UNIVERSIDADE DE SÃO PAULO
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO, CONTABILIDADE E ATUÁRIA
DEPARTAMENTO DE ADMINISTRAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO

Análise da Maturidade em Gestão de Riscos Corporativos: um estudo de múltiplos casos em grandes empresas do Brasil

Jefferson Luiz Bution

Orientador: Prof. Dr. Fábio Lotti Oliva

SÃO PAULO
2022

Prof. Dr. Carlos Gilberto Carlotti Júnior
Reitor da Universidade de São Paulo

Prof.ª. Dr.ª Maria Dolores Montoya Diaz
Diretora da Faculdade de Economia, Administração, Contabilidade e Atuária

Prof. Dr. João Maurício Gama Boaventura
Chefe do Departamento de Administração

Prof. Dr. Felipe Mendes Borini
Coordenador do Programa de Pós-Graduação em Administração

Jefferson Luiz Bution

Análise da maturidade em Gestão de Riscos Corporativos: um estudo de múltiplos casos em grandes empresas do Brasil

Tese apresentada ao Programa de Pós-Graduação em Administração do Departamento de Administração da Faculdade de Economia, Administração, Contabilidade e Atuária da Universidade de São Paulo, como requisito parcial para a obtenção do título de Doutor em Ciências.

Orientador: Prof. Dr. Fábio Lotti Oliva

Versão corrigida

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

São Paulo

2022

Catalogação na Publicação (CIP)
Ficha Catalográfica com dados inseridos pelo autor

Bution, Jefferson Luiz.
Análise da maturidade em Gestão de Riscos Corporativos: um estudo de múltiplos casos em grandes empresas do Brasil / Jefferson Luiz Bution. - São Paulo, 2022.
110 p.

Tese (Doutorado) - Universidade de São Paulo, 2023.
Orientador: Fábio Lotti Oliva.

1. Gestão de riscos corporativos. 2. Modelo de avaliação. 3. Modelo de maturidade. 4. Maturidade em gestão de riscos corporativos. 5. Gestão de riscos. I. Universidade de São Paulo. Faculdade de Economia, Administração, Contabilidade e Atuária. II. Título.

AGRADECIMENTOS

Agradeço especialmente à minha esposa Beatriz, que me apoiou e dividiu vitórias e desafios, sobretudo nos anos complicados vividos ao longo da pandemia de Covid-19.

Aos meus filhos Victor, que nasceu durante mais esta conquista, e Leonardo, nascido ainda durante o tempo dedicado ao mestrado. Ambos foram fonte de motivação e inspiração mesmo nos momentos mais árduos.

Também aos meus pais, que sempre apoiaram meu desenvolvimento e proveram as bases dos meus valores e de minha formação pessoal, acadêmica e profissional.

Ao meu orientador, prof. Dr. Fábio Lotti Oliva, quem desde o início esteve próximo de minha tese, sempre disponível, a qualquer dia e horário, e, principalmente, me proporcionou valiosas oportunidades de pesquisa além deste estudo.

Estou grato também aos colegas do grupo de pesquisas em Gestão de Riscos Corporativos da USP, pelas diversas pesquisas que conduzimos em grupo, pelas discussões, *insights* e debates sobre minha tese e pelas informações e sugestões que tornaram o curso mais agradável.

Agradeço também aos profissionais que dedicaram seu tempo e aos gestores que compartilharam experiências e conhecimento ao logo das inúmeras videoconferências que enriqueceram minha pesquisa e tornaram esta tese viável.

Finalmente, à Faculdade de Economia, Administração, Contabilidade e Atuária da Universidade de São Paulo, pelo investimento e estrutura imprescindíveis.

Reconhecimento de Fomento à Pesquisa

Agradeço à Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) pelo financiamento da pesquisa aqui apresentada. Linha de fomento de programas regulares, grupo bolsa de doutorado no país, processo nº 2019/15700-4. As opiniões, hipóteses e conclusões ou recomendações expressas neste material são de responsabilidade dos autores e não necessariamente refletem a visão da FAPESP.

RESUMO

A Gestão de Riscos Corporativos (GRC) vem ganhando destaque pela capacidade de administrar riscos de forma coordenada ao planejamento estratégico e especial reconhecimento pela contribuição à preservação e criação de valor nas organizações. Apesar disso, formas de avaliar o nível de maturidade em GRC ainda estão em discussão pela academia e gestores encontram dificuldades para adaptar tais formas às especificidades de seus negócios. Este estudo conduziu uma Revisão Sistemática da Literatura (RSL) que revelou que, embora largamente empregados em gestão de organizações, os poucos modelos de maturidade e de avaliação existentes em GRC são teóricos ou adaptados para setores específicos. Modelos de avaliação são ferramentas de gestão capazes de aferir o estado atual, compará-lo com padrões e permitir o planejamento de melhorias, enquanto modelos de maturidade servem como padrão de comparação. Neste contexto, o objetivo da pesquisa apresentada nesta tese é propor um Modelo Operacional para Avaliação da Maturidade em GRC (MAM-GRC). Para atingi-lo, um modelo de avaliação inicial foi estruturado a partir de uma RSL e extensiva fundamentação teórica. Em sequência, essa versão evoluiu com a adição de perspectivas de profissionais experientes em GRC de diversos setores, por meio de entrevistas. Depois, a nova versão foi aplicada em três casos através de entrevistas com gestores dessas organizações. Ao final, o MAM-GRC foi avaliado quanto a sua aplicabilidade e utilidade por meio de um questionário. Esta pesquisa oferece uma contribuição teórica ao empregar uma abordagem qualitativa para avançar no aperfeiçoamento, utilidade e funcionalidade dos modelos de maturidade em GRC e mover seus níveis de análise em direção a aplicações. Também oferece uma contribuição prática, uma vez que apresenta ferramentas e instruções para a aplicação gerencial do MAM-GRC. A contribuição social é a diminuição dos riscos a que a sociedade está exposta, uma vez que organizações com maiores níveis de maturidade em GRC têm melhor resposta aos impactos negativos de suas atividades econômicas.

