

## **GESTÃO DE RISCOS, GOVERNANÇA CORPORATIVA E ALINHAMENTO ESTRATÉGICO: UM ESTUDO DE CASO**

### **RESUMO**

Este estudo objetiva analisar o processo de gestão de riscos em uma organização do setor de previdência privada. Especificamente, busca identificar as relações entre gestão de riscos corporativos, governança corporativa e gestão estratégica nessa organização, a qual é uma das maiores empresas de previdência privada do Brasil. A pesquisa é de natureza exploratória e o método adotado é o estudo de caso único. Constatou-se um ganho de eficiência na gestão de riscos em função de uma visão integrada, na forma de portfólio de riscos, suportada por um processo estruturado e contínuo, inserido no contexto da sua governança corporativa. Atualmente essa organização está buscando conectar os riscos estratégicos à análise e formulação da estratégia, com o objetivo de explorar o lado positivo dos riscos, na forma de oportunidades estratégicas. Pode-se concluir que governança corporativa e gestão estratégica têm se tornado elementos indissociáveis da gestão de riscos corporativos na empresa estudada.

**Palavras-chave:** Estratégia. Gestão de Riscos Corporativos. Governança Corporativa. Gestão Estratégica. Previdência Privada.

## **RISK MANAGEMENT, CORPORATE GOVERNANCE AND STRATEGIC ALIGNMENT: A CASE STUDY**

### **ABSTRACT**

This study aims to analyze the corporate risk management process within a private pension organization. Specifically, it seeks to identify the relationships between corporate risk management, corporate governance and strategic management in this organization, which is one of the largest private pension companies in Brazil. The research is exploratory in nature and the method adopted is an in-depth single case study. An efficiency improvement in the management of risks was evidenced by an integrated vision, in the form of a risk portfolio, supported by a structured and continuous process, solidly embedded in the context of its corporate governance. Currently, this organization is seeking to connect strategic risks to strategy analysis and formulation in order to explore the positive side of risks, in the form of strategic opportunities. As a conclusion corporate governance and strategic management have become inseparable elements of corporate risk management in the company studied.

**Keywords:** Strategy. Corporate Risk Management. Corporate Governance. Strategic Management. Private Pension.

---

## GESTIÓN DE RIESGOS, GOBERNANZA CORPORATIVA Y ALINEACIÓN ESTRATÉGICA: UN ESTUDIO DE CASO

### RESUMEN

Este estudio tiene como objetivo analizar el proceso de gestión de riesgos en una organización del sector de pensión privada. En concreto, busca identificar las relaciones entre gestión de riesgos corporativos, gobernanza corporativa y gestión estratégica en esa organización, la cual es una de las mayores empresas de pensión privada de Brasil. La investigación es de naturaleza exploratoria y el método adoptado es el estudio de caso único. Se constató una ganancia de eficiencia en la gestión de riesgos en función de una visión integrada, en forma de portafolio de riesgos, soportada por un proceso estructurado y continuo, insertado en el contexto de la gobernanza corporativa. Actualmente esta organización está buscando conectar los riesgos estratégicos al análisis y formulación de la estrategia, con el objetivo de explorar el lado positivo de los riesgos, en la forma de oportunidades estratégicas. Se puede concluir que la gobernanza corporativa y la gestión estratégica se han convertido en elementos indisolubles de la gestión de riesgos corporativos en la empresa estudiada.

**Palabras clave:** Estrategia. Gestión de Riesgos Corporativos. Gobernanza Corporativa. Gestión Estratégica. Pensión Privada.

Marcelo Oleskovicz <sup>1</sup>  
Fábio Lotti Oliva <sup>2</sup>  
Marcelo Caldeira Pedroso <sup>3</sup>

---

<sup>1</sup> Doutorando no Programa de Pós-Graduação em Administração do Departamento de Administração da Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo - FEA/USP. Brasil. E-mail: [moleskovicz@gmail.com](mailto:moleskovicz@gmail.com)

<sup>2</sup> Doutor em Administração pela Universidade de São Paulo - USP. Professor da Universidade de São Paulo - USP. Brasil. E-mail: [fabiousp@usp.br](mailto:fabiousp@usp.br)

<sup>3</sup> Livre-Docente em Administração pela Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo – FEA/USP. Professor da Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo – FEA/USP. Brasil. E-mail: [mpedroso@usp.br](mailto:mpedroso@usp.br)

## 1 INTRODUÇÃO

O conceito de Gestão de Riscos Corporativos (GRC), desenvolvido na década de 90, ganhou impulso nos anos 2000, em grande parte devido à crise global iniciada em 2008 (Wu & Olson, 2010). À medida que se desenvolve, o GRC tem proporcionado às empresas sair de um patamar de foco em conformidade e prevenção para uma visão estratégica, que busca oportunidades na identificação e resposta aos riscos (Collier, 2009; COSO, 2004). Esse movimento vem sendo motivado por fatores como a aversão a incertezas por parte dos *stakeholders*, volatilidades de mercado, globalização e exigências relativas à conformidade (Arnold, Benford, Canada, & Sutton, 2015). Desse modo, a adoção desta abordagem por parte das empresas tem sido amplamente estimulada por agências de risco, associações de profissionais, órgãos legislativos, órgãos reguladores, mercados de ações, normas internacionais, organizações e consultorias (Arena, Arnaboldi & Azzone, 2010), tornando-se rapidamente um conceito dominante no âmbito da gestão estratégica (Bhimani, 2009; Mikes, 2011).

Por ter como base a gestão integrada de riscos, na forma de portfólio, o GRC naturalmente demanda o alinhamento entre gestão de riscos, governança corporativa e estratégia (Bromiley, McShane, Nair & Rustambekov, 2015). Uma gestão holística de riscos requer um bom sistema de governança e o GRC pode ser considerado como a gestão de riscos com a adição da governança de riscos (Lundqvist, 2015). O crescimento da importância do GRC se deve à maior atenção dada à gestão de riscos no contexto de governança corporativa, o que, de certo modo, mudou o foco do GRC de integração de riscos para governança de riscos (Altuntas, Berry-Stölzle & Hoyt, 2011). Quanto ao alinhamento estratégico, a integração entre o GRC e a gestão estratégica garante uma maior habilidade na identificação de correlações entre riscos nas organizações, com consequente geração de valor (Farrell & Gallagher, 2015).

