



Revista Facultad de Ciencias Económicas: Investigación y Reflexión

ISSN: 0121-6805

Facultad de Ciencias Económicas Universidad Militar  
Nueva Granada

Marques, Leandro; Habitzreuter Muller, Suzana; Zanievicz da Silva, Márcia

**Gestão de riscos corporativos: percepção dos *chief risk officers*\***

Revista Facultad de Ciencias Económicas: Investigación y Reflexión, vol. XXVII, núm. 2, 2019, Julho-Dezembro, pp. 105-126  
Facultad de Ciencias Económicas Universidad Militar Nueva Granada

DOI: <https://doi.org/10.18359/rfce.3932>

Disponível em: <https://www.redalyc.org/articulo.oa?id=90962879007>

- Como citar este artigo
- Número completo
- Mais informações do artigo
- Site da revista em [redalyc.org](http://redalyc.org)



Sistema de Informação Científica Redalyc

Rede de Revistas Científicas da América Latina e do Caribe, Espanha e Portugal

Sem fins lucrativos acadêmica projeto, desenvolvido no âmbito da iniciativa  
acesso aberto



## Gestão de riscos corporativos: percepção dos *chief risk officers*\*

Leandro Marques<sup>a</sup> ■ Suzana Habitzreuter Muller<sup>b</sup> ■ Márcia Zanievicz da Silva<sup>c</sup>

**Resumo:** O objetivo deste artigo foi verificar como a gestão de riscos se materializa nas organizações. Para tanto, realizou-se pesquisa descritiva com abordagem quantitativa por meio de levantamento. O instrumento de coleta de dados compreendeu um questionário estruturado enviado à CROs de empresas brasileiras, auditores e consultores de gestão de riscos. Um total de 22 respostas foi obtido. A análise dos dados revela que há pouco conhecimento por parte dos entrevistados sobre as obras que versam sobre gestão de riscos apresentadas na pesquisa, indicando assim pouca utilização destas como estratégias de capacitação pelos CROs. Em relação às ferramentas e técnicas de gestão de riscos, constatou-se que as técnicas elencadas pelo COSO (2007) são pouco utilizadas pelos respondentes, sendo que as mais utilizadas são as de menor complexidade de aplicação. Em relação aos motivos para a adoção da GRC na empresa, o mais recorrente foi a exigência por parte de órgãos reguladores.

**Palavras-chave:** Gestão de riscos; GRC; gestão do conhecimento; *chief Risk Officer* (CRO).

**Fecha de recibido:** 30/01/2019 Fecha de aprobado: 22/05/2019

**Como citar:** Marques, L., Habitzreuter, S. y Zanievicz, M. (2019). Gestão de riscos corporativos: percepção dos chief risk officers. *Revista Facultad de Ciencias Económicas*, 27(2), 105-126. rev.fac.cienc. econ. doi: <https://doi.org/10.18359/rfce.3932>

**JEL:** G30, G32, G39.

---

\* Este artigo é baseado em uma pesquisa científica realizada pelos autores.

**a** Mestre em Ciências Contábeis pelo Programa de Pós-Graduação em Ciências Contábeis da Universidade Regional de Blumenau (PPGCC/FURB). Professor do Curso de Ciências Contábeis na Faculdade La Salle – MT. E-mail: leamarqu@gmail.com

**b** Mestre em Ciências Contábeis pelo Programa de Pós-Graduação em Ciências Contábeis da Universidade Regional de Blumenau (PPGCC/FURB). E-mail: suzanahm2013@gmail.com

**c** Doutora em Ciências Contábeis e Administração pelo Programa de Pós-Graduação em Ciências Contábeis da Universidade Regional de Blumenau (PPGCC/FURB). Professora do Programa de Pós-Graduação em Ciências Contábeis da Universidade Regional de Blumenau (PPGCC/FURB). E-mail: marciaz@gmail.com

## *Corporate Risk Management: Perception of the Chief Risk Officers*

**Abstract:** The purpose of this paper is to verify how risk management materializes in organizations. To do this, a descriptive research was conducted with a quantitative approach by means of a survey. The data collection instrument was a structured questionnaire sent to the Chief Risk Officers (CROs) of Brazilian companies, auditors and risk management consultants. A total of 22 responses were obtained. Data analysis reveals that –among those interviewed– there is little knowledge about work related to the risk management presented in the research; this indicates a scarce use of this work as training strategies for CROs. Concerning tools and risk management techniques, it was found that the techniques identified by COSO (2007) are rarely used by respondents, while the most used are those less complicated to implement. Among the reasons behind GRC adoption in a company, the most common reason was by request of regulatory bodies.

**Keywords:** Risk management; GRC; knowledge management; *Chief Risk Officer*; CRO.

## *Gestión de riesgos corporativos: percepción de los Chief risk officers*

**Resumen:** El objetivo de este artículo fue verificar cómo la gestión de riesgos se materializa en las organizaciones. Para ello, se realizó una investigación descriptiva con un enfoque cuantitativo por medio de encuesta. El instrumento de recolección de datos consistía en un cuestionario estructurado enviado a Chief risk officers (CROs) de empresas brasileñas, auditores y consultores de gestión de riesgos. Un total de 22 respuestas fueron obtenidas. El análisis de los datos revela que entre los entrevistados existe poco conocimiento acerca de los trabajos relacionados con la gestión de riesgos presentados en la investigación, lo cual indica un uso escaso de estos trabajos como estrategias de capacitación para los CROs. En cuanto a las herramientas y técnicas de gestión de riesgos, se constató que las técnicas señaladas por el COSO (2007) son poco utilizadas por los encuestados, mientras que las más utilizadas son las que son menos complicadas en su aplicación. Con respecto a los motivos detrás de la adopción de GRC en una empresa, el más común fue su exigencia por parte de órganos reguladores.

**Palabras clave:** Gestión de riesgos; GRC; gestión de conocimiento; *Chief Risk Officer*; CRO.

## Introdução

O risco tem sido um tema de análise em diversas disciplinas, atividades profissionais e ações práticas. As áreas que têm ampliado o interesse sobre os riscos e formas de gerenciá-lo vão desde desastres naturais, ameaças tecnológicas e condições de trabalho até impactos na saúde, crime, terrorismo e poluição (Renn, 2008). Especificamente no contexto organizacional, o interesse pela gestão de riscos cresceu rapidamente nos últimos 15 anos e têm sido impulsionado por entidades reguladoras, associações profissionais e até mesmo empresas de *rating* que o consideram como uma ferramenta capaz de prover a gestão de informações para otimizar os lucros e o valor da empresa.

De acordo com Nocco e Stulz (2006) a crescente atenção à gestão dos riscos tem provocado mudanças na estrutura organizacional e nas competências requeridas para determinadas funções. Desta maneira, até a alguns anos, o cargo de gerente de riscos (normalmente, uma posição de nível operacional na tesouraria das empresas), ocupava-se principalmente com tarefas relacionadas à contratação de seguros. No entanto, segundo os referidos autores, a ampliação do foco de atuação da gestão de riscos, tais como riscos operacionais, de mercado, financeiros e estratégicos, elevou a função de gerenciar riscos a um patamar superior, sendo desempenhada em um número crescente de empresas, por um executivo sênior denominado *Chief Risk Officer* (CRO).

Considerando-se que a Gestão de Riscos Corporativos (GRC) se constitui como um processo que combina, de forma integrada, as atividades de gerenciamento de risco de toda a empresa (Gatzert & Martin, 2015), supõe-se que a pessoa responsável pela gestão de riscos, no caso o CRO, possua um entendimento abrangente sobre os principais riscos ao qual a organização está exposta, bem como domine ferramentas que contribuam para o gerenciamento e a mitigação dos riscos.

Ocorre que, tanto o conhecimento sobre os tipos de riscos quanto o domínio de ferramentas para gestão não são exclusivamente tácitos, eles

necessitam serem adquiridos por meio de processos formais de instrução. No entanto, dada à contemporaneidade da GRC, as fontes formais de obtenção de conhecimento sobre risco e gestão de riscos organizacionais ainda estão em processo de construção, e pouco se sabe sobre as fontes de aquisição de conhecimento, adotado pelos CROS para desempenhar suas funções. Deste contexto, emerge a questão problema que norteia esta pesquisa: Quais as estratégias de aprendizagem consideradas relevantes pelos *Chief Risk Officers* para desenvolver competências e habilidades sobre gestão de riscos e como a gestão de risco se materializa nas organizações?

Em decorrência do problema de pesquisa, o estudo tem por objetivo verificar como a gestão de risco se materializa nas organizações. Para tal, buscou-se conhecer os motivos que levam as empresas a adotarem a GRC; apontar as técnicas utilizadas pelos CROS para identificar e avaliar os riscos; conhecer as estratégias de aprendizagem consideradas relevantes pelos *Chief Risk Officers* para desenvolver competências e habilidades sobre gestão de riscos; e relacionar características pessoais e organizacionais com as estratégias de aprendizagem, os motivos de adoção e as técnicas utilizadas para gerenciar os riscos.

Salienta-se aqui, que não foram localizadas pesquisas semelhantes no contexto nacional, o que assinala uma lacuna de pesquisa, justificando desta maneira a realização deste estudo. Além disso, os resultados podem contribuir para determinar o quão útil para a prática são as obras publicadas sobre Gestão de Riscos Corporativos, ao mesmo tempo, sinalizar fragilidades e necessidades na literatura sobre GRC atualmente disponível. A escolha do CRO para a condução do estudo deu-se em função de que estes profissionais têm como responsabilidade a concepção de estruturas de gerenciamento de risco, a implementação da GRC, a comunicação das políticas e a fiscalização dos processos (Power, 2005) devendo, portanto, terem uma visão holística do gerenciamento de riscos.

## Referencial Teórico

### Gestão de Riscos Corporativos

Tendo por base Renn (1992), Paxson e Wood (1998), Collier, Berry e Burke (2007), *Committee of Sponsoring Organizations of the Treadway Commission* (COSO, 2004) e Instituto Brasileiro de Governança Corporativa (IBGC, 2007) pode-se definir risco como a probabilidade de que algum evento ocorra ocasionando resultados inesperados que afetarão a consecução dos objetivos organizacionais. De acordo com Jorion (2000), o gerenciamento de riscos constitui-se no processo pelo qual várias exposições são identificadas, mensuradas e controladas. Para Collier *et al.* (2007) a gestão de riscos é o processo pelo qual as organizações metodicamente enfrentam os riscos inerentes às suas atividades na busca dos objetivos organizacionais e em todo o conjunto de suas atividades. Neste sentido, o gerenciamento de riscos deve “contribuir para a perenidade da organização, atendendo aos seus objetivos estatutários e estratégicos” (IBGC, 2007, p. 10).

