UNIVERSIDADE DE SÃO PAULO
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO E CONTABILIDADE
DEPARTAMENTO DE ADMINISTRAÇÃO
PROGRAMA DE MESTRADO PROFISSIONAL EM EMPREENDEDORISMO

GERENCIAMENTO DE RISCOS CORPORATIVOS EM PEQUENAS E MÉDIAS EMPRESAS: ANÁLISE DE UMA EMPRESA NACIONAL DO SETOR DE TI

Anderson Doi

Orientador: Prof. Dr. Fábio Lotti Oliva

SÃO PAULO
2017

Prof. Dr. Marco Antonio Zago
Reitor da Universidade de São Paulo

Prof. Dr. Adalberto Américo Fischmann
Diretor da Faculdade de Economia, Administração e Contabilidade

Prof. Dr. Roberto Sbragia
Chefe do Departamento de Administração

Prof. Dr. Martinho Isnard Ribeiro de Almeida
Coordenador do Programa de Mestrado Profissional em Empreendedorismo

ANDERSON DOI

GERENCIAMENTO DE RISCOS CORPORATIVOS EM PEQUENAS E MÉDIAS EMPRESAS: ANÁLISE DE UMA EMPRESA NACIONAL DO SETOR DE TI

Dissertação apresentada ao Programa de Pós-graduação em Mestrado Profissional em Empreendedorismo do Departamento de Administração da Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo, como requisito parcial para obtenção do título de Mestre em Ciências.

Orientador: Prof. Dr. Fábio Lotti Oliva

Versão Corrigida

(versão original disponível na Faculdade de Economia, Administração e Contabilidade)

SÃO PAULO

2017

FICHA CATALOGRÁFICA
Elaborada pela Seção de Processamento Técnico do SBD/FEA/USP

Doi, Anderson
Gerenciamento de riscos corporativos em pequenas e médias empresas: análise de uma empresa nacional do setor de TI / Anderson Doi. -- São Paulo, 2017.
87 p.

Dissertação (Mestrado) – Universidade de São Paulo, 2017.
Orientador: Fábio Lotti Oliva.

1. Administração de risco 2. Pequenas e médias empresas 3. Tecnologia da informação 4. Gerenciamento de riscos corporativos 5. Identificação de riscos 6. Avaliação de riscos I. Universidade de São Paulo. Faculdade de Economia, Administração e Contabilidade. II. Título.

CDD – 658.155

AGRADECIMENTOS

Agradeço primeiramente à minha família, que me deu estrutura e condições para que este trabalho pudesse ser realizado. Em especial aos meus pais, que sempre pensaram e incentivaram a minha educação, e à minha esposa, que me deu suporte em todos os momentos.

Agradeço também aos coordenadores do Mestrado Profissional em Empreendedorismo da FEA-USP, que se dedicaram, trabalharam e buscaram sempre o melhor para o curso e seus alunos de pós-graduação.

Ao meu orientador Professor Doutor Fábio Lotti Oliva, que me orientou, incentivou e me apoiou em todo o processo de realização da dissertação.

Aos meus empregadores, que possibilitaram a análise da empresa, compartilharam opiniões, informações e tornaram possível a realização dessa pesquisa.

RESUMO

Os riscos fazem parte do cotidiano das empresas. Eles variam conforme sua natureza, a chance de ocorrer e o impacto que pode ocasionar às organizações. Por diversas razões, as empresas de pequeno e médio portes estão mais suscetíveis à imprevisibilidade e aos efeitos negativos dos riscos. Desse modo, é essencial que criem processos capazes de gerenciar os riscos de modo contínuo e sistêmico. Entretanto, o que se pode constatar é que ainda são raros os casos de empresas desses portes que possuam esses mecanismos de gestão. Essas empresas são fundamentais para o sistema econômico nacional, tanto pela geração de empregos quanto pelo crescimento do PIB e desenvolvimento do país. Na revisão bibliográfica desta pesquisa, o autor busca expor os principais conceitos existentes para o termo "risco" que, apesar de ser objeto de estudo há muito tempo, ainda possui definições bastante distintas; busca também apresentar aspectos importantes sobre o Gerenciamento de Riscos Corporativos e detalhar os dois principais modelos usados no mundo: COSO e ISO 31000, além de apresentar um modelo de identificação de riscos que abrange toda cadeia de valor das empresas. Como objetivos, identificar e avaliar quais são os principais riscos envolvidos na gestão de uma pequena empresa nacional do setor de TI, além de propor uma estratégia de tratamento para eles. A metodologia escolhida foi a pesquisa ação, na qual o pesquisador possui uma postura direta e ativa sobre a pesquisa e sobre a problemática. A pesquisa foi realizada sob uma abordagem qualitativa de caráter exploratório. Após identificação, avaliação e proposição de uma estratégia para tratamento dos riscos, conclui-se que é possível a implementação de um processo de Gerenciamento de Riscos Corporativos em uma empresa de pequeno porte e esse processo pode criar condições favoráveis para sobrevivência e crescimento das organizações. Muitos riscos descritos na literatura, que afetam negativamente as pequenas e médias empresas em vários países do globo, foram identificados na empresa analisada, enfatizando a necessidade de gestão dos riscos de um modo sistêmico, abrangente e contínuo. São poucas as pesquisas sobre este tema, na literatura nacional e, portanto, são fundamentais os estudos que possam contribuir para melhor entendimento deste universo.

Palavras chave: Administração de Riscos. Pequenas e médias empresas. Tecnologia da Informação. Gerenciamento de riscos corporativos. Identificação de riscos. Avaliação de riscos. Tratamento de riscos.

ABSTRACT

Risks are part of everyday business. They vary according to their nature, the chance to occur and the impact they can have on organizations. For various reasons, small and medium-sized enterprises are more susceptible to unpredictability and the negative effects of risks. In this way, it is essential that they create processes capable of managing risks in a continuous and systemic way. However, what can be seen is that there are still rare cases of companies of these sizes that have these management mechanisms. These companies are fundamental to the national economic system, both for the generation of jobs and for the GDP growth and development of the country. In the bibliographic review of this research, the author seeks to expose the main concepts existing for the term "risk" that, despite being object of study for a long time, still has quite different definitions; he also seeks to present important aspects of Enterprise Risk Management and to detail the two main models used in the world: COSO and ISO 31000, in addition to presenting a model of risk identification that covers the entire value chain of companies. The objectives are to identify and evaluate the main risks involved in the management of a small national IT company, and propose a treatment strategy for them. The methodology chosen was action research, in which the researcher has a direct and active attitude about the research and the problem. The research was carried out under a qualitative approach from an exploratory perspective. After identifying, evaluating and proposing a risk management strategy, it was possible to conclude that it is possible to implement an Enterprise Risk Management process in a small company, and this process can create favorable conditions for the survival and growth of the organization. Many risks described in the literature, which negatively affect small and medium enterprises in several countries of the globe, were identified in the analyzed company, emphasizing the need for risk management in a systemic, comprehensive and continuous way. There are few researches on this topic, in the national literature and, therefore, are fundamental studies that can contribute to a better understanding of this universe.

Keywords: Risk management. Small and medium enterprises. Information technology. Enterprise risk management. Identification of risks. Risk assessment. Treatment of risks.

LISTA DE QUADROS

Quadro 1 – Principais riscos de empresas brasileiras 24
Quadro 2 – Principais riscos da empresa avaliada 50
Quadro 3 – Agentes dos riscos 54
Quadro 4 – Causas e consequências dos riscos 56
Quadro 5 – Probabilidade e impacto dos riscos 57
Quadro 6 – Priorização dos riscos 63
Quadro 7 – Tratamentos propostos aos riscos 65
Quadro 8 – Impacto dos tratamentos 66

LISTA DE FIGURAS

Figura 1 – Componentes do gerenciamento de riscos corporativos 26
Figura 2 – Processo de gestão de risco 32
Figura 3 – Relacionamento entre os componentes da estrutura para gerenciar riscos 33
Figura 4 – Modelo de identificação dos riscos no ambiente de valor 34
Figura 5 – Exposição ao risco..... 36
Figura 6 – Matriz de risco..... 37
Figura 7 – Ciclo da pesquisa ação 44
Figura 8 – Aplicação do modelo de identificação de riscos no ambiente de valor 51
Figura 9 – Riscos no ambiente de valor 52
Figura 10 – Agentes do ambiente de valor 53
Figura 11 – Interação entre empresa e concorrentes 55
Figura 12 – Matriz de riscos 62
Figura 13 – Matriz de riscos da empresa avaliada..... 62
Figura 14 – Estrutura da pesquisa..... 70

LISTA DE ABREVIATURAS E SIGLAS

ABES - Associação Brasileira de Empresas de Software

ABNT - Associação Brasileira de Normas Técnicas

ADR - American Depositary Receipt

COSO - Committee of Sponsoring Organizations of the Treadway Commission

CRM - Customer Relationship Management

ERM - Enterprise Risk Management

FERMA - Federation of European Risk Management Associations

GRC - Gerenciamento de Riscos Corporativos

IBGC - Instituto Brasileiro de Governança Corporativa

IDC - International Data Corporation

ISO - International Organization for Standardization

PMEs - Pequenas e Médias Empresas

TI - Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO 15

1.1 Contextualização 15

1.2 Problemática 17

2 RELATO DA EXPERIÊNCIA 19

2.1 Histórico 19

2.2 A empresa 19

3 QUESTÃO DE PESQUISA E OBJETIVOS 21

3.1 Questão de pesquisa 21

3.2 Objetivos 21

4 REFERENCIAL TEÓRICO 23

4.1 Risco 23

4.2 Gerenciamento de riscos corporativos 25

4.2.1 COSO 28

4.2.2 ISO 31000 30

4.2.3 Identificação de riscos no ambiente de valor 33

4.2.4 Avaliação de riscos 35

4.2.5 Tratamento dos riscos 38

4.3 Gerenciamento de riscos corporativos em pequenas e médias empresas 40

5 PROCEDIMENTOS METODOLOGICOS 43

5.1 Conceituação 43

5.2 Pesquisa ação 43

5.3 Etapas da pesquisa ação 45

6 ANÁLISE DOS RESULTADOS 49

6.1 Identificação dos riscos da empresa analisada 49

6.2 Avaliação dos riscos da empresa analisada 55

6.3 Estratégia de tratamento dos riscos da empresa analisada 64

7 CONSIDERAÇÕES FINAIS 69

7.1 Atendimento aos objetivos da pesquisa 69

7.2 Atendimento aos procedimentos metodológicos 71

7.3 Implicações gerenciais 71

7.4 Limitações da pesquisa 74

7.5 Futuras pesquisas 75

8 REFERÊNCIAS 77

1 INTRODUÇÃO

1.1 Contextualização

Riscos são inerentes a qualquer tipo de empresa e setor econômico. Segundo Chapman e Cooper (1983), podem ser vistos como a possibilidade de ganhos ou perdas econômica ou financeira, como consequência da incerteza associada ao seguir um determinado curso de ação.

Com o aumento da quantidade de variáveis e agentes, e consequentemente da complexidade no ambiente de negócios, temos como resultado um aumento também no grau de incertezas, tornando mais difícil o processo de planejamento e gerenciamento de empresas (OLIVA, 2016). Saber como identificar, avaliar e administrar os riscos e conseguir mapear corretamente os seus componentes (OLIVA et al. 2014), são atividades essenciais para garantir a sobrevivência das organizações e também uma forma de criar valor de modo sustentável.

O *Enterprise Risk Management* (ERM), ou Gerenciamento de Riscos Corporativos (GRC), em português, é uma abordagem para identificar, analisar e planejar respostas de forma proativa para uma ampla gama de riscos em uma organização (BOWLING e RIEGER, 2005; CHAPMAN, 2003). Seus principais componentes envolvem: identificação, análise e avaliação, controle e monitoramento dos riscos (TAYLOR, 20015; TUMMALA et al., 1997).

Diversas pesquisas sobre o tema defendem que o GRC fornece uma abordagem sistêmica e lógica para tomada de decisões, redução de custos, aumento dos lucros, melhora na comunicação, garantindo assim o alinhamento da empresa com seus objetivos e missão, protegendo a reputação da empresa e aumentando, consequentemente, a confiança dos *stakeholders*. Segundo Hoyt e Liedenberg (2011), a implementação de ações de Gerenciamento de Riscos também aumenta o valor da empresa.

O GRC é um termo geralmente relacionado a grandes corporações e frequentemente presente nas estratégias de governança corporativa dessas instituições. Nos últimos anos, vem ganhando bastante destaque tornando-se um processo vital para sobrevivência e crescimento das empresas.

Apesar de operarem nos mesmos ambientes de grandes organizações, Pequenas e Médias Empresas (PMEs) raramente utilizam o gerenciamento de risco como uma ferramenta de

gestão empresarial (PANIGRAHI, 2012). A necessidade do gerenciamento de riscos talvez seja ainda maior para essas organizações, visto que além de atuarem no mesmo cenário de grandes corporações, possuem algumas desvantagens como menor disponibilidade de capital ou o acesso mais restrito a profissionais especializados, estando, portanto, mais suscetíveis aos efeitos prejudiciais de riscos. Acredita-se amplamente que os processos de gestão de riscos são menos desenvolvidos nesse setor (SMIT e WATKINS, 2012).

O grupo das PMEs vem sendo reconhecido como o grande propulsor do crescimento econômico mundial. Essas empresas surgem e se desenvolvem devido à sua agilidade e adaptabilidade em atender ao mercado e à sua disponibilidade em criar novas formas de se trabalhar. No entanto, a maioria ainda se encontra altamente vulnerável a choques externos (BERRY, 2002; LAFORET e TANN, 2006).

Hoje em dia, é possível encontrar em diversos países agências governamentais de fomento ao desenvolvimento das PMEs. Isso pode ser visto não apenas através de entidades públicas, mas também privadas, como incubadoras ou aceleradoras de empresas que têm no setor de Tecnologia da Informação (TI) seu principal alvo. Estamos vivendo em um mundo cada vez mais dependente da gestão da informação, onde a grande base para o crescimento das corporações tem sido a tecnologia.

Em especial no mercado de TI, o gerenciamento de risco deveria ser analisado com bastante cautela, dado que é um ambiente extremamente volátil, em rápida ascensão e transição e está cada dia mais competitivo. Na Era da Informação, algumas empresas como *Facebook*, *You Tube, Whatsapp, Google,* entre diversas outras, fundadas por empreendedores que enxergaram um mercado pouco ou nada explorado, hoje despertam o sonho da rápida ascensão profissional e financeira e do negócio próprio, em milhões de pessoas.

Segundo o estudo Mercado Brasileiro de Software e Serviços (2015), produzido pela *International Data Corporation* (IDC) em parceria com a Associação Brasileira das Empresas de Software (ABES, 2015), a indústria brasileira de TI movimentou US$ 60 bilhões em 2014 – um volume 6,17% maior que o ano de 2013. Do total, US$ 25,2 bilhões foram gerados pelo setor de softwares e serviços, sem exportações.

O Brasil está na 8º posição de maiores mercados nesse setor, sendo o 1º da América Latina. De acordo ainda com a pesquisa, esse grupo é formado por 45,62% de microempresas, 49,02% de pequenas, 4,33% de médias e apenas 1,03% de grandes empresas. Analisando

esses dados, verifica-se a importância das PMEs no setor de TI e deste último para a economia do país.

Dessa maneira, estudos sobre gestão de riscos em pequenas e médias empresas são fundamentais para que seja possível criar condições mais favoráveis à sobrevivência e desenvolvimento desses tipos de organizações, que hoje são peças extremamente importantes para o bom funcionamento e expansão do nosso ecossistema econômico.

1.2 Problemática

No passado, as empresas costumavam cuidar dos riscos de forma reativa e isolada. Ainda não havia muitos estudos sobre esse tema e ainda era um assunto muito obscuro para a maioria dos gestores. Hoje em dia, é sabido que atuar desta maneira é ineficaz e muito perigoso (FRIGO e ANDERSON, 2011), quanto mais soubermos sobre como evitar os efeitos nocivos dos riscos e aproveitar os positivos, maior a chance de sobrevivência e maior a probabilidade de crescimento sustentável das organizações.

O mundo se tornou mais dinâmico, o número de agentes e fatores críticos aumentou, o tempo para tomada de decisões ficou mais curto, e nesse ambiente mais complexo a previsibilidade das ações ficou mais difícil (OLIVA, 2016). Por causa do fenômeno da globalização e do livre comércio, a competitividade está cada dia mais acirrada em diversos setores econômicos e a tendência mundial tem caminhado na direção de redução das barreiras protecionistas e flexibilização da legislação em favor da abertura de mercado (FILHO, 2014). Por essa e outras razões, o gerenciamento de riscos se torna uma ferramenta essencial para o planejamento e o processo de tomada de decisões.

Mas implantar um programa de gerenciamento de riscos, por si só, ainda não é suficiente. É necessário que a abordagem seja feita de forma integrada e holística. Ela deve ocorrer com total alinhamento às estratégias e às regras de governança empresariais (BROMILEY et al., 2014). Ainda é muito raro encontrar pequenas e médias empresas que dão a devida importância a isso. Normalmente a análise e o tratamento dos riscos ocorrem de forma isolada e passiva (SIREGAR, 2015).

Nos dias atuais, dada a relevância do assunto, é bastante comum encontrar pesquisas sobre o tema Gerenciamento de Riscos Corporativos, todavia estas se focam em práticas e modelos criados para grandes corporações. Ainda faltam estudos que possam analisar esse cenário no

setor das PMEs no mundo, e no Brasil isto não é diferente. Existem poucos estudos sobre o tema que tenham o foco neste segmento de empresas e se torna ainda mais raro no setor de TI.

Segundo dados da Associação Brasileira das Empresas de Software - ABES (2015, p.5):

> O mercado doméstico de Tecnologia da Informação, que inclui hardware, software e serviços, movimentou 60 bilhões de dólares em 2014, representando 2,6% do PIB brasileiro e 3% do total de investimentos de TI no mundo, um resultado praticamente igual às participações apontadas no ano anterior. Deste valor, 11,2 bilhões vieram do mercado de software e 13,9 bilhões do mercado de serviços, sendo que a soma destes dois segmentos continuou a superar os 40% do mercado total de TI, mantendo a tendência de passagem do país para o grupo de economias com maior grau de maturidade, que privilegiam o desenvolvimento de soluções e sistemas.

Conhecendo a importância das PMEs do setor de TI para o contexto econômico brasileiro, a percepção de que as gestões dos riscos dessas organizações são feitas de formas insuficientes e a importância que a gestão de riscos pode ter para a sobrevivência e crescimento delas, este estudo pode contribuir de forma significativa para um melhor entendimento sobre esse problema.

Através de uma análise detalhada de uma pequena empresa nacional do setor de TI, esta pesquisa pretende ainda identificar e avaliar quais são os principais riscos envolvidos na gestão dessa organização e propor uma estratégia de tratamento para eles.

2 RELATO DA EXPERIÊNCIA

2.1 Histórico

O autor deste trabalho atua como gerente financeiro de uma pequena empresa de TI, com capital 100% nacional e 14 anos de existência, a qual foi o objeto de pesquisa deste trabalho. Além das funções comuns ao setor financeiro, como Tesouraria, Controladoria e Planejamento Financeiro, o profissional busca também identificar, avaliar e criar mecanismos de gerenciamento para todas as fontes de riscos, mesmo que de modo não estruturado.

Atualmente, a empresa não possui uma estrutura e nem atividades ou processos formais para essa função. Apesar de os sócios-administradores reconhecerem a importância da gestão de riscos, a ideia de implantar um projeto de gerenciamento próprio e especifico para isso ainda não está totalmente madura e dessa forma, a empresa acaba atuando de forma não sistemática e de modo insuficiente e reativo.

Dado esse cenário, o autor motivou-se pelo estudo e análise da empresa em que atua, com um foco para avaliação e gerenciamento dos riscos presentes nesse ambiente. Ele entende ainda que este é um assunto ainda muito escasso na literatura brasileira e que este trabalho pode, em muito, contribuir para uma melhor compreensão da problemática.