Palavras-chave: Gestão de riscos corporativos; Modelo de avaliação, Modelo de maturidade, Maturidade em gestão de riscos corporativos; Gestão de riscos.

ABSTRACT

Enterprise Risk Management (ERM) has gained prominence for its capacity to manage risks in coordination with strategic planning and has been recognized for its contribution to organization´s preservation and creation of value. Despite this, ways to assess the maturity level of ERM are still under discussion by academia, and managers face difficulties while adapting such ways to the specifics of their businesses. This study conducted a Systematic Literature Review (SLR) which found that, although largely employed in business management, the few existing maturity and evaluation models in ERM are theoretical or specifics to some sectors. Assessment models are management tools which are used to measure the current state, compare it with standards, and allow improvement plannings, while maturity models serve as the comparison standard. In this context, the objective of the research presented in this thesis is to propose an Operational Model for Maturity Assessment in ERM (MAM-GRC). To achieve this, an initial assessment model was composed with grounds on the SLR and the extensive theoretical review. Subsequently, this version evolved with the addition of experienced ERM professional's perspectives from different sectors, through interviews. Afterwards, the new version was applied in three real organizations. In the end, the MAM-GRC was evaluated for its applicability and usefulness through a questionnaire. This research offers a theoretical contribution by employing a qualitative approach to advance the improvement, usefulness, and functionality of maturity models in GRC, thus moves the level of analysis towards applications. It also offers a practical contribution as it presents tools and instructions for the managerial application of MAM-GRC. The social contribution is the reduction of risks to which society is exposed since organizations with higher levels of maturity in ERM are more responsive to the negative effects of their economic activities.

Keywords: Enterprise risk management; Assessment model, Maturity model, Maturity in enterprise risk management; Risk management.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BPM	*Business Process Management*
BPO	*Business Process Orientation*
CMM	*Capability Maturity Model*
COSO	*Committee of Sponsoring Organizations of the Treadway Comission*
CRO	*Chief Risk Officer*
DOI	*Direct Object Identifier*
FNQ	Fundação Nacional da Qualidade
GRC	Gestão de Riscos Corporativos
GTR	Gestão Tradicional de Riscos
ISSO	*International Organization for Standardization*
KRI	*Key Risk Indicator*
MAM-GRC	Modelo de Avaliação de Maturidade em Gestão de Riscos Corporativos
RIMS	*Risk and Insurance Management Society*
RMIS	*Risk Management Information System*
RSL	Revisão Sistemática da Literatura
SEI	*Software Engineering Institute*
VUCA	*Volatility, Uncertainty, Complexity and Ambiguity*

SUMÁRIO

1. INTRODUÇÃO

A rápida transformação do ambiente de negócios impõe desafios que requerem agilidade de gestores na avaliação de riscos e, mais do que proteção, rápidas adaptações nas estratégias dos negócios para aproveitar oportunidades ou preparar-se para as adversidades resultantes das modificações de cenários (Khan et al., 2016).

Diante dessa complexidade do ambiente de negócios, novos agentes têm surgido nas relações empresariais e, mesmo os conhecidos, tem reagido de forma inesperada e por vezes antagônica, exercendo pressões que exigem das empresas novas atenções (Bohnert et al., 2018).

Destaca-se o fato de, mesmo fora dos ambientes acadêmico e empresarial, a sociedade ter se envolvido no tema e demonstrado progressivo interesse pelos riscos assumidos pelas organizações, com extensiva cobertura pela imprensa. Isso porque, com frequência, as falhas na gestão dos riscos das empresas ultrapassam seus limites organizacionais e impõem de forma coletiva suas consequências econômicas, políticas e sociais. São exemplos na recente história brasileira as tragédias no setor de mineração e os casos de fraudes sistemáticas em grupos empresariais do setor de infraestrutura, diretamente conectados às falhas na condução dos riscos das organizações envolvidas (The Economist, 2019).

Frente ao crescente desafio imposto pela velocidade das mudanças, gestores tem incorporado o acrônimo VUCA (*Volatility, Uncertainty, Complexity and Ambiguity*) para definir as variações no ambiente e têm sido forçados a aumentar a agilidade estratégica de seus negócios como resposta à escalada da volatilidade, incerteza, complexidade e ambiguidade desse ambiente (Burke, 1985; Weber & Tarba, 2014).

Uma gestão de riscos proporcionalmente mais madura e ativamente ligada a agilidade estratégica e às novas pressões passam então a fazer mais sentido que a abordagem convencional, conhecida como Gestão Tradicional de Riscos (GTR), e que tem foco em mitigação (Kaplan & Mikes, 2012). A GTR é usualmente segmentada por áreas funcionais, processos ou unidades de negócios, e tem se mostrado ineficiente para acompanhar mudanças repentinas, principalmente pela sua forma de administração confinada em “silos” (Dionne, 2013; Soltanizadeh et al., 2016).

Nesse contexto, a Gestão de Riscos Corporativos (GRC) emergiu de um esforço para incorporar elementos estratégicos a partir de uma gestão mais abrangente e holística dos riscos empresariais, assim expandida em relação a visão em silos (Bromiley et al., 2014). Partindo

dos trabalhos de Kloman (1976, 1992), a GRC ganhou força após 2002 por sua contribuição às novas práticas administrativas exigidas por stakeholders e cristalizadas principalmente nas leis americanas Sarbanes-Oxley, daquele ano, e pela mais recente reforma Dodd-Frank, de 2010 (Florio & Leoni, 2017).