A abordagem tradicional de gestão de riscos envolve métodos não integrados, com o intuito de enfrentar diversos riscos em diferentes unidades da empresa (silos) (Liebenberg & Hoyt, 2003), nesse caso, as exposições individuais ao risco são tratadas separadamente (Berry & Phillips, 1998). No entanto, nos últimos anos, houve uma mudança de paradigma em relação à maneira de visualizar a gestão de riscos, ao invés de olhá-la sob o prisma tradicional da gestão de riscos por silos, as organizações têm migrado para uma abordagem integrativa (holística) de gestão de riscos (Gordon, Loeb, & Tseng, 2009), nessa condição, os gestores podem identificar, avaliar e selecionar as respostas adequadas que coincidem com o apetite de risco da empresa (Soltanizadeh, Rasid, Golshan, Quoquab, & Basiruddin, 2014).

Jorion (2000) atenta para a necessidade de uma gestão de riscos realizada de forma integrada. Na concepção do autor, um sistema ideal de gerenciamento de riscos deve propiciar um panorama completo dos riscos à que a empresa está exposta. Visão semelhante é compartilhada por Ching e

Colombo (2013, p. 24) que afirmam que “a gestão de risco deve analisar a empresa como um todo e não cada tipo de risco e/ou cada área da empresa separadamente”. Desta forma, a abordagem holística sobrepõe-se à gestão de riscos baseada em silos por fornecer aos gestores uma compreensão sistêmica das interdependências entre os diferentes riscos aos quais estão expostos (McShane, Nair, & Rustambekov, 2011).

Para o COSO (2004, p. 4) o gerenciamento de riscos corporativos é:

[...] 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 compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.

Por meio da definição do COSO (2004) pode-se perceber que a Gestão de Riscos Corporativos envolve toda a organização, em todos os níveis hierárquicos, no estabelecimento de estratégias que permitam administrar os riscos ao qual a empresa está exposta, possibilitando o cumprimento de seus objetivos estratégicos.

O objetivo da Gestão de Riscos Corporativos é a gestão integrada de todos os riscos enfrentados por uma companhia, sejam estes relacionados à governança corporativa, auditoria, cadeias de abastecimento, sistemas de distribuição, tecnologia da informação ou recursos humanos (McShane *et al.*, 2011; Gatzert & Martin, 2015). A longo prazo, a Gestão de Riscos Corporativos pode também melhorar a resiliência corporativa, ou seja, a capacidade de a empresa se antecipar e responder às mudanças (COSO, 2017).

De acordo com Olson e Wu (2008) existem mais de oitenta *frameworks* de gestão de riscos, alguns elencados por Daud, Yazid e Hussin (2010), tais como o Relatório King II, a Norma de Gestão de Riscos da Federação de Gestão de Risco Europeia (FERMA), a ISO 31000:2009 e o documento *Enterprise Risk Management: Integrated Framework* do COSO (2004). Os autores salientam que apesar de tais *frameworks* possuírem nomes diferentes,

serem elaborados por diferentes órgãos e em diferentes países, todos compartilham um tema em comum, a identificação, priorização e quantificação dos riscos, a fim de ajudar as organizações a gerir de forma eficaz a sua exposição aos riscos (Daud *et al.*, 2010). Dentre os diversos *frameworks* existentes, o *Enterprise Risk Management: Integrated Framework* do COSO é um dos mais disseminados (Olson & Wu, 2008).

O objetivo do COSO (2004) não é a eliminação total dos riscos, mas sim, a administração deles em níveis aceitáveis pela empresa. Para tanto, ele estabelece uma sequência de eventos, fazendo com que os gestores levem em consideração os riscos aos quais as empresas estão expostas, bem como avaliem quais os controles necessários para o gerenciamento destes riscos (Zonatto & Beuren, 2009).

Recentemente, o *framework* do COSO (2004) passou por uma atualização a fim de refletir o surgimento de novos riscos, cada vez mais complexos, e a evolução da gestão de riscos. Essa atualização, publicada em 2017, destaca a importância de considerar o risco no processo de definição da estratégia empresarial, assim como, na avaliação do desempenho corporativo (COSO, 2017).

## Gestão do Conhecimento

A perspectiva da empresa baseada no conhecimento deriva, em parte, da teoria baseada em recursos, e tem se desenvolvido na literatura de gestão estratégica a partir de autores como Spender (1996), Nonaka e Takeuchi (1997), Cole (1998), dentre outros e, de acordo com Alavi e Leidner (2001) postula que os serviços prestados por recursos tangíveis dependem de como eles são combinados e aplicados, que por sua vez é uma função do *know-how* da empresa (isto é, o conhecimento). Ainda, segundo Alavi e Leidner (2001), este conhecimento é incorporado na organização e envolve a cultura e a identidade organizacional, as rotinas, políticas, sistemas e documentos, bem como os indivíduos.

Segundo Chait (1999) e Smith (2001), a gestão do conhecimento nas organizações é o processo formal e dirigido para determinar quais informações os membros possuem que poderiam beneficiar outros integrantes e, em seguida, desenvolvendo maneiras de torná-la facilmente

disponíveis, esse processo contempla como o conhecimento é capturado, avaliado, tratado, armazenado, fornecido e utilizado.

Ressalta-se também que os estudos sobre gestão do conhecimento segregam-no em conhecimento tácito e explícito. O conhecimento tácito é subjetivo, representa habilidades, ideias, percepções e experiências pessoais difíceis de serem formalizadas, transferidas e explicadas; enquanto que o conhecimento explícito é relativamente fácil de ser codificado, transferido e reutilizado, já que é facilmente organizado em bases de dados e outras formas de publicação (Silva, 2004). De acordo com Brown e Dugid (2001) o conhecimento tácito pode ser utilizado para fomentar a criatividade e a inovação ao passo que o explícito possibilita tornar o ambiente de trabalho previsível facilitando a realização das tarefas.

Adicionalmente, conforme Devenport e Prusak (2003) há cinco formas de gerar conhecimento: Aquisição, Recursos Dedicados, Fusão, Adaptação e Rede de Conhecimento. A Aquisição ocorre por intermédio de compra, de outras empresas ou contratação de novos colaboradores. Os Recursos Dedicados geram conhecimento a partir da criação de grupos específicos para criação de conhecimento, por exemplo, por meio de pesquisa e desenvolvimento e universidades corporativas. Quanto à Fusão é o processo de geração de conhecimento a partir da criação de grupos de trabalho multidisciplinares, formado deliberadamente por membros com diferentes conhecimentos e habilidades. Já a Adaptação gera conhecimento pela existência de recursos internos receptivos às mudanças, que são absorvidas em um processo contínuo de aprendizagem. Por fim, a Rede de Conhecimento funciona como um condutor, formal ou informal, do pensamento inovador (Devenport & Prusak, 2003).

Para Takeuchi e Nonaka (2008, p. 24) a produção de novos conhecimentos organizacionais envolve um processo que amplia o conhecimento criado pelos indivíduos e solidifica-o como parte da rede de conhecimento da organização. “Esse processo é decorrente de uma iteração contínua, dinâmica e simultânea entre o conhecimento tácito e o explícito”. Por fim, segundo Smith (2001), existe tensão entre processo e prática. Processo



representa o conhecimento explícito, ou como o conhecimento é organizado. Prática representa o conhecimento tácito, ou a forma como o trabalho é realmente feito. As empresas que lidam com sucesso com tais tensões e usam os vários tipos de conhecimento tácito e explícito em seu proveito, podem ser mais bem sucedidas na consecução dos objetivos organizacionais.

## Procedimentos Metodológicos

A pesquisa, quanto aos objetivos, caracteriza-se como descritiva. Quanto aos procedimentos, caracteriza-se como um levantamento e para ser operacionalizada adota uma abordagem quantitativa (Raupp & Beuren, 2006).

Quanto à população inicial do estudo, corresponde a 37 *Chief Risk Officers* que atuam em empresas brasileiras cadastrados na rede social LinkedIn, na qual realizou-se uma busca com a palavra-chave “*chief risk officer*” no campo “cargo”. Após a identificação dos CROS efetuou-se contato, primeiramente por intermédio do próprio LinkedIn, a fim de apresentar a pesquisa aos CROS e enviar-lhes o *link* do questionário. Posteriormente procedeu-se ao contato telefônico com os participantes para verificar se estes haviam recebido o *link* e também para confirmar o endereço eletrônico. Neste momento, o questionário foi reenviado, por correio eletrônico ou por meio do sistema de mensagens do LinkedIn.

O processo de seleção da amostra resultou em 11 respostas válidas dos CROS. Em virtude da amostra ser pouco representativa, optou-se por enviar também para auditores e consultores de gestão de riscos. Para tanto, efetuou-se uma busca no *site* do Instituto dos Auditores Independentes do Brasil (IBRACON) o que permitiu identificar 132 empresas associadas que foram contatadas por e-mail, telefone ou pelo fale conosco da empresa. Observa-se que das 132 empresas, não foi possível o contato com 36, por falta de informações suficientes. Por fim, realizou-se também busca no portal Google com as palavras-chave: “consultoria” e “gestão de riscos”. Esta busca retornou mais 11 empresas de consultoria, que também foram contatadas por telefone e correio eletrônico. Ao final do processo de

coleta obtiveram-se 22 respostas válidas, sendo 15 respondentes do sexo masculino e 72,7% da amostra com idade entre 21 e 40 anos.

Para a coleta dos dados, utilizou-se um questionário estruturado em quatro blocos, elaborado com base no estudo de Fraser, Schoening-Thiessen e Simkins (2008), que objetivou determinar quão útil os executivos de risco consideravam a literatura publicada sobre gestão de riscos. O primeiro bloco destinou-se a identificar o perfil dos respondentes e compreendeu questões que indagavam sobre gênero, idade, tempo de atuação na área de gestão de riscos, designação do cargo atualmente ocupado, tempo no cargo atual e capacitações realizadas para o desempenho da atual função. O segundo bloco do instrumento de coleta de dados objetivou identificar o perfil das organizações participantes da pesquisa. Para tanto, compreendeu questões acerca do setor de atuação, porte da empresa, tempo de adoção do sistema de Gestão de Riscos Corporativos, motivos que levaram à implementação da GRC e número de funcionários envolvidos com gestão de riscos na organização.

Quanto ao terceiro bloco de perguntas, destinou-se a identificar quais as ferramentas e técnicas que os respondentes utilizam na Gestão de Riscos Corporativos. Neste bloco, foram apresentadas as ferramentas elencadas no COSO (2007) para o processo de identificação e avaliação de riscos. Os participantes foram solicitados a responder, por meio de uma escala *Likert*, o nível de utilização de cada uma das ferramentas e técnicas apresentadas. Também indagou-se sobre a utilização de consultoria externa para assuntos relacionados à GRC e quais os benefícios oriundos desta prática. Por fim, o último bloco do questionário dedicou-se a identificar os instrumentos de capacitação utilizados pelos respondentes e o nível de importância atribuído pelos CROS a cada instrumento. Para a elaboração deste bloco de perguntas realizou-se, primeiramente, uma busca bibliográfica por obras (livros e normas) e cursos divulgados na internet que tratassem de Gestão de Riscos Corporativos. Efetuou-se pré-teste com um pesquisador e um consultor da área de gestão de riscos, resultando na reformulação do quarto bloco do questionário. Deste modo, após a revisão, chegou-se a um total

de 16 obras e 6 cursos que compuseram as perguntas do quarto bloco, apresentadas no Quadro 1.