A abordagem de riscos estratégicos depende do contexto organizacional (Kaplan & Mikes, 2012). Estudos acadêmicos sobre GRC, principalmente em nível estratégico, são incipientes e raramente figuram em publicações em administração (Bromiley et al., 2015).

Esta pesquisa pretende analisar o processo de gestão de riscos em uma organização do setor de previdência privada. Mais especificamente, busca identificar as relações entre gestão de riscos corporativos, governança corporativa e gestão estratégica na empresa estudada.

O estudo se propõe a responder a seguinte questão de pesquisa: como é realizada a gestão estratégica de riscos em uma empresa do setor de previdência privada brasileiro, sob a ótica de governança corporativa e gestão estratégica?

No setor de previdência privada no Brasil, escopo desta pesquisa, valores financeiros expressivos estão expostos a riscos inerentes ao setor. Estes incluem o descasamento de prazos entre ativos e passivos em horizontes extremamente longos e questões atuariais específicas do setor, além de incertezas usualmente encontradas em outras indústrias, como os riscos operacionais e de mercado. Embora exista alguma semelhança com o mercado financeiro, do ponto de vista estratégico o setor de previdência privada também apresenta suas especificidades.

Buscando a contextualização da pesquisa, este trabalho foi realizado na empresa EPP (nome fictício), uma das maiores empresas de previdência privada do Brasil. Com dedicação exclusiva a este negócio, a empresa oferece planos de previdência complementar aberta para pessoas físicas e jurídicas, nas modalidades Plano Gerador de Benefício Livre (PGBL) e Vida Gerador de Benefício Livre (VGBL). A instituição tem como missão proporcionar soluções de segurança financeira e serviços de alta qualidade para viabilizar os projetos de vida de seus clientes. Trata-se de uma sociedade anônima de capital fechado. Conforme dados de fevereiro de 2016, a empresa atende a uma carteira de aproximadamente dois milhões de clientes, com mais de R\$ 150 bilhões em ativos sob sua gestão.

Além dos desafios relacionados ao setor de previdência privada e ao porte da empresa estudada, duas importantes mudanças no âmbito regulatório do setor estão em curso, com impacto relevante para o GRC. A primeira mudança diz respeito a uma nova norma da Susep (Superintendência de Seguros Privados, órgão do governo brasileiro responsável pelo controle e fiscalização dos mercados de seguro, previdência privada aberta, capitalização e resseguro) que define regras para a gestão de riscos, prevista para 2016. Dentre as regras desta norma, figuram a formalização do apetite ao risco, a inserção da gestão de riscos no sistema de gestão da empresa e a segregação entre as equipes que realizam o monitoramento dos riscos e as que tomam decisões sobre investimento.

A segunda mudança é relativa à Resolução 4.444 do CMN (Conselho Monetário Nacional), que dá aos gestores uma maior liberdade para alocar os recursos, aumentando a diversificação do patrimônio dos clientes em planos de previdência privada, o que pode ser traduzido em novas possibilidades em termos de riscos e retornos.

Na esteira deste cenário, intensificam-se riscos e oportunidades e o alinhamento entre GRC, governança corporativa e gestão estratégica assume relevância ainda maior.

Além desta introdução, o trabalho divide-se em fundamentação teórica, método, resultados e discussão.

## 2 FUNDAMENTAÇÃO TEÓRICA

‘Esse tópico aborda três elementos: gerenciamento de riscos corporativos (GRC), governança corporativa e gestão estratégica. Cada um destes é discutido a seguir.

### Gerenciamento de Riscos Corporativos (GRC)

Existe clara divergência acerca do conceito de GRC entre as fontes que o definem. Bromiley et al. (2015) apontam dois espectros que evidenciam estas diferenças: o primeiro é o de maior distinção e contempla desde as fontes que consideram riscos como algo totalmente independente dos objetivos da organização (por exemplo, Miccolis, 2000; AS/NZS, 1995; S&P, 2008) até as que definem riscos em termos de atingimento de seus objetivos (por exemplo, IIA, 2001; COSO, 2004). O segundo abrange desde os que claramente definem riscos como um problema a ser mitigado (por exemplo, S&P, 2008; RIMS, 2011) até os que os consideram como uma fonte potencial de criação de valor (por exemplo, IBGC, 2007; CAS, 2003).

Alguns consensos, entretanto, tem surgido em torno do que constitui os principais elementos do GRC. Entre eles, os ganhos de eficiência na gestão de um portfólio corporativo de riscos, em oposição à administração de riscos de forma individual, sejam eles

associados a partes da organização ou a atividades. Também tem se tornado frequente o reconhecimento de que não somente os riscos tradicionais, como acidentes, mas também os riscos estratégicos devem fazer parte do GRC (Oliva, Sobral, Damasceno, Teixeira, Grisi, Fischmann. & Santos, 2014; Oliva, 2016). Da mesma forma, o GRC tem explorado cada vez mais o lado positivo dos riscos, buscando aproveitar oportunidades para aumento de vantagem competitiva (Bromiley et al. 2015).

O COSO – *Committee of Sponsoring Organizations of the Treadway Commission* – define o GRC como:

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

A estrutura integrada proposta pelo COSO tem sido o modelo mais empregado no Gerenciamento de Riscos Corporativos (RIMS, 2011). Esse *framework* é representado na forma de uma matriz tridimensional (Figura 1), onde a primeira dimensão traz os oito componentes do GRC, a segunda contempla as categorias de objetivos da organização, e a terceira dimensão identifica os níveis na estrutura organizacional (COSO, 2004).



