestão de Riscos para definir como e com qual periodicidade os riscos serão identificados, avaliados, tratados e monitorados e como será medido o desempenho da própria gestão de riscos. Além disso, a mesma Instrução Normativa ressalta que a política de gestão de riscos deve especificar as diretrizes sobre como a gestão de riscos será integrada ao planejamento estratégico, aos processos e às políticas da organização.

Para cumprir a exigência legal, garantir o cumprimento da missão institucional e ter êxito em atingir os objetivos estabelecidos, é necessário que a gestão destes órgãos e entidades seja capaz de tomar decisões corretas para enfrentar de maneira proativa os eventos que possam afetar os seus resultados. Dessa forma, a gestão de riscos precisa ser ativa, objetiva e integrada aos planos estratégicos, programas, projetos e processos das organizações.

Diante do contexto apresentado nos parágrafos anteriores, surgem as constatações que motivam a formulação da questão norteadora da presente pesquisa: De que forma a integração entre o COSO-ERM e o BPM poderá auxiliar no processo de gestão de riscos dos órgãos e entidades do Poder Executivo Federal?

Considerando o COSO-ERM como referência de modelo de gestão de riscos (isto não implicou no julgamento deste ser o melhor modelo ou o mais adequado) e as técnicas de gerenciamento de processos de negócios do BPM, que apresentam requisitos para que as organizações tornem seus processos mais eficientes, e levando em consideração o problema anteriormente apresentado, esta pesquisa possui como principal objetivo, analisar, sob o ponto de vista teórico, a possibilidade de integração entre o COSO-ERM e o BPM, no processo de gestão de riscos dos órgãos e entidades do Poder Executivo Federal.

Com as mudanças que vêm sendo introduzidas na administração pública, a qualidade da gestão dos gestores públicos torna-se fundamental para a melhoria dos resultados alcançados pelo setor público. As atividades públicas possuem características próprias, pois visam produzir resultados e valores essenciais à população, o que requer conteúdos e metodologias específicas, que sejam adaptadas à realidade dos órgãos e entidades da Administração Pública Federal.

No setor público, os riscos devem ser gerenciados mantendo-se, em primeiro plano, o interesse público. Essa tarefa de estimar os riscos e avaliar alternativas tecnicamente válidas e socialmente aceitáveis, recai sobre o dirigente máximo de cada órgão ou entidade, que passa a ser o principal responsável pelo estabelecimento da estratégia de organização e pela estrutura de gerenciamento de riscos, devendo estar preparado para tomar decisões.

Dentro deste contexto, precisam ser analisadas algumas alternativas, como a combinação de modelos de gestão riscos com técnicas de gerenciamento de processos, avaliando esses requisitos, a fim de que as organizações tornem seus processos mais eficientes, gerando melhores processos decisórios e consequentemente melhores resultados.

Visando o alcance dos objetivos acima propostos, este artigo está organizado da seguinte forma: Introdução; Gestão de riscos nos órgãos e entidades do Poder Executivo Federal; COSO *Enterprise Risk Management - Integrated Framework*; *Business Process Management* (BPM); Método de pesquisa; COSO-ERM integrado com o BPM; Principais limitações do COSO-ERM e do BPM; e Considerações finais.

2. Gestão de riscos nos órgãos e entidades do Poder Executivo Federal

A Controladoria-Geral da União (CGU) e o Ministério do Planejamento, Orçamento e Gestão (MP) determinaram aos órgãos e entidades do Poder Executivo Federal, por meio da Instrução Normativa Conjunta MP/CGU n° 01/2016, a adoção de uma série de medidas para a sistematização de práticas relacionadas à gestão de riscos, controles internos e governança, com destaque para a política de gestão de riscos a ser instituída, a qual deve especificar ao menos: princípios e objetivos organizacionais, diretrizes, competências e responsabilidades para a efetivação da gestão de riscos no âmbito do órgão ou entidade (Brasil, 2016).

Para Assi (2012), é importante estabelecer claramente os objetivos e o comprometimento da organização em relação à gestão de riscos. Abordar quais são as principais justificativas da organização para gerenciar riscos e as ligações entre os objetivos e as políticas da organização em consonância com a política de gestão de riscos.

Os riscos são enfrentados por todas as organizações e são inerentes a qualquer atividade. Eles interferem na possibilidade da organização sobreviver e na qualidade de seus produtos e serviços. O risco é inerente aos negócios e sempre estará presente, podendo ser de baixo ou alto nível de perigo, dependendo das medidas preventivas e de segurança existentes. Não existe forma prática de reduzi-lo a zero (AVALOS, 2009; ASSI, 2012).

Por isso, a gestão de riscos e o planejamento estratégico são importantes para as organizações públicas diante do cenário atual de transformações e desafios que passam o país e o mundo, bem como para definir o rumo das organizações no longo prazo.

Segundo Kanaane et al. (2010), o planejamento estratégico no setor público tem como foco a missão, a visão e as metas a serem alcançadas, considerando as demandas e expectativas dos cidadãos e da sociedade. O planejamento estratégico será um mecanismo facilitador da gestão pública na medida em que forem adotadas práticas voltadas a dimensionar e agilizar os processos. De forma semelhante, Andrade (2012), comenta que o planejamento elaborado pelos órgãos públicos deve estar alinhado com as prioridades definidas por seus gestores, considerando as políticas governamentais que podem influenciar seus objetivos.

Tendo em vista que os riscos podem surgir da incerteza natural de vários cenários, como o político, o econômico, o social, entre outros, um dos instrumentos de governança para lidar com isso é a gestão de riscos. Segundo a ABNT (2009, p. 23) "A gestão de riscos é vista como central nos processos de gestão da organização, de tal forma que os riscos sejam considerados em termos do efeito da incerteza sobre os objetivos". Contudo, o sucesso da gestão de riscos irá depender da "[...] eficácia da estrutura de gestão que fornece os fundamentos e os arranjos que irão incorporá-la através de toda a organização, em todos os níveis" (ABNT, 2009, p. 8).

Segundo Freitas (2002, p. 53),

> A gestão de risco no setor público se apresenta como poderosa ferramenta gerencial para os administradores públicos, tanto no sentido de aumentar a segurança e o desempenho no emprego dos recursos públicos, quando de incentivar a mudança e a inovação nas entidades e programas governamentais.