Em função da impossibilidade de contemplarem-se todas as obras que versam sobre gestão de riscos no instrumento de coleta de dados, optou-se por abordar apenas as obras mais referenciadas. No entanto, ao final do quarto bloco, uma pergunta aberta permitiu que os respondentes incluíssem

outras obras ou cursos não elencados no questionário que julgassem importantes para a capacitação em Gestão de Riscos Corporativos.

Antes de levar o instrumento a campo foi aplicado um segundo pré-teste. Participaram outras duas pessoas que trabalham e pesquisam sobre gestão de riscos, sendo que nenhuma das duas faz parte da amostra final do estudo. Depois de validado,

**Quadro 1.** Obras e cursos contemplados na pesquisa

Obra	Autor/Ano
Norma de Gestão de Riscos - FERMA	FERMA (2002)
Medindo e Gerenciando Riscos Operacionais em Instituições Financeiras	Christopher Lee Marshall (2002)
Controladoria: De Risco-Retorno em Instituições Financeiras	Osias Brito (2003)
Gerenciamento de Riscos Corporativos - Estrutura Integrada ( <i>Enterprise Risk Management - Integrated Framework</i> )	COSO (2004)
Gerenciamento de risco: abordagem conceitual e prática: uma visão integrada dos riscos de crédito, operacional e de mercado.	Michel Crouhy, Dan Galai e Robert Mark (2004)
Guia de Orientação para Gerenciamento de Riscos Corporativos	IBGC (2007)
Gestão de Risco: uma abordagem orientada a riscos operacionais	Osias Brito (2007)
The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage	Yossi Sheffi (2007)
The Black Swan: The Impact of the Highly Improbable	Nassim Nicholas Taleb (2007)
Risk Management and calculative cultures	Anette Mikes (2009)
Gestão estratégica do risco	Aswath Damodaran (2009)
NBR ISO 31000 - Gestão de Riscos: Princípios e Diretrizes	ISO (2009)
<i>Basel III: A global regulatory framework for more resilient banks and banking systems</i> (Basiléia III)	BCBS (2010)
Managing the Multiple Dimensions of Risk	Robert S. Kaplan e Anette Mikes (2011)
From counting risk to making risk count: Boundary-work in risk management	Anette Mikes (2011)
Managing Risks: A New Framework	Robert S. Kaplan e Anette Mikes (2012)
Curso	Instituição
Gestão de Riscos ( <i>Enterprise Risk Management: An Introduction</i> )	Instituto dos Auditores Internos do Brasil
Introdução ao Gerenciamento de Riscos Corporativos	IAudit Consultoria Empresarial
Gestão de Riscos Corporativos	Trevisan Escola de Negócios
Gestão de Riscos e Compliance (MBA)	FECAP
Compliance e Gerenciamento de Riscos	FIPECAFI
Auditoria Interna e Controle de Riscos	FIPECAFI

Fonte: Elaborado pelos autores.



o instrumento foi digitado no site do *Google Forms* e enviado conforme exposto anteriormente. A coleta dos dados ocorreu entre setembro de 2015 e fevereiro de 2016. Após a obtenção das respostas, os dados foram tabulados em planilha eletrônica. A análise ocorreu mediante estatística descritiva e Análise de Componentes Principais (ACP).

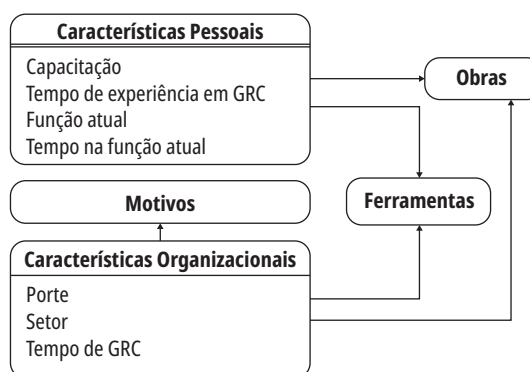
A ACP “é uma técnica de análise exploratória multivariada que transforma um conjunto de variáveis correlacionadas num conjunto menor de variáveis independentes, combinações lineares das variáveis originais, designadas por ‘componentes principais’” (Maroco, 2003, p. 231). De acordo com Banet e Morineau (1999) as variáveis da ACP podem ser representadas por vetores em um plano fatorial, sendo que o ângulo formado pelas variáveis revela a correlação existente entre elas. Deste modo, ângulos próximos a 0° denotam forte correlação positiva, ângulos próximos a 180° indicam forte correlação negativa e ângulos próximos a 90° sugerem a ausência de correlação (Banet & Morineau, 1999).

Destarte, procederam-se a ACP a fim de identificar a correlação entre as características pessoais dos respondentes e das empresas e os motivos, ferramentas e obras identificadas na pesquisa. A Figura 1 ilustra as relações a serem testadas.

Estudos anteriores evidenciam que características pessoais do CRO possuem forte influência sobre o nível de adoção da Gestão de

Riscos Corporativos (Daud *et al.*, 2010). Assim, são analisadas as correlações entre as características pessoais (capacitação, tempo de experiência em GRC, função atualmente exercida e tempo na função atual) com as ferramentas utilizadas pelos respondentes e com as obras lidas.

Do mesmo modo, características da empresa, tal como seu tamanho, também se encontram associadas à GRC (Baxter, Bedard, Hoitash & Yezegel, 2013). Logo, também foram testadas as relações entre as características organizacionais (porte da empresa, setor de atuação e tempo que realiza GRC) com as ferramentas utilizadas e os motivos que levaram à adoção da GRC e as obras lidas. A seguir descrevem-se os resultados encontrados.



**Figura 1.** Relações a serem testadas

Fonte: Elaborado pelos autores.

**Tabela 1.** Características profissionais dos respondentes

Capacitação	Código	N	%	Função atual	Código	N	%
Sim	CSIM	8	36,36%	Chief Risk Officer	CROS	11	50,00%
Não	CNAO	14	63,64%	Auditor	CRON	3	13,64%
				Gerente de Riscos	CRON	3	13,64%
				Outros	CRON	5	22,73%
Total		22	100%	Total		22	100%
Experiência em Gestão de Riscos	Código	N	%	Tempo na função atual	Código	N	%
Menos de 1 ano	GM1	4	18,18%	Menos de 1 ano	FM1	7	31,82%
De 1 a 5 anos	G1A5	7	31,82%	De 1 a 5 anos	F1A5	6	27,27%
De 5 a 10 anos	G5A10	0	0,00%	De 5 a 10 anos	F5A10	2	9,09%
De 10 a 15 anos	G10A15	4	18,18%	De 10 a 15 anos	F10A15	5	22,73%
Acima de 15 anos	GM15	7	31,82%	Acima de 15 anos	FM15	2	9,09%
Total		22	100%	Total		22	100%

Fonte: Dados da pesquisa.

## Análise Dos Dados

O perfil dos participantes da pesquisa foi identificado por meio das questões do primeiro bloco do questionário. Na Tabela 1 encontram-se sintetizadas algumas informações acerca dos respondentes, tais como função atual, tempo na função e experiência em GRC.

Observa-se em relação ao tempo de atuação na área de gestão de riscos que 50% dos respondentes possuem pouco tempo de atuação (entre menos de 1 ano até 5 anos), e que os 50% restantes apresentam mais de 10 anos de experiência na área. No que tange à função atual desempenhada, verificou-se que 11 pessoas (50%) desempenham a função de *Chief Risk Officer* (CRO), também identificou-se as funções de auditor (13,64%) e gerente de riscos (13,64%). Em relação ao tempo em que o respondente ocupa a atual função, pôde-se perceber que, assim como no tempo de experiência, houve maior concentração de respostas nas faixas iniciais, o que denota pouco tempo de experiência no cargo, o que talvez, como aponta Nocco e Stulz (2006), possa ser explicado pela contemporaneidade da gestão de risco como uma ferramenta de controle gerencial.

Buscou-se investigar também se para desempenhar a função atual o respondente teria realizado alguma capacitação específica. Como nota-se na

Tabela 1 apenas 8 respondentes afirmaram que sim, ou seja, realizaram cursos específicos para o cargo que ocupam. Entre os cursos citados pelos respondentes encontram-se cursos de *Compliance*, Controle Interno, Governança, Gestão de Riscos e *Business Continuity*, bem como certificações em ISO 27001, em *Business Continuity* (CBCP) e em Risco e Controle de Sistemas de Informação (*Certified in Risk and Information Systems Control*) - (CRISC) indicando uma predominância de aquisição de conhecimento de forma tácita.

Quanto ao perfil das empresas em que atuam os respondentes a Tabela 2 descreve algumas características.

Nota-se que a maioria das empresas é do setor de serviços (40,9%), seguidas por empresas do setor financeiro (31,8%) e de indústria e comércio (13,6%). Dentre as atividades contempladas nestes setores encontram-se, por exemplo, empresas do ramo automobilístico, de imóveis, seguros, consultorias e auditorias. Em relação ao porte, houve maior concentração de empresas de grande porte (31,8%), entretanto também se identificaram respondentes provenientes de microempresas (22,7%). Destaca-se que, tanto as microempresas quanto as pequenas empresas identificadas na amostra correspondem às empresas de auditoria e consultoria em gestão de riscos.

**Tabela 2.** Perfil das empresas

Setor	Código	N	%	Pessoas envolvidas com GRC		N	%
Serviços	SERV	9	40,9%	Até 10 pessoas		17	77,3%
Financeiro	FIN	7	31,8%	De 11 a 20 pessoas		2	9,1%
Indústria	IND	3	13,6%	De 21 a 30 pessoas		2	9,1%
Comércio	COM	3	13,6%	Acima de 30 pessoas		1	4,6%
Total		22	100%	Total		22	100%
Porte da empresa	Código	N	%	Tempo de adoção da GRC	Código	N	%
Microempresa	MICRO	5	22,7%	Menos de 1 ano	EM1	4	18,2%
Pequena empresa	PEQ	3	13,6%	De 1 a 5 anos	E1A5	4	18,2%
Média empresa	MED	3	13,6%	De 5 a 10 anos	E5A10	6	27,3%
Média-grande empresa	MDG	4	18,2%	De 10 a 15 anos	E10A15	3	13,6%
Grande empresa	GRAN	7	31,8%	Acima de 15 anos	EM15	5	22,7%
Total		22	100%	Total		22	100%

Fonte: Dados da pesquisa.

Pode-se verificar também que o número de pessoas envolvidas com gestão de riscos nas empresas participantes da pesquisa não é tão elevado, uma vez que em apenas cinco empresas há mais de 10 pessoas envolvidas com GRC. Tal resultado é consistente com a pesquisa realizada pela Deloitte (2014), que demonstrou que a média de profissionais que atuam na gestão de riscos é de nove funcionários por empresa. No que diz respeito ao tempo de adoção formal de um sistema de GRC, percebe-se uma maior distribuição das respostas, sendo que o destaque vai para a faixa de 5 a 10 anos (27,3%).