**Figura 1** - Estrutura Integrada para Gestão de Riscos Corporativos

Fonte: COSO (2004)

O modelo de gerenciamento de riscos corporativos proposto pelo comitê COSO, em 2014,

COSO – Enterprise Risk Management Framework, normalmente identificado por COSO II ou COSO

ERM, tem como origem a proposta do modelo de controles internos de 1992, COSO - *Internal Control – Integrated Framework*, normalmente identificado por COSO I ou COSO ICF. O COSO ICF foi proposto para auxiliar as organizações a avaliar e aperfeiçoar seus sistemas de controle interno e atualmente é parte integrante das políticas, normas e regulamentos organizacionais. Com as mudanças do ambiente de negócios, adicionado aos escândalos de fraudes financeiras que culminaram com falências de grandes corporações e consequentemente mudanças no ambiente político-legal, estimulou o início do desenvolvimento de um modelo de gerenciamento de riscos corporativos em 2001 que finalizou com a proposta do COSO ERM. O COSO ERM incorpora o modelo COSO ICF e solidifica a importância de identificar, avaliar e tratar os riscos corporativos. Já em 2013, o comitê COSO propõe uma atualização do modelo de controles internos de 1992, COSO - *Internal Control – Integrated Framework* versão 2013, normalmente identificado por COSO III ou COSO ICF 2013, dessa forma, o modelo propõe uma atualização dos processos de controles internos das organizações por meio de novos conceitos traduzidos em 17 princípios distribuídos por cada uma das cinco componentes do modelo. O COSO ICF 2013 traduz as diversas mudanças no ambiente operacional e no ambiente dos negócios nos últimos 20 anos, quais sejam, a globalização dos negócios, o aprofundamento da governança corporativa, o aumento da complexidade dos negócios, a maior regulamentação nos negócios, a intensificação do uso das tecnologias e o aumento de fraudes nos negócios (COSO, 2004; COSO 2013; PWC, 2017; Coopers & Lybrand, 1997; Gaitán, 2006).

No modelo COSO, as incertezas são associadas a riscos e oportunidades, podendo implicar destruição ou criação de valor. Os riscos são gerenciados na forma de portfólio e como um processo contínuo. Recomenda, ainda, que o GRC seja aplicado ao processo de definição dos objetivos estratégicos, quando da avaliação de riscos de diferentes alternativas, com alinhamento e suporte à missão da empresa (COSO, 2004).

Além dos elementos do *framework*, a estrutura contempla um tópico sobre funções e responsabilidades onde descreve papéis, desde a alta administração até o nível operacional, trazendo de maneira implícita componentes de governança corporativa (COSO, 2004).

Cabe ainda destacar que a gestão do portfólio de riscos, realizada de forma estruturada por meio da implantação do gerenciamento de riscos corporativos pode contribuir para a melhoria dos resultados das organizações, particularmente na forma de ganhos operacionais (Callahan. & Soileau, 2017; Florio & Leoni, 2017).

Com base nessa discussão, apresenta-se a proposição 1:

**A gestão de um portfólio de riscos permite ganhos de eficiência em relação à administração de riscos na forma individual.**

### Governança Corporativa

A ênfase nos benefícios da abordagem de portfólio de riscos do GRC deu-se simultaneamente ao avanço nos padrões de governança em direção à gestão de riscos, uma vez que uma gestão integrada de riscos demandava estrutura, organização e comunicação adequadas (Kleffner, Lee & McGannon, 2003).

Aebi, Sabato & Schmid (2012) definem governança de riscos como os aspectos de governança corporativa do Gerenciamento de Riscos Corporativos. A governança de riscos envolve estimular a cultura de riscos na organização, com uma estrutura organizacional para suportar a gestão de riscos e mecanismos de governança para sua formalização. Essencialmente, a governança de riscos suporta o processo de integração de riscos (Lundqvist, 2015).

Muitos estudos acerca de GRC têm a governança como foco central e enfatizam o papel da governança de riscos na implantação do GRC (Beasley, Branson & Pagach, 2015; Liebenberg & Hoyt, 2003; Pagach & Warr, 2011). Outras pesquisas apontam melhor governança em organizações onde existe um GRC (Altuntas, Berry-Stölzle & Hoyt, 2011; Baxter, Bedard, Hoytash & Yezegel, 2013). Baxter, Bedard, Hoytash & Yezegel (2013) afirmam que o maior desempenho das empresas que possuem um GRC pode ser atribuído à percepção do investidor acerca da credibilidade e consistências nos retornos como resultados da governança corporativa.

Lundqvist (2015) propõe uma divisão conceitual de GRC, separando os elementos da gestão de riscos tradicional e a governança de riscos (Figura 2).



**Figura 2** - Proposta de conceituação para gestão de riscos corporativos  
Fonte: adaptado de Lundqvist (2015)

Com base nessa discussão, apresenta-se a proposição 2:

**A governança de riscos, inserida na Governança Corporativa, suporta o processo de integração de riscos.**

#### Gestão Estratégica

O processo de gestão de riscos influencia e é influenciado pela estratégia das organizações (Meulbroek, 2002). Em empresas com maior nível de maturidade em GRC, usualmente identifica-se a sua inserção nos processos de estratégia corporativa (Ahmad, Ng & McManus, 2014; Baxter, Bedard, Hoitash & Yezegel, 2013; Beasley, Branson & Pagach, 2015).

Nesse sentido, esse trabalho apresenta a proposição 3:

**Quanto maior a integração do GRC com o planejamento estratégico, maior seu nível de maturidade.**

A integração efetiva da gestão de riscos com o processo de formulação estratégica permite focar no atingimento dos retornos esperados e, ao mesmo tempo, alinhar os riscos ao apetite da organização (Gibbs & DeLoach, 2006).

Embora exista uma tendência de associar GRC e estratégia, poucas fontes adotam uma definição de risco estratégico, ou mesmo alguma categorização de riscos. Para o Instituto Brasileiro de Governança Corporativa (IBGC) não há uma classificação consensual e exaustiva de riscos, a qual deve ser construída de acordo com as especificidades de cada organização (IBGC, 2007).

Slywotzky e Drzik (2005) consideram como riscos estratégicos o conjunto de eventos que podem destruir a trajetória de crescimento e valor para o acionista, mas que também podem ser convertidos em oportunidades. Frigo e Anderson (2011) definem riscos

estratégicos como aqueles que impedem a organização de atingir seus objetivos estratégicos. Dessa forma, os riscos devem ser contemplados na formulação, execução e gestão da estratégia, buscando criar e proteger valor para os acionistas e stakeholders. O IBGC associa os riscos estratégicos às decisões da alta administração e ao potencial de perdas substanciais de valor econômico (IBGC, 2007). Kaplan e Mikes (2012) propõem o conceito de riscos de estratégia, definidos como os riscos que não são inerentemente indesejáveis e que são necessários para obtenção dos retornos almejados. Uma gestão eficaz dos riscos de estratégia permite incorrer em maiores riscos, implicando vantagem competitiva sobre os concorrentes.