Em contraste com a GTR, que objetiva proteção, a GRC pretende gerar valor à empresa (COSO, 2004; Hahn & Kuhn, 2012). Nesse paradigma, a internalização da eficiência em gestão de riscos é uma capacidade empresarial que se acumula e resulta em vantagem competitiva (Harrington, Niehaus, & Risko, 2002).

Para o *Committee of Sponsoring Organizations of the Treadway Comission* (COSO), a GRC é um processo aplicado na definição de estratégias para criar um ambiente seguro quanto ao atingimento dos objetivos, administrando-os de forma que estejam dentro do apetite à riscos da organização (COSO, 2004, 2017).

Dadas essas características de processo e de capacidades da Gestão de Riscos Corporativos, os modelos de maturidade foram a ela aplicados de diversas formas, embora modelos de maturidade em GRC ainda sejam escassos (Oliva, 2016).

Modelos de maturidade são ferramentas de gestão capazes de aferir o estado atual, de compará-lo a padrões e de fornecer subsídios para planejar a evolução de processos de negócios (Röglinger et al., 2012). São formas simples e eficazes de mensurar competências organizacionais por meio de estágios ou níveis incrementais que acumulam as capacidades dos níveis anteriores (Van Looy, 2014). Podem ser conceituais ou operacionais, porém, como qualquer modelo, são apenas representações da realidade para um propósito específico (Wacker, 1998).

Nesta tese, uma revisão sistemática da literatura foi conduzida a partir de mais de 5mil documentos científicos iniciais. Como um de seus resultados, constatou-se que modelos de maturidade no contexto da GRC são frequentemente desenhados para propósito específico, como identificado por von Känel, Cope, Deleris, Nayak, & Torok (2010), e escassos, como concluiu Oliva (2016).

Evidência disso é que dos 177 artigos sobre GRC filtrados de *journals* de administração, apenas cinco propuseram um modelo de maturidade, dos quais dois são teóricos, dois são específicos para os setores de construção e saneamento, e apenas um é multisetorial com fundamentação empírica, ainda que sem características operacionais. Essa revisão sistemática da literatura está propriamente descrita nos capítulos seguintes.

Dessa forma, fica evidente a dificuldade para encontrar na literatura acadêmica um modelo de maturidade que seja diretamente aplicável (i.e. operacional) para avaliar a maturidade em GRC de organizações. Nesse contexto, esta tese presta uma contribuição teórica por desenvolver um Modelo Operacional para Avaliação da Maturidade em Gestão de Riscos Corporativos para preencher essa lacuna.

Também presta uma contribuição gerencial, uma vez que demonstra como utilizar o modelo para priorizar ações de melhoria nas organizações. O modelo desenvolvido foi mais simplesmente denominado MAM-GRC, acrônimo de Modelo de Avaliação de Maturidade em GRC.

Para apresentar o MAM-GRC, esta pesquisa empreendeu seis etapas metodológicas. Nas três primeiras etapas, um modelo foi construído a partir de extensa base teórica. Na quarta etapa, o modelo inicial foi aperfeiçoado com o resultado de entrevistas em profundidade com profissionais qualificados em gestão de riscos de diferentes áreas e indústrias. Na quinta etapa, o MAM-GRC foi aplicado em três organizações de setores distintos, com níveis diferentes de maturidade em GRC. Finalmente, na sexta etapa, uma pesquisa por meio de questionário serviu de base para avaliar a utilidade e a aplicabilidade do MAM-GRC.

A seguir são apresentados como parte desse primeiro capítulo o problema de pesquisa, os objetivos definidos para contribuir com sua solução e as justificativas pertinentes. Os capítulos seguintes desta tese apresentam, no Capítulo 2, uma revisão da literatura sobre os modelos de maturidade aplicados à gestão de negócios, os fundamentos da Gestão de Riscos Corporativos e os modelos de maturidade existentes para a GRC, o que inclui uma revisão sistemática da literatura.

O Capítulo 3 apresenta os aspectos metodológicos desta tese e o caminho percorrido para desenvolver e aplicar o MAM-GRC. O quarto Capítulo mostra os resultados obtidos com o aperfeiçoamento do modelo, com sua aplicação em três organizações e da sua avaliação de utilidade e aplicabilidade. Com o objetivo de alavancar o impacto real da pesquisa desenvolvida, o Capítulo 4 também inclui uma descrição detalhada sobre a forma de aplicar o MAM-GRC e sobre como utilizá-lo para decisões gerencias em organizações reais.

Finalmente, o quinto Capítulo apresenta as considerações finais sobre a pesquisa e discorre sobre o atendimento aos seus objetivos, suas contribuições teóricas e gerenciais, bem como suas limitações.

1.1. Problema de pesquisa

Existem diversas estruturas conceituais que objetivam mensurar a Gestão de Riscos Corporativos. Elas frequentemente o fazem por meio de atribuição de pontuações, classificações em *rankings*, qualificações e quantificações de atributos ou níveis de implementação nas organizações. A maior parte desses *frameworks* provêm de grupos privados, como organizações setoriais ou consultorias, e foram criados em resposta a diretrizes impostas por reguladores ou para aplicação em projeto customizado ou em indústria específica (RIMS, 2011; von Känel et al., 2010).