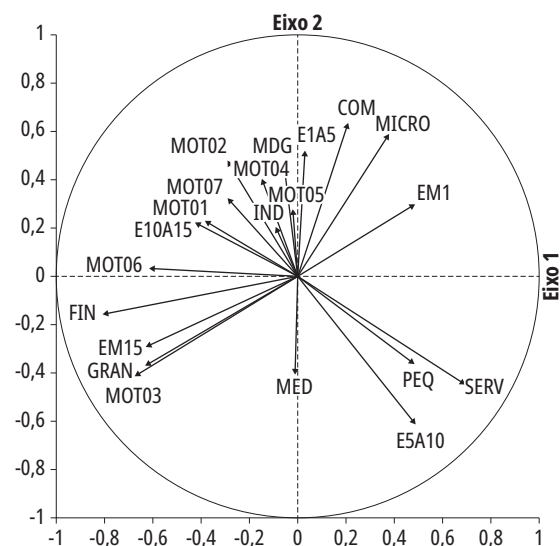
Indagou-se quais os motivos que levaram sua organização a adotar práticas de gestão de riscos. Foram apresentados sete motivos, sendo que o respondente poderia assinalar mais de uma opção, tendo a alternativa de indicar algum motivo adicional não contemplado no instrumento. Os resultados encontram-se na Tabela 3.

A exigência de entidades reguladoras foi o motivo com maior taxa de resposta para justificar a adoção da GRC, o resultado converge com o estudo de Collier *et al.* (2007) que verificaram que exigências regulatórias são motivadoras para práticas de gestão de riscos e com os resultados de Paape e Speklé (2012) que evidenciaram que o grau de implementação da GRC é influenciado pelo ambiente regulatório.

Além da exigência regulatória, os motivos mais recorrentes para a adoção da GRC são: melhorar a compreensão e o controle dos riscos (54,44%), melhorar a governança corporativa ou atender requisitos do conselho (40,91%) e minimizar surpresas (40,91%). Tais resultados estão em consonância

com os resultados de Fraser *et al.* (2008), em que melhorar a compreensão e o controle dos riscos e melhorar a governança corporativa ou atender requisitos do conselho foram os dois motivos mais citados para a implantação do processo de gestão de riscos nas empresas investigadas pelos autores.

Estes resultados também concordam com os achados de Collier *et al.* (2007), em que a gestão de riscos foi impulsionada por uma resposta institucional aos apelos para melhorar a governança corporativa. Entretanto, em relação aos achados de Paape e Speklé (2012) não houve concordância, visto que os autores concluíram que a governança parece não influenciar a adoção da GRC.



**Figura 2.** Mapa fatorial entre os motivos para a adoção da GRC e características organizacionais

Fonte: Dados da pesquisa.

**Tabela 3.** Motivos que levaram as empresas a adotar a GRC

Motivos	Código	Quantidade	%
Exigência de entidades reguladoras	MOT01	14	63,6%
Melhorar a compreensão e o controle dos riscos	MOT02	12	54,6%
Melhorar a Governança Corporativa ou atender requisitos do Conselho	MOT03	9	40,9%
Minimizar surpresas	MOT04	9	40,9%
Auxiliar na alocação de recursos	MOT05	8	36,4%
Atender diretrizes estabelecidas no Planejamento Estratégico	MOT06	6	27,3%
Emissão de ADR's	MOT07	2	9,1%

Fonte: Dados da pesquisa.

Com o intuito de tentar identificar características organizacionais que possam estar associadas aos motivos relatados pelas empresas para a adoção da GRC, apresenta-se na Figura 2 o mapa fatorial gerado pela Análise de Componentes Principais.

Percebe-se que a adoção da GRC em função de exigências de entidades reguladoras (MOT01) mostrou-se positivamente associada a empresas do setor industrial (IND) e financeiro (FIN), de grande porte (GRAN) e que adotam a GRC entre 10 e 15 anos (E10A15). Salienta-se que tal motivo apresentou ausência de correlação com microempresas (MICRO), empresas do setor comercial (COM) e que adotaram a GRC há menos de um ano (EM1); e correlação negativa com empresas do setor de serviços (SERV) e de pequeno porte (PEQ).

Em relação à adoção da GRC para melhorar a compreensão e o controle dos riscos (MOT02), observa-se que este motivo está positivamente relacionado com empresas do setor industrial (IND) e comercial (COM), porém sem correlação com empresas do setor financeiro (FIN). Estes resultados ensejam uma reflexão acerca das motivações subjacentes à adoção da Gestão de Riscos Corporativos. Como observou-se anteriormente, a exigência por parte de entidades reguladoras exerce um papel fundamental na opção das empresas pela implantação da GRC.

Assim sendo, há que se refletir então se o processo de gestão de riscos presente em tais empresas é de fato utilizado como suporte à gestão e a tomada de decisões ou se apenas cumpre requisitos regulatórios com características meramente figurativas. O resultado apresentado pela ACP aponta que a exigência imposta por entidades reguladoras está mais associada às empresas do setor financeiro do que a motivação para melhorar a compreensão e o controle dos riscos, fornecendo indícios de que nestas organizações a GRC seja apenas uma formalidade.

Estes resultados são reforçados ao constatar-se que o terceiro motivo (melhorar a Governança Corporativa ou atender requisitos do Conselho – MOT03) mostrou-se associado positivamente às empresas do setor financeiro (FIN), ou seja, além de pressões externas do ambiente regulatório, também pressões internas advindas do Conselho de

Administração parecem explicar melhor a adoção da GRC em empresas deste setor, ao invés de motivos ligados à utilização da Gestão de Riscos para auxílio da gestão e tomada de decisão.

Somado a este fato, verifica-se ainda que não houve associação entre a adoção da GRC para minimizar surpresas (MOT04) ou auxiliar na alocação de recursos (MOT05) e as empresas do setor financeiro (FIN), ao passo que o atendimento de diretrizes estabelecidas no Planejamento Estratégico (MOT06) mostrou-se forte e positivamente correlacionado, acentuando a constatação de que a GRC, nas empresas financeiras investigadas, constitui-se em elemento para atender exigências (externas ou internas) e não para a gestão.

Relativamente à adoção da GRC em função de atender requisitos do Conselho ou melhorar a Governança Corporativa (MOT03), evidenciou-se que esta não se encontra associada às empresas de nenhum setor, além do financeiro (FIN), apresentando também correlação positiva com empresas de grande porte (GRAN) e com processo formal de gestão de riscos estabelecido há mais de 15 anos (EM15).

Em relação ao quarto e quinto motivos observados, qual seja minimizar surpresas (MOT04) e auxiliar na alocação de recursos (MOT05), observou-se correlação positiva com as variáveis IND e COM, indicando assim que empresas industriais e comerciais adotam a GRC pelos motivos supramencionados. Tais motivos também estão positivamente associados com a variável E1A5, que denota adoção da GRC entre um e cinco anos.

O sexto motivo, atender diretrizes estabelecidas no Planejamento Estratégico (MOT06), não está associado a nenhuma variável de setor além do financeiro (FIN) e apresenta correlação positiva fraca com empresas de grande porte (GRAN). Finalmente, no que concerne à adoção da GRC em função da emissão de ADR's observa-se que esta mostrou-se positivamente associada com as variáveis que indicam o setor industrial (IND) e financeiro (FIN), com porte médio-grande (MDG) e com GRC estabelecida entre 10 e 15 anos (E10A15). No entanto, mostrou-se negativamente associada a empresas do setor de serviços (SERV) e de pequeno porte (PEQ), fato que era esperado.

## Ferramentas utilizadas na gestão de riscos

O terceiro bloco do questionário buscou identificar quais as ferramentas utilizadas pelos respondentes na gestão de riscos. Para tanto, foram elencadas as técnicas listadas pelo COSO (2007) para identificação e avaliação de riscos e solicitado que os respondentes indicassem o grau de utilização de cada técnica. A seguir, na Tabela 4, encontram-se sintetizadas as respostas obtidas.

Observa-se que as médias obtidas das respostas sobre a utilização das técnicas listadas pelo COSO (2007) são moderadamente baixas, uma vez que ficaram muito próximas a 2, que na escala utilizada correspondia a “utilizo raramente”. Tal resultado converge ao que foi constatado por Fraser *et al.* (2008), que identificaram que as técnicas e ferramentas propostas pelo COSO são utilizadas raramente pela maioria dos respondentes da pesquisa e estão alinhadas com a indicação, pelos respondentes, de que a gestão de risco tende a ser um mecanismo *proforma* para atender à regulação externa ou diretrizes do conselho de administração, sem, no entanto, ter suas potencialidades efetivamente utilizadas para o processo de gestão organizacional.

Em relação às técnicas para a identificação dos riscos, a técnica de análise do fluxo de processo é a mais utilizada, com a única média que chegou a casa de 3 pontos (utilizo algumas vezes), seguida por indicadores de evento e alerta de mudança (2,5), questionários e pesquisas (2,3) e rastreamento de dados (2,3). Já para a avaliação dos riscos as técnicas que se destacaram foram: categorização de riscos (média de 2,8), análise de cenários (2,7) e valor em risco (2,6). Pode-se perceber que as técnicas mais utilizadas são também as mais simples, ao passo que técnicas mais complexas, tais como árvore de eventos, teste de estresse e distribuição de perda apresentaram baixa utilização. Este achado é consonante com os resultados do estudo de Collier *et al.* (2007), em que os entrevistados afirmaram que manter técnicas de gestão de risco mais simples era melhor.

Deve-se, entretanto, analisar os dados de forma cautelosa, visto que os desvios-padrão

calculados apresentaram-se elevados em virtude da grande variabilidade de respostas, conforme pode-se observar na Tabela 4. Assim, destaca-se, por exemplo, que dentre as técnicas para identificação dos riscos a análise do fluxo do processo e questionários e pesquisas foram as que apresentaram maior concentração de respostas nos itens 4 e 5, ao passo que a técnica de seminário com facilitadores, apesar de não possuir a menor média, apresentou maior concentração de respostas no item “não conheço”.

Além das técnicas acima apresentadas, indagou-se se o respondente utiliza outras técnicas na gestão de riscos. Entre as técnicas citadas encontram-se: análise de impacto no negócio (*Business Impact Analysis* – BIA), Matriz de SWOT e ferramentas do *Control Objectives for Information and related Technology* (COBIT).

Quanto à contratação de consultoria externa para tratar de assuntos relacionados à gestão de riscos, constatou-se que apenas 31,8% das empresas utilizam consultores externos para tratar de tais assuntos. Em relação aos benefícios que um consultor externo pode trazer à GRC, as respostas mais recorrentes foram: trazer profissionais com experiência externa, compartilhar diferentes opiniões e pontos de vista, trazer técnicas atualizadas e redução de custos fixos.