2.2 A empresa

A empresa a ser estudada é uma consultoria de TI, especializada em sistemas de *Customer Relationship Management* (CRM) que foi fundada em 2003. Atualmente, a empresa é composta por quatro sócios, cada um com 25% do total das quotas.

Todos os sócios são formados em engenharia, com foco em informática, vieram de outras consultorias de TI e já possuem conhecimento técnico sobre os sistemas que prestam serviços. Cada um fica responsável por uma área diferente da empresa, liderando e dando suporte aos demais da equipe.

A CRM tem como clientes, hoje, grandes empresas nacionais e multinacionais, nos mais diversos setores da economia, tais como varejo, bens de consumo, turismo, alimentos, entre

outros. A maior parte dos seus clientes estão no Brasil, mas a empresa atua também em outros países como Colômbia, Costa Rica, México e outros.

Nos últimos cinco anos a empresa vem crescendo em um ritmo bastante acelerado e, por essa razão, vem profissionalizando algumas áreas funcionais que estão demandando melhores profissionais. Apesar disso, dentro dessas áreas, não se encontra nenhum setor especifico dedicado à gestão de riscos.

Apesar da consciência sobre a importância de se ter um controle global de riscos, a empresa não possui atualmente nenhum sistema para isso, bem como nenhum profissional especializado no assunto. Essa é a principal motivação do autor para a escolha desta empresa como objeto de estudo, bem como a definição do tema e escopo de pesquisa.

3 QUESTÃO DE PESQUISA E OBJETIVOS

3.1 Questão de pesquisa

Como a implantação de um processo de Gerenciamento de Riscos Corporativos pode contribuir para a gestão de riscos em uma pequena empresa nacional do setor de TI?

3.2 Objetivos

Objetivo geral:

- Pesquisar sobre os riscos corporativos em uma pequena empresa do setor de TI.

Objetivos específicos:

- Identificar os principais riscos em uma pequena empresa do setor de TI;
- Avaliar os principais riscos em uma pequena empresa do setor de TI; e
- Propor estratégias para tratar os principais riscos em uma pequena empresa do setor de TI.

4 REFERENCIAL TEÓRICO

4.1 Risco

Não existe uma definição única e absoluta para risco, que varia de acordo com o contexto no qual ele está inserido. Nos últimos anos, com o aprofundamento de pesquisas sobre este tema, diversos autores têm apresentado conceitos diferentes. De acordo com Raz e Hilson (2005), na literatura não é possível encontrar um consenso com relação à sua definição. Todavia, o termo "risco" tem sido utilizado para expressar incerteza sobre determinados eventos e suas consequências.

Alguns autores entendem que riscos compreendem apenas os aspectos negativos da incerteza. Mitchel (1995) define risco em termos de probabilidade de perda e a significância e impacto que essa perda tem para a empresa. Macdonald (2004) generalizou risco como a probabilidade de um evento negativo ocorrer, multiplicado pelo quão prejudicial esse evento pode ser, que pode ser resumido pela função:

$$Risco = f(evento, probabilidade, impacto)$$

Já outros – como Zeno (2007), Rocha e Belchior (2004) e Bergamini Júnior (2005) –, englobam os aspectos positivos, as oportunidades, dentro da definição de risco. Em alguns casos, as ameaças acabam se transformando em oportunidades que, se aproveitadas, poderão agregar valor à organização.

Para o Instituto Brasileiro de Governança Corporativa – IBGC (2007, p.11),

> [...] risco é proveniente da palavra *risicu* ou *riscu*, em latim, que significa ousar (*to dare*, em inglês). Costuma-se entender "risco" como possibilidade de "algo não dar certo", mas seu conceito atual envolve a quantificação e qualificação das incertezas, tanto no que diz respeito às "perdas" como aos "ganhos", com relação ao rumo dos acontecimentos planejados, seja por indivíduos, seja por organizações.

No documento *Enterprise Risk Management: Integrated Framework* do *Committee of Sponsoring Organizations of the Treadway Commission* (COSO, 2007), encontra-se que risco é tudo aquilo que foge ao planejado pela empresa. Para Paxson e Wood (1998, p. 159), "[...]

pode simplesmente ser definido como exposição à mudança. É a probabilidade de que algum evento futuro ou um conjunto de eventos ocorra".

A classificação dos tipos de riscos também é bastante heterogênea. Sadgrove (2005) classifica os riscos em quatro grandes categorias: financeiro, operacional, estratégico e riscos de *compliance*. Já Harland et al. (2003) os utiliza em uma perspectiva mais ampla. A pesquisa desses autores, através de uma análise de trabalhos anteriores, identifica onze tipos diferentes de riscos: estratégico, operacional, fornecimento, cliente, redução de ativos, competitividade, reputação, financeiro, fiscal, regulatório e legal.

Em estudo conduzido em 2005 pela Deloitte – empresa líder em consultoria empresarial – de 1993 a 2004, foram identificados os 15 riscos mais prejudiciais para as empresas brasileiras:

Quadro 1 – Principais riscos de empresas brasileiras

Natureza dos ricos	***Riscos***
Riscos estratégicos	(1) redução da demanda; (2) problemas com clientes e insolvência; (3) problemas com fusões e aquisições; (4) pressões por preço; (5) regulatório;
Riscos operacionais	(6) descontrole dos custos operacionais; (7) problemas contábeis; (8) problemas de logística; (9) não-conformidade com as regulações; (10) elevação dos custos;
Riscos financeiros	(11) altas taxas de inadimplência e altas taxas de juros; (12) estratégias financeiras fracas; e
Riscos externos	(13) crise no setor de atuação; (14) problemas econômicos no país sede; (15) vulnerabilidades legais.

Fonte: Autor (2017) baseado no estudo da Deloitte (2005)

Em finanças, quanto maior o risco, maior o retorno esperado. Seguindo esse raciocínio, empreender significa buscar um retorno econômico-financeiro adequado ao nível de risco associado à atividade. Todas as tomadas de decisão no ambiente corporativo, independentemente do tipo e importância, envolvem de modo indireto a relação risco x retorno (PADOVEZE e BERTOLUCCI, 2008).

Assumir riscos poderá transformar empresas em líderes em seus mercados, mas também poderá levá-las a estrondosos fracassos. Organizações que têm consciência disso e entendem que riscos podem ser gerenciados a fim de subsidiar os administradores na tomada de decisões, conseguem maximizar os ganhos e reduzir os prejuízos (GRACE et al., 2015).

Pode-se dizer que tanto a definição do termo risco como suas classificações são bastante amplas e não existe um consenso conceitual entre os autores. Desse modo, para este trabalho foi utilizada para risco o conceito apresentado por Mitchel (1995) e Macdonald (2004), avaliando-se apenas os aspectos negativos dos riscos.

4.2 Gerenciamento de riscos corporativos

É extremamente importante que os riscos sejam monitorados com muita cautela. Raghavan (2005) sustenta que a sobrevivência de uma organização depende de sua habilidade em prever e se preparar para eventos futuros em vez de reagir quando o inevitável ocorrer. Pode-se dizer que administrá-los corretamente significa ter o poder de controlar, até certo grau, o desempenho da empresa.

Cada vez mais a complexidade do ambiente corporativo, seja externo ou interno, tem aumentado. O número de agentes tem crescido, as operações estão mais complicadas, a tecnologia mais avançada e o fator humano mais capacitado. Todos esses fatores tornam as tomadas de ação mais difíceis de serem previstas (OLIVA, 2016).

Diante desse cenário, as organizações têm investido altas somas de recursos em sistemas de gerenciamento de riscos. Esses sistemas estabelecem quais itens, de que modo, quais ações serão tomadas e como serão tratados os riscos. Jorion (1997, p.4) define o gerenciamento de risco como "[...] o processo pelo qual várias exposições são identificadas, mensuradas e controladas".

Para Urciuoli e Crenca (1989), é o processo que tem como intenção resguardar os ativos da companhia contra perdas, através de ferramentas específicas (prevenção, seguros, retenções, etc.) e com custos apropriados. Já Head (2009) define o gerenciamento de riscos como um processo de planejar, organizar, gerenciar e controlar recursos para atingir determinados objetivos, mesmo na ocorrência de eventos imprevisíveis, sejam eles positivos ou negativos.

Uma afirmação importante sobre o gerenciamento é dada por Moeller (2007), quando diz que a gestão de riscos não está voltada à eliminação deles, e sim à sua identificação, mensuração e controle. Adverte ainda que uma adequada estrutura de controle pode oferecer aos gestores melhores condições para avaliar a quais riscos as empresas estão sendo expostas.

No passado, os riscos organizacionais eram examinados apenas uma vez, de modo isolado e compartimentalizado. Essas avaliações eram feitas por um gerente funcional ou líder da unidade de negócios, com uma mínima visão de como ações e decisões particulares poderiam afetar outros aspectos da organização (FRIGO e ANDERSON, 2011).

As vertentes mais recentes caminham no sentido de uma abordagem coordenada, interativa e mais global, identificando e gerenciando todos os riscos em conjunto (BROMILEY et al., 2014; MCSHANE, NAIR e RUSTAMBEKOV, 2011). Para Oliva (2016), a avaliação dos riscos não deve ficar restrita à empresa, mas a toda sua cadeia de valor. Essa visão mais holística vem para superar as limitações das vertentes mais antigas e tradicionais. Hoyt e Lidenberg (2011) se referem a essa nova abordagem como "Gerenciamento de Risco Integrado" ou "Gerenciamento de Riscos Holísticos".

Hoje, o termo *Enterprise Risk Management* (ERM), traduzido para o português como Gerenciamento de Riscos Corporativos (GRC), tem sido bastante utilizado por diversas entidades e pesquisadores ao se referirem a essa abordagem mais abrangente.

Para o COSO (2007, p. 7):

> Existe um relacionamento direto entre os objetivos que uma organização se empenha em alcançar e os componentes do gerenciamento de riscos corporativos, que representam aquilo que é necessário para o seu alcance. Esse relacionamento é apresentado em uma matriz tridimensional em forma de cubo.

Figura 1 – Componentes do gerenciamento de riscos corporativos

Fonte: COSO (2007)

O estudo diz ainda que “essa representação ilustra a capacidade de manter o enfoque na totalidade do gerenciamento de riscos de uma organização, ou na categoria de objetivos, componentes, unidade da organização ou qualquer um dos subconjuntos” (COSO, 2007, p. 7).

Muitos pesquisadores definem o GRC pela sua importância e benefícios nos processos de tomada de decisões. Dessa forma, é essencial que eles estejam intrinsicamente desenhados e trabalhados de acordo com as estratégias da empresa (FRIGO e ANDERSON, 2011). Bromiley et al. (2014) também argumentam que o GRC requer um alinhamento com a governança corporativa e a estratégia empresarial.

A *International Organization for Standardization* (ISO 31000, 2009) preconiza, de modo mais genérico, que um sistema de gestão de riscos deve: criar valor; ser parte integral dos processos organizacionais; ser parte da tomada de decisões que explicitamente envolvem incertezas; ser sistemático e estruturado; estar baseado nas melhores informações disponíveis; ser especifico para a empresa; considerar os fatores humanos; ser transparente e inclusivo; ser dinâmico, interativo e responsivo a mudanças; e estar em processo de melhoria contínua.

Outro ponto bastante discutido na literatura sobre a gestão de riscos é quanto aos benefícios que esta pode proporcionar. Alguns autores afirmam que as empresas buscam dois principais objetivos: *Compliance* – aderência a diretrizes, regulações e legislação –, e performance – otimização de eficiência e eficácia (ARENA, ARNABOLDI e AZZONE, 2010; MIKES, 2011). Outros dizem que as empresas buscam mitigar os prejuízos e explorar as oportunidades (HOYT e LIDENBERG, 2013; NOCCO e STULZ, 2006).

Por outro lado, Chapman (2003) analisou que diversos programas de implementação de gestão de riscos falham em alcançar seus objetivos; outros autores, como McShane et al. (2011), concluíram que a relação entre o GRC e a performance da empresa é inconclusiva.

Apesar disso, Barton et al. (2002) acreditam que o custo de oportunidade em negligenciar o GRC é muito grande. Os autores constataram que a má administração dos riscos levou a grandes perdas financeiras, redução de valor e danos significantes na reputação das empresas estudadas.

Atualmente existem várias metodologias de gestão de risco, entre as quais se destacam:

- Norma de Gestão de Riscos Australiana AS/NZS 4360 (2004) – *Risk Management Guidelines;*
- Norma de Gestão de Riscos da FERMA: *Risk Management Standard* emitida em 2002 pela *Federation of European Risk Management Associations*;
- Gestão de Risco Empresarial: *ERM – Enterprise Risk Management Framework*, emitida pelo COSO em 2007; e
- ISO 31000 da *International Organization for Standardization* emitida em 2009.

Os dois principais modelos, reconhecidos mundialmente, são os dois últimos.

Segundo Santos, Vasconcelos e Tribolet (2007), o modelo proposto pelo COSO possui várias referências que dão suporte à sua eficácia e é aceito pela grande maioria dos auditores em todo o mundo. Ele atua diretamente no ambiente de controle das atividades e busca estar intimamente relacionado às estratégias e objetivos organizacionais.

Já a norma ISO 31000 tem como objetivo criar um conjunto de procedimentos para o gerenciamento de riscos que possam ser generalizados para qualquer tipo de empresa, independente do seu tamanho ou área de atuação.

Para melhor compreensão dos modelos de GRC, o autor buscará apresentar as principais características destes dois últimos exemplos. Além disso, será apresentado também um modelo teórico elaborado por Oliva (2016) para identificação dos riscos corporativos, que contempla toda cadeia de valor da empresa.

4.2.1 COSO

O modelo COSO surgiu em 1992, consequência da preocupação de algumas entidades norte-americanas com fraudes em documentos contábeis. O *Committee of Sponsoring Organizations of the Treadway Commission* – em português, Comitê de Organizações Patrocinadoras da *Treadway* –, é uma entidade sem fins lucrativos e tem como objetivo principal auxiliar empresas e outras entidades a avaliar e aprimorar seus sistemas de controle interno; busca a melhoria nos relatórios financeiros, avanço na efetividade dos controles internos e da governança corporativa, tendo como pilar de suas ações, a ética (COSO, 2007).

A entidade preconiza uma sistematização dos processos de controles internos, que deve assegurar, com razoável grau de certeza, que os objetivos de economia e eficiência, proteção

patrimonial e adesão às políticas e estratégias adotadas pela empresa sejam alcançados e garantam que a veracidade das informações contábeis e financeiras estejam em total conformidade com as normas e legislações locais (ATTIE, 2009). O COSO (2007, p.6) estabelece uma sequência de eventos, que contempla até oito ambientes diferentes a serem analisados em uma organização:

- **Ambiente interno:** o ambiente interno compreende o tom de uma organização e fornece a base pela qual os riscos são identificados e abordados pelo seu pessoal, inclusive a filosofia de gerenciamento de riscos, o apetite a risco, a integridade e os valores éticos, além do ambiente em que estes estão;
- **Fixação dos objetivos:** os objetivos devem existir antes que a administração possa identificar os eventos em potencial que poderão afetar a sua realização. O gerenciamento de riscos corporativos assegura que a administração disponha de um processo implementado para estabelecer os objetivos que propiciem suporte e estejam alinhados com a missão da organização e sejam compatíveis com o seu apetite a riscos;
- **Identificação de eventos:** os eventos internos e externos que influenciam o cumprimento dos objetivos de uma organização devem ser identificados e classificados entre riscos e oportunidades. Essas oportunidades são canalizadas para os processos de estabelecimento de estratégias da administração ou de seus objetivos;
- **Avaliação de riscos:** os riscos são analisados, considerando-se sua probabilidade e impacto como base para determinar o modo pelo qual deverão ser administrados. Esses riscos são avaliados quanto à sua condição de inerentes e residuais:
    - Risco inerente: risco natural e ausência de qualquer ação que a direção possa realizar para alterar a probabilidade de ocorrência ou de impacto;
    - Risco residual: resultante do processo de tomada de ações e aplicação das melhores práticas de controles internos ou da reposta da organização ao risco.
- **Resposta a risco:** a administração escolhe as respostas aos riscos – evitando, aceitando, reduzindo ou compartilhando –, desenvolvendo uma série de medidas para alinhar os riscos com a tolerância e com o apetite a risco;
- **Atividade de controle:** políticas e procedimentos são estabelecidos e implementados para assegurar que as respostas aos riscos sejam executadas com eficácia;
- **Informação e comunicação:** as informações relevantes são identificadas, colhidas e comunicadas de forma e no prazo que permitam que cumpram suas responsabilidades.

A comunicação eficaz também ocorre em um sentido mais amplo, fluindo em todos níveis da organização.

- **Monitoramento:** a integridade da gestão de riscos corporativos é monitorada e são feitas as modificações necessárias. O monitoramento é realizado através de atividades gerenciais contínuas ou avaliações independentes ou de ambas as formas.

Cada empresa deve possuir sua própria estrutura de controle das atividades, pois depende de algumas variáveis, como o perfil do administrador, a estrutura da organização e as peculiaridades da atividade que a empresa exerce.

Segundo Souza et al. (2011), o modelo COSO é recomendado para as empresas americanas que estão sujeitas à Lei Sarbanes-Oxley e também para as empresas brasileiras com ADRs. De modo geral, pode-se dizer que o modelo se aplica muito bem a grandes empresas, pois além dos benefícios que o modelo propicia nos controles internos, ele também se atém aos cuidados necessários na divulgação externa das informações gerenciais sobre essas organizações.

4.2.2 ISO 31000

A norma ISO 31000 foi publicada em 2009 pela *International Organization for Standardization* e é a mais recente norma internacional sobre gestão de riscos. Ela se baseia na AS/NZS 4360 de 2004 e foi elaborada por uma comissão formada por uma delegação de 35 países. A comissão formada era composta por especialistas em gestão de riscos de diversas áreas, como a financeira, qualidade, meio ambiente, saúde, segurança e outros.

O Brasil, tendo como representante a ABNT (Associação Brasileira de Normas Técnicas), também colabora com o desafio de tornar a ISO 31000 uma norma geral de gerenciamento de riscos. O resultado desse trabalho contempla a opinião e experiência dos mais diversos especialistas no tema.

Como é comum a diversas outras normas da ISO, ela também tem como objetivo fornecer princípios, guias e terminologias comuns, de forma a se obter uma padronização das metodologias já existentes. Para esse caso, atenta especificamente para o gerenciamento de riscos. Para Brasiliano (2009 p. 19), ela "[...] veio integrar as metodologias e terminologias existentes afirmando não existir, ainda, consenso em relação aos conceitos utilizados na gestão de riscos".

Essa característica torna possível que a ISO 31000 tenha uma abordagem ampla e genérica, podendo ser utilizada por qualquer tipo de empresa ou setor, além disso, estabelece princípios e diretrizes para administrar qualquer forma de risco de modo sistemático, transparente e confiável, não importando contexto no qual está inserido.