Os estudos sobre gestão de riscos mencionados anteriormente refletem a importância e a atualidade deste assunto para a gestão das organizações públicas. A partir da Instrução Normativa Conjunta MP/CGU n° 01/2016, pode-se verificar o real interesse do Governo brasileiro para que, efetivamente, os órgãos públicos adotem medidas para implementar uma política de gestão de riscos. Agora, o dirigente máximo de cada órgão ou entidade passa a ser o principal responsável pelo estabelecimento da estratégia de organização e pela estrutura de gerenciamento de riscos. Dentro deste cenário, também será papel do dirigente máximo,

estabelecer, de forma continuada, o monitoramento e o aperfeiçoamento dos controles internos da gestão, com a instituição de comitês de governança, riscos e controles.

3. COSO *Enterprise Risk Management - Integrated Framework*

Em 1985 foi criada, nos Estados Unidos, a *National Commission on Fraudulent Financial Reporting* (Comissão Nacional sobre Fraudes em Relatórios Financeiros), também conhecida como *Treadway Commission*. A criação da comissão foi uma iniciativa independente do setor privado, formada por representantes das principais associações de classes de profissionais ligados à área financeira, com a finalidade de estudar as causas da ocorrência de fraudes em relatórios financeiros e contábeis e elaborar recomendações para empresas abertas, para seus auditores e instituições educacionais (Borgerth, 2007).

Em 1992 esta comissão publicou um trabalho para o estudo e aplicação dos controles internos, o *Internal Control – Integrated Framework* (Controle Interno – Estrutura Integrada). Posteriormente a Comissão transformou-se em Comitê, passando a ser conhecida como COSO – *The Committee of Sponsoring Organizations of the Treadway Commission* (Comitê das Organizações Patrocinadoras da Comissão *Treadway*).

Para Borgerth (2007), as recomendações do COSO são tidas como referência para controles internos. O COSO (2013, p. 6) apresenta uma definição abrangente ao definir que "Controle interno é um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade". Essa definição reflete alguns conceitos fundamentais. O controle interno é:

> Conduzido para atingir objetivos em uma ou mais categorias – operacional, divulgação e conformidade; Um processo que consiste em tarefas e atividades contínuas – um meio para um fim, não um fim em si mesmo; Realizado por pessoas – não se trata simplesmente de um manual de políticas e procedimentos, sistemas e formulários, mas diz respeito a pessoas e às ações que elas tomam em cada nível da organização para realizar o controle interno; Capaz de proporcionar segurança razoável - mas não absoluta, para a estrutura de governança e alta administração de uma entidade; Adaptável à estrutura da entidade – flexível na aplicação para toda a entidade ou para uma subsidiária, divisão, unidade operacional ou processo de negócio em particular (COSO, 2013, p. 6).

Em 2004, o COSO publicou o *Enterprise Risk Management - Integrated Framework* (Gerenciamento de Riscos Corporativos - Estrutura Integrada), conhecido como COSO-ERM ou COSO II, que estendeu o *Internal Control – Integrated Framework* (conhecido como

COSO-IC ou COSO I), ampliando o alcance dos controles internos, tendo como foco, o gerenciamento de riscos corporativos.

Uma versão atualizada do COSO-IC foi publicada em 2013 com a inclusão de melhorias, como a formalização de conceitos fundamentais introduzidos na estrutura original e esclarecimentos para facilitar seu uso e sua aplicação. Esses conceitos se transformaram em princípios, que são associados aos cinco componentes proporcionando clareza no desenvolvimento e na implementação dos sistemas de controle interno (COSO, 2013).

A Figura 1 apresenta uma comparação entre os dois *frameworks,* representados por seus cubos, nas quais as três faces visíveis representam: tipos de objetivos (face superior), os componentes do processo de gestão de riscos (linhas horizontais) e a organização e as unidades de uma organização, na terceira dimensão do cubo.

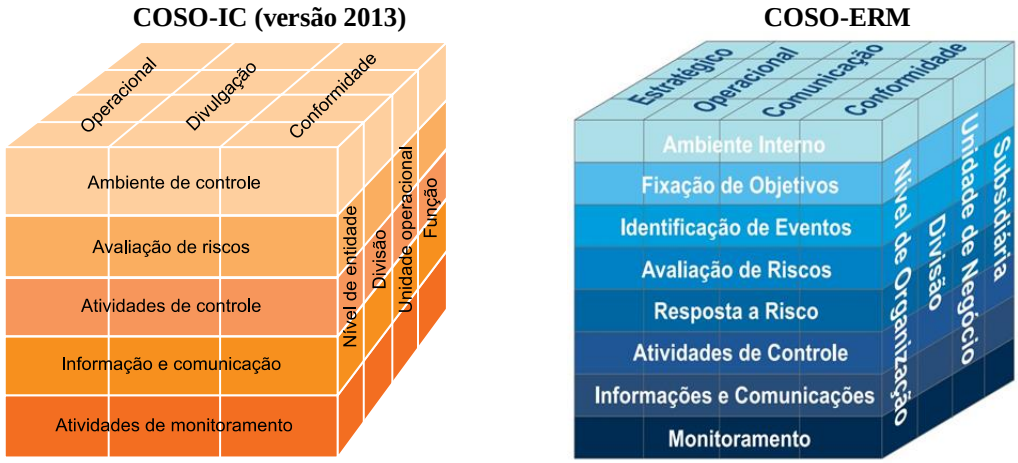

Figura 1 – Comparação entre o Cubo do COSO-IC e o Cubo do COSO-ERM
Fonte: COSO (2013) e COSO (2007)

Enquanto o COSO-IC aborda a estrutura de controles internos, o COSO-ERM aborda o paradigma de gestão de riscos, ambos por meio da proposição de um modelo integrado. Neste estudo será dado enfoque ao COSO-ERM em função da abordagem dada ao gerenciamento de riscos deste *framework.*

O COSO-ERM preconiza a agregação dos riscos e uma visão global e estratégica dos mesmos a partir alta administração. Outro ponto a ser destacado se refere aos três componentes que foram acrescentados na metodologia: a fixação de objetivos, a identificação de eventos e a resposta aos riscos.