São exemplos de modelos de indústria específica a Iniciativa para ERM da Standard & Poor´s, com foco no setor financeiro e ênfase em crédito, e o Modelo COBIT, do Instituto de Governança de TI, com foco em tecnologia da informação (ISACA, 2019; Standard & Poor´s, 2007). Exemplos de reações a reguladores são o Modelo Integrado do COSO, conhecido por ser um agregador e norteador de princípios, e o modelo da *Risk and Insurance Management Society* (RIMS), que tem foco na comparação de capacidades (i.e. *benchmarking*), ambos com origem na função dos Controles Internos das organizações (COSO, 2017; RIMS & Logic Manager, 2014).

Todavia, a abundância de modelos em GRC desenvolvidos por associações industriais, consultorias, ou disponíveis por assinatura não tem paralelo na academia (von Känel et al., 2010). Para compor a revisão da literatura desta tese, foram pesquisados 177 artigos de Gestão de Riscos Corporativos de forma sistematizada. Dentre todas essas publicações, apenas cinco Modelos de Maturidade em GRC foram encontrados, dos quais apenas um é multisetorial e tem base empírica. Ainda assim, esse modelo não tem características operacionais. Dentre os outros quatro Modelos de Maturidade restantes, dois são teóricos e dois foram desenhados especificamente para os setores de construção e saneamento.

Fica evidente, portanto, que os Modelos de Maturidade em Gestão de Riscos Corporativos são frequentemente desenhados para propósito específico, como von Känel et al. (2010) reconheceram, e escassos, como identificado por Oliva (2016). Disso decorre o primeiro problema desta pesquisa: a carência na literatura acadêmica de um Modelo de Maturidade em Gestão de Riscos Corporativos com ancoragem teórica e base empírica em mais de um setor.

Um segundo problema tem origem na dificuldade de aplicação ou operacionalização dos modelos de maturidade em Gestão de Riscos Corporativos disponíveis na literatura. Do ponto

de vista dos gestores, um modelo tem a função de identificar as áreas de desenvolvimento, avaliar o progresso da GRC e subsidiar um planejamento de melhoria (Yeo & Ren, 2009).

Como exemplos desse problema em GRC, tanto o modelo proposto pela RIMS (2006), um dos mais utilizados como ferramenta de avaliação por organizações de todos os tipos, quanto o modelo da Standard & Poor´s (2007), largamente empregado por empresas do setor financeiro, não incorporam as relações entre os agentes externos a empresa e abordam riscos como um problema a ser mitigado, portanto sem o atributo estratégico da GRC (Bromiley et al., 2014)

Corroborando com esses dois problemas, Wendler (2012) fez um mapeamento sistemático sobre o desenvolvimento e utilização de modelos de maturidade em mais de 20 áreas de gestão e, em todas elas, encontrou lacunas de validação e deficiências de aplicação dos modelos existentes. Concluiu que frequentemente há pouca ou nenhuma validação empírica, que autores tem maior preocupação em propor do que em validar modelos, e que a maioria dos modelos de maturidade encontrados devem ser melhorados. Wendler (2012) não contemplou modelos de gestão de riscos em seu estudo. Contudo, se sua conclusão é válida para áreas que utilizam mais intensivamente os modelos de maturidade, é provável que em Gestão de Riscos Corporativos não seja diferente.

Finalmente, um terceiro problema advém da própria evolução da Gestão de Riscos Corporativos, que tem se transformado em um guarda-chuva com cada vez mais responsabilidades, inclusive a de administrar riscos provenientes de grupos e atores fora de seus limites organizacionais (Arena et al., 2017). Nesse contexto, os riscos que inicialmente eram analisados de forma restrita às atividades da empresa passaram a ser avaliados sob o ponto de vista de novos agentes e suas relações (Manuj & Mentzer, 2008; Oliva et al., 2022). Tais agentes podem ser clientes, fornecedores, concorrentes, parceiros de inovação, ou quaisquer outros operadores com influência na geração ou potencial para a destruição de valor (Grace et al., 2015). O problema decorrente dessa tendência é que os modelos existentes não incorporam explicitamente as capacidades de gerir relações entre agentes (Oliva et al., 2011; Oliva, 2016).

Assim, para contribuir com possíveis soluções aos problemas elencados, esta tese apresenta uma pesquisa para responder a seguinte pergunta-problema:

Como determinar o Nível de Maturidade em Gestão de Riscos Corporativos das empresas e quais são as ações necessárias para elevar esse nível?

Para responder a essa pergunta foram definidos um objetivo de pesquisa principal, quatro objetivos secundários e algumas definições operacionais, apresentados a seguir.

1.2. Objetivos de pesquisa

Para investigar o problema de pesquisa proposto, e considerando sua orientação a solução de problemas das organizações, a seguir estão detalhados os objetivos geral e específicos dessa pesquisa, assim como as definições operacionais principais do objetivo geral (Aken, Berends, & Bij, 2012; Aken & Romme, 2009).

Objetivo geral: *Analisar o nível de maturidade em Gestão de Riscos Corporativos em grandes organizações.*

Objetivos específicos:

1. *Identificar as práticas de gestão de riscos essenciais para avaliar o nível de maturidade em Gestão de Riscos Corporativos.*
2. *Determinar elementos de Gestão de Riscos Corporativos suficientes para definir níveis de maturidade em Gestão de Riscos Corporativos.*
3. *Propor um modelo operacional para avaliar a maturidade em Gestão de Riscos Corporativos.*
4. *Identificar as ações gerenciais pertinentes para elevar, a cada nível, a maturidade em Gestão de Riscos Corporativos das organizações avaliadas pelo modelo.*

Definições operacionais:

Analisar: Definido pelo cumprimento dos quatro objetivos específicos da pesquisa para conceber, propor, aplicar e avaliar o Modelo Operacional para Avaliação da Maturidade em Gestão de Riscos Corporativos, denominado MAM-GRC.