O processo de gestão de riscos apresenta cinco etapas, sendo eles (ISO 31000, 2009):

1. **Comunicação e consulta:** as partes interessadas, internas e externas, devem ser comunicadas e consultadas durante todas as fases do processo de gestão de riscos; para isso, pode-se valer de quaisquer recursos e ferramentas que possam facilitar e melhorar a comunicação ao longo de todo processo;
2. **Estabelecimento do contexto:** articular objetivos e definir parâmetros internos (estrutura organizacional, responsabilidades, processos, sistemas de informação e relação entre as partes interessadas) e externos (ambiente legal, social, cultural e político; financeiro, tecnológico etc.) que serão considerados na condução dos trabalhos, estabelecendo os critérios de risco para o restante do processo;
3. **Processo de avaliação de riscos:** é o processo como um todo, visto de forma global, em que se tem a identificação, analise e avaliação dos riscos envolvidos:
    a. Identificação: esta etapa consiste em listar e identificar os possíveis riscos que possam impactar os objetivos estratégicos da organização, inclusive os relacionados aos ativos intangíveis da organização. Além disso, a identificação assume um papel de extrema importância, pois as etapas posteriores serão baseadas nela e, por essa razão, ela deve ser abrangente e crítica. Devem constar todos os riscos possíveis, estando suas fontes sob controle da organização ou não;
    b. Análise: com os riscos listados, na etapa seguinte a organização buscará identificar quais são as possíveis causas e fontes dos riscos, se suas consequências serão benéficas ou maléficas para a empresa e quais as probabilidades para que ocorram. É importante considerar que a interdependência dos diferentes riscos e suas fontes possam existir. A análise pode ter características quantitativas, qualitativas ou uma combinação das duas, e também o grau de detalhamento pode variar, de acordo com a necessidade da informação;

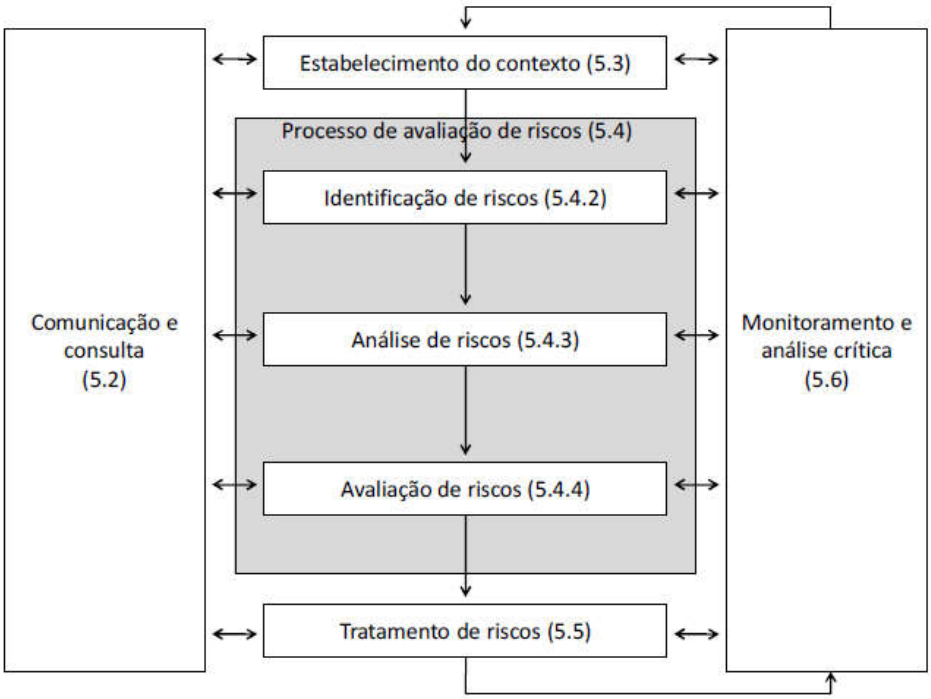
c. Avaliação: este item tem como finalidade auxiliar na tomada de decisões com base nos resultados da etapa anterior. É nesse momento que se avaliam quais riscos terão necessidade de tratamento e como se dará sua priorização. Em alguns casos, poderá haver a necessidade de retomar a etapa anterior, pois as informações podem não ser suficientes para a efetiva avaliação do risco.

4. **Tratamento dos riscos:** trata-se da seleção e implementação de opções para modificar o risco. Uma vez implementado o tratamento, há necessidade de novos controles e modificação dos existentes, e isso deve ocorrer de maneira sistemática. Além disso, as opções para o tratamento de risco não são, de todo o modo, mutuamente exclusivas.

5. **Monitoramento e análise crítica:** processo de vigilância e checagem regulares, devendo ser periódicos e/ou acontecer em resposta a um evento específico. As responsabilidades relativas a esse monitoramento e análise devem ser claras e bem definidas para sua eficácia.

A Figura 2, a seguir, ilustra como os tópicos se relacionam:

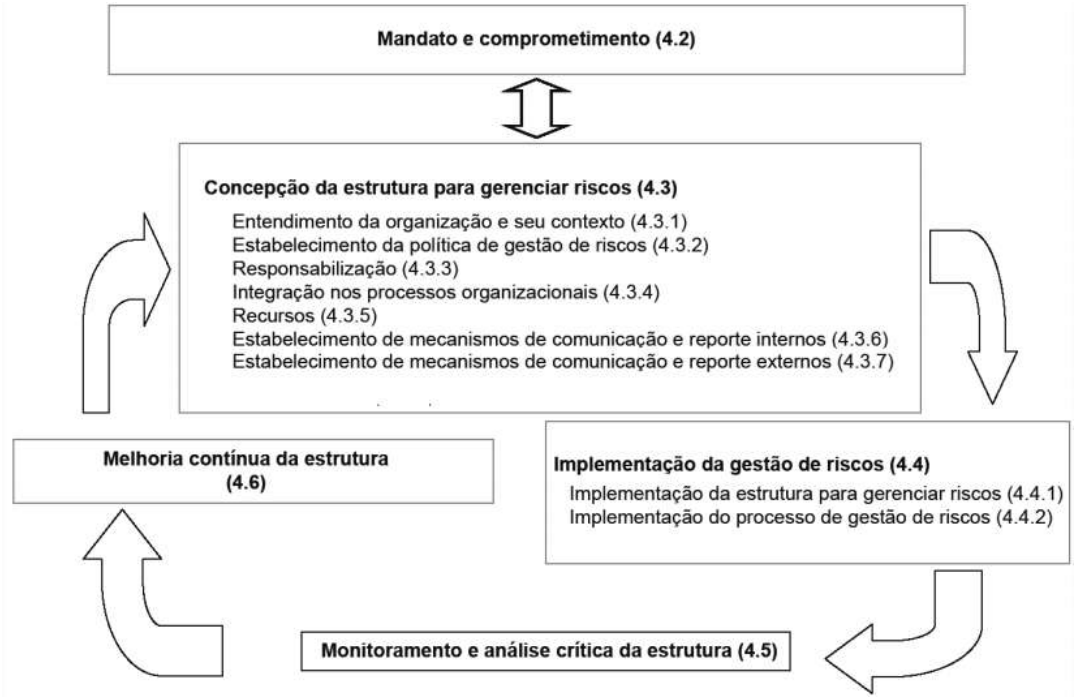
Figura 2 – Processo de gestão de risco



Fonte: ABNT NBR ISO 31000, 2009, p.14

Os componentes necessários da estrutura para gerenciar riscos e a forma como eles se inter-relacionam de maneira interativa, são mostrados na Figura 3, a seguir:

Figura 3 – Relacionamento entre os componentes da estrutura para gerenciar riscos



Fonte: ABNT NBR ISO 31000 (2009, p. 9)

Vale ressaltar que a ISO 31000 não é um modelo de gestão de riscos por si só, mas sim um conjunto de princípios e diretrizes que auxiliam as empresas na integração de sua gestão de risco com um sistema de gestão global. Justamente por isso, o modelo de GRC de cada empresa deve ser único e ser adaptado de acordo com as necessidades de cada uma. A Norma preconiza que o processo de gestão de riscos seja: "parte integrante da gestão, incorporado na cultura e nas práticas e adaptado aos processos de negócios da organização" (ISO 31000, 2009, p. 13).

4.2.3 Identificação de riscos no ambiente de valor

Com base em diversas literaturas, cujos temas estão focados em Nova Economia Institucional, Cadeia de Suprimentos e Análise de Riscos Corporativos, Oliva (2016) propôs um modelo para a etapa de identificação de riscos, que difere um pouco dos apresentados anteriormente. A principal diferença está na abrangência da análise, que vai além das fronteiras da organização.

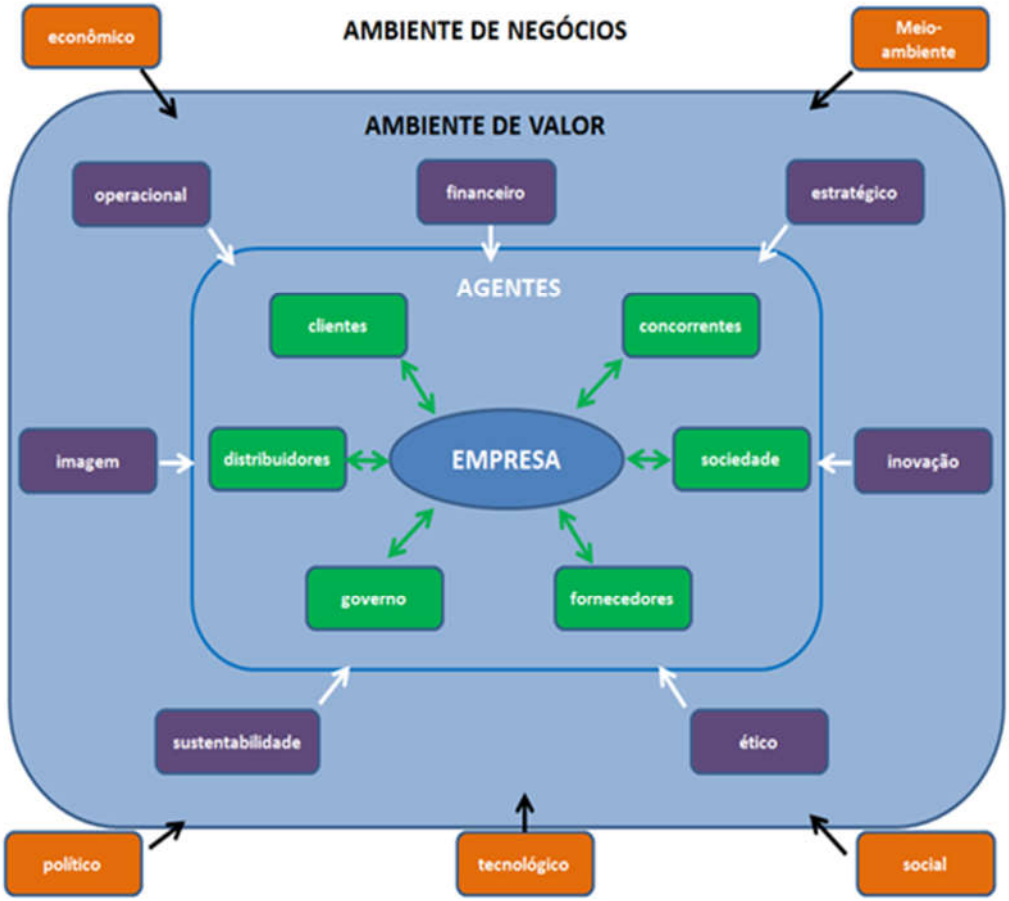
Em seu modelo, Oliva (2016) separa o ambiente que uma organização está inserida em dois grandes grupos: Ambiente de Negócios e Ambiente de Valor.

No primeiro, existem forças que podem interferir diretamente no segundo e, por consequência, interferir nos objetivos da empresa, mas ela não possui ou possui muito pouco poder de interferência. As principais forças são: econômico, meio-ambiente, político, social e tecnológico.

Já no segundo, compreendem-se as forças da indústria que a empresa está inserida e que podem influenciar no destino da empresa que, nesse caso, também pode interferir para alterar esse destino. Os principais agentes desse ambiente são: clientes, distribuidores, governo, fornecedores, sociedade e concorrentes.

A análise da relação com esses principais agentes pode levar a empresa a verificar quais são os riscos envolvidos nessas interações, sendo os principais: operacional, financeiro, estratégico, inovação, ético, sustentabilidade e imagem.

Figura 4 – Modelo de identificação dos riscos no ambiente de valor



Fonte: Oliva (2016)

A Figura 4 representa esse modelo e mostra como se relacionam as forças presentes no ambiente de negócios e ambiente de valor da empresa e suas interações com os agentes.

Os riscos corporativos surgem das suas relações internas do ambiente de valor e da relação da empresa com o ambiente de negócios. Além disso, os riscos não devem ser analisados de forma isolada, mas sim de maneira sistemática e orgânica.

O modelo não restringe os riscos apenas aos que aparecem na imagem anterior, mas apenas cita os principais. Cabe ao gestor ou pessoa responsável pela identificação dos riscos definir a melhor forma de categorização dos mesmos. Além disso, o modelo também não se limita ao porte da empresa, sendo possível sua utilização para qualquer atividade, tamanho e mercado.

4.2.4 Avaliação de riscos

Nas normas da ISO 31000, o processo de avaliação (item 5.4 da Figura 2) compreende três etapas: identificação, análise e avalição dos riscos. Já no COSO (2007), a avaliação compreende uma única etapa, que consiste na análise dos riscos, considerando sua probabilidade e impacto.

Os riscos são avaliados em uma base inerente e em outra residual. O primeiro ocorre na ausência de qualquer tipo de ação tratamento ou ação que possa alterar a probabilidade ou impacto do risco – é ele em sua essência, original. Já o risco residual, como o próprio nome diz, é o evento que remanesce depois de alguma forma de tratativa do risco inerente (CHING, 2011).

Tendo como premissa que os riscos são inerentes aos ambientes de negócios, altamente voláteis, e que o resultado de uma empresa está intrinsicamente relacionado ao grau de exposição aos riscos, é fundamental que no processo de avaliação defina-se a propensão aos riscos da empresa, isto é, qual é a quantidade de riscos que a organização está disposta a aceitar no desempenho de suas atividades (COSO, 2007; DAMODARAN, 2009).

Dantas et al. (2010, p. 8) afirmam que “a disposição em assumir risco é influenciada, de certa forma, pela cultura da organização, ressaltando-se a premissa de que há uma relação positiva entre nível de exposição a riscos e o retorno alcançado”.

Esse perfil da empresa normalmente toma forma através de mapas ou matrizes, diagramas, gráficos e listas que a empresa cria para o processo de gestão dos riscos (FRASER e SIMKINS, 2016). A matriz de riscos é uma ferramenta para análise qualitativa dos riscos, composta basicamente de dois eixos, sendo um deles a probabilidade de ocorrência do risco e o outro, o grau de impacto que pode levar para a empresa (PAULO et al., 2007).

A matriz deve representar também o perfil de apetite de risco da organização. Na Figura 5, a área verde da matriz representa a região que a empresa aceita ficar exposta aos riscos, já a área vermelha, é a região de exposição inaceitável. Os riscos que estão nessa região terão algum tipo de tratamento. A área de exposição intermediária cabe à empresa avaliar as medidas cabíveis para gerenciamento deles.

Figura 5 – Exposição ao risco

Fonte: Adaptado de IBGC (2007)

O COSO (2012b) também aconselha o uso da matriz (ou mapa) de riscos para uma melhor percepção dos eventos. Para isso, ele sugere a utilização dos critérios e escalas presentes na Figura 6, tanto para classificar o impacto quanto à frequência.

O modelo abaixo proposto é apenas uma ilustração de como a ferramenta pode ser utilizada, mas cabe ressaltar que cada empresa pode criar a sua própria matriz, condizente com sua propensão ao risco e também com os critérios de classificação.

Figura 6 – Matriz de risco

	Impacto				
Frequência	Insignificante	Mínimo	Moderado	Alto	Catastrófico
Quase certo					
Provável					
Possível					
Improvável					
Raro					

Fonte: Adaptado de COSO (2012b)

As análises qualitativas, como a matriz de risco, são normalmente empregadas quando não há como quantificar características dos riscos, ou quando não existem dados confiáveis em quantidade suficientes para avaliações quantitativas ou ainda, como ocorrem em muitas pequenas e médias empresas, quando o custo-benefício para sua análise não é viável (ARENA et al., 2011). Elas têm como objetivo permitir a incorporação de aspectos subjetivos na análise, possibilitando incorporar aspectos intangíveis na avaliação (MILLET e WEDLEY, 2002).

Normalmente, as avaliações de riscos se fazem através de uma combinação de técnicas tanto qualitativas quanto quantitativas. Estas últimas são utilizadas em situações mais complexas e sofisticadas e trazem mais precisão às avaliações e, devido às suas próprias características, exigem um rigor metodológico mais apurado e requerem dados mais confiáveis; além disso, os modelos matemáticos utilizados muitas vezes são complexos e de difícil aplicação (ARENA et al., 2011). As técnicas quantitativas mais comuns são (COSO, 2007; DANTAS et al., 2010):

a) **Referências de mercado (*benchmarking*):** utilizadas para comparações em eventos ou processos específicos, comparam medições e resultados utilizando métricas comuns, bem como identificam oportunidades de melhoria. A comparação é realizada

com outras empresas ou entidades que atuam no mesmo mercado ou em outros semelhantes.

b) **Modelos probabilísticos:** modelos matemáticos utilizados para avaliar a probabilidade de ocorrência e respectivos impactos de determinados eventos, sob determinadas condições e premissas. Com base em dados históricos ou simulações, busca-se avaliar resultados futuros. Um exemplo é o *Value at Risk* (VaR), muito utilizado para cálculo de risco de mercado, nas distribuições de perdas para cálculo do risco de crédito ou de risco operacional, entre outros;

c) **Modelos não probabilísticos:** normalmente são realizados através de análises de critérios subjetivos, que podem também ser baseados em dados históricos ou através de simulações, ou ainda através de análises qualitativas. Incluem-se nessa categoria as medições de sensibilidade, testes de estresse, análises de cenários, entre outros. A matriz de riscos pode ser classificada como modelo não probabilístico.

4.2.5 Tratamento dos riscos

O tratamento dos riscos ocorre depois da etapa de avaliação. A eliminação total dos riscos é praticamente impossível. Dessa forma, a empresa deve direcionar seus recursos de acordo com a priorização estabelecida na etapa anterior de avaliação e assim reduzir as probabilidades ou impactos que eventos adversos possam causar à organização. É ainda altamente recomendável que haja um alinhamento entre a estrutura de controle, os objetivos estratégicos e o nível de exposição desejado pela empresa (IBGC, 2007).

Assim a organização estabelece quais tipos de tratamentos serão utilizadas para cada risco identificado e avaliado. Para o COSO (2004b p.55), os tratamentos ou respostas aos riscos são:

a) **Evitar:** descontinuação das atividades que geram riscos. Evitar riscos que possam implicar a descontinuação de uma linha de produtos, o declínio da expansão em um novo mercado geográfico ou a venda de uma divisão.

b) **Reduzir:** são adotadas medidas para reduzir a probabilidade ou o impacto dos riscos, ou até mesmo, ambos. Tipicamente, esse procedimento abrange qualquer uma das centenas de decisões do negócio no dia a dia.

c) **Compartilhar:** redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco. As técnicas comuns compreendem a aquisição de produtos de seguro, a realização de transações de *hedge* ou a terceirização de uma atividade.
d) **Aceitar:** nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos.

Ainda segundo o COSO (2007, p. 62):

> 'Evitar' sugere que nenhuma opção de resposta tenha sido identificada para reduzir o impacto e a probabilidade a um nível aceitável. 'Reduzir' ou 'Compartilhar' reduzem o risco residual a um nível compatível com as tolerâncias desejadas ao risco, enquanto 'Aceitar' indica que o risco inerente já esteja dentro das tolerâncias ao risco.

Na definição dos tratamentos dos riscos, os gestores podem, por exemplo, ter como referência que um risco de baixo impacto e pouca probabilidade de ocorrência não deva requerer muita atenção. Já um risco com elevada chance de ocorrência e um potencial de impacto significativo devem ter um acompanhamento mais próximo e exigir uma atenção maior. Entre esses dois extremos, podem existir diversos outros riscos que deverão ser analisados caso a caso (DANTAS et al., 2010).

O tratamento de riscos, segundo a ISO 31000 (2009), ocorre selecionando e implementando uma ou mais opções de tratamentos e envolve um processo cíclico que compreende as seguintes atividades: avaliação do tratamento de riscos já realizado; decisão se os níveis de risco residual são toleráveis; a definição e implementação de um novo tratamento para os riscos, se não forem toleráveis; e avaliação da eficácia desse tratamento.