Por sua vez, o Tribunal de Contas da União apresenta um comparativo de modelos de gestão de riscos, dentre eles o COSO-IC e o COSO-ERM, reproduzido no Quadro 1:

Características	COSO-IC	COSO-ERM
Considera oportunidades além de riscos.	Não	Sim
Necessidade de instituir Política de Gestão de Riscos.	Não	Sim
Necessidade de serem definidos "critérios" de riscos.	Parcialmente	Sim
Declara que o processo de gestão de riscos é customizável.	Sim	Sim
Encoraja buscar a melhoria contínua da gestão de riscos.	Parcialmente	Sim
Gestão de riscos embutida na rotina dos processos de trabalho e na cultura.	Não	Sim
Associação de riscos com objetivos.	Sim	Sim
Aplicável na seleção da estratégia.	Não	Sim
Recomenda criar e manter um portifólio/registro corporativo de riscos.	Não	Sim
Alerta sobre necessidade de considerar o custo de tratamento de riscos.	Sim	Sim
Orienta à necessidade de documentar as atividades de gestão de riscos.	Parcialmente	Sim
Declara que os riscos devem ter "proprietários".	Parcialmente	Sim
Implementar a gestão de riscos não é garantia de total sucesso.	Sim	Sim

Quadro 1 – Comparação entre as características do COSO-IC e o COSO-ERM[1]
Fonte: Adaptado do TCU

Apesar da avaliação de riscos ser um componente presente no COSO-IC, todo foco está no processo de controle interno da organização, e não estão contempladas todas as atividades e outros aspectos importantes para a realização de um processo completo de gestão de riscos. Dessa forma, o COSO-IC, embora utilize práticas de avaliação de riscos, não tem sido elaborado com o objetivo de ser um modelo de gestão de riscos em sentido estrito, diferentemente do COSO-ERM.

Segundo o COSO (2007), o gerenciamento de riscos corporativos tem por finalidade: alinhar o apetite a risco com a estratégia adotada; fortalecer as decisões de resposta aos riscos; reduzir surpresas e prejuízos operacionais; identificar e administrar riscos múltiplos e entre empreendimentos; aproveitar as oportunidades; e otimizar o capital.

Apesar do COSO ter sua origem com foco na iniciativa privada, sua estrutura tem sido também utilizada no setor público. No Brasil, o próprio Tribunal de Contas da União (TCU), por meio do Acórdão n° 821/2014 – Plenário, reconheceu a importância do gerenciamento de riscos nas organizações ao afirmar ser de sua competência a intensificação de ações que promovam a melhoria da gestão de riscos e dos controles da Administração Pública (Brasil, 2014). O TCU vem recomendando (Acórdão n° 2518/2017 - Primeira Câmara) que órgãos adotem, no gerenciamento de seus riscos e na definição de seus controles, os fundamentos dos modelos de gestão de riscos Coso I e Coso II (Brasil, 2017).

No âmbito internacional, de acordo com Wanderley et al. (2015), a INTOSAI (Organização Internacional de Entidades de Fiscalização Superiores) e o *Government Accountability Office* (GAO), Entidade Fiscalizadora Superior dos Estados Unidos da

[1] Comparativo completo disponível em http://portal.tcu.gov.br/gestao-e-governanca/gestao-de-riscos/modelos-de-gestao-de-riscos/comparativo-entre-modelos.htm.

América, utilizam a estrutura do COSO tendo como foco o setor público. Com a atualização do COSO em 2004, a INTOSAI incorporou esse modelo com o objetivo de contribuir para uma compreensão unificada de controle, por parte das Entidades Fiscalizadoras Superiores (EFS). Por sua vez, o GAO, empregou a estrutura de controle interno do COSO para ser utilizado como diretriz para que os administradores públicos americanos avaliassem a operação dos controles internos em suas instituições e determinassem a necessidade de aprimoramento e correções.

O COSO-ERM definiu oito componentes em sua estrutura: Ambiente de Controle; Fixação de Objetivos; Identificação de Eventos; Avaliação de Riscos; Resposta aos Riscos; Atividades de Controle; Informações e Comunicações; e Monitoramento. A seguir serão abordados cada um deles.

O ambiente interno inclui entre outros elementos, integridade, valores éticos e competência das pessoas, maneira pela qual a gestão delega autoridade e responsabilidades, estrutura de governança organizacional e políticas e práticas de recursos humanos. De acordo com o COSO (2007, p. 27), o ambiente interno é "a base para todos os outros componentes do gerenciamento de riscos corporativos, o que propicia disciplina e estrutura".

Todos os níveis da organização devem ter objetivos fixados e comunicados. A explicitação de objetivos, alinhados à missão e à visão da organização, é necessária para permitir a identificação de eventos que potencialmente impeçam sua consecução.

Segundo o COSO (2007, p. 5), "com base na missão estabelecida por uma organização, a administração estabelece os planos principais, seleciona as estratégias e determina o alinhamento dos objetivos nos níveis da organização". O COSO-ERM divide os objetivos em quatro categorias: estratégicos – metas gerais, alinhadas com sua missão; operações – utilização eficaz e eficiente dos recursos; comunicação – confiabilidade de relatórios; conformidade – cumprimento de leis e regulamentos pertinentes.

Na identificação de eventos, a administração considera uma variedade de fatores que podem dar origem a riscos e a oportunidades no contexto de toda a organização. "Eventos são incidentes ou ocorrências originadas a partir de fontes internas ou externas que afetam a implementação da estratégia ou a realização dos objetivos. Os eventos podem provocar impacto positivo, negativo ou ambos" (COSO, 2007, p. 46). Os riscos inerentes à própria atividade da organização devem ser identificados e relacionados em seus diversos níveis.

Os eventos devem ser avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência. A avaliação de riscos deve ser feita por meio de análises quantitativas, qualitativas

ou da combinação de ambas. Os riscos devem ser avaliados quando à sua condição de inerentes e residuais. Segundo o COSO (2007), risco inerente é aquele que a organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos. Por sua vez, o risco residual é aquele que ainda permanece após a resposta da administração.

Após realizar a avaliação, a organização deve identificar qual estratégia de resposta aos riscos que vai seguir (evitar, transferir, aceitar ou tratar os riscos) em relação aqueles mapeados e avaliados. Essa escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco.

Ao selecionar as respostas aos riscos, a organização identifica as atividades de controle que serão implementadas. As atividades de controle são políticas e procedimentos estabelecidos e executados para mitigar os riscos que a organização tenha optado por tratar. Esses procedimentos de controle devem estar distribuídos por toda a organização, em todos os níveis e em todas as funções e servem como mecanismos de gestão, sendo importantes elementos do processo por meio do qual uma organização busca atingir seus objetivos. Segundo o COSO (2007), as atividades de controle são procedimentos e políticas que norteiam as ações individuais na implementação das políticas de gestão de riscos, com a finalidade de assegurar que as respostas aos riscos sejam realizadas.