Nível de maturidade em Gestão de Riscos Corporativos: Definido pelo modelo de Oliva (2016) em cinco níveis: Insuficiente, Contingencial, Estruturado, Participativo e Sistêmico.

Grandes organizações: Três organizações de grande porte estabelecidas no Brasil, de setores distintos, e de diferentes níveis de maturidade em GRC.

1.3. Justificativa

Ao desenvolver um Modelo Operacional para Avaliação da Maturidade em Gestão de Riscos Corporativos (MAM-GRC) esta pesquisa colabora, inicialmente, para suprir a escassez de ferramentas de avaliação de GRC que tenham bases tanto teórica quanto empírica e, ao mesmo tempo, não sejam específicas para determinada indústria.

Logo, proporciona a pesquisadores uma ferramenta de mensuração de GRC capaz de ser diretamente implementada e apta a assistir estudos futuros que demandem uma medida de GRC das organizações investigadas, ainda que sejam de diferentes setores. Também, para as organizações, o MAM-GRC pode instrumentalizar uma autoavaliação com o objetivo de identificar o estado atual da GRC e, por consequência, as áreas a serem desenvolvidas. Pode, ainda, subsidiar um planejamento de melhoria e servir como critério para avaliar o progresso de implementação da GRC (Yeo & Ren, 2009).

Ao aplicar o método de estudo de caso múltiplo, de abordagem qualitativa, a pesquisa viabiliza o estudo da efetividade da gestão de riscos com evidências que normalmente são tradas de forma superficial pelos estudos quantitativos de grande amostragem (Kaplan & Mikes, 2012). Em adição, a literatura sobre Gestão de Riscos Corporativos menciona com frequência sugestões para que futuras pesquisas sejam feitas com diferentes setores, uma vez que há uma concentração de estudos em empresas financeiras, tais como bancos e seguradoras. Dessa forma, ao estudar casos específicos, essa pesquisa desafia a fraqueza das generalizações (Choi et al., 2015; Dionne, 2013).

Sobre esse assunto, Kaplan & Mikes (2012, 2016) concluíram que *surveys* sobre melhores práticas não são capazes de revelar se, e como, gestores de riscos conseguiram interromper atividades que ultrapassaram os limites aceitáveis do ‘apetite a risco’ da organização. Ou como gestores de risco fizeram escolhas entre stakeholders quando tiveram que decidir suas prioridades. Isso porque, a final de contas,

> “As empresas revelam seu real apetite a riscos não quando fazem afirmações clichê, mas quando tem que atuar em relação aos valores que estão por trás dele em situações de teste verdadeiro e em circunstâncias que as force a um *trade-off* entre seus diversos grupos de stakeholders” ,(Kaplan & Mikes, 2016 p. 16, tradução nossa).

Também por isso, essa pesquisa colabora para a melhor determinação de um limite para a Gestão de Riscos Corporativos em relação ao ambiente externo à organização. Esse limite ainda não é bem definido e o escopo da GRC tem sido discutido sob a ótica de stakeholders

(Grace et al., 2015), de agentes externos (Arena et al., 2017) e da própria estratégia empresarial (Bohnert et al., 2018).

Uma metáfora válida é a de um alvo para ilustrar a empresa no centro com circunferências concêntricas a cada nível mais externo ao ambiente organizacional. Se por um lado há um reconhecimento recente de que os riscos não estão apenas dentro das organizações, ou no centro do alvo, por outro lado não há um limite definido a partir do qual não se deva mapear riscos, ou a partir de qual circunferência mais externa do alvo a Gestão de Riscos Corporativos passa a ser ineficaz e o *arms lenght* passa a prevalecer (Arena et al., 2017; Oliva, 2016).

Apesar de não haver ainda uma resposta assertiva para esse problema, é provável que a fronteira não seja rígida ou delineada como na metáfora do alvo, mas um gradiente pelo qual as pesquisas mais recentes têm se expandido. Nessa fronteira teórica da GRC, Oliva (2016) introduziu o conceito de concorrência entre cadeias de valor ao verificar que agentes com objetivos comuns competem por recursos, mercados e profissionais com outras cadeias de valor. Também encontrou evidências de que gestores de grandes empresas brasileiras consideram muito relevantes os riscos relativos às relações com agentes de sua cadeia.

São exemplos na cadeia de valor os riscos sociais, de imagem, éticos, tecnológicos, do ambiente natural, entre outros que tem origem não apenas nos tradicionais agentes mais próximos da cadeia produtiva, como fornecedores e distribuidores, mas também em agentes mais periféricos ou de ambientes mais abrangentes, como governo e sociedade (Oliva, 2016).

Logo, a abrangência de um modelo operacional de maturidade em GRC em relação ao ambiente de valor da empresa pode contribuir para o debate sobre o próprio escopo da GRC. Ou, na metáfora anterior, até a que distância do centro do alvo os riscos devem ser reconhecidos e geridos.

A viabilidade dessa pesquisa resulta, primeiro, da existência de modelos de maturidade em GRC, ainda que poucos, sobre os quais se possa avançar em direção a um modelo operacional e, enfim, a um modelo de avaliação. Segundo, pelo número de profissionais que gentilmente contribuíram para a pesquisa e ao interesse do tema a essas organizações. Dessa forma, essa pesquisa contribui para o aumento da vantagem competitiva das empresas ao oferecer uma ferramenta que auxilia no incremento da Gestão de Riscos Corporativos e, em última instância, aumenta o nível de maturidade em GRC das organizações.