As opções não são, de todo o modo, mutuamente exclusivas ou adequadas em todas circunstâncias. As empresas costumam se beneficiar quando há uma combinação de formas de tratamento. Elas podem tomar os seguintes aspectos (ISO 31000, 2009):

a) Ação de evitar o risco ao se decidir não iniciar ou descontinuar a atividade que dá origem ao risco;
b) Tomada ou aumento do risco na tentativa de tirar proveito de uma oportunidade;
c) Remoção da fonte de risco;
d) Alteração da probabilidade;
e) Alteração das consequências;
f) Compartilhamento do risco com outra parte ou partes; e

g) Retenção do risco por uma decisão consciente e embasada.

Entretanto, as empresas devem levar em consideração as limitações de recursos para determinar a estratégia de tratamento. Elas devem avaliar os custos e benefícios que estão envolvidos na seleção das respostas aos riscos, tanto diretos quanto indiretos, além dos custos de oportunidades. Em muitos casos, a quantificação tanto dos benefícios quanto dos custos é difícil, devido a subjetividade (COSO, 2007).

A ISO 31000 (2009) também entende que a seleção da opção mais adequada envolve equilibrar tanto os custos e esforços na execução, quanto os benefícios decorrentes de sua implantação, além de alinhamento com os requisitos legais, regulatórios, responsabilidade social, proteção ambiental, entre outros.

4.3 Gerenciamento de riscos corporativos em pequenas e médias empresas

Diferentemente de grandes corporações, em que as decisões são tomadas com base em análises de dados e objetividade, nas PMEs elas são, em sua maioria, tomadas com base na subjetividade e julgamento dos sócios-administradores (AGRAWAL, 2016).

As pequenas e médias empresas atuam no mesmo ambiente econômico das grandes corporações, mas nem por isso pode-se dizer que atuam em iguais condições, em especial quanto à exposição e gerenciamento dos riscos.

Um estudo realizado por Zacharakis et al. (1999) identificou alguns dos motivos para as falhas de pequenos negócios que incluem tanto causas internas quanto externas. As causas internas incluem gestão fraca, falta de planejamento de gestão de riscos e falhas em adotar um limiar adequado para assumir riscos. Como causas externas incluem-se políticas governamentais, competição com grandes empresas, guerras, desastres naturais e recessões econômicas. Também foi identificado que o excesso de confiança poderia, com frequência, gerar problemas para o insucesso dos pequenos negócios.

De acordo com o Centro de Consultoria e Pesquisa do Instituto de Contadores Públicos da Inglaterra e País de Gales (VIRDI, 2005) e o Governo de Singapura (2012), os principais desafios enfrentados pelas PMEs são: altos níveis de *turnover* de empregados, escassez de mão de obra qualificada, riscos de TI, mudanças de mercados e comprometimento de imagem.

Raghavan (2005) identificou em seu trabalho que os principais riscos que correm as PMEs são: baixa abordagem profissional, dependência excessiva em poucos funcionários chaves, falta de alavancagem da estrutura financeira, competição intensiva, baixa lucratividade, inabilidade de acompanhar o avanço tecnológico, altas taxas de *turnover* e conhecimento raso do mercado.

Dado todo esse cenário, é de extrema importância que os gestores das PMEs tenham consciência que a perpetuação e o crescimento de suas empresas são influenciados diretamente pelo modo como fazem a gestão dos riscos.

De acordo com Watt (2007) a gestão dos riscos em pequenas e médias empresas normalmente é reflexo da forma que os donos agem perante as ameaças e oportunidades. Isso não significa que os riscos não estejam sendo administrados, mas os donos das empresas o fazem de modo bastante empírico e simplista. De modo geral, eles agem utilizando a intuição, que costuma ser bastante aguçada nos empresários.

Todavia, para Nthlane (1995) essa forma de gestão de riscos é ineficaz. As decisões tomadas para controle e resolução de eventuais problemas são reativas, lentas e muitas vezes são analisadas de modo superficial. Ele constata que proprietários de PMEs não possuem conhecimentos suficientes para analisar e utilizar técnicas de redução de riscos (eliminação dos riscos, prevenção do risco, redução, transferência ou aceitação).

O mesmo autor diz ainda que as ações desses empresários são centradas em evitar os riscos em vez de criar métodos próprios de gestão e, quando não podem ser evitados, esses empresários buscam normalmente transferir o risco para seguradoras.

Dessa forma, é essencial que essas empresas implantem processos de gerenciamento de riscos corporativos de modo sistêmico, abrangente, exequível. De acordo com Agrawal (2016), o GRC em PMEs cria vantagens competitivas, especialmente em tempos de crises, porque ele ajuda a identificar oportunidades e a evitar perigos iminentes.

Verbano e Venturini (2013) identificaram um padrão nos estudos recentes sobre gerenciamento de riscos em PMEs, em que os autores centram o foco principalmente nos instrumentos de identificação e avaliação dos riscos, enquanto existe uma lacuna grande em trabalhos que estudam o tratamento dos riscos.

Já Siregar (2015), em seu estudo sobre o gerenciamento de riscos em pequenas e médias empresas da Indonésia, identificou que esses tipos de organizações possuem poucos conhecimentos sobre identificação dos riscos e práticas de gerenciamento de riscos – em

especial, a abordagem sistêmica e de compreensão da identificação dos riscos e o conhecimento teórico das práticas gerenciais.

No mesmo trabalho o autor ainda conclui que as PMEs precisam desenvolver diretrizes para a identificação dos riscos, aprimorar o conhecimento teórico sobre o tema, adaptar os modelos de gerenciamento de riscos para versões mais simplificadas e adequá-los melhor às necessidades desse tipo de empresas.

Brustbauer (2014) afirma que apesar de os empresários serem familiarizados com os seus negócios, eles não são capazes de identificar todos os riscos relacionados à suas empresas. Essa constatação reforça o trabalho de Siregar (2015).

Uma forte abordagem de GRC pode ajudá-los a administrar os riscos em todas suas etapas. Além disso, o GRC também oferece chances de as empresas identificarem oportunidades e vantagens competitivas, deste modo melhorando sua competitividade e sucesso de suas ações. Assim, os administradores das PMEs devem ser encorajados a implementarem o GRC em suas empresas. Apesar de isso demandar um grande esforço, os benefícios no longo prazo justificam o trabalho (BRUSTBAUER, 2014).

Para que a implementação do GRC tenha sucesso e seja realizado da melhor forma possível, é imprescindível o apoio da alta gestão e dos sócios (LUNDQVIST, 2015). Apesar de a implementação do GRC trazer grandes benefícios para as empresas, isso não quer dizer que elas não terão prejuízos implementando essas práticas (STULZ, 2008).

Quando o GRC é colocado em prática de forma insatisfatória ou errada, isso apenas irá gerar uma sensação de insegurança: os riscos serão gerenciados de modo incorreto e isso pode levar a grandes prejuízos (HUDIN e HAMID, 2014). É essencial que não apenas ocorra a implementação do GRC nas PMEs, mas que elas sejam feitas do modo corretos e eficazes.

5 PROCEDIMENTOS METODOLOGICOS

5.1 Conceituação

Do ponto de vista da forma, este trabalho abordou sua análise de modo qualitativo e com objetivo exploratório e descritivo. A pesquisa qualitativa considera que há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números. A interpretação dos fenômenos e a atribuição de significados são básicas no processo de pesquisa qualitativa, não requer o uso de métodos e técnicas estatísticas.

Segundo Gil (2008), as pesquisas podem ser classificadas quanto aos objetivos ou quanto aos procedimentos técnicos utilizados. Para este trabalho iremos utilizar esta última abordagem, que pode ser considerada como o delineamento da pesquisa. Ela estabelece a forma de trabalhar os dados coletados. "O delineamento refere-se ao planejamento da pesquisa em sua dimensão mais ampla, que envolve tanto a diagramação quanto a previsão de análise e interpretação de coleta de dados". (GIL, 2008, p.43).

A técnica escolhida é a pesquisa ação, definida por Thiollent (2007, p.16) como:

> A pesquisa ação é um tipo de pesquisa social com base empírica que é concebida e realizada em estreita associação com uma ação ou com a resolução de um problema coletivo e no qual os pesquisadores e os participantes representativos da situação ou do problema estão envolvidos de modo cooperativo ou participativo.

Nesse tipo de trabalho, o pesquisador tem participação ativa, assim como todos os outros envolvidos na situação-problema. Justamente por essa forma de participação e pela presença de uma grande interação colaborativa entre pesquisador e os participantes, Gil (2008) alerta que deve haver um cuidado para que não se perca a objetividade que se exige na pesquisa científica, principalmente no que se refere à análise e interpretação dos dados obtidos com o estudo.

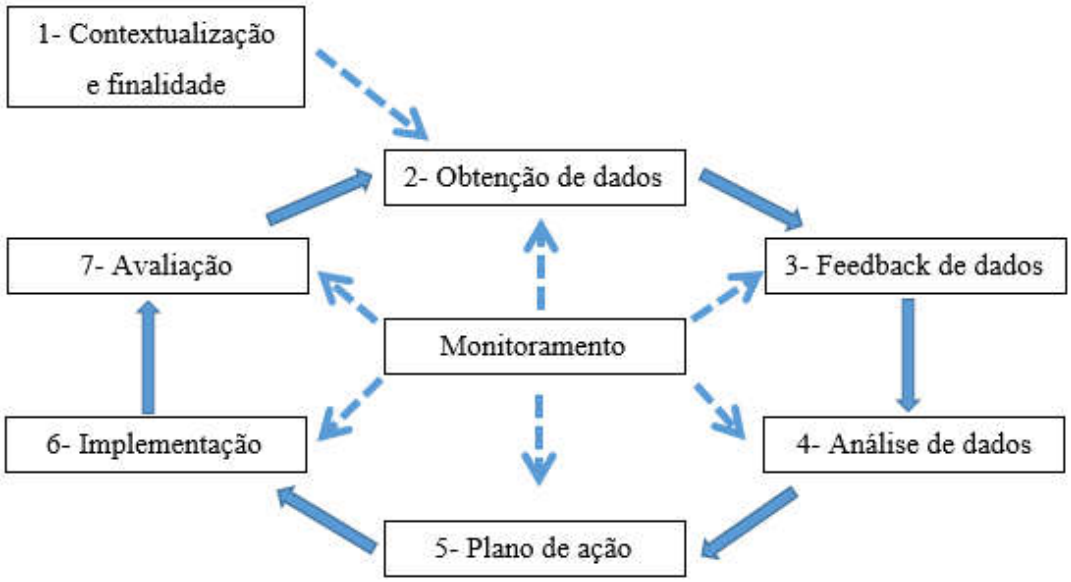
5.2 Pesquisa ação

Para Coghlan (2002), a pesquisa ação é uma abordagem que tem como finalidade a construção de um conhecimento ou teoria sobre a ação que tenha sido tomada diante de

determinado problema. O fato de o autor desta dissertação ser funcionário na empresa objeto deste estudo e a necessidade de aprofundar seu conhecimento na gestão de riscos em pequenas empresas, levou-o à escolha do método da pesquisa ação.

As etapas para a pesquisa ação, segundo Coghlan (2002) são:

Figura 7 – Ciclo da pesquisa ação



Fonte: Traduzido de Coghlan, 2002.

Dentro desse contexto, o pesquisador como ator participante da pesquisa ação buscou identificar quais os principais riscos presentes na empresa objeto de estudo deste trabalho, tendo como embasamento teórico o modelo teórico proposto por Oliva (2016), abrangendo toda sua cadeia valor.

Seguindo as diretrizes propostas pela ISO 31000 (2009) e o COSO (2007), analisou ainda quais as principais fontes e causas desses riscos e classificou-os conforme o tipo e natureza. Além disso avaliou quais as probabilidades de ocorrência de cada um deles e mensurou o impacto e a relevância que cada evento pode gerar à organização. Tendo todos os dados organizados e analisados, foi proposta uma estratégia para tratamento e mitigação dos riscos identificados.

Como contribuição acadêmica, além de uma visão crítica sobre a importância do GRC em pequenas e médias empresas de TI e uma análise sobre os principais riscos presentes nesse setor, esta dissertação irá também propor uma estratégia de tratamento para os riscos avaliados.

Para o desenvolvimento desta pesquisa, o pesquisador utilizou as seguintes técnicas de intervenção:

a) Entrevistas semiestruturadas com os sócios da empresa.
b) Reuniões com funcionários da empresa analisada;
c) Reuniões com os sócios da empresa.
d) Pesquisa bibliográfica sobre o tema de Gestão de Riscos;
e) Coleta e levantamento de dados primários;
f) Coleta e levantamento de dados secundários;

Para cada etapa da pesquisa ação apresentada na Figura 7, serão detalhadas as formas que as ferramentas acima foram utilizadas, quais dados foram possíveis de serem obtidos e de que modo as informações foram trabalhadas e analisadas.

5.3 Etapas da pesquisa ação

1- Contextualização e finalidade

Para esta etapa – a primeira – o pesquisador deve responder a dois principais questionamentos: um deles é sobre o porquê esse projeto é necessário, e o outro é contextualizar, indicando quais forças sociais, políticas, econômicas e técnicas levam à necessidade de uma ação.

Deste modo, o autor agendou uma primeira reunião com os sócios-diretores da empresa estudada a fim de explicar o contexto ao qual a empresa está inserida e apresentou a importância do trabalho desenvolvido.

Além da alta administração, o pesquisador também realizou reuniões com alguns funcionários da empresa, que ajudaram na coleta dos dados e acompanhamento do projeto, para que também estivessem alinhados sobre a pesquisa, do mesmo modo que os diretores.

2- Obtenção dos dados

Na segunda etapa, munido de informações e instruções obtidas na etapa anterior, o pesquisador agendou entrevistas, seguindo um roteiro preestabelecido com os sócios da empresa, as quais foram realizadas individualmente, em sessões únicas e registradas em formulários, para consultas posteriores.

Nessa etapa, o pesquisador buscou identificar, pela percepção dos sócios, quais são os principais riscos presentes na cadeia de valor da empresa, quais impactos eles podem levar e quais as probabilidades de ocorrência. Além disso, quais seriam, em suas opiniões, as melhores formas de tratamento dos mesmos.

Além da visão dos sócios, o pesquisador buscou também coletar dados primários e informações através de reuniões com alguns funcionários da empresa, que foram selecionados conforme o acesso que possui a determinadas informações, sendo estas todas relacionadas à gestão de riscos.

Outras formas de coleta de dados foram realizadas através de acesso a sistemas com dados financeiros, documentos e relatórios contábeis, documentos com informações gerenciais, além de outros documentos que podiam ser utilizados pelo pesquisador. Tendo o pesquisador como um autor na busca de uma solução para situação-problema, muitas informações foram obtidas de forma empírica, no ambiente de trabalho que o pesquisador se encontra.

Como gerente financeiro da empresa estudada, o autor tem acesso a todos esses documentos, sistemas e informações.

3- Feedback de dados

Após a segunda etapa, o autor realizou uma análise sobre a qualidade e quantidade das informações, bem como a importância de cada um deles – terceira etapa. Foi-se constatado que eles eram suficientes para a conclusão da pesquisa e não foram necessárias novas reuniões e entrevistas, nem coleta de mais dados, sejam eles primários ou secundários.

4- Análise de dados

De posse das entrevistas, relatórios e informações, o autor passou a estruturar melhor esses dados obtidos – quarta etapa – tornando possível uma análise mais profunda dos riscos que estão presentes no ambiente da empresa estudada.

Esta análise buscou apresentar a visão dos sócios-diretores entrevistados, bem como a visão deste autor, que possui participação ativa na pesquisa-ação. Sabendo da importância da imparcialidade sobre o trabalho, o pesquisador se ateve às informações obtidas nas etapas anteriores preocupando-se, o quanto possível, em fazer suas análises de modo imparcial.

Tendo como característica a pesquisa qualitativa e descritiva, não foram realizados cálculos ou extrapolações, mas sim uma análise muito mais detalhada e profunda, que os métodos quantitativos não conseguem explorar.

Para a análise dos dados, utilizou-se a técnica de triangulação. Essa técnica permite que a o fenômeno estudado seja abordado de diferentes formas, ou por meio de métodos múltiplos, em tempos e com base em fontes diferentes (EASTERBY-SMITH, et al, 1999). Para Weiss (1998), quando se utiliza o referido método as evidências obtidas são consideradas fortes, pois se reduzem eventuais vieses no processo de coleta.

Outra técnica utilizada foi adequação ao padrão. A lógica é a comparação de um padrão fundamentalmente empírico com outro de base prognostica (ou com várias outras previsões alternativas). Se o estudo for explanatório, os padrões podem se relacionar às variáveis dependentes ou independentes do estudo (ou a ambas). Se o estudo de caso for descritivo, a adequação ao padrão ainda assim é relevante, já que o padrão previsto de variáveis específicas é definido antes da coleta de dados (YIN, 2005).

5- Plano de ação

No plano de ação, estabelecem-se quais serão as ações a serem tomadas para elaboração da estratégia a ser adotada para o tratamento dos riscos. Para a realização desta etapa, o pesquisador levou em consideração a opinião dos envolvidos no processo de GRC, sua própria experiência e também o que a literatura disponibiliza de informações sobre o tema.

Devido à complexidade do assunto abordado, o tipo de pesquisa, as características da empresa analisada, entre outros fatores, o plano de ação proposto é exclusivo e único para o caso apresentado. Ele serve para ilustrar de modo realista e com riqueza de detalhes como ocorre grande parte do processo de GRC em PMEs do setor de TI.

6- Implementação

A implementação é a própria apresentação da estratégia e do plano proposto para os sócios-proprietários e a conclusão deste trabalho para a comunidade acadêmica e demais interessados no conhecimento sobre gerenciamento de riscos em pequenas e médias empresas do setor de Tecnologia da Informação.

7- Avaliação

A avaliação é a etapa final do ciclo, onde é possível avaliar de fato quais resultados foram gerados com o desenvolvimento e sistemática da solução proposta para a situação-problema. Nota-se que não há necessidade de sucesso quanto ao processo, mas ao final do ciclo, deve gerar conhecimento e aprendizado.

Além disso, não é um processo com apenas um começo, meio e fim, mas ele se torna um ciclo que se retroalimenta e a cada conclusão geram-se novos conhecimentos. A Figura 7 ilustra esse conceito de modo simplificado.

8- Monitoramento

Em cada etapa do ciclo da pesquisa-ação, existe a necessidade de monitoramento a fim de evitar eventuais problemas que possam surgir no andamento do processo. O monitoramento deve ocorrer em tempo real e de modo contínuo.

Essa ação é realizada pelo próprio pesquisador, dando a ele condições de manter sob controle o desenvolvimento da pesquisa e criando condições para obter novos dados e informações que possam ser relevantes para este trabalho.

6 ANÁLISE DOS RESULTADOS

Dado a metodologia de pesquisa, tendo o autor como ator participante do objeto estudado e do tema proposto, de modo empírico, o pesquisador buscou estruturar um modelo de gestão de riscos corporativos que pudesse ser aplicado na empresa em que labora.

Conforme apresentado anteriormente, a empresa estudada não possui hoje qualquer processo formal de gestão de risco. Dentro do contexto das PMEs, ela também não possui recursos para criar um departamento específico para esse fim. O autor desta pesquisa, com o cargo de gerente financeiro, é a pessoa mais próxima à gestão de fato de riscos da empresa, juntamente com os sócios-gestores dela. Desse modo, o modelo de GRC proposto pelo autor foi específico para a empresa que trabalha, dada todas suas particularidades de setor, porte, sociedade e gestão.

Para tanto, o autor baseou-se no modelo teórico de identificação de riscos proposto por Oliva (2016), para a primeira etapa do processo de avaliação e seguiu o que é proposto pela ISO 31000 (2009) e COSO (2007), para as etapas de avaliação e tratamento dos riscos.