As informações relevantes devem ser identificadas, coletadas e comunicadas, a tempo de permitir que as pessoas cumpram suas responsabilidades. As informações devem conter os dados produzidos internamente, bem como, informações sobre eventos, atividades e condições externas, que possibilitem o gerenciamento de riscos e a tomada de decisão. A comunicação das informações produzidas deve atingir todos os níveis, por meio de canais claros e abertos, permitindo que a informação circule em todos os sentidos.

Através do monitoramento procura-se avaliar a qualidade da gestão de riscos e dos controles internos da gestão, através de atividades gerenciais contínuas e/ou avaliações independentes. Busca-se assegurar que os controles internos funcionem como previsto e que sejam modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos da organização.

4. *Business Process Management* (BPM)

BPM CBOK é a sigla para *Business Process Management Commom Body of Knowledge* (Corpo Comum de Conhecimentos em Gerenciamento de Processos de Negócio).

O guia BPM CBOK, como a própria sigla já esclarece, trata-se de um corpo de conhecimento e não de uma metodologia de trabalho. É um documento que contém uma visão sobre todas as fases para a realização de um projeto de BPM. Esse documento é elaborado pela associação internacional ABPMP – *Association of Business Process Management Professionals* (Associação dos Profissionais de Gerenciamento de Processos de Negócio), que é uma entidade sem fins lucrativos, dedicada à promoção dos conceitos e práticas de BPM.

De acordo com a ABPMP (2013), o guia BPM CBOK foi projetado para oferecer uma compreensão geral da prática BPM e um panorama abrangente de conceitos, melhores práticas e lições aprendidas pela ABPMP. O guia está organizado em áreas de conhecimento, que podem ser compreendidas como as fases reconhecidas e aceitas como necessárias para a implementação, sustentação e habilitação do BPM.

Para compreender o que é o *Business Process Management* (Gerenciamento de Processos de Negócios) serão abordados dois conceitos importantes: processo de negócio e funções de negócio.

Segundo a ABPMP (2013), no contexto de BPM, um processo de negócio é uma agregação de atividades e comportamentos executados para alcançar um ou mais resultados. É um trabalho que entrega valor para os clientes ou apoia/gerencia outros processos e dependendo do caso, demandam contribuições de múltiplas funções de negócio. Dessa forma, o fluxo desses processos pode transpor diferentes áreas funcionais da organização.

Por sua vez, as funções de negócio são grupos de atividades e competências especializadas, relacionadas a objetivos ou tarefas particulares, normalmente representadas por departamentos dentro das organizações, com uma orientação vertical de comando e controle (ABPMP, 2013).

A ABPMP define Gerenciamento de Processos de Negócio da seguinte forma:

> É uma disciplina gerencial que integra estratégias e objetivos de uma organização com expectativas e necessidades de clientes, por meio do foco em processos ponta a ponta. BPM engloba estratégias, objetivos, cultura, estruturas organizacionais, papéis, políticas, métodos e tecnologias para analisar, desenhar, implementar, gerenciar desempenho, transformar e estabelecer a governança de processos (ABPMP, 2013, p. 40).

No decorrer dos anos houve uma evolução da Gestão de Processos. Essa evolução ocorreu em três ondas. A primeira onda foi o *Total Quality Management* (TQM), Qualidade Total em português, que teve início na década de 50 com Deming e Juran. O TQM teve seu

reconhecimento através da divulgação das normas ISO (*International Organization for Standardization*) que são voltadas para estabelecer regras para um sistema de gestão da qualidade. A segunda onda ocorreu na década de 90, com a reengenharia de processos, difundida por Davenport e Hammer. E a terceira onda é o *Business Process Management*, que veio para suprir as deficiências que os modelos de Gestão de Processos demonstraram ao longo da história (Smith e Fingar, 2007 citado em Mariano e Müller, 2012).

Com a evolução da Gestão de Processos, ao longo das últimas décadas, as organizações vivenciaram um processo de transformação estrutural, devido ao crescimento da competitividade, resultando em comportamentos mais flexíveis e horizontais, paulatinamente substituindo as tradicionais estruturas funcionais (Maranhão e Macieira, 2014).

Com o BPM, a organização passa a ser gerenciada em torno de seus processos de negócio, através de um gerenciamento horizontal e trabalho orientado ao processo como um todo. A visão que era orientada ao produto ou serviço, baseada na departamentalização e na hierarquia passa a ser uma visão orientada ao cliente, através de um gerenciamento horizontal. De acordo com a ABPMP (2013, p. 39), "[…] embora a estruturação funcional continue válida, pois a especialização leva à produtividade, a geração de valor passa a ser gerenciada horizontalmente em uma visão notadamente interfuncional ponta a ponta."

Existem diversos modelos propostos na literatura para orientar a gestão de processos de negócios, sendo que a maioria deles assume a forma cíclica baseada no modelo PDCA, com as atividades organizadas em fases e se repetindo a cada fase, por esta razão fala-se em ciclos de vida BPM (Baldam, 2008).

De acordo com a ABPMP (2013), os processos de negócio devem ser gerenciados em um ciclo contínuo para manter sua integridade, permitindo a transformação. O guia BPM CBOK apresenta um ciclo de vida com as seguintes fases: Planejamento; Análise; Desenho; Implementação; Monitoramento e Controle; e Refinamento. A seguir é feita uma pequena descrição de cada fase do ciclo.

De acordo com a ABPMP (2013), na fase de planejamento deve ser realizado um plano e uma estratégia dirigida aos processos da organização, analisando suas estratégias e metas. Combinado com isto, deve-se prover ainda uma estrutura e um direcionamento contínuo de processos centrados no cliente. Nesta etapa também são avaliados os pontos fortes e fracos da organização e identificadas e elencadas as responsabilidades e papéis organizacionais relacionados à gerência de processos.

Na fase de análise do ciclo de vida BPM é preciso compreender os atuais processos organizacionais no contexto das metas, objetivos desejados e organização como um todo. O objetivo é coletar e organizar a informação sobre os processos da organização. A análise de processos assimila informações oriundas de planos estratégicos, modelos de processos e medição de desempenho, a fim de entender completamente os processos de negócio no escopo da organização como um todo, sendo sustentada por técnicas e metodologias que facilitam a obtenção do contexto e o diagnóstico da atual situação do negócio.