A originalidade da pesquisa é dada inicialmente pela própria lacuna na literatura, evidenciada pela revisão sistemática da literatura sobre Modelos de Maturidade em Gestão de Riscos Corporativos, anteriormente introduzida e oportunamente detalhada nos capítulos a

seguir. Também, pela evidência do tema de gestão de riscos, que tem ultrapassado a academia e está em discussão pela própria sociedade, com implicações em novas exigências morais, éticas e regulatórias. Entretanto, apesar das crescentes determinações regulatórias, há evidências de que empresas adotam níveis mais maduros de gestão de riscos por motivações mais econômicas do que por obrigações oficiais (Pagach & Warr, 2011).

Nesse mesmo contexto, incrementos no nível de maturidade em GRC nas grandes corporações ultrapassam as vantagens econômicas dos negócios *per se* e vão além da contribuição prática e prescritiva para o aumento da vantagem competitiva das empresas. São também de interesse da sociedade, uma vez que empresas mais maduras em GRC são capazes de identificar, informar, compartilhar e gerir níveis realistas de riscos com seus stakeholders, o que inclui os colaboradores, governo e a sociedade (Beasley, Branson, & Pagach, 2015).

Finalmente, o consequente impacto social do aumento do nível de maturidade em Gestão de Riscos Corporativos das organizações é o melhor gerenciamento dos riscos a que a sociedade está exposta através do maior conhecimento, da melhor avaliação e do tratamento mais eficiente dos possíveis impactos negativos das atividades empresariais, incluindo a prevenção de comportamentos oportunistas (COSO, 2017; IRM, 2018; ISO 31000, 2018; Paape & Speklé, 2012).

2. REFERENCIAL TEÓRICO

Este capítulo apresenta a fundamentação teórica que subsidia a pesquisa e sustenta o atingimento do seu objetivo geral de analisar o nível de maturidade em GRC em grandes organizações. Para isso, revisita estudos seminais e atuais sobre os temas de Modelo de Maturidade e de Gestão de Riscos Corporativos. Ainda, apresenta os resultados de uma Revisão Sistemática da Literatura (RSL) sobre Modelos de Maturidade em Gestão de Riscos Corporativos. Os caminhos metodológicos e a fundamentação teórica para a RSL são detalhados no Capítulo 3 - Metodologia.

2.1. Modelos de maturidade, antecedentes, tipos e aplicações em gestão

Os conceitos essenciais para o desenvolvimento de modelos de maturidade tiveram origem nas preocupações com o controle de qualidade de manufaturas nos anos 1930 e foram cristalizados no fim dos anos 1970 (Van Looy, 2014). Nolan (1979) propôs seis níveis incrementais de capacidade de processamento de dados no mesmo ano em que o clássico livro de Philip B. Crosby, "*Quality is Free: The Art of Making Quality Certain*" trouxe a proposição de um modelo com cinco níveis acumulativos de maturidade e seis categorias de melhores práticas para qualidade (Crosby, 1979). Ambos são modelos que apresentam estágios sucessivos que complementam os anteriores e, por isso, apresentaram uma forma simples e eficaz de medir e analisar negócios (Carmona et al., 2017).

Alguns anos mais tarde, os modelos de maturidade receberam um importante incremento ao serem aplicados para o desenvolvimento de softwares. Essa evolução contou com a iniciativa do departamento de defesa estadunidense que, a partir da necessidade de avaliar riscos de desenvolvedores e fornecedores participantes de licitações para a aquisição de softwares, formou o Instituto de Engenharia de Software (*Software Engineering Institute* - SEI) na universidade Carnegie Mellon (Röglinger et al., 2012).

O SEI desenvolveu então o *Capability Maturity Model* (CMM), que tem sido permanentemente atualizado e é referência para o desenvolvimento de softwares. Neste contexto, destaca-se o papel de Watts S. Humphrey, quem aproveitou sua experiência na IBM e participou da fundação do SEI. Ele é aclamado como o introdutor dos conceitos de processo,

de capacidade e de gestão ao CMM, bem como disseminador dos modelos de maturidade a partir da publicação de "*Managing the Software Process*", (Humphrey, 1989).

Nos anos 1990, os modelos de maturidade proliferaram-se em diversas áreas a partir do pressuposto de que as empresas poderiam melhorar seu desempenho se compreendessem a organização através de uma nova ótica por processos. Essa abordagem foi invocada por Hammer & Champy (1993) como uma "reengenharia da corporação". Boa parte da gestão de negócios então adaptou-se para o *Business Process Management* (BPM).

No paradigma do BPM, métodos testados de gestão com uma abordagem integrada e orientada a processos (*Business Process Orientation* – BPO) podem fornecer fundamentos para desafios atuais e futuros em administração. Dentre os benefícios do enfoque por processos estão listados a maior satisfação de clientes, maior eficiência, redução de custos, maior transparência, maior agilidade de negócios e facilidade em cumprir normas (Van Looy, 2014; vom Brocke et al., 2014).

Mais recentemente, modelos de maturidade são tão presentes na administração que tanto gestores quanto acadêmicos precisam empreender esforço para selecionar o modelo adequado dentre tantas possibilidades. Entretanto, a maior parte deles é descritiva e poucos modelos atingem o nível prescritivo. Dessa forma, em algumas áreas de gestão os modelos de maturidade oferecem pouca ajuda, tanto na identificação de níveis de maturidade, como para guiar a adoção de melhorias, por sua própria superabundância (Röglinger et al., 2012).