Conforme apresentado nos procedimentos metodológicos, o autor buscou fazer a análise utilizando a técnica de triangulação, utilizando pelo menos três perspectivas diferentes para validação dos dados, bem como o uso da técnica de adequação padrão, ao utilizar de modelos existentes na literatura para apoiar no estudo dos dados coletados empiricamente.

Já a adequação ao padrão ocorre na utilização de modelos existentes na literatura e aplicados na prática, na análise da empresa estudada. Diferentes modelos, teorias e normas foram utilizadas na elaboração deste trabalho e a técnica de adequação ao padrão, foi importante, pois permitiu justamente a comparação de um padrão empírico com outro prognóstico.

6.1 Identificação dos riscos da empresa analisada

O modelo proposto por Oliva (2016) para identificação dos riscos foi escolhido pelo autor devido à abordagem mais ampla e sistêmica do gerenciamento dos riscos. O pesquisador busca uma visão que rompa as fronteiras da organização e inclui toda sua cadeia de valor.

Com base em informações coletadas de fontes primárias e secundárias da empresa estudada, reuniões com pessoas envolvidas de alguma forma na gestão de riscos da empresa, entrevistas

semiestruturadas com dois sócios da empresa e conhecimento do próprio autor, foram identificados os principais riscos a que a empresa está sujeita, classificados de acordo com o Modelo de Identificação de Riscos no Ambiente de Valor, proposto por Oliva (2016).

Os principais riscos identificados foram:

Quadro 2 – Principais riscos da empresa avaliada

Identificação	***Natureza***	***Riscos***	***Detalhamento***
A	Riscos operacionais	Descontrole dos custos e despesas	Problemas nos controles de custos e despesas da empresa
B	Riscos operacionais	Problemas contábeis	Falhas nos lançamentos contábeis
C	Riscos operacionais	Não conformidade com as regulações	Problemas ao não seguir à legislação (trabalhista, fiscal, civil etc.) do modo correto, consciente ou inconscientemente;
D	Riscos operacionais	Execução de projetos	Falhas na execução de projetos, ou prejuízo sistema do cliente
E	Riscos financeiros	Inadimplência	Falta de recebimento dos serviços prestados
F	Riscos financeiros	Estratégias financeiras ruins	Tomada de decisões prejudiciais à gestão financeira da empresa
G	Riscos financeiros	Captação de recursos	Problemas gerados devido à captação de empréstimos
H	Riscos estratégicos	Parcerias	Problemas com parceiros
I	Riscos estratégicos	Clientes	Problemas com clientes / queda de demanda
J	Riscos estratégicos	Produtos	Investimento em produtos com baixo retorno
K	Riscos de inovação	Novas tecnologias	Entrada de novos produtos ou empresas no mercado que possam substituir a atual
L	Risco de imagem	Reputação	Problemas com a marca da empresa
M	Riscos de mercado	Crise no setor de atuação	Problemas no setor de TI
N	Riscos de mercado	Problemas econômicos do país	Instabilidade econômica de causas diversas (política, social, ambiental etc.)
O	Riscos legais	Mudança na legislação	Alteração na legislação que possa interferir na empresa
P	Riscos éticos	Informações confidenciais	Acesso indevido a informações sigilosas
Q	Riscos estratégicos	Problemas na sociedade	Saída de algum dos sócios-gestores da empresa
R	Riscos estratégicos	Dependência de funcionários chaves	Concentração de conhecimento e importância em determinados funcionários chaves.

Fonte: Autor (2017)

Um número maior de tipos de riscos traz um detalhamento melhor para o GRC, entretanto quando eles são demais, cria-se uma complexidade que acaba prejudicando. Assim, cada empresa deve avaliar a melhor forma de classificar os riscos a que estão sujeitas e buscar criar um modelo que seja ideal para o setor que atua e a forma que trabalha.

Deste modo, para adequar o modelo à realidade da empresa estudada, ele foi alterado, excluindo o agente "distribuidores" – a empresa atua como prestadora de serviços –, e incluindo o agente "parceiro". Além disso, foram retirados os riscos de sustentabilidade e incluídos os de mercado e o legal. A Figura 8, a seguir, representa a aplicação do modelo de Oliva (2016):

Figura 8 – Aplicação do modelo de identificação de riscos no ambiente de valor

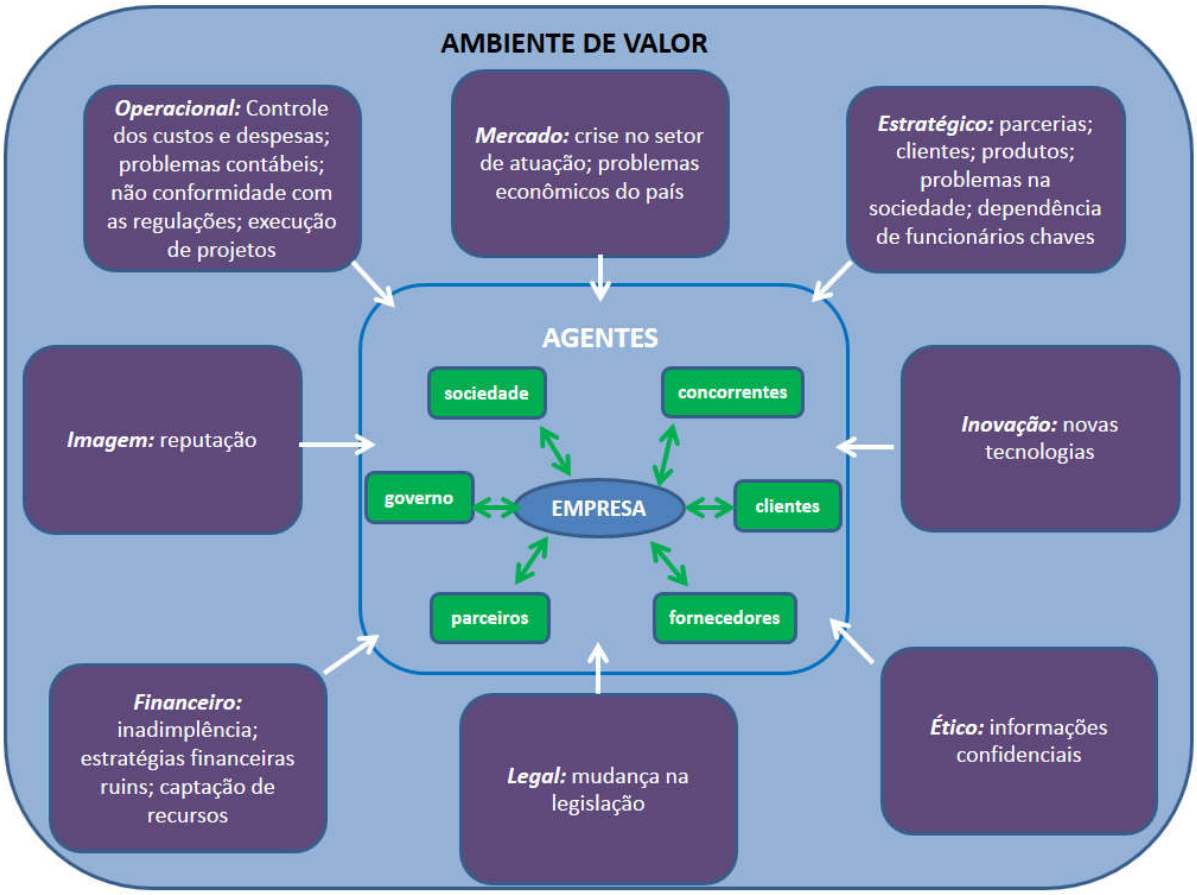
Fonte: Adaptado de Oliva (2016)

As forças presentes no Ambiente de Negócios (político, tecnológico, social, econômico e meio ambiente) estão em constante interação com o Ambiente de Valor e podem afetar

diretamente esse universo, mas há pouca coisa que a organização pode fazer para tentar controlá-los. Diferentemente do que ocorre no Ambiente de Valor, em que a empresa possui mais condições de modificar e algumas vezes até controlar os eventos que ocorrem nessa esfera. Tendo maior controle sobre estes eventos, é possível também ter melhor gestão sobre os riscos.

Muitos deles, que foram identificados no ambiente de valor da empresa analisada, estão também presentes na literatura apresentada na revisão bibliográfica deste trabalho. Mudanças de mercados, comprometimento de imagem, dependência excessiva em poucos funcionários chaves, competição intensiva, inabilidade de acompanhar o avanço tecnológico são alguns desses riscos e que também foram descritos como principais fatores que afetam negativamente as PMEs em países como Inglaterra, País de Gales, Singapura e Índia (VIRDI, 2005; GOVERNO DE SINGAPURA, 2012; RAGHAVAN, 2005). A figura 9 apresenta os principais riscos identificados na empresa e classificados de acordo com sua natureza.

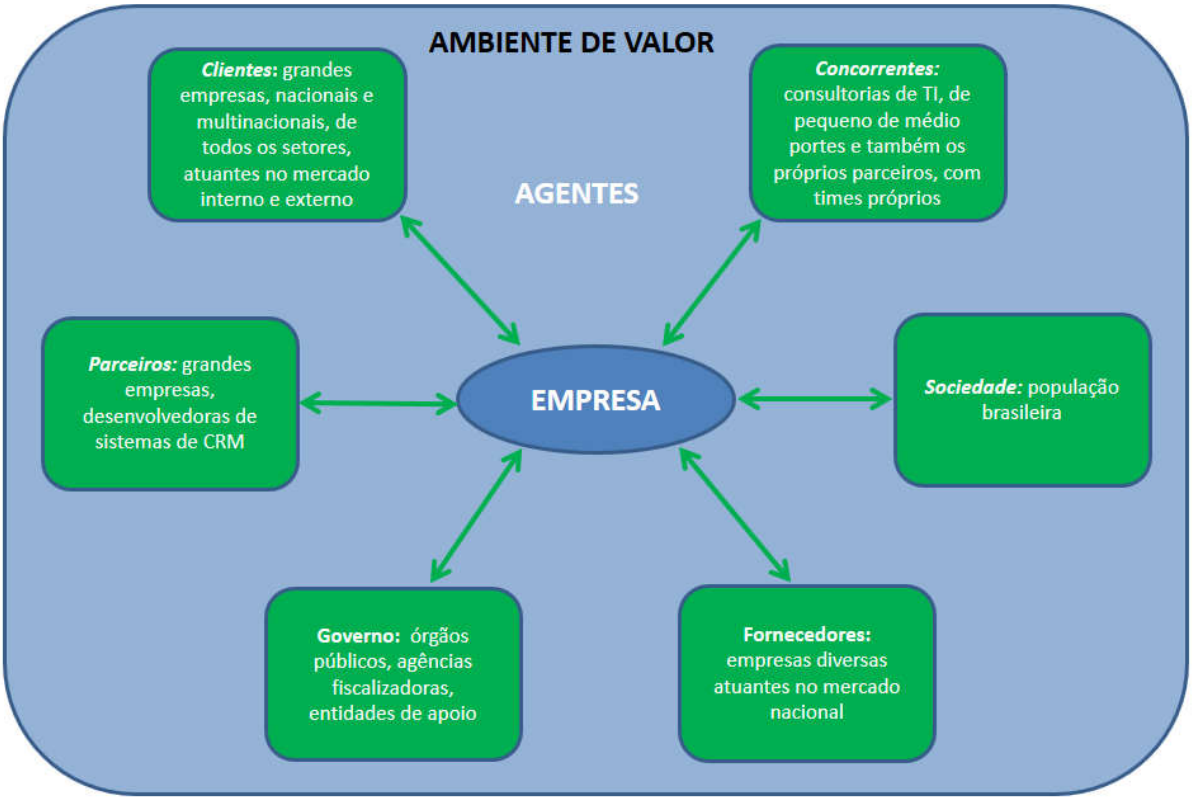
Figura 9 – Riscos no ambiente de valor



Fonte: Autor (2017)

De acordo com o modelo de Oliva (2016), os principais riscos advêm da interação entre os agentes com os quais a empresa possui algum tipo de conexão. Os agentes são diversos em quantidades, tipos, estruturas e complexidade e foram caracterizados na figura 10 abaixo. Como o processo de GRC não é estático, essa estrutura do modelo também não é e os gestores devem ficar atentos quanto às modificações que possam surgir para que a identificação dos riscos não fique comprometida.

Figura 10 – Agentes do ambiente de valor



Fonte: Autor (2017)

O processo é complexo, pois determinada entidade pode ser mais de um agente dentro do modelo e um mesmo agente pode ser o causador de mais de um tipo de risco. No caso específico da empresa avaliada, uma única organização possui relação com a empresa como parceiro, cliente, concorrente e fornecedor e pode ser fonte de mais de um risco. O Quadro 3 a seguir ilustra a situação.

Quadro 3 – Agentes dos riscos

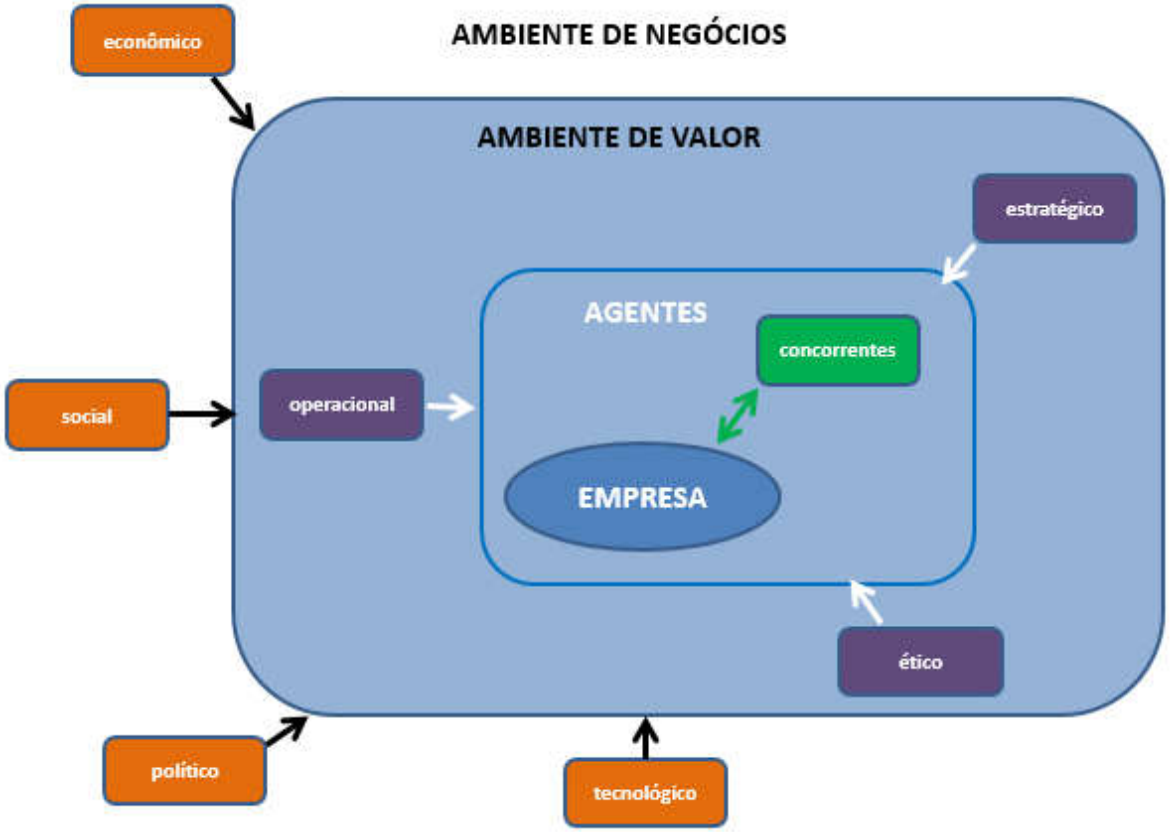
Agentes	*Natureza*	*Riscos*
Empresa, concorrentes	Riscos operacionais	Controle dos custos e despesas
Empresa, fornecedores	Riscos operacionais	Problemas contábeis
Empresa	Riscos operacionais	Não conformidade com as regulações
Clientes	Riscos operacionais	Execução de projetos
Clientes	Riscos financeiros	Inadimplência
Fornecedores	Riscos financeiros	Estratégias financeiras ruins
Fornecedores	Riscos financeiros	Captação de recursos
Parceiros	Riscos estratégicos	Parcerias
Clientes, concorrentes	Riscos estratégicos	Clientes
Empresa, clientes	Riscos estratégicos	Produtos
Concorrentes	Riscos de inovação	Novas tecnologias
Clientes, fornecedores	Risco de imagem	Reputação
Governo	Riscos de mercado	Crise no setor de atuação
Governo	Riscos de mercado	Problemas econômicos do país
Governo	Riscos legais	Mudança na legislação
Empresa, concorrentes	Riscos éticos	Informações confidenciais
Empresa	Riscos estratégicos	Problemas na sociedade
Empresa	Riscos estratégicos	Dependência de funcionários chaves

Fonte: Autor (2017)

A relação da empresa, por exemplo, com os clientes, pode gerar riscos operacionais (execução de projetos), financeiros (inadimplência), estratégicos (clientes) e de imagem (reputação). Às vezes, os riscos surgem internamente da própria empresa, e em sua maioria são os riscos operacionais, ou seja, falhas nos próprios processos internos da organização, mas não, necessariamente, se restringindo a eles.

No caso analisado, por exemplo, a interação entre a empresa e os concorrentes podem levar a riscos operacionais, estratégicos ou éticos, dentro do seu ambiente de valor. Além disso, esses mesmos riscos podem sofrer interferência de agentes do ambiente de negócios, como econômico, social, político e tecnológico. A Figura 11, a seguir, representa essa interação. Ou seja, os riscos não devem ser avaliados de modo isolado. Pelo contrário, devem-se analisar o contexto em que ele está inserido, suas relações com outros agentes e quais influencias externas eles podem sofrer.

Figura 11 – Interação entre empresa e concorrentes



Fonte: Autor (2017)

6.2 Avaliação dos riscos da empresa analisada

Todos os riscos devem entrar em alguma das classificações propostas, conforme sua natureza e, posteriormente, eles devem ser detalhados quanto às suas causas, consequências e probabilidade de ocorrência, e quais impactos podem gerar para a empresa.

No entanto, nem todos os riscos precisarão de gerenciamento. É nesta etapa de avaliação que serão analisados quais riscos necessitarão de acompanhamento ou intervenção, e quais não. Para que isso seja possível, eles devem ser analisados com maior detalhamento. Esta etapa de avaliação dos riscos irá seguir as diretrizes do COSO (2007), com uso da ferramenta de matriz de riscos, para análise da probabilidade e impacto dos riscos.