Para a ABPMP (2013), o desenho de processos é a definição formalizada de objetivos e entregáveis, bem como a organização de atividades e regras necessárias para produzir um resultado desejado. Inclui o ordenamento das atividades em um fluxo de trabalho baseado nos relacionamentos das atividades e a integração com outros processos internos e externos, bem como a identificação e associação de competências necessários para a execução.

A implementação é uma fase do ciclo de vida BPM que tem como objetivo permitir e pôr em ação a execução dos processos como foram definidos e documentados, na forma de um fluxo de trabalho. É o momento de realizar efetivamente o desenho aprovado do processo de negócio na forma de procedimentos e fluxos de trabalhos documentados, testados e ainda considerando a criação de políticas e procedimentos novos e/ou revisados.

A fase de monitoramento e controle é executada através de atividades que visam mensurar e monitorar os processos de negócio a fim da obtenção de informações para os gestores de processos de negócio ajustarem os recursos e atingirem os objetivos. É nesta fase do ciclo BPM que será possível descobrir se os processos estão alinhados com esses objetivos, monitorando-se indicadores adequados à avaliação dos resultados obtidos.

Na fase refinamento do ciclo BPM será dado início a melhoria contínua dos processos. A etapa de refinamento é responsável pela transformação dos processos, no sentido de melhoria, onde é implementado o resultado da análise de desempenho previamente efetuada. Essa fase aborda desafios associados à gestão de mudanças perante a organização, à melhoria contínua e à otimização de processos como um todo.

5. Método de pesquisa

O presente estudo caracteriza-se, quanto à abordagem, como uma pesquisa qualitativa. Em relação à sua natureza trata-se de uma pesquisa aplicada, que pretende gerar conhecimentos em relação a utilização do COSO-ERM e do BPM no gerenciamento de riscos dos órgãos e entidades do Poder Executivo Federal. Em relação à estratégia adotada, a

pesquisa pode ser classificada como sendo um estudo exploratório. Quanto aos procedimentos da pesquisa esta é caracterizada como pesquisa bibliográfica e documental.

No primeiro momento foram analisadas, por meio da pesquisa bibliográfica e documental, informações sobre a gestão de riscos nos órgãos e entidades do Poder Executivo Federal, visando à obtenção de conceitos relacionados ao tema. Foram analisados também alguns pontos da Instrução Normativa Conjunta MP/CGU n° 01/2016, como a adoção de uma série de medidas para a sistematização de práticas relacionadas à gestão de riscos, controles internos e governança, com destaque para a política de gestão de riscos a ser instituída nos órgãos e entidades do Poder Executivo Federal.

Em seguida foram analisados, os fundamentos de gerenciamento de riscos do COSO-ERM visando à obtenção de informações sobre a estrutura do modelo de gestão de riscos proposta por esse *framework* através dos seus componentes, bem como o posicionamento do Tribunal de Contas da União sobre o tema através de acórdãos já publicados. Posteriormente foram analisados, os fundamentos do BPM a fim da compreensão dos seus conceitos e das fases do seu ciclo de vida.

6. COSO-ERM integrado com o BPM

O COSO-ERM foi utilizado como referência de modelo de gestão de riscos (isto não implicou no julgamento deste ser o melhor modelo ou o mais adequado). A escolha se deu em razão do que consta no art. 16, da Instrução Normativa MP/CGU n° 01/2016, que orienta sobre a estrutura do modelo de gestão de riscos e menciona que a alta administração, bem como seus servidores ou funcionários, devem observar os seguintes componentes: ambiente interno; fixação de objetivos; identificação de eventos; avaliação de riscos; resposta a riscos; atividades de controles internos; informação e comunicação; e monitoramento. Embora a Instrução Normativa MP/CGU n° 01/2016 não se reporte diretamente ao COSO-ERM, ela traz exatamente todos os seus componentes mencionados na seção onde consta a estrutura do modelo de gestão de riscos. Por esse motivo, foi escolhido o modelo do COSO-ERM.

Outro ponto que cabe destaque e que motivou este estudo, está presente no art. 17, da Instrução Normativa Conjunta MP/CGU n° 01/2016. A política de gestão de riscos, a ser instituída pelos órgãos e entidades do Poder Executivo Federal deve especificar como a gestão de riscos será integrada ao planejamento estratégico, aos processos e às políticas da organização. Diante disso, foi analisada a possibilidade de integração entre o COSO-ERM e o BPM no processo de gestão de riscos dos órgãos e entidades do Poder Executivo Federal.

Considerando que os objetivos institucionais devem estar presentes de forma clara no planejamento estratégico da organização e que para cada objetivo devem existir ações que são realizadas por meio de processos de negócio, ao realizar a identificação desses processos, poderão ser identificados os eventos (riscos ou oportunidades), avaliados e tratados os riscos e potencializadas as oportunidades. Os riscos identificados poderão ser mitigados através da implementação de controles, aumentando a probabilidade de alcance dos objetivos, desafios e metas estabelecidas.

Tendo como referência, recente estudo realizado por Ferreira (2016), que apresentou uma metodologia composta por um conjunto de fases e uma ferramenta de apoio para realizar o gerenciamento de riscos em processos de negócios de forma integrada com o ciclo de vida BPM, entretanto, utilizando um outro ciclo, o ciclo de vida proposto pelo guia BPM CBOK, e realizando um agrupamento e posicionamento diferente, foi elaborado no formato de um ciclo, atividades organizadas integrando os componentes do COSO-ERM com o ciclo de vida do BPM, conforme pode ser observado na Figura 2:

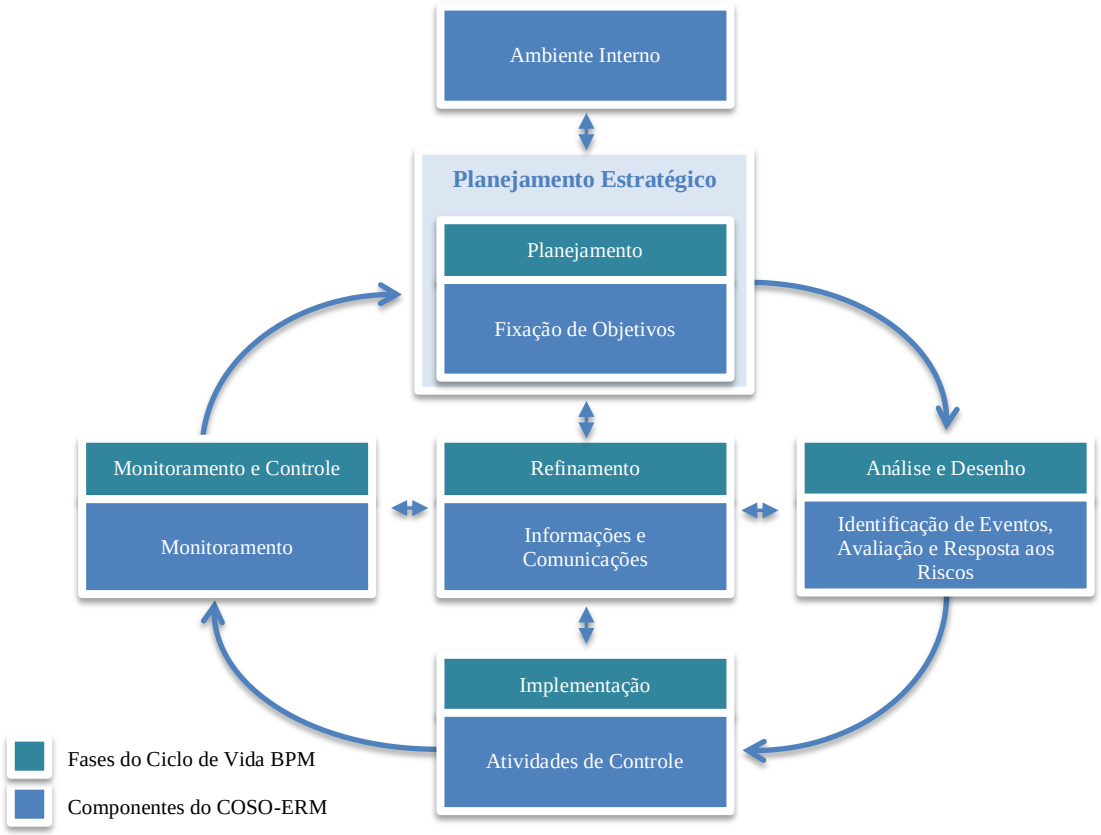

Figura 2 - Ciclo de Vida BPM integrado com os componentes do COSO-ERM
Fonte: Adaptado de Ferreira (2016)

A Figura 2 apresenta as principais atividades de cada abordagem de gerenciamento de riscos do COSO-ERM e a fase do ciclo de vida BPM com que cada atividade possui uma maior compatibilidade. No topo da Figura 2 está representado o Ambiente Interno, que segundo o COSO (2007, p. 27) é "a base para todos os outros componentes do gerenciamento de riscos corporativos, o que propicia disciplina e estrutura". Esse componente é afetado fortemente pelo histórico e cultura da organização e influencia o modo pelo qual as estratégias e os objetivos são estabelecidos, os negócios são estruturados, e os riscos são identificados, avaliados e geridos. Dentro da organização serve para que os seus membros criem consciência dos riscos que podem ser apresentados na instituição. Para o COSO (2007, p. 28), "quando a filosofia de administração de riscos está adequadamente desenvolvida, entendida e aceita pelo pessoal da organização, ela estará em condições de identificar e administrar riscos com eficácia".

O componente Fixação de Objetivos do COSO-ERM e a fase de Planejamento do ciclo de vida BPM, tendo como plano de fundo, o Planejamento Estratégico, apresentam compatibilidade em função de que precisam estar alinhados com a estratégia da organização. Existe uma relação direta entre os objetivos, que é aquilo que a entidade deseja atingir, e os componentes do gerenciamento de risco que representam o que é necessário para atingir esses objetivos. Nesta etapa é necessário definir os objetivos no âmbito estratégico e alinhar o projeto BPM com a estratégia da organização. A partir dos objetivos é possível estabelecer o apetite a riscos da organização.

As fases de Análise e Desenho do ciclo de vida BPM apresentam relação com os componentes de Identificação de Eventos, Avaliação e Respostas aos Riscos do COSO-ERM. Embora sejam realizadas em etapas distintas, os componentes do COSO-ERM apresentam uma sequencia de atividades que podem ser agrupadas e integradas com as fases de Análise e Desenho do ciclo BPM.

Na fase de Análise do BPM são coletadas e organizadas as informações sobre os processos da organização. Posteriormente é realizada, dentro do ciclo BPM, a modelagem dos processos através do ordenamento das atividades em um fluxo de trabalho, com base nos relacionamentos das atividades e a integração com outros processos internos e externos. Nessa etapa, entre outras técnicas de identificação de eventos, a análise de fluxo de processo pode ser utilizada para que os eventos possam ser identificados e considerados à luz dos objetivos de processo, conforme preceitua o COSO-ERM.

Após a identificação de eventos, estes devem ser avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência, por meio de análises quantitativas e/ou qualitativas. Em seguida a organização deve identificar qual estratégia que vai seguir (evitar, transferir, aceitar ou tratar os riscos) em relação aos riscos mapeados e avaliados.

A fase de Implementação do ciclo BPM pode ser agrupada com o componente Atividades de Controle do COSO-ERM. As atividades de controle são as políticas e os procedimentos que garantem que as respostas aos riscos sejam realizadas de forma apropriada e efetiva. Esta etapa também pode incluir a combinação da implementação dos processos que foram definidos e documentados na fase anterior do ciclo BPM, na forma de um fluxo de trabalho e também novos processos definidos em função das atividades de controle que serão implementadas para mitigar os riscos identificados na etapa anterior.

A fase de Monitoramento e Controle do ciclo BPM pode ser agrupada com o componente Monitoramento do COSO-ERM. Essa combinação pode auxiliar na identificação do desempenho dos processos de negócio e na descoberta de possíveis riscos não identificados em etapas anteriores. Essa integração pode contribuir para uma possível melhoria de desempenho dos processos de negócio, juntamente com o monitoramento do processo de Gestão de Riscos e as modificações necessárias que podem vir a serem realizadas.

O componente Informações e Comunicações do COSO-ERM, posicionado no centro da Figura 2, se justifica pelo fato de que toda informação relevante, relacionada aos objetivos, riscos, controles e processos deve ser captada e comunicada a todos os níveis da organização. Durante qualquer etapa do processo de gerenciamento de riscos, bem como do ciclo BPM, podem ser identificadas informações relevantes e comunicadas em tempo hábil para que os responsáveis tomem as devidas providências.