Sem adotar uma definição para riscos estratégicos, a Federation of European Risk Management Associations (FERMA, 2003) os classifica em: de concorrência, mudanças dos clientes, mudanças no setor, demanda, pesquisa e desenvolvimento, capital intelectual e integração em fusões e aquisições. A segmentação de Slywotzky e Drzik (2005) categoriza os riscos estratégicos em: setor, tecnologia, marca, concorrência, cliente, projetos e estagnação, estabelecendo, ainda, subcategorias.

Embora categorize os objetivos das organizações em estratégicos, operacionais, comunicação e conformidade (Figura 1), o modelo do COSO não propõe uma segmentação para os riscos.

Com base nessas questões, esse trabalho considera a proposição 4:

**A conexão da gestão de riscos com a formulação da estratégia permite uma gestão eficaz dos riscos que conferem vantagem competitiva e criam valor para a organização.**

### 3 MÉTODO

O método de pesquisa utilizado é o estudo de caso. A pesquisa é de natureza exploratória e se propõe

a responder a seguinte questão de pesquisa: como é realizada a gestão estratégica de riscos em uma empresa do setor de previdência privada brasileiro, sob a ótica de governança corporativa e gestão estratégica?

Para o levantamento de dados e informações deste estudo foram planejadas entrevistas

semiestruturadas. Duas entrevistas foram realizadas em maio de 2016, guiadas pelos tópicos apresentados no Quadro 1. A primeira entrevista envolveu o Diretor Técnico Gestão de Riscos e o Gerente de Controles Internos e *Compliance* e a segunda contou com a Superintendente de Estratégia.

GESTÃO DE RISCOS CORPORATIVOS	GOVERNANÇA CORPORATIVA	GESTÃO ESTRATÉGICA
<ul style="list-style-type: none"> <li>▪ Histórico e motivações da implantação do GRC</li> <li>▪ Processo de GRC</li> <li>▪ Segmentação de riscos</li> <li>▪ Riscos estratégicos</li> <li>▪ Apetite ao risco e objetivos da organização</li> <li>▪ Riscos como oportunidades</li> <li>▪ Ferramentas</li> </ul>	<ul style="list-style-type: none"> <li>▪ Gestão de riscos integrada (portfólio) vs. funcional</li> <li>▪ Estrutura organizacional - GRC</li> <li>▪ Papéis e responsabilidades</li> <li>▪ Processo decisório</li> <li>▪ Conexão entre governança e GRC</li> <li>▪ Aspectos regulatórios</li> </ul>	<ul style="list-style-type: none"> <li>▪ Planejamento estratégico</li> <li>▪ Alinhamento entre gestão estratégica e GRC</li> <li>▪ Projetos estratégicos</li> </ul>

**Quadro 1** - Tópicos principais considerados nas entrevistas

Fonte: Os autores

O estudo utilizou, ainda, dados secundários, fornecidos pela empresa e disponíveis em fontes públicas (tais como no *website* da empresa). Além de fornecer dados gerais acerca da empresa, esta fonte permitiu que informações relativas à gestão de riscos, governança corporativa e estratégia subsidiassem o planejamento e a realização das entrevistas, bem como a elaboração da análise de resultados.

#### 4 RESULTADOS

Em 2014, com apoio de consultoria externa, a EPP iniciou a implantação de seu GRC como parte do Mapa Estratégico 2014-2017, tendo o COSO como modelo de referência. Dentro desta iniciativa criou a Diretoria Técnica de Gestão de Riscos, englobando a já

existente Gerência de Controles Internos e *Compliance*. Definiu como missão desta diretoria assessorar a definição de diretrizes estratégicas de gestão de riscos e zelar pela adequada identificação, mensuração, gerenciamento e reporte dos riscos corporativos que possam comprometer o atingimento dos objetivos estratégicos da companhia.

Naquele mesmo ano foi realizado um mapeamento dos principais riscos da organização, com a participação das áreas de negócio, e tendo como critério a influência na obtenção dos objetivos estratégicos da empresa. Este trabalho resultou na identificação de 17 riscos principais, sendo que a cada risco foi atribuído um responsável. Embora a EPP não divulgue estes riscos, ela publica as oito categorias em que estão agrupados, conforme apresentado no Quadro 2.

CATEGORIA DE RISCO	DESCRIÇÃO
Risco de Mercado	Oscilações de preços de ativos ou diferenças entre indexadores e prazos de posições ativas e passivas
Risco de Liquidez	Falta de recursos para cumprimento de compromissos nas datas previstas
Risco de Crédito	Não cumprimento de obrigações financeiras pactuadas pela contraparte ou deterioração de suas condições de crédito
Risco Operacional	Processos inadequados ou ineficientes, erros, falhas nos sistemas de TI, problemas operacionais e fraudes ou ocorrências externas
Risco de Subscrição	Aplicação inadequada de metodologias ou premissas atuariais, incluindo falhas na especificação técnica do produto e nas condições de aceitação e precificação
Risco Legal	Não conformidade a aspectos legais envolvendo produtos, contratos firmados e obrigações regulatórias, trabalhistas, fiscais, societárias, comerciais, cíveis e penais, entre outras
Risco de Imagem	Deterioração da credibilidade ou da reputação por mau desempenho do dever de fidúcia, práticas antiéticas, divulgação de informações negativas e falhas na comunicação
Risco Estratégico	Comprometimento da viabilidade do negócio. Falhas de planejamento e posicionamento mercadológico, incapacidade de aplicação das estratégias definidas, credibilidade e alterações diversas na regulamentação do mercado de atuação ou do cenário macroeconômico

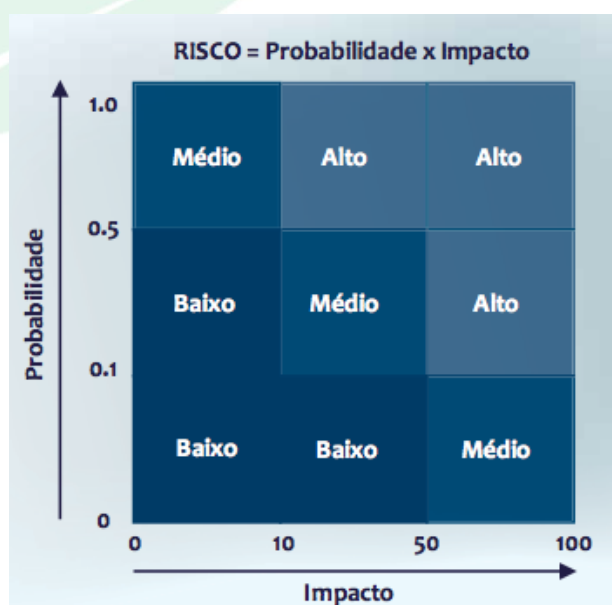
**Quadro 2** - Categorias de riscos da EPP

Fonte: EPP (2016)

Para cada um dos 17 riscos, foram identificadas suas causas e subcausas, gerando matrizes de impacto e probabilidade, conforme ilustrado na Figura 3. Vale ressaltar que uma causa pode estar associada a mais de um risco e, conseqüentemente, mais de uma categoria, com diferentes graus de impacto. Deste modo, cada risco foi avaliado sob a

ótica de cada categoria. Estas avaliações foram tanto quantitativas quanto qualitativas, dependendo do risco analisado e suas causas.