2.1.1. Modelos de maturidade e modelos de avaliação

No contexto de modelos de maturidade baseados em processos, Tarhan, Turetken, & Reijers (2016) conduziram uma revisão sistemática da literatura a partir de 2899 modelos em diversas áreas de gestão e destacaram uma aparente confusão entre *Modelo de Maturidade* e *Modelo de Avaliação*. O último, do inglês *Assessment Model*. Os autores definiram as diferenças a partir de suas observações e conceitos propostos pela ISO/IEC 15.504, de 2004. Para os autores,

> A avaliação de processo investiga pontos fortes, fracos ou ausentes na definição ou aplicação de um processo em relação a um modelo de referência. Ao avaliar o nível de maturidade de uma organização, o modelo de maturidade atua como o modelo de referência contra o qual o status atual é conferido utilizando o modelo de avaliação ou método. A avaliação fornece um entendimento sobre a situação atual do processo e permite classificar a qualidade do processo com base nesse entendimento. As descobertas de uma avaliação de processo são

> normalmente utilizadas para revelar as lacunas em relação ao modelo, o qual, então, serve de partida para o desenvolvimento de um plano para a melhoria do processo (Tarhan et al., 2016, p. 129, tradução nossa).

A *International Organization for Standardization* (ISO) revisou em 2015 a norma utilizada por Tarhan et al. (2016) e publicou a ISO/IEC 33001:2015, atualmente (2022) em fase final de revisão. Nela constam as seguintes definições (ISO, 2015, p. 3, tradução nossa):

> **Modelo de maturidade de capacidade** (*capability maturity model*): modelo que contém os elementos essenciais de processos efetivos para uma ou mais disciplinas e descreve um caminho evolutivo de melhorias conforme: ad hoc, imaturo, processos disciplinados e processos maduros com qualidade e efetividade melhorada.
>
> **Maturidade organizacional** (*organizational maturity*): âmbito pelo qual uma organização tem, de forma consistente e explícita, implementado processos que são documentados, gerenciados, medidos, controlados e continuamente melhorados. Nota: Maturidade organizacional pode ser medida via avaliações.
>
> **Maturidade de processo organizacional** (*organizational process maturity*): o âmbito pelo qual uma unidade organizacional consistentemente implementa processos, dentro de um escopo definido, que contribui para o alcance de suas necessidades de negócios (atuais ou projetadas). Nota: O escopo definido é o do modelo de maturidade especificado.
>
> **Nível de maturidade** (*maturity level*): ponto em uma escala ordinal de maturidade de processo organizacional que caracteriza a maturidade da unidade organizacional avaliada no escopo do modelo de maturidade utilizado.
>
> **Modelo de medição de processo** (*process measurement framework*): esquema para ser utilizado na qualificação das características de um processo implementado.
>
> **Desempenho de processo** (*process performance*): âmbito pelo qual a execução de um processo atinge seu objetivo.

Portanto, a principal diferença entre um modelo de maturidade e um modelo de avaliação é que um modelo de maturidade tem a intenção de servir como um modelo de referência para ser comparado, enquanto um modelo de avaliação permite medir o estado atual e possibilita identificar lacunas (ISO, 2015; Tarhan et al., 2016).

2.1.2. Modelos conceituais e modelos operacionais

As definições de modelo são bastante amplas do ponto de vista científico. Para Wacker (1998), as boas práticas para suporte empírico e construção de teorias prescrevem a elaboração de modelos para construir relações e estabelecer a lógicas de suas ligações. Em pesquisas sociais, um modelo pode estar presente em uma fase teórica, que é a formulação de um problema de pesquisa e a indicação das relações com fatos empíricos. Ou ainda em uma segunda fase, “que pode ser definida como o processo que sofre uma variável (ou um conceito) a fim de

se encontrar os correlatos empíricos que possibilitem sua mensuração ou classificação" (Gil, 2010, p. 81).

Mazzon & Berndt (1978, p. 11) explicam o processo de criação de modelos da seguinte forma:

> "O domínio conceitual da realidade começa através de idealizações, ou seja, pela criação de um objeto-modelo ou modelo conceitual de uma coisa ou de um fato, assim, um modelo conceitual é uma representação de um objeto, ora perceptível, ora imperceptível, sempre esquemática parcial e, sob certos aspectos, convencional. Estabelece, em termos amplos, a definição de um particular problema que será resolvido; especifica o domínio das variáveis que poderão ser usadas e define essencialmente a própria natureza do problema"

Assim, um modelo conceitual tem o objetivo de analisar relações baseadas em uma teoria, por isso também denominados modelos teóricos, enquanto um modelo operacional pretende capturar a realidade observada através da instrumentalização do modelo teórico. Modelos operacionais formam a ligação entre um modelo teórico e as evidências e são geralmente constituídos de codificações de natureza qualitativa ou métricas de natureza quantitativa (Bryman, 2008).

Os conceitos de operacionalização variam nas abordagens qualitativas e quantitativas, mas distinguem a composição dos modelos operacionais a partir de bases teóricas, ou modelos teóricos. Assim, modelos operacionais geralmente procedem os teóricos ou conceituais, principalmente quando existe a relação de complementaridade ou realimentação entre pesquisa quantitativa e qualitativa. É preciso considerar que ambos os modelos não são capazes de incorporar a realidade completa e são formas idealizadas dos fenômenos (Echambadi et al., 2006; Shah & Corley, 2006).

Portanto, a principal diferença entre um modelo conceitual e um modelo operacional é que o modelo conceitual faz análises de relações com base em uma teoria, enquanto um modelo operacional instrumentaliza o modelo teórico em um contexto real.