Da mesma forma foi posicionada no centro da Figura 2, a fase Refinamento do ciclo BPM, em função de que durante qualquer etapa do processo, podem ser identificadas informações relevantes que podem dar início a uma ação de melhoria contínua dos processos.

Pelas análises realizadas, embora o ciclo de vida do BPM apresente condições para acompanhar todos os componentes do COSO-ERM, ressalta-se a sua importância no componente de Identificação de Eventos. Segundo o COSO (2007), a metodologia de identificação de eventos de uma organização poderá empregar uma combinação de técnicas com ferramentas de apoio, dentre elas a técnica de análise do fluxo de processo. Essa técnica considera os fatores internos e externos que afetam as entradas, as tarefas ou atividades, as

responsabilidades e as saídas que se combinam para formar um processo, auxiliando na identificação dos eventos que podem afetar o cumprimento dos objetivos da organização.

A Figura 3 apresenta um exemplo de diagrama que representa de forma ilustrativa, os riscos e as oportunidades identificadas na análise de um fluxo de processo:

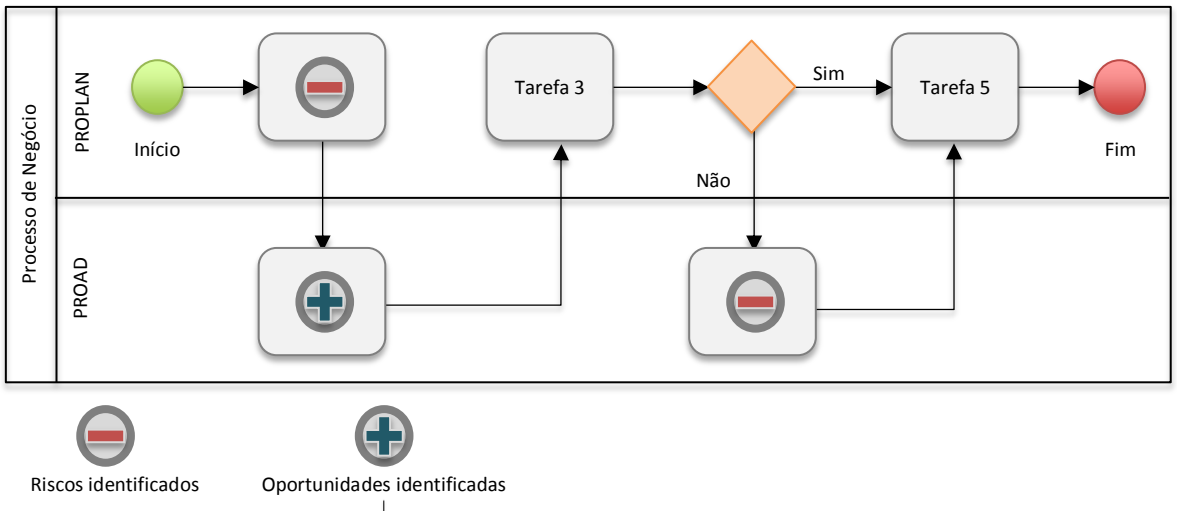

Figura 3 – Diagrama de processo com riscos e oportunidades identificadas
Fonte: Elaborado pelos autores

A Figura 3 demonstra possíveis eventos que podem ser identificados ao se analisar as atividades (tarefas) de um fluxo de processo. Em cada tarefa de um processo de negócio, podem ser identificados riscos que representam a possibilidade de que um evento ocorra e afete negativamente a realização dos objetivos. Da mesma forma, podem ser identificadas oportunidades que representam a possibilidade de que um evento ocorra e influencie favoravelmente a realização dos objetivos.

De modo geral, a análise do fluxo de processo diz respeito à representação esquemática de um processo, visando entender melhor os inter-relacionamentos de seus componentes de entrada, tarefas, saída e responsabilidades. Após esse mapeamento, os eventos podem ser identificados e considerados à luz dos objetivos de processo. Da mesma forma que em outras técnicas de identificação de eventos, a análise de fluxo de processo pode ser utilizada para observar um nível simples ou detalhado na organização (COSO, 2007).

7. Principais limitações do COSO-ERM e do BPM

O próprio COSO (2007) apresenta algumas limitações da sua metodologia. Embora o controle interno tenha sido bem projetado e seja corretamente operacionalizado, apenas

proporcionará uma segurança razoável aos gestores, quanto ao cumprimento dos objetivos de uma organização. A possibilidade de atingí-los é afetada pelas limitações inerentes a todos os sistemas de controle interno, inclusive pelas ocorrências de falhas humanas que podem comprometer o processo decisório ou mesmo levar a erros e enganos que acarretem problemas. Além disso, os controles podem ser burlados por conluio e os gestores podem desconsiderar o processo de gerenciamento de risco e controle interno. Outro fato restritivo é a necessidade de se considerar a relação custo x benefício para controlar, transferir, minimizar ou eliminar determinado tipo de risco. Um controle jamais poderá ter um dispêndio maior que o benefício que ele trará.

Com relação às limitações do BPM, a implementação de práticas de gestão de processos é complexa, uma vez que cruza departamentos e, progressivamente, fronteiras organizacionais como clientes, fornecedores e parceiros envolvidos nas atividades da organização. Segundo a ABPMP (2013), os principais problemas estão relacionados a cultura organizacional, inércia e interesses ocultos. Muito do esforço de BPM é gerenciar o resultado do desempenho agregado do processo ponta a ponta e não apenas aumentar o controle sobre atividades e tarefas individuais. Para adquirir resiliência operacional, a cultura e as atitudes da organização também devem ser modificadas.

8. Considerações finais

Para atingir o objetivo de analisar, sob o ponto de vista teórico, a possibilidade de integração entre o COSO-ERM e o BPM, no processo de gestão de riscos dos órgãos e entidades do Poder Executivo Federal, foram apresentadas informações sobre a importância da gestão de riscos, a legislação aplicada e os conceitos relacionados ao tema. Em seguida foram analisados os fundamentos do COSO-ERM e do ciclo de vida do BPM. As análises realizadas evidenciaram que a integração entre o COSO-ERM e o BPM podem auxiliar no processo de gestão de riscos dos órgãos e entidades do Poder Executivo Federal.