Esta avaliação de impacto e a respectiva probabilidade gerou a atribuição de uma nota a cada risco, permitindo a elaboração de um *ranking* dos riscos inerentes.



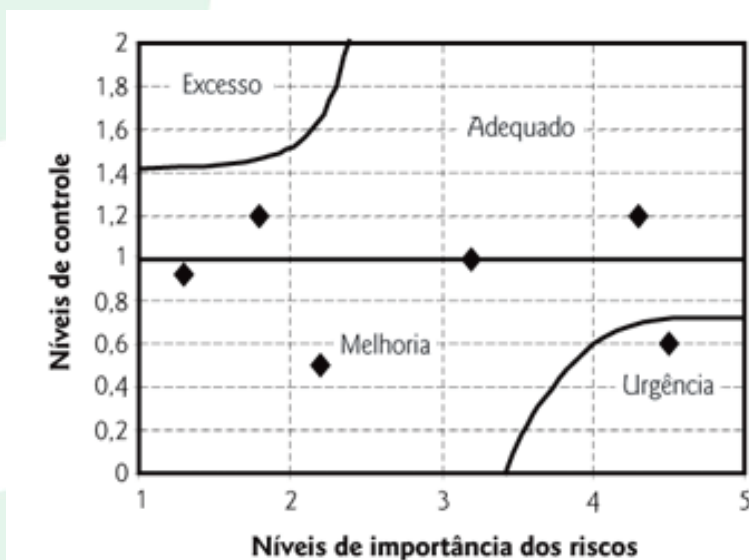
**Figura 3** - Matriz de impacto vs. probabilidade

Fonte: Os autores



O passo seguinte foi a construção de uma matriz de riscos, onde os riscos foram distribuídos ao longo do eixo das abscissas, conforme as notas atribuídas. No eixo das coordenadas foram considerados os níveis de controle de cada risco. Deste

modo, pôde-se avaliar se os níveis de controle estavam adequados à severidade de cada risco. A Figura 4 ilustra a lógica desta matriz, a qual consolida uma visão de portfólio de riscos.



**Figura 4 - Exemplo de Matriz de Riscos**

Fonte: adaptado de Paulo, Fernandes, Rodrigues & Eidt (2007)

O ajuste necessário no nível de controle de cada risco, na forma de resposta ao risco, teve como critério o apetite ao risco definido pela alta direção, a qual participou desta análise. Obtiveram-se, assim, os objetivos para níveis de riscos residuais compatíveis com o apetite da organização. Estes ajustes foram então convertidos em projetos (quando aplicáveis), e priorizados de acordo com as restrições de recursos da empresa.

Atualmente este ciclo está consolidado como um processo contínuo, em que os riscos e as matrizes são revistados periodicamente, ou à medida que eventos demandam revisão, apontando falhas ou excessos de controle. Da mesma forma, novos riscos são avaliados à medida que surgem.

As ferramentas utilizadas neste processo foram desenvolvidas internamente. A matriz de riscos está sendo incorporada ao sistema de gestão da EPP, de modo a proporcionar plena integração das decisões do dia-a-dia com a gestão de riscos. Também está em curso a integração da matriz de riscos com os processos de monitoramento.

Quanto à inserção do GRC na estrutura de governança corporativa, diversos órgãos estão diretamente envolvidos na governança de riscos (Figura 5), em linha com a prática de decisões colegiadas destacada no modelo de gestão da empresa:

- O Comitê de Riscos, subordinado ao Comitê Consultivo, tem a responsabilidade de avaliar

e acompanhar riscos em temas que envolvem as diretrizes e políticas de gestão de riscos. É um órgão estatutário formado pelo diretor-presidente, quatro diretores e dois membros indicados pelos acionistas. O diretor técnico de Gestão de Riscos é um convidado permanente do comitê;

- A Diretoria Técnica de Gestão de Riscos, com atuação independente, se reporta ao diretor-presidente e ao Comitê Consultivo, e é o órgão não estatutário que, em conjunto com a Superintendência de Auditoria, tem a responsabilidade pelo GRC;
- O Comitê de Auditoria é um órgão estatutário constituído por três membros eleitos pelo Conselho de Administração, ao qual se reporta, e presta assessoria nas atividades de auditoria, o que inclui procedimentos de avaliação de riscos;
- A Comissão de Riscos, órgão não estatutário, apoia a Diretoria nas questões relacionadas à gestão e controle de riscos;
- A Superintendência de Auditoria Interna reporta-se ao diretor-presidente e ao Comitê de Auditoria, e é o órgão não estatutário responsável por esta atividade.