A fim de identificar que características organizacionais e pessoais podem estar associadas às técnicas de gestão de riscos empregadas procedeu-se à ACP, com posterior construção do mapa fatorial. Para tanto, cada ferramenta foi transformada em uma variável binária, que assumiu o valor de 1 nos casos em que a resposta dada correspondia à *utilizo em grande extensão* (4) e *utilizo o máximo possível* (5), indicando utilização da ferramenta em questão. Para as demais respostas (0 - *não conheço*; 1 - *conheço, porém não utilizo*; 2 - *utilizo raramente*; e 3 - *utilizo algumas vezes*) a variável foi codificada como 0, indicando não utilização da técnica pela empresa. Na Figura 3, apresentam-se os mapas fatoriais elaborados para as características organizacionais e as ferramentas de gestão de riscos identificadas.

O mapa fatorial A apresenta o resultado da ACP para as ferramentas de identificação de riscos e as



**Tabela 4.** Utilização das técnicas do coso (2007) na Gestão de Riscos Corporativos

<b>Técnicas para Identificação de Riscos</b>	<b>Código</b>	<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>Total</b>	<b>Média</b>	<b>DP</b>
Análise do Fluxo de Processo	FI01	3	2	0	6	8	3	22	3,0	1,6
Indicadores de Evento e Alerta de Mudança	FI02	2	4	5	6	3	2	22	2,5	1,4
Questionários e Pesquisas	FI03	3	5	4	3	6	1	22	2,3	1,6
Rastreamento de Dados de Eventos de Perdas	FI04	4	3	4	6	4	1	22	2,3	1,5
Inventário de Eventos	FI05	4	3	4	7	3	1	22	2,2	1,5
Entrevistas	FI06	4	5	3	5	4	1	22	2,1	1,6
Seminários com Facilitadores	FI07	5	6	3	7	1	0	22	1,7	1,3
Diagrama Espinha-de-Peixe/Árvore de Eventos	FI08	4	7	4	6	1	0	22	1,7	1,2
<b>Técnicas para Avaliação de Riscos</b>	<b>Código</b>	<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>Total</b>	<b>Média</b>	<b>DP</b>
Categorização de Riscos	FA01	4	3	0	5	6	4	22	2,8	1,8
Análise de Cenário	FA02	3	5	1	3	7	3	22	2,7	1,8
Valor em Risco	FA03	4	2	2	7	5	2	22	2,6	1,6
Questionários	FA04	4	4	0	5	9	0	22	2,5	1,6
Benchmarking	FA05	3	4	2	7	4	2	22	2,5	1,6
Matriz de Riscos	FA06	4	4	2	5	5	2	22	2,4	1,7
Análise de Sensibilidade	FA07	3	4	5	4	4	2	22	2,4	1,6
Teste de Estresse	FA08	3	4	6	4	4	1	22	2,2	1,4
Distribuição de Perda	FA09	5	3	5	5	3	1	22	2,0	1,5
Back-testing	FA10	6	5	2	3	6	0	22	1,9	1,6
Mapa de Calor	FA11	4	6	5	5	1	1	22	1,8	1,4

Legenda: 0 - Não conheço; 1 - Conheço, porém não utilizo; 2 - Utilizo raramente; 3 - Utilizo algumas vezes; 4 - Utilizo em grande extensão; 5 - Utilizo o máximo possível.

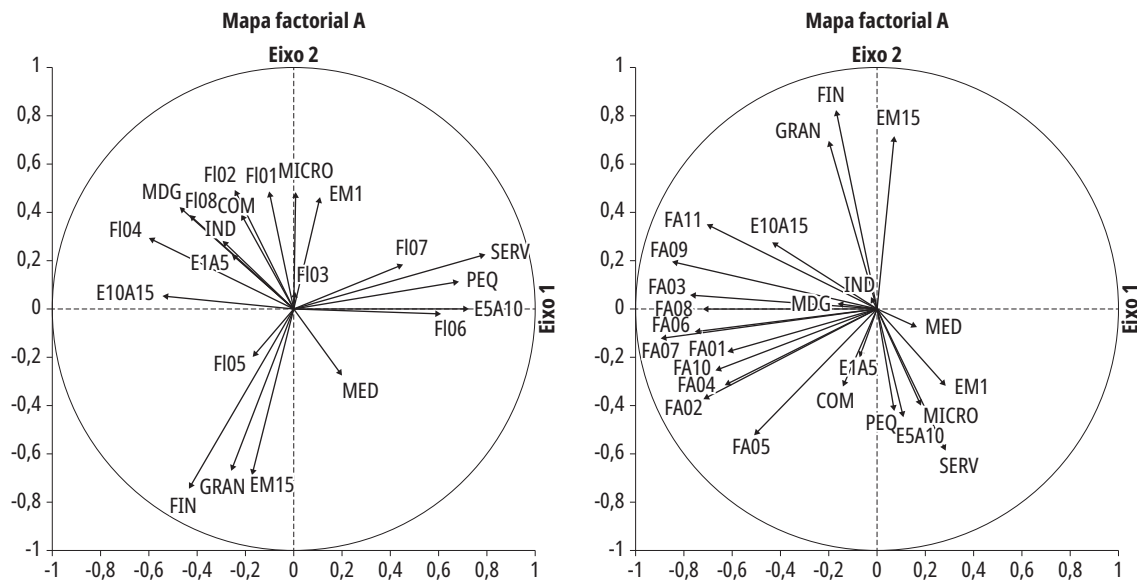
Fonte: Dados da pesquisa.

características organizacionais, enquanto o B apresenta as ferramentas de avaliação de riscos e as características da empresa. Em relação às ferramentas de identificação de riscos observa-se que empresas do setor financeiro (FIN), de grande porte (GRAN), com gestão de riscos implementada há mais de 15 anos (EM15) apresentaram associação positiva com a ferramenta de inventário de eventos (FI05) e correlação negativa com questionários e pesquisas (FI03). A ferramenta árvore de eventos (FI08) mostrou-se positivamente associada às empresas industriais (IND), de médio-grande porte (MDG), com GRC implementada entre 1 e 5 anos (E1A5). Empresas comerciais (COM) mostraram-se positivamente associadas com indicadores de evento e alerta de

mudança (FI02), enquanto empresas de prestação de serviços (SERV) mostraram maior correlação com questionários e pesquisas (FI03), entrevistas (FI06) e seminários com facilitadores (FI07). Tais ferramentas também apresentaram associação positiva com empresas de pequeno porte (PEQ) e com GRC implantado entre 5 e 10 anos (E5A10).

Relativamente às ferramentas de avaliação de riscos observa-se que empresas do comércio (COM), com GRC entre 1 e 5 anos (E1A5) apresentam-se associadas positivamente às ferramentas: categorização de riscos (FA01), análise de cenários (FA02), questionários (FA04), *benchmarking* (FA05) e *back testing* (FA10). A variável IND, que representa as empresas do setor industrial mostrou-se





**Figura 3.** Mapa fatorial para as ferramentas da GRC e características organizacionais

Fonte: Dados da pesquisa.

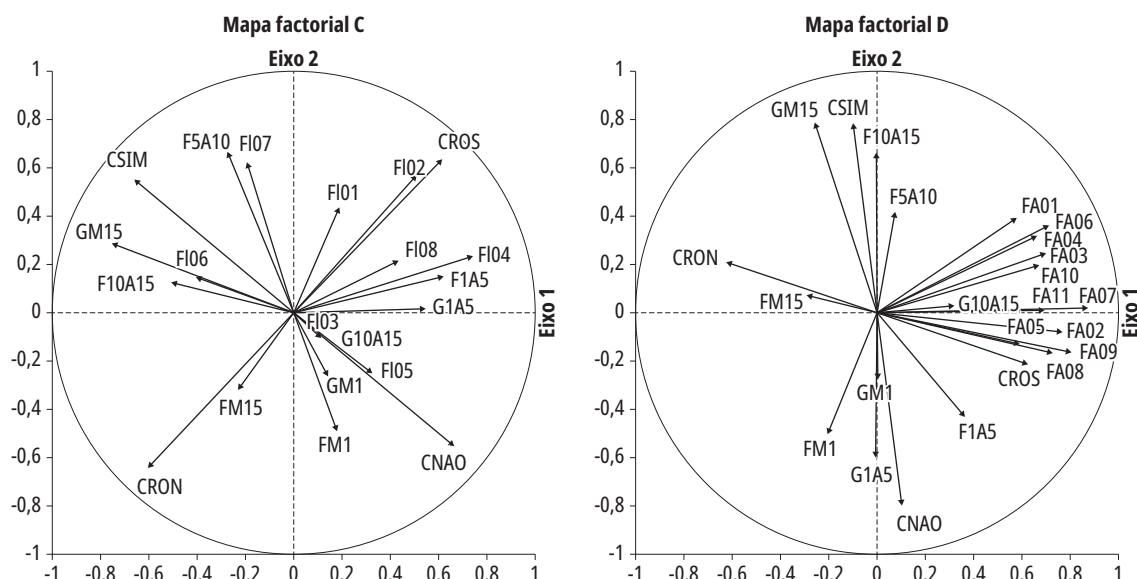
correlacionada positivamente com as ferramentas de distribuição de perdas (FA09) e mapa de calor (FA11). No entanto, estas técnicas revelaram associação negativa com empresas prestadoras de serviço (SERV), sendo que esta variável também apresentou ausência de correlação com as ferramentas análise de cenários (FA02) e questionários (FA04). De modo geral, empresas de maior porte (MDG e GRAN) parecem estar mais associadas a ferramentas mais sofisticadas, como por exemplo, valor em risco (FA03), teste de estresse (FA08) e distribuição de perdas (FA09).

Além das características organizacionais, também buscou-se analisar a associação entre as ferramentas de gestão de riscos e as características dos indivíduos. Na Figura 4 apresentam-se os mapas fatoriais elaborados a partir da ACP.

O mapa fatorial C apresenta a associação entre as características pessoais e as técnicas de identificação de riscos. Observa-se que, em relação à capacitação os respondentes que realizaram algum tipo de treinamento para desempenhar sua atual função (CSIM) apresentaram maior associação com as ferramentas entrevistas (FI06) e seminários com facilitadores (FI07). Estas técnicas também estão associadas às pessoas que desempenham sua função entre 5 e 15 anos (F5A10 e F10A15). Para os

que declararam não receber capacitação para o desempenho de sua função (CNAO), observa-se maior associação positiva com questionários e pesquisas (FI03) e inventário de eventos (FI05). Em relação à função exercida, constata-se que às pessoas que ocupam o cargo de CRO (CROS) apresentam associação positiva com as ferramentas análise do fluxo de processo (FI01), indicadores de evento e alerta de mudança (FI02) e árvore de eventos (FI08), ao passo que os que desempenham outras funções (CRON) não apresentaram associação positiva com nenhuma das técnicas de identificação de riscos analisadas.

Com relação às ferramentas de avaliação de riscos (mapa fatorial D) verifica-se que a capacitação para exercer a função (CSIM) não apresentou associação positiva com nenhuma ferramenta. No que concerne ao cargo desempenhado, pode-se observar que o cargo de CRO (CROS) mostrou-se forte e positivamente associado às ferramentas de análise de cenário (FA02), *benchmarking* (FA05), análise de sensibilidade (FA07), teste de estresse (FA08), distribuição de perda (FA09) e mapa de calor (FA11). Este resultado fornece indícios de que o CRO domina práticas de GRC, visto que os demais cargos (CRON) não apresentaram correlação positiva com nenhuma ferramenta. Destaca-se ainda



**Figura 4.** Mapa fatorial para as Ferramentas da GRC e características pessoais

Fonte: Dados da pesquisa.

que, a experiência em GRC pode exercer papel fundamental nas práticas de gestão de riscos empregadas pela empresa, uma vez que a experiência entre 10 e 15 anos (G10A15) mostrou-se positivamente correlacionada com todas as técnicas de gestão de riscos, o que é consistente com a existência de conhecimento tácito.