As causas e consequências dos riscos identificados são descritos abaixo:

Quadro 4 – Causas e consequências dos riscos

Riscos	***Causas***	***Consequências***
Descontrole dos custos e despesas	Falha humana, falta de conhecimento, aumento da concorrência	Precificação errada dos projetos, falha no planejamento financeiro, estabelecimento dos *budgets*, pressão por preços menores
Problemas contábeis	Falha humana, falta de conhecimento	Problemas fiscais (cálculo errado dos impostos) e análise financeiras errados
Não conformidade com as regulações	Falta de conhecimento, divergência de interpretação	Autuação dos órgãos do governo, responsáveis pela fiscalização
Execução de projetos	Falha humana, falta de conhecimento	Retrabalho, multas, quebra de contratos
Inadimplência	Clientes com problemas financeiros, análise de crédito mal realizado	Problemas de fluxo de caixa
Estratégias financeiras ruins	Prazos muito longos de recebimento ou muito curto para pagamentos	Problemas de fluxo de caixa
Captação de recursos	Captação de empréstimos muito altos, juros altos	Falta de condições para pagamento do empréstimo
Parcerias	Escolha dos parceiros errados, conflito com parceiros	Dificuldades de geração de receitas
Clientes	Perda de um cliente importante, entrada de novos clientes	Perda de receitas e dificuldades de geração de novas receitas
Produtos	Desenvolvimento de produtos que o mercado não aceite	Baixa rentabilidade
Novas tecnologias	Mercado altamente inovador	Tornar a tecnologia atual que a empresa utiliza obsoleto
Reputação	Experiências ruins com clientes, reclamações que se tornam públicas e prejudicam a imagem da empresa	Perda de confiança dos clientes e potenciais clientes
Crise no setor de atuação	Crise no setor que a empresa atua	Dificuldades de geração de receitas
Problemas econômicos do país	Diminuição da atividade econômica do país	Dificuldades de geração de receitas
Mudança na legislação	Interferência do Governo no mercado	Alteração no modo de criação de valor da empresa
Informações confidenciais	Acesso de pessoas indevidas a informações estratégicas da empresa	Possibilidade de perder a vantagem competitiva para os concorrentes
Problemas na sociedade	Morte, briga, aposentadoria, estilo de vida (perda de pessoa chave da empresa)	Problemas de gestão, perda de contatos importantes, perda de confiança e credibilidade
Dependência de funcionários chaves	Delegação de atividades chaves, acesso a contatos importantes, descentralização de poder	Perda de clientes importantes, falhas operacionais, perda da continuidade de projetos importantes

Fonte: Autor (2017)

Na avaliação dos riscos, estes devem ser analisados quanto à probabilidade de ocorrência e impacto do evento. Assim, serão classificados utilizando gradação de frequência (do menor para o maior): raro, improvável, possível, provável e quase certo. Para classificação do impacto, utilizou-se a gradação (também do menor para maior): insignificante, mínimo, moderado, alto e catastrófico.

A Quadro 5 representa a classificação dos riscos identificados:

Quadro 5 – Probabilidade e impacto dos riscos

Riscos	***Probabilidade de ocorrência***	***Impacto do evento***
Controle dos custos e despesas	Possível	Alto
Problemas contábeis	Possível	Moderado
Não conformidade com as regulações	Possível	Moderado
Execução de projetos	Provável	Mínimo
Inadimplência	Provável	Moderado
Estratégias financeiras ruins	Improvável	Alto
Captação de recursos	Raro	Alto
Parcerias	Improvável	Catastrófico
Clientes	Possível	Moderado
Produtos	Improvável	Alto
Novas tecnologias	Raro	Catastrófico
Reputação	Raro	Alto
Crise no setor de atuação	Improvável	Moderado
Problemas econômicos do país	Possível	Moderado
Mudança na legislação	Possível	Alto
Informações confidenciais	Improvável	Alto
Problemas na sociedade	Possível	Alto
Dependência de funcionários chaves	Possível	Alto

Fonte: Autor (2017)

Apesar de a análise de probabilidade de ocorrência *versus* impacto do evento ocorrer primordialmente de forma qualitativa, em alguns dos riscos avaliados, dados numéricos podem ser levados em consideração, dando direções tanto para definição da probabilidade quanto do impacto.

O descontrole dos custos e despesas ocorre quando não há acompanhamento dos gastos ao realizar implantação de projetos em clientes ou quando não se consegue controlar gastos necessários para a realização das atividades de suporte da empresa. Isso pode ocorrer por falha humana ou falta de conhecimento dos funcionários, ao estabelecer parâmetros importantes para a empresa de forma equivocada, como o custo/hora dos consultores, que pode levar a precificações erradas na venda de projetos, ou um planejamento financeiro com falhas, fazendo com que a empresa defina orçamentos de gastos superdimensionados. Outra

causa pode ser o aumento da concorrência, gerando pressão por preços menores, fazendo com que o planejamento de vendas não se concretize e a empresa fique com uma estrutura muito grande para o volume de serviços prestados, levando a uma ociosidade muito grande e descontrole dos gastos. Como a atividade é realizada de modo interpretativo por funcionários, existe a possibilidade de ocorrência e o seu impacto é elevado, pois interfere diretamente na operação da empresa.

Os problemas contábeis podem ter como causas também a falha humana, por alguma falta de atenção ou pela própria falta de conhecimento. As consequências são principalmente de ordens fiscais, como cálculos equivocados de impostos, mas também podem levar a análises financeiras erradas, fazendo com que a empresa tome decisões com base em informações irreais. A empresa analisada possui uma empresa terceirizada para as atividades de contabilidade, mas ainda assim, elas são desempenhadas por pessoas, que são falíveis. Do mesmo modo do risco anterior, é possível que ela ocorra e tem um impacto moderado, pois gera custos por falhas, reduzindo a lucratividade da empresa, mas não a ponto de levar ao fechamento da organização.

A não conformidade com as regulações podem vir de diversas esferas, como federal, estadual ou municipal, bem como diversas áreas (fiscal, trabalhista, societária, ambiental, etc). A legislação no Brasil é bastante confusa, caótica e complexa, o que por divergências de interpretação ou mesmo falta de conhecimento pode levar empresários a não seguir o que regra o Governo. A principal consequência são as autuações dos órgãos de controle. Justamente por essas características da legislação do país e a dificuldade de interpretação, é possível que o risco ocorra e o impacto é moderado, pois pode levar a multas diversas.

Alguns riscos de natureza operacional, como falha na execução de projetos, têm como principais consequências o retrabalho, multas por não cumprimento de contratos ou até mesmo a quebra deles. As principais causas são falha humana ou falta de conhecimento. Por isso o processo de aprendizado se torna tão importante em serviços de consultoria. A falta de experiência muitas vezes é o principal causador de falhas no desenvolvimento de projetos. Como os projetos fazem parte do dia-a-dia da empresa, como parte fundamental do *core business*, é provável que o risco ocorra, entretanto, o impacto é pequeno.

Os riscos financeiros de inadimplência e estratégias financeiras ruins levam a problemas de fluxo de caixa. A inadimplência porque obviamente se a empresa não recebe o que lhe é devido, acaba tendo dificuldades para pagar os custos correspondentes e a estratégia financeira ruim pode levar a desequilíbrios de caixa, como um prazo de pagamento menor que o de recebimento, por exemplo, ou gerar situações que exija maior necessidade de caixa

desnecessariamente, levando a um risco de inadimplência da própria empresa. Como a empresa já utiliza um indicador de prazo médio de recebimento e prazo médio de pagamento, a chance de ocorrer um desequilíbrio é baixo, mas o impacto é alto. Já para a inadimplência, como qualquer operação, é provável que isso ocorra um dia, entretanto o impacto varia conforme o tamanho do projeto ou como foram negociadas as condições de recebimento, no caso, colocou-se moderado devido à essa condição.

Apesar de a empresa raramente buscar captação de recursos externos, a possibilidade existe e como qualquer financiamento, o risco de contrair uma dívida que não consiga ser paga, apesar de baixa, ela existe e o impacto é alto.

Como relatado anteriormente, a empresa analisada é parceira de uma grande multinacional do setor de TI. A relação é bastante próxima, sendo que a empresa parceira ajuda na geração de receitas. Essa relação, caso deixe de ser benéfica para ambas as partes, torna-se muito ruim para a parte mais vulnerável, que é a empresa avaliada. Esta última é uma das maiores parceiras, em implantação de projetos de CRM, sendo uma das referências de parceiros. A probabilidade de ocorrer algum problema a ponto de levar a quebra da relação é improvável e ao mesmo tempo o impacto pode ser catastrófico, fazendo com que o contrato existente entre ambas finalizem e a empresa deixe de operar com os produtos dessa marca.

Nesse mercado que a empresa atua, as relações comerciais costumam ser duradouras, ou seja, após a implantação do projeto, muitas vezes o relacionamento permanece com os serviços de suporte. Assim, a carteira de clientes não costuma ser extensa e os contratos comerciais costumam ter valores significativos. Perder um cliente importante pode ser bastante prejudicial para a empresa, por isso manter uma boa relação com os clientes é extremamente importante. A empresa atualmente possui aproximadamente em sua carteira 25 clientes ativos, sendo que 10 deles representam por 50% do faturamento global. Não há uma grande concentração, por esse motivo a probabilidade foi considerada possível e o impacto moderado.

Como um dos pilares de receitas é o desenvolvimento de produto, outro risco pode ser justamente o uso de recursos e esforço no desenvolvimento de um sistema que o mercado não aceite. A receita advinda de sua comercialização pode não ser suficiente para cobrir os custos de desenvolvimento e comercialização. O produto já existe e as melhorias são mais incrementais, não havendo necessidade de um esforço muito grande para desenvolvimento do início, além disso, já existem cases de sucesso com grandes empresas. O risco de iniciar um novo produto ou que as melhorias exijam muito esforço são pouco prováveis, mas caso ocorra, o impacto é alto.

O mercado de Tecnologia da Informação é altamente dinâmico e inovador. Assim, a empresa deve ficar atenta quanto ao surgimento de novas tecnologias que possam vir a substituir as atuais. Esse processo normalmente é lento e costuma ser possível mapear atividades relacionadas a novas tecnologias. Por essa razão a probabilidade de isso ocorrer é raro, mas caso ocorra o impacto é catastrófico e a empresa deve conseguir se reestruturar para se adaptar ao novo cenário.

Um dos piores problemas para uma empresa é ter sua reputação denegrida. Isso pode afetar diretamente as vendas, faz com que o s clientes percam a confiança e principalmente afeta na captação de novos clientes. As causas podem ser diversas, como experiências ruins em projetos, alguma reclamação que se torna pública e prejudique a imagem da empresa, alguma notícia ruim que por acaso possa envolver o nome da empresa, entre outros. Probabilidade bem baixa e impacto bem elevado.

Os riscos de origem externa como alguma crise no setor de atuação da organização ou algo mais abrangente, como problemas econômicos no país inteiro, acabam afetando não apenas a empresa, mas diversas outras. As pessoas acabam não consumindo, o que reduz as receitas das organizações, o que leva a uma redução dos investimentos como um todo e prejudica toda a economia.

Outro risco que a empresa possui muito pouco controle é quando há alguma alteração da legislação vigente e que pode afetar diretamente a forma de gestão e operação dela. Isso pode alterar totalmente o modo de criação de valor, das mais diferentes formas, como prejudicando a geração de receitas, ou alterando os custos diretos ou ainda, modificando o modo de gerir e operacionalizar a empresa.

O acesso de pessoas indevidas às informações confidenciais da empresa também pode ser um risco. A organização pode perder sua vantagem competitiva, caso dados estratégicos fiquem acessíveis a concorrentes ou pessoas que possam vir a prejudicar a empresa. Esse risco é difícil de prever, mas também é verdade que a empresa investe pouco em segurança. A probabilidade é baixa e o impacto é elevado.

Problemas na sociedade também podem ocorrer e gerar consequências desastrosas para a organização. Cada sócio exerce um papel fundamental na empresa e atuam diretamente na gestão e operação da mesma. Caso por qualquer motivo, um deles decida se retirar da sociedade, pode causar um grande impacto negativo, como problemas de gestão, perda de contatos importantes, perda de confiança dos funcionários e clientes e perda de credibilidade. As causas para que isso ocorra também pode ser bastante variada, como o falecimento de algum deles, briga diversas, aposentadoria, mudança no estilo de vida, entre outros.

Por fim, a dependência de funcionários chaves acaba ocorrendo conforme a empresa cresce e precisa delegar atividades vitais na responsabilidade de funcionários igualmente importantes. Além disso, pela função desempenhada, esses funcionários têm acesso também a contatos importantes e caso algum deles deixe de trabalhar na empresa, ela pode acabar perdendo clientes relevantes, os projetos e atividades desempenhadas por esses funcionários podem perder sua continuidade e podem levar consigo informações importantes da empresa. A empresa cerca de 6 funcionários chaves, que representa algo em torno de 7,5% do total de funcionários, todos com longo tempo de atuação pela empresa, com conhecimento técnico, histórico de muitas situações vividas na organização e conhecem a fundo a forma de a empresa trabalhar.

Tanto os problemas na sociedade quanto a dependência dos funcionários chaves são possíveis de ocorrerem e têm um impacto elevado.

A partir dessas informações, a empresa deve avaliar, com base em seu perfil de risco, quais serão aceitáveis, quais deles ficarão sob atenção e quais riscos são inaceitáveis para a organização.

Para esse tipo de análise, ela não deve ficar restrita apenas aos aspectos tangíveis e que foram mensurados, mas também deve avaliar de modo qualitativo, incluindo informações que são importantes para a análise, mas que não passaram pelas etapas de mensuração.

Uma boa forma de avaliar isso é utilizar a matriz de riscos, que avalia o impacto do evento x probabilidade de ocorrência e, através dela, verificar quais eventos ficaram dentro da faixa de aceitável (verde), intermediária (amarela) e inaceitável (vermelha).

A matriz ou mapa de riscos, a seguir (Figura 12), foi criada para refletir o apetite de risco da empresa. A área verde indica a região de exposição aceitável, a zona vermelha representa a exposição inaceitável, enquanto a área amarela indica a zona intermediária de exposição ao risco.

Figura 12 – Matriz de riscos

Probabilidade de ocorrência						
	Quase certo					
	Provável					
	Possível					
	Improvável					
	Raro					
		Insignificante	Mínimo	Moderado	Alta	Catastrófico
	Impacto do evento					

Fonte: Autor (2017) baseada no modelo do IBGC (2007)

Cada organização deve gerar a sua matriz, de acordo com o seu perfil de aceitação dos riscos. Por meio dessa matriz, é possível estabelecer prioridades de tratamento e planejar melhor quais serão as ações a serem tomadas para cada risco identificado e analisado.

Os riscos identificados por algarismos alfabéticos de acordo com a tabela 2 acima, foram então classificados na matriz de acordo com sua probabilidade de ocorrência e impacto do evento, conforme o mapa de risco abaixo (Figura 13):

Figura 13 – Matriz de riscos da empresa avaliada

Probabilidade de ocorrência						
	Quase certo					
	Provável					
	Possível			B, C, I, N	A, E, O, Q, R	
	Improvável		D		F, M, P	H
	Raro				G, J, L	K
		Insignificante	Mínimo	Moderado	Alto	Catastrófico
	Impacto do evento					

Fonte: Autor (2017) baseada no modelo do IBGC (2007)

Como pode-se verificar, alguns riscos ficaram na faixa de exposição aceitável e outros na faixa de risco que necessitam de atenção (zona intermediária). Nenhum deles se apresentou na faixa de exposição inaceitável. A partir dessa matriz, torna-se possível estabelecer estratégias para o gerenciamento de riscos.

É importante salientar que o gerenciamento dos riscos não ocorre de modo estático, pelo contrário, os riscos estão em constantes mudanças e, ao longo do tempo, sofrem alterações que podem levá-los a mudanças na classificação da matriz levando a empresa a alterar as prioridades e formas de tratamento.

Para o estágio de maturidade do GRC, disponibilidade de recursos e custo e eficiência da análise, os envolvidos na gestão da organização optaram por não utilizar qualquer tipo de análise quantitativa/probabilística. Além da insuficiência de dados disponíveis para a sua realização, o esforço e custo para essa análise não seriam adequados.

Nessa etapa, deve-se também definir o modo de priorização para o tratamento dos riscos. Cada empresa define quais critérios serão levados em conta nessa análise, grau de importância de cada um deles e assim, estabelecer sua lista de prioridades.

A empresa analisada seguiu a seguinte priorização:

Quadro 6 – Priorização dos riscos

Identificação	***Riscos***	***Prioridade***
A	Controle dos custos e despesas	1º
B	Problemas contábeis	4º
C	Não conformidade com as regulações	4º
D	Execução de projetos	7º
E	Inadimplência	1º
F	Estratégias financeiras ruins	3º
G	Captação de recursos	6º
H	Parcerias	2º
I	Clientes	4º
J	Produtos	6º
K	Novas tecnologias	5º
L	Reputação	6º
M	Crise no setor de atuação	3º
N	Problemas econômicos do país	4º
O	Mudança na legislação	1º
P	Informações confidenciais	3º
Q	Saída de algum dos sócios-gestores da empresa	1º
R	Dependência de funcionários chaves	1º

Fonte: Autor (2017)

No caso analisado, foram levados em consideração os dados da matriz de riscos, ou seja, a probabilidade e os impactos, dentro do perfil de apetite de risco da empresa. Caso alguns riscos se encontrassem dentro da região de exposição inaceitável, seriam esses riscos que teriam prioridades no tratamento, enquanto que os situados na região de exposição aceitável seriam os últimos a serem tratados, caso fossem.

6.3 Estratégia de tratamento dos riscos da empresa analisada

Tomando como base as diretrizes do ISO 31000 (2009) e o COSO (2007), este trabalho buscou apresentar estratégias para o tratamento dos riscos identificados e avaliados anteriormente. A etapa de avalição é fundamental para o melhor entendimento dos riscos que estão presentes no ambiente de valor da organização.

A empresa possui poucas formas de intervenções para os riscos com origem de fontes externas, como no caso de novas tecnologias, crise no setor de atuação, problemas econômicos do país e mudanças na legislação e por isso as ações são muito mais reativas. São os riscos gerados pelo Ambiente de Negócios, no modelo de Oliva (2016).

Mas isso não implica que eles não devam ser gerenciados, pelo contrário, eles devem sim ser monitorados e, quando possíveis, tratados. Muitos deles podem levar a impactos relevantes e dessa maneira a empresa deve estar muito bem preparada para essas ações reativas.

Já os riscos com fontes internas são mais influenciados pelas decisões e ações da empresa. Nesse caso, a empresa deve possuir uma postura mais proativa buscando antecipar-se aos efeitos negativos desses riscos.

Segundo a ISO 31.000, as formas de tratamento dos riscos são:

a) Ação de evitar o risco ao se decidir não iniciar ou descontinuar a atividade que dá origem ao risco;
b) Tomada ou aumento do risco na tentativa de tirar proveito de uma oportunidade;
c) Remoção da fonte de risco;
d) Alteração da probabilidade;
e) Alteração das consequências;
f) Compartilhamento do risco com outra parte ou partes; e
g) Retenção do risco por uma decisão consciente e embasada.

Com base na etapa anterior, pode ser verificado que nenhum risco se encontra dentro da zona de "exposição inaceitável", alguns se encontram na zona de "exposição aceitável" (D, G, J, L) e serão apenas monitorados e existem os que se encontram na zona intermediária (A, B, C, E, F, H, I, K, M, N, O, P, Q e R) e que seguirão para tratamento.

Os tratamentos propostos são:

Quadro 7 – Tratamentos propostos aos riscos

Identificação	***Riscos***	***Tratamento proposto***	***Resultado***
A	Controle dos custos e despesas	Verificação dupla dos dados e capacitação	Alteração (queda) da probabilidade de ocorrer
B	Problemas contábeis	Verificação dupla dos dados e capacitação	Alteração (queda) da probabilidade de ocorrer
C	Não conformidade com as regulações	Monitoramento e apoio de especialistas	Retenção do risco por uma decisão consciente e embasada
E	Inadimplência	Investimento maior em capital de giro	Alteração das consequências
F	Estratégias financeiras ruins	Criação e revisão de indicadores de performance financeiras	Alteração (queda) da probabilidade de ocorrer
H	Parcerias	Diversificação das parcerias e redução da dependência	Remoção da fonte de risco
I	Clientes	Diversificação da carteira de clientes e redução da dependência de clientes	Remoção da fonte de risco
K	Novas tecnologias	Monitoramento do mercado	Retenção do risco por uma decisão consciente e embasada
M	Crise no setor de atuação	Monitoramento do mercado	Retenção do risco por uma decisão consciente e embasada
N	Problemas econômicos do país	Monitoramento do mercado	Retenção do risco por uma decisão consciente e embasada
O	Mudança na legislação	Monitoramento do mercado	Retenção do risco por uma decisão consciente e embasada
P	Informações confidenciais	Melhorar a segurança da rede/dados confidenciais	Alteração (queda) da probabilidade de ocorrer
Q	Problemas na sociedade	Criar um Acordo de Acionista	Remoção da fonte de risco
R	Dependência de funcionários chaves	Criar mecanismos de retenção para funcionários chaves	Alteração (queda) da probabilidade de ocorrer

Fonte: Autor (2017)

Essa etapa não deve ocorrer sem que se estabeleça uma estratégia prévia. Isso porque os riscos não devem ser analisados de modo isolado, mas sim como um conjunto, dentro de um contexto e de acordo com o perfil da empresa.