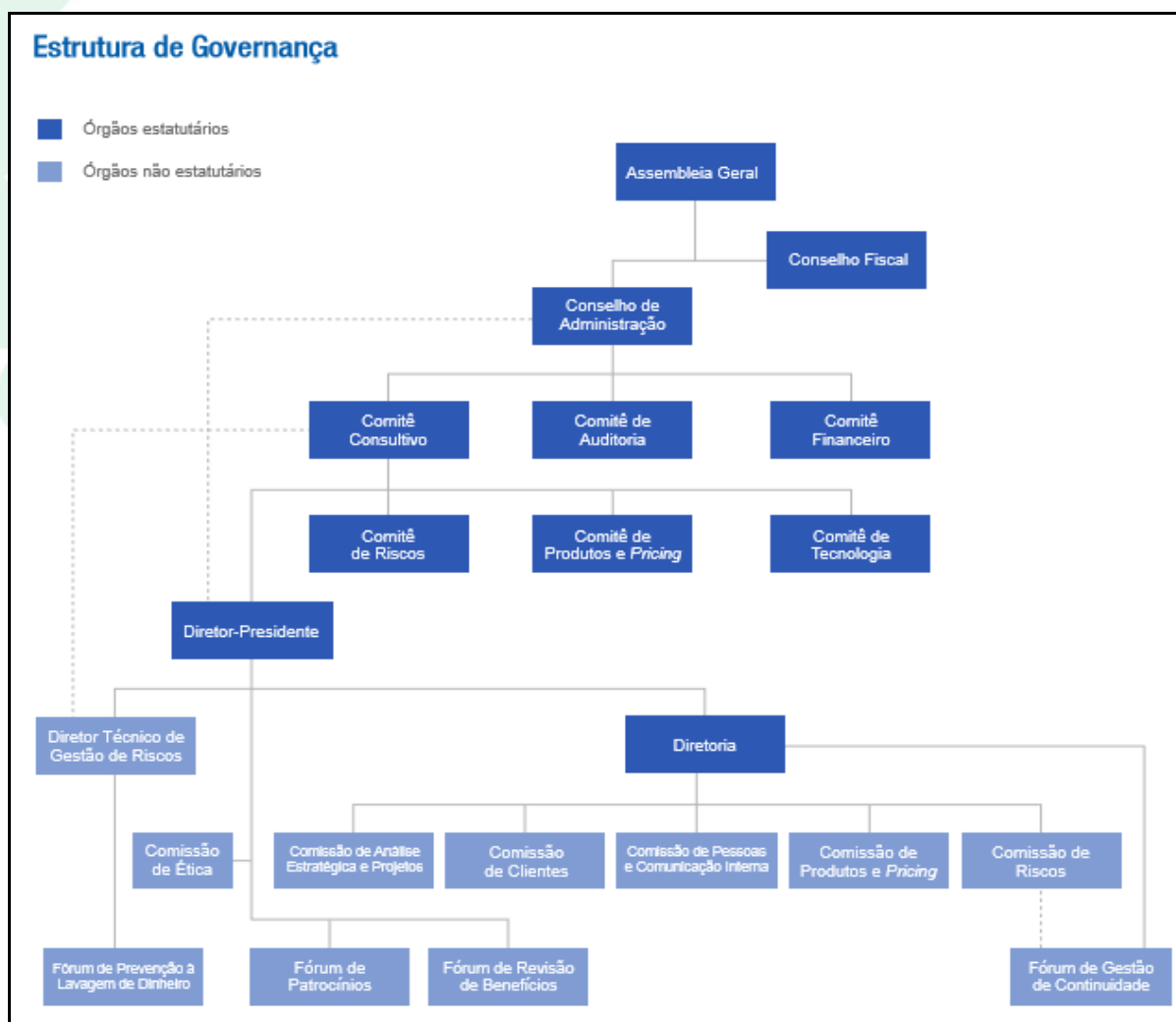
A EPP estabelece três linhas de atuação para a gestão de riscos: a primeira envolve todos os

responsáveis pelos negócios e processos; a segunda, a Diretoria Técnica de Gestão de Riscos; e a terceira é representada pelo Comitê de Riscos e pelo Comitê de Auditoria. A terceira linha é responsável pela auditoria da primeira e da segunda linha. Desta forma, a empresa se antecipa a uma norma da Susep que vai regulamentar, em 2016, a segregação entre as equipes que realizam o monitoramento dos riscos e as que tomam decisões sobre investimento.

A alta administração é a responsável pela definição do apetite ao risco, o qual representa o nível de perdas que o acionista está disposto a assumir. Este apetite é constituído pelos objetivos estratégicos, representados em parâmetros quantitativos e qualitativos, os quais por sua vez direcionam os limites operacionais. Deste modo, grande parte das decisões pode ser tomada sem que se consulte o Conselho de

Administração. Embora este apetite esteja formalizado em um documento, a empresa considera extremamente desafiadora a missão de obter uma visão única e integrada de apetite ao risco.

Como responsável pelo GRC, a Diretoria Técnica de Gestão de Riscos tem a incumbência de fornecer avaliações independentes acerca dos riscos da primeira linha. Um papel adicional deste órgão é a consultoria interna. Determinada área, por exemplo, ao planejar alguma iniciativa, mesmo que dentro dos seus limites de apetite ao risco, pode receber apoio técnico, incluindo aporte metodológico. De um modo geral, o foco da Diretoria Técnica de Gestão de Riscos não é simplesmente inibir iniciativas incompatíveis com o apetite ao risco, mas auxiliar na busca por alternativas viáveis.



**Figura 5 - Estrutura de Governança da EPP**

Fonte: EPP

Do ponto de vista de estratégia, a EPP considera como riscos estratégicos aqueles que comprometem a viabilidade do negócio, conforme

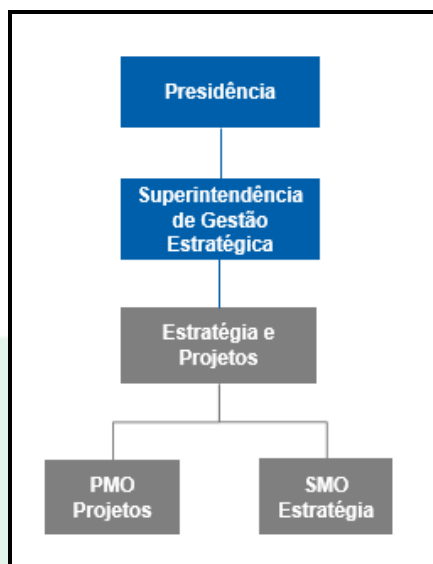
descrito no Quadro 2. Estes riscos estão associados a deficiências na gestão estratégica ou a fatores externos. Vale ressaltar que a empresa considera não somente os

riscos estratégicos, mas todos os 17 riscos das oito categorias adotadas como riscos que podem afetar os objetivos estratégicos.

A gestão estratégica da EPP fica a cargo da Superintendência de Gestão Estratégica, a qual se reporta ao diretor-presidente. Esta superintendência também é responsável por projetos corporativos, estratégicos ou não, entre outras atribuições. Conta com um escritório de estratégia (SMO) e um escritório

de projetos (PMO), conforme apresentado na Figura 6, e responde pelos riscos de estratégia e de imagem.

O processo de planejamento estratégico da empresa é realizado em um ciclo anual, coordenado pelo escritório de estratégia, e inicia-se pela análise do ambiente externo. Esta análise subsidia a formulação da estratégia, etapa em que se definem aspectos de escopo de atuação, posicionamento mercadológico e modelo de negócios.