## Obras e cursos mais relevantes em gestão de riscos

Por fim, o último bloco do questionário destinou-se a identificar as obras e cursos considerados pelos respondentes como relevantes para a aquisição de conhecimento sobre gestão de riscos. Primeiramente, analisaram-se as obras sobre gestão de riscos indicadas como as mais lidas, para na sequência avaliar as obras consideradas pelos respondentes como de maior relevância. A Tabela 5 sumariza os resultados relacionados às obras mais lidas. Os dados estão distribuídos em uma escala de 1 a 5, em que 1 indica desconhecimento da obra e 5 denota que o respondente leu mais de 80% de seu conteúdo.

O *framework* Gerenciamento de Riscos Corporativos – Estrutura Integrada elaborada pelo COSO (2004), o Guia de Orientação para Gerenciamento de Riscos Corporativos (IBGC, 2009), a NBR ISO

31000 (ISO, 2009) e o livro *Gestão de Risco: uma abordagem orientada a riscos operacionais* (Britto, 2007) foram as obras com maior indicação de leitura, visto que apresentaram as maiores médias. Em contrapartida obras internacionais acadêmicas, tais como os artigos de Mikes (2009), Kaplan e Mikes (2011) e Mikes (2011) acabaram tendo as médias mais baixas, o que indica pouca leitura dessas obras pelos respondentes.

Salienta-se, entretanto, que a média geral de leitura de todas as obras apresentou-se baixa, oscilando entre 2,1 e 3,3 informação que sinaliza baixa utilização das obras sugeridas para fins de aprendizagem. Contudo, deve-se destacar também a grande variabilidade das respostas, o que contribui para o decréscimo das médias. Nesse sentido, pode-se notar que o Gerenciamento de Riscos Corporativos (COSO, 2004) apresentou grande concentração de respostas no item 4, ou seja, li entre 10% e 80%. Analisando-se ainda a obra do COSO (2004), pode-se perceber que o número de respondentes que leu mais de 10% da obra (13 no total) é maior do que o número de respondentes que leu menos (9 no total), porém, mesmo assim sua média não chegou a 4. Constata-se ainda a grande dispersão dos dados por meio dos desvios-padrão calculados, que oscilaram de 1,2 a 1,7.

Em relação à importância atribuída às obras sobre gestão de riscos, os resultados são sintetizados na Tabela 6. Os dados estão distribuídos em uma escala de 1 a 5, em que 1 indica que a obra não é relevante para GRC e 5 que indica que a obra é de leitura obrigatória para GRC. As obras sobre gestão de riscos são apresentadas em ordem decrescente de média. Ressalta-se que, para a construção da Tabela 6 e das médias nela apresentadas, foram levadas em consideração apenas as respostas provenientes de pessoas que possuíam conhecimento sobre a obra em questão, ou seja, aqueles que responderam “li entre 10% e 80%” e “li mais que 80%” na questão anterior.

Pode-se observar que a obra que os respondentes consideram agregar maior valor para a gestão de riscos é *Basel III: A global regulatory framework for more resilient banks and banking systems* (BCBS, 2010), seguida pela NBR ISO 31000 - Gestão de Riscos: Princípios e Diretrizes (ISO, 2009) e pelo livro *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage* (Sheffi, 2007). Destaca-se que a Estrutura Integrada do COSO (2004), apesar de ser a mais lida, aparece apenas em décimo primeiro lugar dentre as obras consideradas mais valiosas para gestão de riscos, com uma média de 3,4. Este resultado converge ao fato de que poucas empresas adotam as técnicas e ferramentas

**Tabela 5.** Obras sobre gestão de riscos mais lidas em ordem decrescente de acordo com a média

Obras sobre Gestão de Riscos	Autor/Ano	Código	1	2	3	4	5	Total	Média	DP
Gerenciamento de Riscos Corporativos - Estrutura Integrada	COSO (2004)	001	3	3	3	10	3	22	<b>3,3</b>	1,3
Guia de Orientação para Gerenciamento de Riscos Corporativos	IBGC (2007)	002	5	5	2	7	3	22	<b>2,9</b>	1,4
NBR ISO 31000 - Gestão de Riscos: Princípios e Diretrizes	ISO (2009)	003	7	1	5	7	2	22	<b>2,8</b>	1,4
Gestão de Risco: uma abordagem orientada a riscos operacionais	Brito (2007)	004	5	4	6	6	1	22	<b>2,7</b>	1,2
Gerenciamento de risco: abordagem conceitual e prática	Crouhy, Galai e Mark (2004)	005	5	5	6	5	1	22	<b>2,6</b>	1,2
Controladoria: De Risco-Retorno em Instituições Financeiras	Brito (2003)	006	6	5	6	2	3	22	<b>2,6</b>	1,4
Gestão estratégica do risco	Damodaran (2009)	007	5	6	5	5	1	22	<b>2,6</b>	1,2
Medindo e Gerenciando Riscos Operacionais em Instituições Financeiras	Marshall (2002)	008	4	9	5	2	2	22	<b>2,5</b>	1,2
<i>Basel III: A global regulatory framework for more resilient banks and banking systems</i> (Basiléia III)	BCBS (2010)	009	10	3	1	4	4	22	<b>2,5</b>	1,7
Managing Risks: A New Framework	Kaplan e Mikes (2012)	010	8	3	5	5	1	22	<b>2,5</b>	1,3
Norma de Gestão de Riscos	FERMA (2002)	011	6	7	6	2	1	22	<b>2,3</b>	1,1
The Black Swan: The Impact of the Highly Improbable	Taleb (2007)	012	9	6	2	3	2	22	<b>2,2</b>	1,4
The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage	Sheffi (2007)	013	10	4	4	3	1	22	<b>2,1</b>	1,3
Risk Management and calculative cultures	Mikes (2009)	014	8	6	5	3	0	22	<b>2,1</b>	1,1
Managing the Multiple Dimensions of Risk	Kaplan e Mikes (2011)	015	10	3	5	4	0	22	<b>2,1</b>	1,2
From counting risk to making risk count: Boundary-work in risk management	Mikes (2011)	016	10	5	3	3	1	22	<b>2,1</b>	1,3

Legenda: 1 - Nunca ouvi falar disso; 2 - Ouvi falar, mas não li realmente; 3 - Li menos de 10%; 4 - Li entre 10% e 80%; 5 - Li mais de 80%.

Fonte: Dados da pesquisa.

propostas pelo COSO na gestão dos riscos, conforme discutido anteriormente.

Além das obras citadas, o instrumento de pesquisa contemplou uma pergunta aberta em que os respondentes poderiam incluir demais obras que julgassem importantes para a gestão de riscos. Dentre as obras que foram citadas estão: COBIT 5 (ISACA, 2012), *Risk IT Framework* (ISACA, 2009), *Manager's Guide to Compliance* (Tarantino, 2006) e Gestão de riscos com controles internos (Assi, 2012).

O COBIT 5 foi desenvolvido pela *Information Systems Audit and Control Association* (ISACA) e constitui-se em um quadro abrangente de princípios, práticas, ferramentas analíticas e modelos que auxiliam as empresas em questões relacionadas à governança e gestão de informação e tecnologia, auxiliando a empresa a maximizar valor e minimizar o risco relacionado à informação (ISACA,

2012). A ISACA também foi responsável pelo lançamento, em 2009, do *Risk IT Framework*, como complemento ao COBIT 4.1 (antecessor do COBIT 5). Este documento fornece um quadro geral para o controle e a governança de informações e tecnologias, definindo boas práticas que permitam à empresa identificar e gerir os riscos de tecnologia da informação.

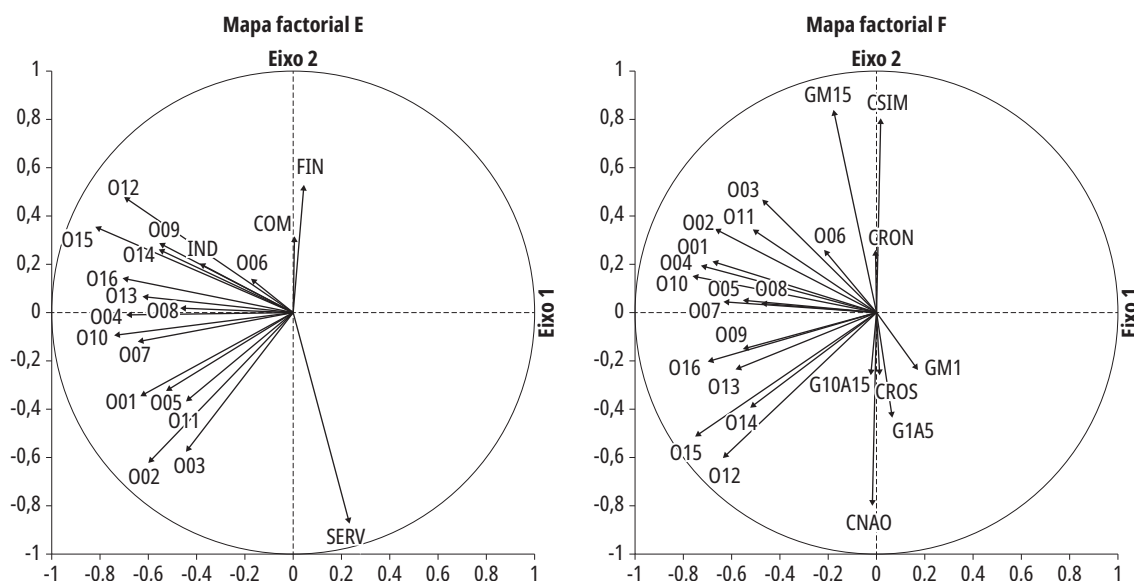
O livro *Manager's Guide to Compliance* de Anthony Tarantino, lançado em 2006, apresenta uma visão geral de diversas normas e regulações mundiais, tais como Lei Sarbanes-Oxley (SOX), COSO, COBIT, Basiléia II e *International Financial Reporting Standards* (IFRS), além de estudos de casos e melhores práticas, com o intuito de auxiliar usuários sobre questões relacionadas à gestão de riscos (Tarantino, 2006).