Muitas vezes, quando se faz o tratamento de um determinado risco, essa ação pode levar à alteração de outro risco, podendo alterar sua probabilidade de ocorrência, impacto, consequência, ter como causa o tratamento proposto, entre outras alterações. Na teoria do COSO (2007), o risco em sua forma original é chamado de "risco inerente", e quando ele sofre alguma modificação, por exemplo de um tratamento, ele passa a ser chamado de risco residual. Ou seja, é fundamental que a estratégia contemple também as implicações que os tratamentos dos riscos podem gerar em outros riscos ou até mesmo que novos possam ser gerados. Deve-se ter em mente também que sempre existirá algum nível de risco residual, mesmo que mínimo. Primeiramente porque os recursos de qualquer empresa são limitados e, segundo, porque os riscos fazem parte das atividades de qualquer organização (COSO, 2007).

Quadro 8 – Impacto dos tratamentos

Identificação	***Riscos***	***Tratamento proposto***	***Qual impacto do tratamento?***
A	Controle dos custos e despesas	Verificação dupla dos dados e capacitação	Aumento da complexidade de operação
B	Problemas contábeis	Verificação dupla dos dados e capacitação	Aumento da complexidade de operação
C	Não conformidade com as regulações	Monitoramento e apoio de especialistas	Nenhum
E	Inadimplência	Investimento maior em capital de giro	Perda da eficiência dos recursos
F	Estratégias financeiras ruins	Criação e revisão de indicadores de performance financeiras	Aumento da complexidade de operação
H	Parcerias	Diversificação das parcerias e redução da dependência	Pode prejudicar o relacionamento e ter impacto sobre as receitas
I	Clientes	Diversificação da carteira de clientes e redução da dependência de clientes	Investimento nas áreas de marketing e comercial
K	Novas tecnologias	Monitoramento do mercado	Nenhum
M	Crise no setor de atuação	Monitoramento do mercado	Nenhum
N	Problemas econômicos do país	Monitoramento do mercado	Nenhum
O	Mudança na legislação	Monitoramento do mercado	Nenhum
P	Informações confidenciais	Melhorar a segurança da rede/dados confidenciais	Necessidade de recursos/investimentos em segurança
Q	Problemas na sociedade	Criar um Acordo de Acionista	Nenhum
R	Dependência de funcionários chaves	Criar mecanismos de retenção para funcionários chaves	Necessidade de recursos/investimentos

Fonte: Autor (2017)

Aspectos que são bastante relevantes e que também devem ser levados em conta quanto aos tratamentos são os custos, tanto diretos quanto indiretos e os benefícios que eles devem gerar. As melhores estratégias de respostas aos riscos são justamente as que conseguem aproveitar com melhor eficiência os usos dos recursos, ou seja, obter os melhores resultados, utilizando o menor custo e esforços (ISO 31000, 2009; COSO, 2007).

Definida a estratégia de tratamento dos riscos, a empresa precisa estabelecer atividades de controle. Elas devem garantir que o plano proposto está sendo conduzido da forma correta e caso surjam imprevistos, estabelecer novas estratégias. Essas atividades de controle fazem parte do monitoramento, que não são detalhados neste trabalho, mas que dentro do contexto de GRC, são muito importantes.

O tratamento de riscos, por si só, pode introduzir riscos. Um risco significativo pode derivar do fracasso ou da ineficácia das medidas de tratamento de riscos. O monitoramento precisa fazer parte do plano de tratamento de forma a garantir que as medidas permaneçam eficazes.

7 CONSIDERAÇÕES FINAIS

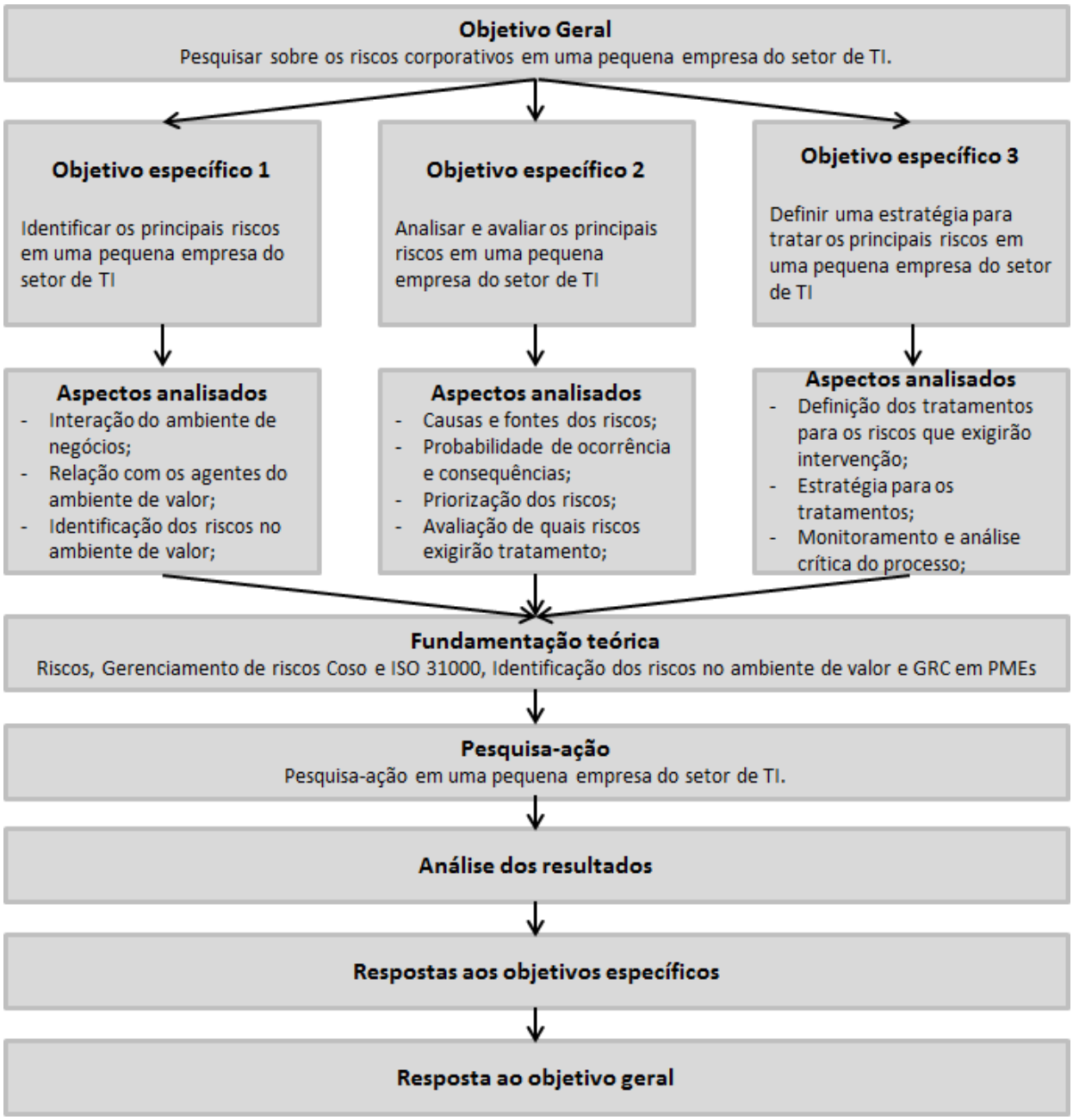
7.1 Atendimento aos objetivos da pesquisa

Diante de tudo que foi exposto neste trabalho, fica claro que é fundamental que proprietários e gestores de pequenas e médias empresas do setor de TI deem a atenção necessária para a gestão de riscos corporativos. A indústria de Tecnologia da Informação é extremamente mutável e dinâmica e os riscos surgem, modificam-se e extinguem-se na mesma velocidade da evolução do mercado.

Entre outros fatores, o que torna a gestão dos riscos é ainda mais importante nas pequenas e médias empresas é que elas possuem um acesso mais restrito ao capital e que, além disso, possuem, de modo geral, uma gestão menos profissional quando comparada a grandes corporações (SMIT e WATKINS, 2012).

Este trabalho buscou justamente apresentar os principais conceitos envolvidos no gerenciamento de riscos corporativos em pequenas e médias empresas do mercado de TI, abordando na revisão teórica os conceitos de riscos, as metodologias e princípios mais atuais e relevantes sobre GRC e também como o processo ocorre nas PMEs. A Figura 14, a seguir, ilustra a estrutura da pesquisa.

Figura 14 – Estrutura da pesquisa



Fonte: Autor (2017)

Assim, os objetivos, tanto geral, quanto os específicos, foram alcançados, com riqueza de detalhes e com um embasamento teórico que deu suporte à análise e a conclusões. A importância deste trabalho torna-se particularmente ainda mais relevante quando verificamos que foi possível aplicar a teoria na prática.

7.2 Atendimento aos procedimentos metodológicos

O processo metodológico escolhido para este trabalho foi o de Pesquisa ação, no qual o pesquisador é também um participante ativo na resolução da situação-problema. A escolha da metodologia foi importante para atingir o objetivo esperado para o trabalho. Além do acesso a informações relevantes, foi possível obter percepções e análises mais profundas sobre o tema proposto, atendendo deste modo à proposta de ser um trabalho exploratório e com uma abordagem qualitativa, com análises em profundidade e informações relevantes.

Entre as técnicas utilizadas para coleta de dados deste trabalho, as que se mostraram mais importantes foram as entrevistas realizadas com sócios da empresa. Através delas foi possível obter informações, opiniões, dados históricos e percepções que não se encontram em nenhum relatório, sistema ou arquivo escrito.

A possibilidade de o pesquisador participar ativamente dentro do contexto estudado, lhe garantiu condições de explorar o cenário da melhor forma, com livre acesso a opiniões de pessoas envolvidas no GRC, dados importantes e percepções que não seriam possíveis, caso fosse um mero expectador. Através desta abordagem, foi possível atender tanto ao objetivo geral quanto aos objetivos específicos da pesquisa. Por essas razões, entende-se que este estudo atendeu aos procedimentos metodológico

7.3 Implicações gerenciais

Em primeiro lugar, buscou-se identificar quais são os principais riscos que podem estar presentes na gestão de uma pequena empresa nacional do setor de TI. Tendo como referências o modelo do COSO (2007), as diretrizes da ISO 31000 (2009) e o modelo teórico proposto por Oliva (2016) de identificação dos riscos no ambiente de valor, foi possível não apenas listar os riscos, como também relacioná-los aos principais agentes presentes no ambiente de valor da empresa e também avaliar como os agentes situados no ambiente de negócios podem interferir nessas relações.

Este trabalhou mostrou que é possível utilizar na prática o modelo teórico de identificação de riscos no ambiente de valor. A escolha pelo modelo de Oliva (2016) foi motivada pela simplicidade de uso – o que é de grande importância para PMEs que, em geral, possuem limitações de recursos –, e principalmente pela abrangência de análise no processo de

identificação de riscos. Essa visão mais ampla permite que a empresa deixe de focar apenas nos riscos operacionais, ligados ao dia a dia da empresa, e consiga avaliar os riscos mais estratégicos que possam vir a comprometer a empresa, no longo prazo. Essa etapa é fundamental no processo de implementação de GRC.

Esta conclusão do autor vai de encontro ao que é apresentado na literatura por Tchankova (2002). O sucesso do GRC está intimamente relacionado à correta identificação dos riscos, pois a falta de habilidade dos gestores em listar todos os fatores que podem trazer perdas e prejuízos para a organização a impossibilita tomar ações preventivas ou ativas necessárias para seu tratamento e ainda podem levar a consequências negativas severas para o desenvolvimento do seu negócio.

Levando em consideração os estudos de Brustbauer (2014) e Siregar (2015) ao afirmarem que, apesar de os empresários conhecerem a fundo o seu negócio, eles não são capazes de identificar todos os riscos, isso não torna o processo menos importante. Muito pelo contrário, estabelecer uma atividade específica para identificar os riscos, cria condições para, muitas vezes, listar itens que passariam despercebidos. Realizar o processo tendo uma ferramenta capaz de estruturá-lo, além de facilitar a operação, também desenvolve condições favoráveis para que um maior número de riscos seja listado.

Este trabalho também constatou que alguns dos riscos identificados na empresa, foram também descritos por outros pesquisadores (VIRDI, 2005; GOVERNO DE SINGAPURA, 2012; RAGHAVAN, 2005), em outros países, como mudanças de mercados, comprometimento de imagem, dependência excessiva em poucos funcionários chaves, competição intensiva, inabilidade de acompanhar o avanço tecnológico. A maioria deles, entretanto, eram específicos do setor e da empresa. Isto reforça a ideia que cada ambiente, sociedade, setor e empresa possuem características próprias e únicas e que demandam gestões igualmente específicas.

A avaliação dos riscos foi outro objetivo secundário proposto para este trabalho. Nesse caso, o autor fundamentou-se nas teorias do ISO 31000 (2009) e COSO (2007). Nesta etapa, foram identificadas as principais causas e consequências dos riscos, bem como a probabilidade de ocorrência e impactos que podem causar à organização. Para estruturar esses dados, foi utilizado uma matriz de risco, na qual o eixo das ordenadas representa a probabilidade de ocorrência e o eixo das abcissas representa o impacto que os riscos podem causar.

Contudo, essa matriz para ter uso completo deve representar também o perfil de apetite de risco da organização. Não existe um modelo único e cada empresa deve desenvolver o seu, tanto das gradações, quanto das áreas de exposição aos riscos. E mesmo essa ferramenta não determina o que deve ser tratado ou não, ela apenas ajuda na análise dos riscos identificados em etapas anteriores.

Em muitos casos, essas informações podem ser insuficientes para determinar se os riscos serão tratados ou não, necessitando de maiores detalhes e um aprofundamento na análise. Para suprir essa demanda de informações, analisam-se os dados dentro de uma perspectiva qualitativa, apresentando informações que muitas vezes não podem ser quantificadas ou avaliadas por meio de uma métrica (COSO, 2007).

Neste trabalho, não foram feitas análises quantitativas devido à falta de dados, grau de maturidade do GRC e também porque o custo-benefício não era vantajoso, indo de encontro que afirmam Arena et al. (2011), ao explicar a preferência das empresas pelo uso de análises qualitativas na avaliação de riscos.

A etapa seguinte, de tratamento dos riscos, não é um processo simples de ser realizado. É necessário estabelecer uma estratégia antes, avaliando se a empresa possui os recursos tanto financeiros quanto de pessoas e tempo necessários para sua execução. Além disso, avaliar com cautela os desdobramentos que as próprias ações de tratamento podem gerar nos atuais riscos identificados (COSO, 2007).

Dependendo da quantidade e relevância dos riscos, a complexidade de definir tratamentos para todos os riscos se torna muito grande, já em outros casos não é necessário propor tratamento para todos eles, ou ainda, em muitos outros casos a empresa não dispõe de recursos suficientes para tratá-los. O autor concorda com Moeller (2007), quando este afirma que o processo de gestão de riscos não está relacionado à eliminação deles, mas sim em sua identificação, mensuração e controle.

Estabelecer uma estratégia antes de iniciar o tratamento é fundamental, não só para eliminar os efeitos negativos dos riscos da melhor maneira possível, mas também devido ao uso mais eficiente dos recursos da organização. Indo mais além, ela deve estar em total alinhamento também com as próprias estratégias da empresa (FRIGO e ANDERSON, 2011; COSO, 2007; ISO 31000, 2009).

Ao propor ações de tratamento, é prudente que estas sejam acompanhadas de cronograma, matriz de responsabilidades, análise dos recursos, análise dos impactos e quaisquer outras

informações que os gestores julguem relevantes para estabelecer a estratégia de tratamento dos riscos.

Por fim, o pesquisador também concorda em partes com Siregar (2015), quando este afirma que as PMEs precisam adaptar os modelos de GRC para versões mais simplificadas e adequá-los melhor às suas necessidades. O autor concorda que é necessário que essas empresas adequem os modelos às suas características, mas não necessariamente ela precisa ser mais simplificada. O que determina a complexidade ou simplicidade do GRC são suas características internas e ambiente no qual se encontra e não apenas seu porte.

7.4 Limitações da pesquisa

O trabalho apresentado atendeu aos objetivos propostos, apresentando com riqueza de detalhes e profundidade os principais aspectos de Gestão de Riscos Corporativos em uma pequena empresa nacional do setor de Tecnologia da Informação. De modo prático e bastante empírico, o autor buscou explorar sua perspectiva como participante na resolução da situação-problema, procurando evitar, ao máximo, qualquer tipo de juízo de valor.

Por outro lado, não foram exploradas neste trabalho todas as etapas do GRC, seguindo o modelo ISO 31000: estabelecimento do contexto, monitoramento e análise crítica, e comunicação e consulta. Não por serem menos importantes, pelo contrário, todas essas etapas são essenciais para uma boa implementação e manutenção do sistema de gestão. A mesma crítica vale para o modelo COSO, no qual as etapas de ambiente interno, fixação dos objetivos, atividades de controle, informação, comunicação e monitoramento não foram consideradas.

Outra limitação é com relação à generalização dos achados e conclusões da pesquisa. Todos os dados e análises foram obtidos de um cenário bastante específico e único. A pesquisa qualitativa dificilmente garante a possibilidade de extrapolação para outros cenários, como ocorre com as técnicas quantitativas.

7.5 Futuras pesquisas

Não existem muitas pesquisas sobre gerenciamento de riscos corporativos em pequenas e médias empresas no país. O Brasil possui um cenário econômico, político e social único, e vive um contexto histórico também bastante específico. A necessidade de novos trabalhos nesse tema é bastante clara para o autor deste trabalho. Há ainda muito o que ser explorado, tanto em pesquisas com caráter quantitativo, quanto qualitativo, dada a escassez de informações sobre o tema.

Para pesquisas futuras, o autor sugere que outros pesquisadores busquem englobar todas as etapas das normas ISO 31000 e COSO que não foram abordadas neste trabalho, abordando uma visão mais holística sobre o processo de gerenciamento de riscos em PMEs.

Além disso, sugere também que pesquisas sejam realizadas utilizando uma abordagem quantitativa, explorando a indústria de modo mais abrangente e menos específico. Esse direcionamento quantitativo pode ser benéfico para o melhor entendimento deste universo.

8 REFERÊNCIAS

ABES - ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE. **Mercado Brasileiro de Software:** panorama e tendências, 1. ed. São Paulo: ABES, 2015.

AGRAWAL, R. Enterprise Risk Management**:** Essential for Survival and Sustainable Development of Micro, Small and Medium Enterprises. **International Review**, n. 1-2, 2016.

ALTMAN, E. I; SABATO, G.; WILSON, N. The Value of non-financial Information in Small and Medium-Sized Enterprise Risk Management. **The Journal of Credit Risk**, v.6, n. 2, p. 1-33, 2010.

ANSOFF, H. I.; MCDONELL, E. J. **Implantando a administração estratégica**. 2. ed. São Paulo: Atlas, 1993.

ARENA, M.; ARNABOLDI, M.; AZZONE, G. The Organizational Dynamics of Enterprise Risk Management**. Accounting, Organizations and Society**, 35, p. 659-675, 2010. Disponível em: <http://dx.doi.org/10.1016/j.aos.2010.07.003>. Acesso em: 05 set. 2015.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. **NBR ISO 31000:** Gestão de Riscos – Princípios e Diretrizes. Rio de Janeiro: ABNT, 2009.