**Figura 6** - Inserção da gestão estratégica no organograma da EPP

Fonte: Os autores

A formulação estratégica é submetida aos Conselhos de Administração e Consultivo e, uma vez aprovada, gera os objetivos estratégicos da companhia, sendo que a cada objetivo é atribuído um responsável.

Os objetivos estratégicos compõem o mapa estratégico, com aplicação da metodologia *Balanced Scorecard* (BSC), com definição de indicadores monitorados trimestralmente.

A partir dos objetivos estratégicos são geradas as iniciativas estratégicas, que neste processo representam a execução da estratégia. Uma vez submetidas e aprovadas pela alta administração, as iniciativas estratégicas seguem para o escritório de projetos e, finalmente são inseridas no processo de orçamentação.

A identidade corporativa da empresa, composta de missão, visão e valores, é revista a cada cinco anos.

A concepção da matriz de riscos inicial não teve sua origem no planejamento estratégico, mas no projeto de implantação do GRC, já descrito nesta seção. A adequação dos níveis de controle de riscos da matriz ao apetite ao risco da EPP se deu na forma de projetos, os quais foram somados às iniciativas estratégicas em andamento no escritório de projetos e

associados aos objetivos estratégicos na composição do mapa estratégico do BSC.

Tendo o GRC se tornado um processo contínuo, atualmente a EPP está buscando conectar a matriz de riscos ao início do processo de planejamento estratégico, ou seja, a análise ambiental e a formulação da estratégia, e não mais diretamente à fase de projetos. Com isto, a empresa tem como expectativa explorar melhor os riscos positivos.

## 5 DISCUSSÃO

Governança corporativa e gestão estratégica têm se tornado elementos indissociáveis do Gerenciamento de Riscos Corporativos. Deste modo, estes temas figuram entre os principais direcionadores do GRC e o seu alinhamento nas organizações tem ganhado crescente relevância.

Uma visão de portfólio, com a inclusão de riscos estratégicos, além dos tradicionais, tem cada vez mais apresentado ganhos de eficiência nas empresas (Bromiley et al., 2015). Também tem havido consenso quanto aos benefícios de se buscar o lado positivo dos riscos, na forma de oportunidades estratégicas. Estas

visões, holística e estratégica, demandam estruturas de governança apropriadas.

Esta pesquisa teve como objetivo explorar este alinhamento na EPP, onde o GRC foi recentemente implantado, mediante a análise do seu processo de gestão de riscos. Neste contexto, valores financeiros expressivos estão expostos a diversos tipos de riscos, alguns deles específicos do setor. Da mesma forma, questões regulatórias têm grande impacto em riscos e oportunidades.

Como pergunta de pesquisa, este estudo buscou entender como é realizada a gestão estratégica de riscos em uma empresa do setor de previdência privada brasileiro, sob a ótica de governança corporativa e gestão estratégica. Para respondê-la, foram realizadas entrevistas semiestruturadas e utilizados dados secundários da empresa, tendo como método o estudo de caso.

Identificou-se que por meio de uma matriz, a EPP garante a visão sistêmica de seus principais riscos, segmentados em categorias, caracterizando a sua gestão em forma de portfólio. Deste modo, as análises acerca de níveis de controle de risco podem ser realizadas de modo integrado, assim como a tomada de decisão quanto à priorização de projetos e recursos relacionados a estes controles. Esta visão holística permite uma gestão mais eficiente dos riscos, confirmando a Proposição 1 deste estudo.

A pesquisa também permitiu constatar a inserção da governança de riscos em uma sólida estrutura de governança corporativa na organização estudada. Estabelecida em três linhas de atuação, a governança de riscos conta com órgãos estatutários e não estatutários, que são compostos por conselhos, comitês e área técnica, com papéis de apoio, auditoria e execução claramente definidos. A governança é reforçada pela ênfase em decisões colegiadas, constante no sistema de gestão da EPP, ao qual o GRC está sendo integrado. Estes resultados vão ao encontro do que se apresenta na Proposição 2 desta pesquisa.

Como principais riscos, a empresa considera aqueles que estão relacionados ao atingimento de seus objetivos estratégicos. Os riscos estratégicos, que compõem uma das categorias dos principais riscos, são aqueles que podem comprometer a viabilidade do negócio e que estão associados a falhas na gestão estratégica ou a fatores externos. Deste modo, todos os principais riscos, e não somente os estratégicos, estão relacionados aos objetivos estratégicos, diferentemente dos conceitos mais comumente encontrados na literatura.

Atualmente a conexão entre o GRC e a gestão estratégica se dá na forma de projetos estratégicos para adequação dos níveis de controle de riscos. Está em andamento a integração do GRC às etapas iniciais de análise ambiental e formulação no ciclo de planejamento estratégico.

Embora estes resultados não possam ser considerados evidências da Proposição 3, constatou-se

que esta integração se inicia em um momento em que os elementos de governança estão plenamente implantados e o GRC já se tornou um processo contínuo na empresa.

Da mesma forma, por ainda não estar presente a conexão entre o GRC e a formulação da estratégia, não existem elementos para confirmar a Proposição 4. Entretanto constatou-se na organização uma expectativa de, com esta iniciativa, melhor explorar a perspectiva de oportunidades nas decisões acerca de riscos.

Pôde-se observar, ainda, que as iniciativas e processos de GRC da EPP sugerem uma antecipação da empresa em relação às demandas e oportunidades em curso no âmbito regulatório.

Por fim, as contribuições identificadas no estudo de caso da EPP podem ser consideradas por outras empresas com iniciativas de GRC em andamento, ou por aquelas que pretendem implantar esta abordagem.