Através de atividades organizadas integrando os componentes do COSO-ERM com o ciclo de vida do BPM, podem ser gerenciados os riscos relacionados aos objetivos institucionais dos órgãos e entidades do Poder Executivo Federal de forma otimizada, através de uma análise de ponta a ponta (horizontal) dos processos envolvidos.

Entretanto, existem limitações que podem dificultar essa integração. As principais limitações estão relacionadas a cultura organizacional, a ocorrências de falhas humanas que

podem comprometer o processo decisório ou mesmo levar a erros e enganos que acarretem problemas, conluios e dispêndios realizados maiores que os benefícios trazidos.

A partir da Instrução Normativa Conjunta MP/CGU n° 01/2016, pode-se verificar o real interesse do Governo brasileiro para que, efetivamente, os órgãos públicos adotem medidas para implementar uma política de gestão de riscos. Por outro lado, deve-se considerar a importância da Gestão de Riscos, não somente pelo aspecto legal, mas pelos benefícios reais que sua implementação pode gerar aos órgãos e entidades da Administração Pública Federal, com a implementação de um adequado sistema de controle e gestão de riscos, para que possam aumentar a segurança da gestão, planejar suas metas, conhecendo melhor os eventos que podem impedir seu cumprimento e, consequentemente, aumentar as chances de viabilizar a execução de seus objetivos estratégicos.

Como trabalho futuro, recomenda-se a análise prática em órgãos e entidades da Administração Pública Federal, avaliando se o estudo teórico aqui apresentado pode ser aplicado de maneira eficiente, verificando assim os benefícios e as limitações dessa integração. Outro trabalho que poderá ser realizado, refere-se a uma análise comparativa entre os principais modelos de gerenciamento de riscos existentes a fim de identificar os pontos positivos e negativos de cada um desses modelos, identificando aqueles que apresentem os melhores componentes para um modelo de gestão de riscos a ser aplicado nos órgãos e entidades da Administração Pública Federal.

Referências bibliográficas

ABNT NBR ISO 31000, de 30 de novembro de 2009. Gestão de riscos - Princípios e diretrizes. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

ABPMP Brasil. (2013). *Guia para o Gerenciamento de Processos de Negócio Corpo Comum de Conhecimento ABPMP BPM CBOK V3.0.* Recuperado de http://www2.unifap.br/claudiomarcio/files/2016/10/Guia-ABPMP-CBOK-2013.pdf

Andrade, A. R. de. (2012). *Planejamento estratégico: formulação, implementação e controle.* São Paulo: Atlas.

Assi, M. (2012). *Gestão de riscos com controles internos: ferramentas, certificações e métodos para garantir a eficiência dos negócios.* (1ª ed.). São Paulo: Saint Paul.

Avalos, J. M. A. (2009). *Auditoria e gestão de riscos*. São Paulo: Saraiva.

Baldam, R. de L. (2008). *Gerenciamento de processos de negócios no setor siderúrgico: proposta de estrutura para implantação* (Tese de Doutourado). Universidade Federal do Rio

de Janeiro, Rio de Janeiro, RJ, Brasil. Recuperado de http://www.sage.coppe.ufrj.br/index.php/publicacoes/teses/2008/21-roquemar-de-lima-baldam-abril2008/file

Borgerth, V. M. da C. (2007). *SOX: entendendo a Lei Sarbanes-Oxley: um caminho para a informação transparente.* (1ª ed.). São Paulo: Thompson Learning.

Brasil. (2014). Acórdão n° 821/2014 – Plenário, de 02 de abril de 2014. *Tribunal de Contas da União*. Recuperado de https://contas.tcu.gov.br/sagas/SvlVisualizarRelVotoAcRtf?codFiltro=SAGAS-SESSAO-ENCERRADA&seOcultaPagina=S&item0=494187

Brasil. (2016). Instrução Normativa Conjunta nº 1, de 10 de maio de 2016. *Ministério do Planejamento, Orçamento e Gestão e Controladoria-Geral da União*. Recuperado de http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=14&data=11/05/2016

Brasil. (2017). Acórdão n° 2518/2017 – Primeira Câmara, de 02 de maio de 2017. *Tribunal de Contas da União*. Recuperado de https://contas.tcu.gov.br/sagas/SvlVisualizarRelVotoAcRtf?codFiltro=SAGAS-SESSAO-ENCERRADA&seOcultaPagina=S&item0=586409

COSO. (2007). *Committee of Sponsoring Organizations of the Treadway Commission. Gerenciamento de Riscos Corporativos - Estrutura Integrada*. Recuperado de https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf

COSO. (2013). *Committee of Sponsoring Organizations of the Treadway Commission. Controle Interno – Estrutura Integrada*. Recuperado de http://www.iiabrasil.org.br/new/2013/downs/coso/COSO_ICIF_2013_Sumario_Executivo.pdf

Ferreira, F. da S. (2016). *R-BPM: uma metodologia para gestão de riscos em iniciativas de BPM* (Dissertação de Mestrado). Universidade Federal de Pernambuco, Recife, PB, Brasil. Recuperado de http://repositorio.ufpe.br/handle/123456789/20057

Freitas, C. A. S. de (2002). Gestão de risco: Possibilidades de utilização pelo setor público e por entidades de fiscalização superior. *Revista do TCU*, 33 (93), 42-54. Recuperado de http://revista.tcu.gov.br/ojs/index.php/RTCU/article/download/844/904

Kanaane, R., Filho, A. F., & Ferreira, M. das G. (2010). *Gestão Pública: planejamento, processos, sistemas de informação e pessoas.* São Paulo: Atlas.

Maranhão, M., & Macieira, M. E. B. (2014). *O processo nosso de cada dia: modelagem de processos de trabalho.* (2ª ed.). Rio de Janeiro: Qualitymark Editora.

Mariano, I. C., & Müller, C. J. (2012). *Melhoria de Processos pelo BPM: Aplicação no Setor Público*. Universidade Federal do Rio Grande do Sul. Recuperado de http://www.lume.ufrgs.br/handle/10183/65643

Wanderley, C. A. N., Fonseca, A. C. P. D. da, & Paula, H. A. de. (2015). Controles internos no setor público à luz da estrutura do COSO: o caso de um órgão de compra da Marinha do Brasil. *ConTexto*, 15 (30). Recuperado de http://www.seer.ufrgs.br/ConTexto/article/viewFile/46627/pdf_52