**Tabela 6.** Obras que possuem maior valor para gestão de riscos em ordem decrescente de acordo com a média

Obras sobre Gestão de Riscos	Autor/Ano	1	2	3	4	5	Total	Média	DP
Basel III: A global regulatory framework for more resilient banks and banking systems	BCBS (2010)	0	0	2	2	4	8	<b>4,3</b>	0,9
NBR ISO 31000 - Gestão de Riscos: Princípios e Diretrizes	ISO (2009)	0	0	2	3	4	9	<b>4,2</b>	0,8
The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage	Sheffi (2007)	0	0	1	2	1	4	<b>4,0</b>	0,8
Controladoria: De Risco-Retorno em Instituições Financeiras	Brito (2003)	0	1	0	3	1	5	<b>3,8</b>	1,1
Medindo e Gerenciando Riscos Operacionais em Instituições Financeiras	Marshall (2002)	0	1	1	0	2	4	<b>3,8</b>	1,5
Norma de Gestão de Riscos - FERMA	FERMA (2002)	0	0	1	2	0	3	<b>3,7</b>	0,6
Gerenciamento de risco: abordagem conceitual e prática: uma visão integrada dos riscos de crédito, operacional e de mercado	Crouhy, Galai e Mark (2004)	0	0	3	2	1	6	<b>3,7</b>	0,8
Gestão estratégica do risco	Damodaran (2009)	0	1	1	3	1	6	<b>3,7</b>	1,0
The Black Swan: The Impact of the Highly Improbable	Taleb (2007)	0	1	1	2	1	5	<b>3,6</b>	1,1
Guia de Orientação para Gerenciamento de Riscos Corporativos	IBGC (2007)	0	1	2	4	2	10	<b>3,4</b>	1,5
Gerenciamento de Riscos Corporativos - Estrutura Integrada ( <i>Enterprise Risk Management – Integrated Framework</i> )	COSO (2004)	1	1	4	6	1	13	<b>3,4</b>	1,0
Risk Management and calculative cultures	Mikes (2009)	0	1	1	1	0	3	<b>3,0</b>	1,0
Managing the Multiple Dimensions of Risk	Kaplan e Mikes (2011)	0	0	1	2	0	4	<b>2,8</b>	1,9
From counting risk to making risk count: Boundary-work in risk management	Mikes (2011)	1	0	2	1	0	4	<b>2,8</b>	1,3
Managing Risks: A New Framework	Kaplan e Mikes (2012)	0	2	1	2	0	6	<b>2,5</b>	1,5
Gestão de Risco: uma abordagem orientada a riscos operacionais	Brito (2007)	1	1	2	2	0	7	<b>2,4</b>	1,5

Legenda: 1 - Não é relevante para GRC; 2 - Algum valor, mas não muito; 3 - Razoavelmente útil; 4 - Muito bom para GRC; 5 - Leitura obrigatória para GRC.

Fonte: dados da pesquisa.



**Figura 5.** Mapa fatorial para as características organizacionais e pessoais e obras lidas

Fonte: dados da pesquisa.

Por fim, a obra *Gestão de Riscos com controles internos* de Marcos Assi foi a única obra nacional a ser citada pelos respondentes. O livro tem por objetivo trazer técnicas e práticas de gestão de riscos e controles internos com base em instruções de órgãos nacionais e internacionais, como por exemplo, o COSO ERM, a SOX e a ISO 31000:2009 (Assi, 2012).

Destaca-se aqui que, ainda em relação às obras sobre gestão de riscos, um dos respondentes enfatizou em sua resposta que se deve “evitar a academia” nas questões concernentes à gestão dos riscos, pois essa encontra-se “fora da realidade”.

Buscou-se identificar também dificuldades que os respondentes eventualmente haviam enfrentado na implantação da GRC e que não haviam encontrado suporte na literatura. Entre as dificuldades mais relatadas, a incorporação da GRC à cultura da empresa foi o que obteve maior destaque, seguida por resistência da alta administração e falta de persistência em manter o sistema implantado.

Finalmente, investigou-se a relação existente entre características organizacionais e pessoais e as obras lidas pelos respondentes. Para tanto, cada obra foi transformada em uma variável binária, que assumiu o valor de 1 nos casos em que a resposta dada correspondia à “li entre 10% e 80%” (4) e “li mais de 80%” (5), indicando assim que o

respondente havia de fato lido substancialmente a obra em questão. Para as demais respostas a variável foi codificada como 0, indicando a não leitura de tal obra pelo respondente. Na Figura 5, apresentam-se os mapas fatoriais gerados a partir da Análise de Componentes Principais.

O mapa fatorial E apresenta as correlações para o setor da empresa e as obras lidas pelos participantes da pesquisa. Pode-se observar que o setor industrial (IND) mostrou-se positivamente correlacionado com diversas obras de gestão de riscos, dentre as quais: *Controladoria: de risco-retorno em instituições financeiras* (O06), *Medindo e gerenciando riscos operacionais em instituições financeiras* (O08), *Basel III: a global regulatory framework for more resilient banks and banking systems* (O09), *The black swan: the impact of the highly improbable* (O12), *The resilient enterprise: overcoming vulnerability for competitive advantage* (O13), *Risk management and calculative cultures* (O14), *Managing the multiple dimensions of risk* (O15) e *From counting risk to making risk count: Boundary-work in risk management* (O16).

O setor financeiro (FIN) e o setor comercial (COM) mostraram-se associados positivamente com as obras *Controladoria: de risco-retorno em instituições financeiras* (O06) e *The black swan:*



*the impact of the highly improbable* (O12). O setor financeiro apresentou relação positiva, embora fraca, com a obra *Basel III: A global regulatory framework for more resilient banks and banking systems* (O09). Tal resultado já era esperado em virtude do conteúdo da obra, que aborda gestão de riscos em instituições financeiras. Por sua vez, o setor de serviços mostrou associação positiva apenas com a NBR ISO 31000 - Gestão de riscos: princípios e diretrizes (O03).

Relativamente às características pessoais dos respondentes verifica-se que a capacitação para o cargo (CSIM) e a função de CRO (CROS) apresentam-se positivamente relacionadas às obras: Controladoria: guia de orientação para gerenciamento de riscos corporativos (O02), NBR ISO 31000 (O03), Controladoria: de risco-retorno em instituições financeiras (O06) e Norma de gestão de riscos FERMA.

(O11). Já a não capacitação (CNAO) e outros cargos (CRON) apresentaram-se associados positivamente à *The black swan: the impact of the highly improbable* (O12), *Risk management and calculative cultures* (O14) e *Managing the multiple dimensions of risk* (O15).

Em relação ao tempo de experiência em GRC constata-se que quanto maior o tempo de experiência maior o número de obras em que se estabelecem correlações positivas. Deste modo, menos de um ano de experiência (GM1) mostrou-se correlacionado negativamente com as obras NBR ISO 31000 - Gestão de riscos: princípios e diretrizes (O03), Controladoria: de risco-retorno em instituições financeiras (O06) e Norma de gestão de riscos

FERMA (O11), ao passo que, experiência de mais de 15 anos em GRC (GM15) mostrou-se positivamente correlacionada às mesmas obras, além da obra Guia de orientação para gerenciamento de riscos corporativos do IBGC (O02).

No que diz respeito aos cursos considerados relevantes para capacitar-se em Gestão de Riscos, os resultados encontram-se sumarizados na Tabela 7. Destaca-se que para o cálculo das médias e dos desvios-padrão levou-se em consideração apenas as respostas compreendidas entre 1 (não relevante para GRC) e 5 (obrigatório para GRC).

O curso considerado mais relevante para Gestão de Riscos é o *Enterprise Risk Management: an introduction* oferecido pelo Instituto de Auditores Internos do Brasil (IIA Brasil). Porém, a média para todos os cursos elencados foram baixas, o que denota que os respondentes atribuem pouca importância a estes cursos. Além dos cursos listados no questionário solicitou-se que o respondente indicasse outros cursos que considerassem relevante para a capacitação em gestão de riscos. Entre os cursos citados figuraram cursos sobre gestão de continuidade de negócios e cursos sobre ISO 31000 (ISO, 2009).

## Conclusão

O objetivo deste artigo foi verificar como a gestão de risco se materializa nas organizações. Para tal, buscou-se conhecer os motivos que levam as empresas a adotarem a GRC; apontar as técnicas utilizadas pelos CROS para identificar e avaliar os riscos; conhecer as estratégias de aprendizagem

**Tabela 7 . Relevância dos cursos sobre gestão de riscos**

Cursos sobre Gestão de Riscos	Instituição	0	1	2	3	4	5	Total	Média	DP
Enterprise Risk Management: An Introduction	IIA Brasil	6	1	6	5	3	1	22	2,8	1,0
Introdução ao Gerenciamento de Riscos Corporativos	Trevisan	7	1	5	7	2	0	22	2,7	0,8
Gestão de Riscos Corporativos	IAudit	7	5	1	4	5	0	22	2,6	1,3
Compliance e Gerenciamento de Riscos	FIPECAFI	7	5	3	2	4	1	22	2,5	1,4
Gestão de Riscos e Compliance (MBA)	FIPECAFI	8	4	3	4	3	0	22	2,4	1,2
Auditoria Interna e Controle de Riscos	FECAP	6	5	3	5	3	0	22	2,4	1,1

Legenda: 0 - Não possuo conhecimento para opinar; 1 - Não é relevante para GRC; 2 - Algum valor, mas não muito; 3 - Razoavelmente útil; 4 - Muito bom para GRC; 5 - Obrigatório para GRC.

Fonte: Dados da pesquisa.



consideradas relevantes pelos *Chief Risk Officers* para desenvolver competências e habilidades sobre gestão de riscos; e relacionar características pessoais e organizacionais com as estratégias de aprendizagem, os motivos de adoção e as técnicas utilizadas para gerenciar os riscos.

No que tange aos motivos que levaram às empresas a adotarem a gestão de riscos, pode-se identificar que o principal motivador é a exigência de entidades reguladoras, o que converge aos achados de Collier *et al.* (2007) e Paape e Speklé (2012).

Por meio da análise dos dados pôde-se perceber que o grau de utilização das ferramentas e técnicas elencadas pelo COSO (2007) para gestão de riscos é baixo, o que converge aos resultados das pesquisas de Fraser *et al.* (2008) e Paape e Speklé (2012). Também identificou-se que técnicas como análise de impacto no negócio (BIA), Matriz de SWOT e ferramentas do COBIT são utilizadas pelos respondentes. Além disso, o resultado desta pesquisa mostra-se consistente com estudos anteriores acerca da associação entre tamanho e o setor de atuação da empresa com práticas de Gestão de Riscos Corporativos (Baxter *et al.*, 2013; Lechner & Gatzert, 2018).

Em relação às estratégias de aprendizagem, investigadas com base em obras e os cursos, constatou-se que a obra mais lida pelos respondentes é a Estrutura Integrada do COSO (2004), sendo que obras acadêmicas internacionais obtiveram as menores médias, o que indica pouco conhecimento dessas obras pelos profissionais brasileiros. Porém ao analisar-se a obra que mais agrega valor para o conhecimento em gestão de riscos, verificou-se que a Estrutura Integrada do COSO (2004) apareceu apenas em décimo primeiro lugar, sendo que a obra considerada como mais relevante foi o *Basel III: a global regulatory framework for more resilient banks and banking systems*. Quanto aos cursos verificou-se que o curso *Enterprise Risk Management: An Introduction* oferecido pelo Instituto de Auditores Internos do Brasil é considerado mais relevante para adquirir conhecimentos sobre gestão de riscos.