## REFERÊNCIAS

- Aebi, V., Sabato, G., & Schmid, M. (2012). Risk management, corporate governance, and bank performance in the financial crisis. *Journal of Banking & Finance*, 36(12), 3213-3226.
- Ahmad, S., Ng, C., & McManus, L. A. (2014). Enterprise Risk Management (ERM) implementation: Some empirical evidence from large Australian companies. *Procedia-Social and Behavioral Sciences*, 164, 541-547.
- Altuntas, M., Berry-Stölzle, T. R., & Hoyt, R. E. (2011). Implementation of enterprise risk management: Evidence from the German property-liability insurance industry. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 36(3), 414-439.
- Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society*, 35(7), 659-675.
- Arnold, V., Benford, T., Canada, J., & Sutton, S. G. (2015). Leveraging integrated information systems to enhance strategic flexibility and performance: The enabling role of enterprise risk management. *International Journal of Accounting Information Systems*, 19, 1-16.
- AS/NZS (1995). *Australian/New Zealand Standard of Risk Management*. Sydney: Standards Australia.
- Baxter, R., Bedard, J. C., Hoitash, R., & Yezegel, A. (2013). Enterprise risk management program quality: Determinants, value relevance, and the financial crisis.

*Contemporary Accounting Research*, 30(4), 1264-1295.

Beasley, M., Branson, B., & Pagach, D. (2015). An analysis of the maturity and strategic impact of investments in ERM. *Journal of Accounting and Public Policy*, 34(3), 219-243.

Bhimani, A. (2009). Risk management, corporate governance and management accounting: Emerging interdependencies. *Management Accounting Research*, 20(1), 2-5.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning*, 48(4), 265-276.

CAS. (2003). *Overview of Enterprise Risk Management*. Casualty Actuarial Society (CAS). Recuperado em 19 junho, 2018, de <http://www.casact.org/area/erm/overview.pdf>.

Callahan, C. & Soileau, J. (2017). Does Enterprise Risk Management enhance operating performance? *Advances in Accounting*, 37, 122-139.

Collier, P. M. (2009). *Fundamentals of risk management for accountants and managers*. New York: Routledge.

Committee of Sponsoring Organizations of the Treadway Commission [COSO]. (2004). Enterprise Risk Management - Integrated Framework.

Committee of Sponsoring Organizations of the Treadway Commission [COSO]. (2013). Internal Control - Integrated Framework.

Coopers & Lybrand. (1997). *Los nuevos conceptos del control interno*. Informe Coso. Madrid: Editorial Díaz de Santos.

Farrell, M., & Gallagher, R. (2015). The valuation implications of enterprise risk management maturity. *Journal of Risk and Insurance*, 82(3), 625-657.

FERMA. (2003). *Normas de Gestão de Riscos*. Federation of European Risk Management Association (FERMA). Recuperado em 19 junho, 2018, de <http://www.ferma.eu>.

Florio, C. & Leoni, G. (2017). Enterprise Risk Management and firm performance: The Italian case. *The British Accounting Review*, 49, 56-74.

Frijo, M. L., & Anderson, R. J. (2011). What is strategic risk management? *Strategic Finance*, 92(10), 21.

Gaitán, R.E. (2006). *Control interno y fraudes* 2a ed. Bogotá: Ecoe Ediciones.

Gibbs, E., & DeLoach, J. (2006). Which comes first... managing risk or strategy-setting? Both! Effectively integrating risk management with the strategy-setting process enables management to focus on achieving its expected return while controlling its accepted risk exposure. *Financial Executive*, 22(1), 34-40.

IBGC. (2007). *Guia de orientação para gerenciamento de riscos corporativos*. Instituto Brasileiro de Governança Corporativa (IBGC). Recuperado em 19 junho, 2018, de <http://www.ibgc.org.br/userfiles/3.pdf>.

IIA. (2001). *Risk or Opportunity – the Choice is Yours*. The Institute of Internal Auditors (IIA). Recuperado em 19 junho, 2018, de <http://usfweb2.usf.edu/uac/documents/riskparadigm.pdf>

Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review*, 90(6), 48-58.

Kleffner, A. E., Lee, R. B., & McGannon, B. (2003). The effect of corporate governance on the use of enterprise risk management: Evidence from Canada. *Risk Management and Insurance Review*, 6(1), 53-73.

Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of Enterprise Risk Management: Evidence from the appointment of Chief Risk Officers. *Risk Management and Insurance Review*, 6(1), 37-52.

Lundqvist, S. A. (2015). Why firms implement risk governance – Stepping beyond traditional risk management to enterprise risk management. *Journal of Accounting and Public Policy*, 34(5), 441-466.

Meulbroek, L. K. (2002). *Integrated risk management for the firm: a senior manager's guide*. Harvard Business School Working Paper n.. 02-046. Available at SSRN 301331.

Miccolis, J. (2000). Enterprise Risk Management in the Financial Services Industry: Still a long way to go. *International Risk Management Institute [IRMI]*, Expert commentary. Recuperado em 19 junho, 2018, de <https://www.irmi.com/articles/expert-commentary/enterprise-risk-management-in-the-financial-services-industry-still-a-long-way-to-go>.

Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society*, 36(4), 226-245.

Oliva, F. L. (2016). A maturity model for enterprise risk management. *International Journal of Production Economics*, 173, 66-79.

Oliva, F.L., Sobral, M.C., Damasceno, F., Teixeira, H.J., Grisi, C.C.H., Fischmann, A.A. & Santos, S.A. (2014). Risks and strategies in a Brazilian innovation – flexfuel technology. *Journal of Manufacturing Technology Management*, 25(6), 916-930.

Pagach, D., & Warr, R. (2011). The characteristics of firms that hire chief risk officers. *Journal of Risk and Insurance*, 78(1), 185-211.

Paulo, W. D. L., Fernandes, F. C., Rodrigues, L. G. B., & Eidt, J. (2007). Riscos e controles internos: Uma metodologia de mensuração dos níveis de controle de riscos empresariais. *Revista de Contabilidade e Finanças*, 43(49), 49-60.

PWC, PricewaterhouseCoopers. Recuperado em 19 junho, 2018, de <http://www.pwc.com>

RIMS, (2011). *FAQ on SRM and ERM. Why Strategic Management? The Risk Management Society (RIMS)*. Recuperado em 19 junho, 2018, de <http://www.rims.org/resources/ERM/Documents/>.

Slywotzky, A. J., & Drzik, J. (2005). Countering the biggest risk of all. *Harvard Business Review*, 83(4), 78-88.

S&P. *Standard & Poor's to Apply Enterprise Risk Analysis to Corporate Ratings*. Standard & Poor's (S&P). Recuperado em 19 junho, 2018, de <http://www.nyu.edu/intercep/ERM%20for%20Non-Financial%20Companies%205.7.08.pdf>.

Wu, D. D., & Olson, D. L. (2010). Introduction to special section on “Risk and technology”. *Technological Forecasting and Social Change*, 77(6), 837-839.