ATTIE, W. **Auditoria**: conceitos e aplicações. 4. ed. São Paulo: Atlas, 2009.

BARTON, T. L.; SHENKIR, W. G.; WALKER, P. L. **Making Enterprise Risk Management Pay Off**. FT Press, Upper Saddle River, 2002.

BERGAMINI JÚNIOR, S. Controles Internos como um Instrumento de Governança Corporativa. **Revista do BNDES**. Rio de Janeiro, v. 12, n. 24, p. 149-188, dez. 2005.

BERRY, A. **The role of the small and medium enterprise sector in Latin America:** implications for South Africa. Unisa Latin American Report, 2002.

BOWLING, D.M.; RIEGER, L.A. Making Sense of COSO's New Framework for Enterprise Risk Management. **Bank Accounting & Finance**, n. 18, p. 29-34, 2005.

BRASILIANO, A. C. R. **Gestão e Análise de Riscos Corporativos:** método brasiliano avançado. São Paulo: Ed. Sicurezza, 2009.

BROMILEY, P.; MCSHANE, M. K.; NAIR, A.; e RUSTAMBEKOV, E. **Enterprise Risk Management:** Review, Critique and Research Directions. Forthcoming: Long Range Planning, 2014.

BRUSTBAUER, J. Enterprise Risk Management in SMEs: Towards a structural model. **International Small Business Journal**, v. 24(I), p. 70-85, 2016.

CHAPMAN, C. Bringing ERM into Focus. **The Internal Auditor**, n. 60, p. 30-35, 2003.

CHAPMAN, C. B.; COOPER, D. F. Risk engineering: Basic controlled interval and memory models. **Journal of the Operational Research Society**, v. 37, p. 51-60, jan. 1983.

CHING, H. Y. Contribuição das boas práticas do mercado para a eficiência na gestão de risco corporativo. **Rebrae – Revista Brasileira de Estratégia**, Curitiba, v.4, n.3, p. 257-273, 2011.

COGHLAN, P. Action research for operations management. **International Journal of Operations & Production Managemen**t, v. 22, n. 2, p. 220-240, 2002.

COSO - COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **Gerenciamento de Riscos Corporativos:** estrutura integrada. Nova York. AICPA, 2007.

COSO - COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **Risk Assessment in Pratice**, 2012b.

COSO - COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **Enterprise Risk Management.** Integraded Framework – Application Techniques. Durham: AICPA, 2004b.

DANTAS, J. A.; RODRIGUES, F. F.; MARCELINO, G. F.; LUSTOSA, P. R. B. Custo-benefício do controle: proposta de um método para avaliação com base no COSO. **Contabilidade, Gestão e Governança.** Brasília, v. 13, n. 2, p. 3-19, 2010.

DAMODARAN, A. **Gestão estratégica do risco**: referência para tomada de riscos empresariais. Porto Alegre: Bookman, 2009.

DELOITTE. **Mundo Corporativo**, v. 3, n. 10, p. 7-9, 2005.

DRUCKER, P. F. **Práticas de Administração de Empresas**. São Paulo: Pioneira, 1981.

EASTERBY-SMITH, M.; THORPE, R.; LOWE, A. **Pesquisa gerencial em administração**: um guia para monografias, dissertações, pesquisas internas e trabalhos de consultoria. São Paulo: Pioneira, 1999.

FILHO, A. R. **Riscos corporativos em uma rede de cooperação:** o caso das empresas associadas à Rede Arrozeiras do Sul. 2014. Tese (Doutorado em Ciências) – Faculdade de Economia, Administração e Contabilidade. Universidade de São Paulo. São Paulo, 2014.

FRASER, J. R. S.; SIMKINS, B. J. The challenges of and solutions for implementing enterprise risk management. **Business Horizons**, v. 59, p. 689-698, 2016. Disponível em: http://dx.doi.org/10.1016/j.bushor.2016.06.007>. Acesso em: 19 jul. 2017.

FRIGO, M. L.; ANDERSON, R. J. Strategic Risk Management: A Foundation for Improving Enterprise Risk Management and Governance. **Journal of Corporate Accounting & Finance**. 2011. Disponível em: <http://dx.doi.org/10.1002/jcaf.20677>. Acesso em: 20 set. 2015.

GIL, A. C. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 1999.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2008.

GOVERNO DE SINGAPURA, SPRING Singapore, Ministry of Trade and Industry. Top Five Risk SMEs Should Address. **The Business Times.** Singapore Press Holdings Ltd, 2012.

GRACE, M. F.; LEVERTY, J. T.; PHILLIPS, R. D.; SHIMPI, P. The Value of Investing in Enterprise Risk Management. **The Journal of Risk and Insurance,** n. 2, p. 289-316, 2015.

HARLAND, C.; BRENCHLEY, R. e WALKER, H. Risk in Supply Networks. **Journal of Purchasing and Supply Management**, n. 9, p. 51-62, 2003. Disponível em: <http://dx.doi.org/10.1016/S1478-4092(03)00004-9>. Acesso em: 17 set. 2015.

HEAD, L. G. **Risk Management:** Why and How. International Risk Management Institute. Dallas, Texas, 2009.

HOYT, R. E.; LIEDENBERG, A. P. The value of enterprise risk management. **The Journal of Risk and Insurance,** v. 78, n. 4, p. 795-822, 2011. Disponível em: <http://dx.doi.org/10.1111/j.1539-6975.2011.01413.x>. Acesso em: 17 set. 2015.

HUDIN, N. S.; HAMID, A. B. A. Drivers to the Implementation of Risk Management Practices: A Conceptual Framework. **Journal of Advanced Management Science**, v. 2, n. 3, Sept. 2014.

IBGC - INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Guia de Orientação para o Gerenciamento de Riscos Corporativos**. São Paulo: IBGC, 2007.

ISO - INTERNATIONAL ORGANIZATION OF STANDARDISATION. **Gestão de riscos:** princípios e diretrizes, 2009. Disponível em: <http://www.iso.org>. Acesso em: 11 set. 2015.

JORION, P. **Value at risk**. Nova York: Wiley, 1997.

LAFORET, S.; TANN J. Innovative Characteristics of Small Manufacturing Firms. **Jornal of Small Business and Entreprise Development**, v. 13 (3), p. 363-380, 2006.

LUNDQVIST, S. A. Why Firms Implement Risk Governance: Stepping Beyond Traditional Risk Management to Enterprise Risk Management. **Journal of Accouting and Public Policy**, n. 34, p. 441-466, 2015.

MACDONALD, D. **Practical Hazops, Trips and Alarms**. Elsevier, Oxford, 2004.

MARIKA A.; MICHELA, A.; GIOVANNI, A. Is enterprise risk management real? **Journal of Risk Research**, v. 14(7), p. 779-797, 2011. Disponível em: <http://dx.doi.org/ 10.1080/13669877.2011.571775>. Acesso em: 05 abr. 2017.

MCSHANE, M. K.; NAIR, A.; RUSTAMBEKOV, E. Does Enterprise Risk Management Increase Firm Value? **Journal of Accouting, Auditing & Finance**. Disponível em: <http://dx.doi.org;10.1177/0148558X11409160>. Acesso em: 11 set. 2015.

MILLET, I.; WEDLEY, W. Modelling risk and uncertainty with analytic hierarchy process. **Journal of Multi-Criteria Decision Analysis,** v.11, p. 97-107, 2002.

MIKES, A. **From Counting Risks and Making Risks Count:** Boundary-Work in Risk Management. Accouting, Organizations, and Society. n.36, p. 226-245, 2011. Disponível em: <http://dx.doi.org/10.1016/j.aos.2011.03.002>. Acesso em: 07 set. 2015.

MITCHEL, V. W. **Organizational Risk Perception and Reduction:** A Literature Review. British Journal of Management, 6, 115-133, 1995. Disponível em: <http://dx.doi.org/10.1111/j.1467-8551.1995.tb00089.x>. Acesso em 17 set. 2015.

MOELLER, R. R. **COSO Enterprise Risk Management:** Understanding the New Integrated ERM Framework. New Jersey: John Wiley & Sons, 2007.

NTLHANE, K. E. **The Application of Risk Management principles to smaller enterprises**. A research report submitted in partial fulfilment of the requirements for the degree of Masters of Business in the Faculty of Management at the University of the Witwatersrand, 1995.

NOCCO, B.; STULZ, R. **Enterprise Risk Management:** Theory and Practice. Journal of Applied Corporate Finance, 18, 8-20, 2006. Disponível em: <http://dx.doi.org/10.1111/j.1745-6622-2005.00042.x>. Acesso em: 12 set. 2015.

OLIVA, F. L.; SOBRAL, M. C.; DAMASCENO, F.; TEIXEIRA, H. J.; GRISI, C. C. H.; FISCHMANN, A. A.; SANTOS, S. A. Risks and Strategies in a Brazilian Innovation – Flexfuel Technology. **Journal of Manufacturing Technology Management**, Birmingham, Inglaterra, vol. 25, no. 6, p. 916 – 930, 2014.

OLIVA, F. L. A Maturity Model for Enterprise Risk Management. **International Journal Production Economics**, v. 173, p. 66-79, 2016.

PADOVEZE, C; BERTOLUCCI, R. G. **Gerenciamento de Risco Corporativo em Controladoria**. 1ª ed. São Paulo: Cengage Learning, 2008

PANIGRAHI, A. K. Risk Management in Micro, Small and Medium Enterprises (MSMEs) in India: A Critical Appraisal. **Asia Pacific Journal of Marketing & Management Revier**, v.1, 2012.

PAULO, W. L.; FERNANDES, F. C.; RODRIGUES, L. G. B.; EIDIT J. Riscos e controles internos: uma metodologia de mensuração dos níveis de controle de riscos empresariais. **Revista Contabilidade & Finanças**, São Paulo, v. 18, n. 43, 2007.

PAXSON, D.; WOOD, D. **The Blackwell Encyclopedic Dictionary of Finance**. Oxford: Blackwell, 1998.

POLTRONIERI, C. C. **Um estudo sobre os controles internos em pequenas e médias empresas de TI**. 88f. 2012. Dissertação (Mestrado em Ciências Contábeis) – Universidade Presbiteriana Mackenzie, São Paulo.

RAGHAVAN, R. S. **Risk Management in SMEs**. The Chartered Accountants of India, 6, 528-535, 2005.

RAZ, T.; HIILSON, D. A comparative review of risk management standards. **Risk Management: An International Journal**, v.7, n.4, p. 53-66, 2005. Disponível em: <http://www.risk-doctor.com/pdf-files/final-issue.pdf>. Acesso em: 18 set. 2015.

ROCHA, P. C.; BELCHIOR, A. D. Mapeamento do gerenciamento de riscos no PMBOK, CMMI-SW e RUP. Simpósio Internacional de Melhoria de Processos de Software, 6, 2003, São Paulo. Anais São Paulo: SIMPROS, 2004.

SADGROVE, K. **The Complete Guide to Business Risk Management**. London: Gower Publishing, 2005.

SANTOS, C.; VASCONCELOS, A.; TRIBOLET, J. **Da framework CEO à auditoria se sistemas da informação**. 2007. Disponível em: <http://www.inesc-id.pt/pt/indicadores/Ficheiros/2114.pdf>. Acesso em: 15 set. 2015.

SIREGAR, M. P. H. H; **Effective Risk Management for Micro, Small and Medium Enterprises (SMEs) in Indonesia to Face Asean Economic Community**. Proceedings of The Australian Academy of Business and Social Sciences Conference, 2014.

SMIT, Y.; WATKINS, J. A. A Literature Review of Small and Medium Enterprises (SME) Risk Management Practices In South Africa. **African Journal of Business Management**, v. 6 (21), p. 6324-6330, 2012.

SOUZA, M. M.; VICENTE, E. F. R.; BORBA, J. A.; LUNKES, R. J. Evidenciação das exigências da Lei Sarbanes-Oxley nas empresas brasileiras que negociam ADRs nos Estados Unidos. **Revista de Informação Contábil**, Blumenau, v. 5, n. 3, p. 98-117, jul./set. 2011.

STULZ, R. M. Risk Management Failures: What are they and when to they happen? **Journal of Corporate Finance**, v. 20, n. 4, p. 58-67, 2008.

TAYLOR, H. Congruence between risk management theory and practice in Hong Kong vendor-driven IT projects. **International Journal of Project Management**, v. 23, p. 437-444, 2005.

TCHANKOVA, L. Risk identification: basic stage in risk management. **Environmental Management and Health**, v. 13, n. 2/3, p. 290-297, 2002.

THIOLLENT, M. **Metodologia da pesquisa-ação.** 15. ed. São Paulo: Cortez, 2007.

TUMMALA, V. M.; LEUNG, H. M.; MOK, C. K.; BURCHETT, J. F. e LEUNG Y. H. Practices, barriers and benefits of using risk management approaches in selected Hong Kong industries. **International Journal of Project Management**, v. 15, n. 5, p. 297-312, 1997.

URCIUOLI, V.; CRENCA, G. **Risk Management:** strategie e processi decisionali nella gestione dei rischi puri d´impresa. ISBA, Rovereto, 1989.

VERBANO, C.; VENTURINI, K. Managing Risks in SMEs: A Literature Review and Research Agenda. **Journal of Technology Management & Innovation**, v. 8, Issue 3, 2013.

VIRDI, A. A. **Risk management among SMEs** – executive report of discovery research, Prepared by the Consultation & Research Centre of the Institute of Chartered Accountants in England and Wales, 2005.

WATT, J. Strategic risk management for small business. In: REUVID, J. (ed). **Managing Businss Risk** 2nd Edition: a practical guide to protecting your business. London – Philadelphia: Kogan Page, 2007.

WEISS, C. H. **Evaluation**. 2.ed. Upper Saddle River: Prentice-Hall, 1998.

YIN, R. K. **Estudo de caso** - planejamento e métodos. 3. ed. Porto Alegre: Bookman, 2005.

ZACHARAKIS, A. L., MEYER, G. D.; DECASTRO, J. Differing perceptions of new venture failure: A matched exploratory study of Venture Capitalists and Entrepreneurs. **Journal of Small Business Management**, 37(3), p. 1-14, 1999.

ZENO, J. M. C. **Risco Legal: Uma introdução ao seu gerenciamento no atual cenário corporativo**. Dissertação (Mestrado em Administração) – Faculdade de Economia e Finanças IBMEC, Instituto Brasileiro de Mercado de Capitais, Rio de Janeiro, 2007.

Apêndice I – Protocolo de Pesquisa

Visão Geral da Pesquisa

Título: Gerenciamento de riscos corporativos em pequenas e médias empresas: análise de uma empresa nacional do setor de TI

Objetivo geral: pesquisar sobre os riscos corporativos em uma pequena empresa do setor de TI.

Objetivos específicos:

1. Identificar os principais riscos em uma pequena empresa do setor de TI;
2. Avaliar os principais riscos em uma pequena empresa do setor de TI; e
3. Propor estratégias para tratar os principais riscos em uma pequena empresa do setor de TI.

Aspectos Metodológicos: Pesquisa exploratória e qualitativa, elaborada através da metodologia de Pesquisa Ação. Explicar para os entrevistados o papel do pesquisador, a importância da pesquisa, como ela está sendo conduzida. Além disso, informar sobre o uso de relatório e uso de informações primárias e secundárias.

Unidade de análise: sócios-gestores da empresa

Fontes de evidência: coleta de dados primários através de entrevistas pessoais e individuais e levantamento de dados secundários com a utilização da técnica de levantamento documental.

Instrumentos de coleta: roteiro de entrevista e análise de documentos.

Pesquisador: Anderson Doi

Dados sobre a organização, sobre o entrevistado e sobre a entrevista

Organização: caracterização da empresa, do mercado que atua, histórico de atividades, sem citar nomes e referências.
Entrevistado: histórico sobre experiência no mercado e na empresa, cargo e conhecimento sobre o tema do trabalho.

Entrevista: Local e data da entrevista, tipo de entrevista utilizada. Nomes devem ser mantidos em sigilo.

Aspectos analisados:

- Caracterizar o respondente: experiência no mercado de atuação, domínio sobre o negócio da empresa, conhecimento sobre gestão de riscos corporativos;
- Identificação dos riscos: listar os principais riscos na visão dos entrevistados e aplicação do modelo teórico de identificação dos riscos no ambiente de valor;
- Avaliação dos riscos: analisar os riscos quanto suas causas e consequência, identificação do perfil de risco da empresa, estabelecimento da Matriz de Risco;
- Tratamento dos riscos: Proposição de ações para tratamento de riscos, avaliação das consequências dos tratamentos, estabelecimento de critérios para elaboração de estratégia de tratamento dos riscos.

Apêndice II – Roteiro para entrevista

NOME: _____

LOCA/DATA: _____ CARGO: _____

As perguntas buscarão avaliar suas percepções sobre a gestão de riscos corporativos da empresa que administra. Lembrando que não existe uma única opção de resposta e nem certos ou errados.

Caracterização do respondente:

1) **Há quanto tempo atua no mercado de TI (CRM)?**
   - Avaliar a experiência do respondente sobre o mercado que atua.

2) **Em sua opinião, qual é o seu conhecimento sobre o negócio da empresa?**
   - Avaliar o conhecimento do negócio

3) **Em sua opinião, qual o seu conhecimento sobre gestão de riscos corporativos?**
   - Avaliar o conhecimento sobre Gestão de Riscos Corporativos

Identificação dos riscos:

4) **Quais são os principais riscos que a empresa está sujeita? Consegue detalhar?**
   - Listar os riscos que a empresa está sujeita, na visão do respondente. Buscar detalha-los.

5) **Consegue identificar quais os agentes envolvidos em cada risco identificado?**
   - Identificar os agentes que a empresa se relaciona e que possam ser influenciadores dos riscos.

Avaliação dos riscos:

6) **Em sua opinião, qual o perfil de apetite ao risco da empresa?**
   - Buscar dados para construção da Matriz de Risco

7) **Quais são as principais causas e consequências dos riscos identificados?**
   - Avaliar as causas e consequências dos riscos

8) **Em sua opinião, quais as probabilidades de ocorrência e impactos dos riscos, de acordo com a gradação abaixo?**

Probabilidade	*Impacto*
Raro	Insignificante
Improvável	Mínimo
Possível	Moderado
Provável	Alto
Quase certo	Catastrófico

- Definir a Matriz de Riscos da empresa

Tratamento dos riscos:

9) **Como cada risco deve ser tratado?**
   - Estabelecer propostas de tratamento para os riscos

10) **Quais fatores devem ser levados em consideração na definição da estratégia de tratamento dos riscos?**
   - Listar os fatores que serão considerados ao estabelecer uma estratégia para tratamento dos riscos

11) **O tratamento dos riscos pode levar ao surgimento de outros riscos ou modificação dos atuais?**
   - Avaliar as consequências dos tratamentos propostos.

Apêndice III – Dados relevantes da empresa

- Ano de fundação: 2003
- Empresa limitada de capital fechado
- Sociedade de 4 pessoas
- Idade média dos sócios: 38 anos
- Funcionários em 2017: Aproximadamente 80
- Funcionários considerados chaves: 6
    - Atuam como consultores e gerente de projetos
    - Possuem em aproximadamente 10 anos de atuação na empresa
    - Possuem conhecimento técnico, conhecem a cultura da empresa e vivenciaram boa parte do histórico de crescimento da organização
    - Conhecem muito bem as operações da empresa
- Faturamento: 15 Milhões
- Carteira de clientes: aproximadamente 25 clientes de grande e médio portes
- Parceiro: grande empresa multinacional do setor de TI
- Atuação nacional (95%) e internacional (5%)
- Empresa de contabilidade externa
- Inexistência de ERP
- Baixo índice de inadimplência
- Produto desenvolvido internamente (CRM) de alta complexidade
    - Protegido através de criptografia
    - Cases de sucesso com grandes empresas
    - Baixa inserção do mercado
    - Divulgação deficiente