O que se constata, no contexto da amostra investigada, é que a gestão de risco está posicionada como um processo periférico e subutilizado,

decorrente de exigências impostas por agentes reguladores ou pelo conselho de administração, o que sugere um uso figurativo, nesse caso, com utilidade limitada, os benefícios da gestão de risco deixam de ser usufruídos e gera desperdício de recursos organizacionais. Constata-se que o conhecimento organizacional sobre a gestão de riscos encontra-se alicerçado no tácito, ou seja, baseado nas habilidades e experiências profissionais que são difíceis de serem explicitadas, formalizadas e transferidas, talvez, a adoção de estratégias para torná-lo explícito contribua para a construção de uma rede de conhecimento na organização e amplie a utilização das ferramentas de gestão de risco para beneficiar a consecução dos objetivos estratégicos.

Em relação às dificuldades enfrentadas pelos respondentes na implantação do GRC que não foram encontradas na literatura, destacou-se a incorporação da gestão de riscos na cultura da empresa. Isso assinala uma lacuna a ser investigada por futuras pesquisas. Destaca-se como limitações do estudo o baixo número de respondentes, o que impede a generalização de resultados. Sugere-se que sejam realizadas novas pesquisas, com outras amostras a fim de validar os resultados aqui encontrados.

## Referências

- Alavi, M., & Leidner, D. E. (2001). Review: knowledge management and knowledge management systems: Conceptual foundations and research issues. En: *MIS quarterly*, 25(1): pp. 107-136.
- Assi, M. (2012). *Gestão de Riscos com Controles Internos*. São Paulo, Brasil: Ed. Saint Paul.
- Banet, T. A., & Morineau, A. (1999). *Aprender de los datos: el análisis de componentes principales*. Barcelona, España: UEB.
- Basel Committee on Banking Supervision – BCBS. (2010). *Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems*. Basel: Bank for International Settlements. Disponível em: <https://www.bis.org/publ/bcbs189.htm>
- 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), pp.1264-1295.

- Berry, A., & Phillips, J. (1998). Enterprise risk management: pulling it together. *Risk Management*, 45(9): pp. 53-58.
- Brito, O. S. (2003). *Controladoria de risco: retorno em instituições financeiras*. São Paulo, Brasil: Saraiva.
- Brito, O. S. (2007). *Gestão de risco: uma abordagem orientada a riscos operacionais*. São Paulo, Brasil: Saraiva.
- Brown, J. S., & Duguid, P. (2001). Knowledge and organization: a social-practice perspective. *Organization Science*, 12(2): pp. 198-213.
- Chait, L. P. (1999). Creating a successful knowledge management system. *Journal of Business Strategy*, 20(2): pp. 23- 26.
- Ching, H. Y., & Colombo, T. M. (2013). Boas práticas de gestão de risco corporativo: estudo de dez empresas. *Revista Brasileira de Estratégia*, 6(1): pp.23-35.
- Cole, R. E. (1998). Introduction: special issue on knowledge and the firm. *Califórnia Management Review*, 40(3): pp. 15-21.
- Collier, P. M., Berry, A. J., & Burke, G. T. (2007). Risk and management accounting: best practice guidelines for enterprise-wide internal control procedures. *CIMA*, 2(11): 1-8.
- Committee of Sponsoring Organizations of the Treadway Commission – COSO. (2004). *Gerenciamento de Riscos Corporativos – Estrutura Integrada: Sumário Executivo*. New York, USA: AICPA.
- Committee of Sponsoring Organizations of the Treadway Commission – COSO. (2007). *Gerenciamento de Riscos Corporativos – Estrutura Integrada: Técnicas de Aplicação*. New York, USA: AICPA.
- Committee of Sponsoring Organizations of the Treadway Commission – COSO. (2017). *Enterprise Risk Management - Integrating with Strategy and Performance: Executive Summary*. New York, USA: COSO.
- Crouhy, M., Galai, D., & Mark, R. (2004). *Gerenciamento de risco: uma abordagem conceitual e prática: uma visão integrada dos riscos de crédito, operacional e de mercado*. Rio de Janeiro, Brasil: Qualitymark.
- Damodaran, A. (2009). *Gestão estratégica do risco*. Porto Alegre, Brasil: Bookman.
- Daud, W. N., Yazid, A. S., & Hussin, H. M. R. (2010). The effect of chief risk officer (CRO) on enterprise risk management (ERM) practices: evidence from Malaysia. *International Business & Economics Research Journal (IBER)*, 9(11): pp. 55-64.
- Deloitte. (2014). *O estágio atual da gestão de riscos: estratégias e ações para o crescimento sustentável*. Disponível em: <http://livrozilla.com/download/895605>
- Devenpor, T. H., & Prusak, L. (2003). *Conhecimento empresarial: como as organizações gerenciam o seu capital intelectual*. Rio de Janeiro, Brasil: Elsevier.
- Federation of European Risk Management Associations – FERMA. (2002). *Norma de Gestão de Riscos*. Disponível em: [http://www.ifc-camboriu.edu.br/~nildo/si/Normas\\_GR.pdf](http://www.ifc-camboriu.edu.br/~nildo/si/Normas_GR.pdf)
- Fraser, J., Schoening-Thiessen, K., & Simkins, B. J. (2008). Who Reads What Most Often? A Survey of Enterprise Risk Management Literature Read by Risk Executives. En: Fraser, J. & Simkins, B. J. (Eds). *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. Hoboken, USA: John Wiley & Sons.
- Gatzert, N., & Martin, M. (2015). Determinants and Value of Enterprise Risk Management: Empirical Evidence from the Literature. *Risk Management and Insurance Review*, 18(1): pp. 29-53.
- Gordon, L. A., Loeb, M. P., & Tseng, C. Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy*, 28(4): pp. 301-327.
- Instituto Brasileiro de Governança Corporativa – IBGC. (2007). *Guia de orientação para o gerenciamento de riscos corporativos*. São Paulo, Brasil: IBGC.
- Information Systems Audit and Control Association – ISACA. (2012). *COBIT 5: A business framework for the governance and management of enterprise IT*. Rolling Meadows: ISACA.
- Information Systems Audit and Control Association – ISACA. (2009). *Risk IT Framework*. Rolling Meadows: ISACA.
- International Organization for Standardization - ISO. (2009). *ISO 31000: 2009: Risk management: principles and guidelines on implementation* = Associação Brasileira de Normas Técnicas – ABNT NBR ISO 31000:2009: *Gestão de Riscos: Princípios e Diretrizes*, Rio de Janeiro, Brasil: ISO.
- Jorion, P. (2000). *Value at Risk: The New Benchmark for Managing Financial Risk*. New York, USA: MacGraw – Hill.
- Kaplan, R. S., & Mikes, A. (2011). Managing the Multiple Dimensions of Risk: part I. *Balanced Scorecard Report*, 13(4): pp. 2-6.
- Kaplan, R. S., & Mikes, A. (2012). Managing risks: a new framework. *Harvard Business Review*, 6(1): pp.1-8.
- Lechner, P., & Gatzert, N. (2018). Determinants and value of enterprise risk management: empirical evidence from Germany. *The European Journal of Finance*, 24(10), pp. 867-887.

- 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): pp. 37-52.
- Maroco, J. (2003). *Análise estatística com utilização do SPSS*. Lisboa, Portugal: Sílabo.
- Marshall, C. L. (2002). *Medindo e Gerenciando Riscos Operacionais em Instituições Financeiras*. Rio de Janeiro, Brasil: Qualitymark.
- McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does enterprise risk management increase firm value?. *Journal of Accounting, Auditing & Finance*, 26(4): pp. 641-658.
- Mikes, A. (2009). Risk management and calculative cultures. En: *Management Accounting Research*, 20(1): 18-40.
- Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. En: *Accounting, Organizations and Society*, 36(4): 226-245.
- Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance*, 18(4): pp. 8-20.
- Nonaka, I., & Takeuchi, H. (1997). *Criação de conhecimento na Empresa*. Rio de Janeiro, Brasil: Campus.
- Olson, D. L., & Wu, D. (2008). *New Frontiers in Enterprise Risk Management*. Berlin, Alemanha: Springer Science & Business Media.
- Paape, L., & Speklé, R. F. (2012). The adoption and design of enterprise risk management practices: an empirical study. *European Accounting Review*, 21(3): pp.533-564.
- Paxson, D., & Wood, D. (1998). *The Blackwell encyclopedic dictionary of finance*. Oxford, Reino Unido: Blackwell Publishers.
- Power, M. (2005). Organizational responses to risk: the rise of the chief risk officer. En: Hutter, B.; Power, M. (Eds). *Organizational Encounters with Risk*. Cambridge: Cambridge University Press.
- Raupp, F. M., & Beuren, I. M. (2006). Metodologia da Pesquisa Aplicável às Ciências Sociais. Em: Beuren, I. M. (Org). *Como elaborar trabalhos monográficos em contabilidade: teoria e prática*. São Paulo, Brasil: Atlas.
- Renn, O. (1992). Concepts of risk: a classification. En: S. Krinsky; D. Golding. *Social theories of risk*. Westport: Praeger.
- Renn, O. (2008). Concepts of Risk: An Interdisciplinary Review Part 1: Disciplinary Risk Concepts. En: *GAIA-Ecological Perspectives for Science and Society*, 17(1): pp. 50-66.
- Sheffi, Y. (2007). *The resilient enterprise: overcoming vulnerability for competitive advantage*. Boston,USA: MIT Press Books.
- Silva, S. L. (2004). Gestão do conhecimento: uma revisão crítica orientada pela abordagem da criação do conhecimento. *Ciência da Informação*, 33(2): pp. 143-151.
- Smith, E. (2001). The role of tacit and explicit knowledge in the workplace. *Journal of Knowledge Management*, 5(4): pp.311-321.
- Soltanizadeh, S., Rasid, S. Z. A., Golshan, N., Quoquab, F., & Basiruddin, R. (2014). Enterprise Risk Management Practices among Malaysian Firms. *Procedia-Social and Behavioral Sciences*, 164(1): pp. 332-337.
- Spender, J. C. (1996). Making knowledge the basis of a dynamic theory of the firm. *Strategic Management Journal*, 17(1): pp. 45-62.
- Takeuchi, H., & Nonaka, I. (2008). *Gestão do conhecimento*. Porto Alegre, Brasil: Bookman.
- Taleb, N. N. (2007). *The Black Swan: the impact of the highly improbable*. New York, USA: Random House.
- Tarantino, A. (2006). *Manager's Guide to Compliance: Sarbanes-Oxley, COSO, ERM, COBIT, IFRS, BASEL II, OMB's A-123, ASX 10, OECD Principles, Turnbull Guidance, Best Practices, and Case Studies*. Hoboken, USA: John Wiley & Sons.
- Zonatto, V. C. S., & Beuren, I. M. (2009). Evidenciação da gestão de riscos do COSO (2004) nos relatórios de administração de empresas com ADR's. En: *Contabilidade, Gestão e Governança*, 12(3).