2.1.3. Objetivos da apresentação de modelos de maturidade pela literatura

Em um estudo que contemplou 237 artigos sobre modelos de maturidade, Wendler (2012) demonstrou que os modelos de maturidade têm sido aplicados a mais de 20 áreas diferentes, sendo a engenharia de software a que mais o emprega pela sua própria origem. O

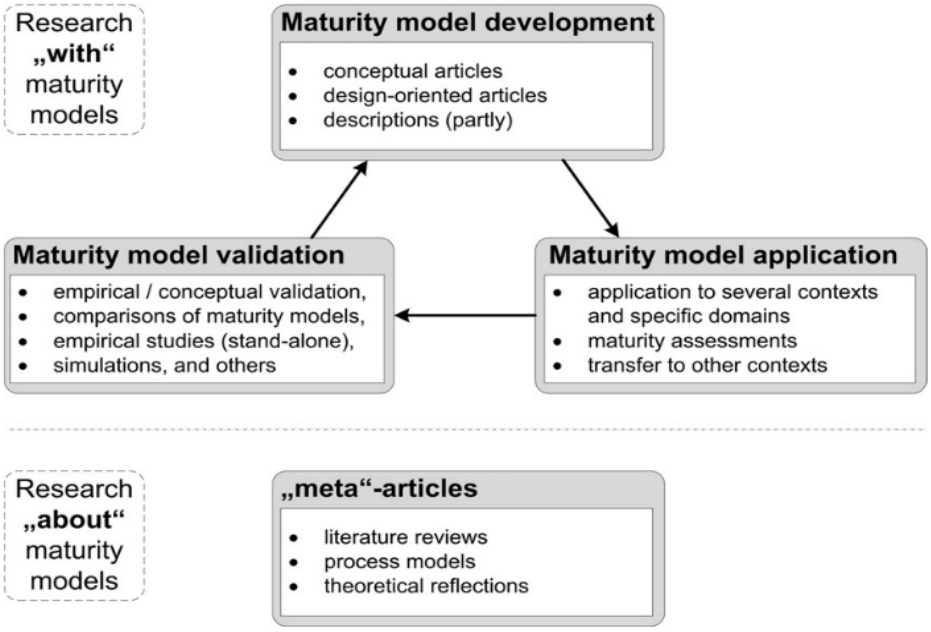
autor descobriu que a maior parte das publicações tratam do desenvolvimento de modelos de maturidade e publicações teóricas ou que discutem os modelos são raras, mesmo nas áreas em que ele é mais utilizado. Ainda, que poucos modelos desenvolvidos foram utilizados por outros autores que não os mesmos que os propuseram.

Em seu trabalho, Wendler (2012, p. 1324) investigou o desenho de pesquisa, o método de pesquisa, a área de aplicação e o modelo utilizado ou desenvolvido. A partir disso, classificou os artigos estudados em quatro tópicos mutuamente exclusivos, conforme:

> **Desenvolvimento de modelo de maturidade (*maturity model development*):** artigos dentro desse tópico tem o objetivo principal de desenvolver ou construir um novo modelo de maturidade. Podem conter modelos conceituais, planejados (*design-oriented*) ou descrições de modelos, se o propósito é a introdução de um novo modelo.
>
> **Aplicação de modelo de maturidade (*maturity model application*):** artigos dentro desse tópico tem o objetivo principal de aplicar os modelos de maturidade em diversos contextos ou áreas específicas. Eles também contêm modelos de avaliação e modelos de transferência.
>
> **Validação de modelo de maturidade (*maturity model validation*):** artigos dentro desse tópico tem o propósito principal de validar modelos de maturidade existentes. Isso inclui validações empíricas ou conceituais, comparações de modelos de maturidade, simulações, e assim por diante.
>
> **Meta-artigos (*meta-articles*):** o principal objetivo dos artigos nesse tópico não é a pesquisa "com", mas a pesquisa "sobre" modelos de maturidade. Eles são, por exemplo, revisões de literatura, modelos de processos para o desenvolvimento de modelos de maturidade, ou outras considerações teóricas.

A Figura 1 apresenta a estrutura de classificação e análise de artigos sobre modelos de maturidade proposto por Wendler (2012), que também foi aplicado por Tarhan et al. (2016).

Figura 1 – Estrutura de classificação de modelos de maturidade de Wendler (2012)



Fonte: *Comprehensive research framework in maturity model research* (Wendler, 2012, p. 1331).

Portanto, os modelos de maturidade também podem ser classificados como de desenvolvimento, aplicação, validação ou meta-artigos.

2.2. Gestão de Riscos Corporativos e suas práticas de gestão

Historicamente, a administração do risco nas organizações tem sido implementada de forma segregada, notadamente como resultado das diferentes partes da estrutura organizacional ou dos processos operacionais e de gestão das corporações. Como exemplo, é comum que áreas financeiras tenham concentrado atenção aos riscos de câmbio e taxas de juros enquanto executivos ligados às operações tenham estado mais preocupados com riscos relacionados à segurança e qualidade (Bromiley et al., 2014).

Essa gestão de riscos tem sido referida Perspectiva Baseada em Silos, do inglês *silo-based perspective*, ou Gestão Tradicional de Riscos (GTR) (Gatzert & Martin, 2015). De forma complementar a GTR, uma maneira coordenada de gerir riscos, também chamada *holística*, teve início com os resultados de (Kloman, 1976, 1992) e ganhou tração após a promulgação em 2002 da lei americana Sarbanes-Oxley. Trata-se da Gestão de Riscos Corporativos (GRC). O desenvolvimento prático e conceitual da GRC vem rapidamente evoluindo desde então e tem despertado interesse tanto de corporações, quanto de instituições de classe, consultorias, auditorias e pesquisadores (Hagigi & Sivakumar, 2009).

Segundo Hoyt e Liebenberg (2011), o primeiro registro acadêmico do termo *Enterprise Risk Management* foi feito em 1996 ao se referir ao trabalho de James Lam na General Electric Capital. O Sr. Lam passou a ser o primeiro *Chief Risk Officer* (CRO) conhecido.

Uma corrente principal da literatura sobre GRC sustenta que ela é capaz de gerenciar um portifólio que consiste em todos os riscos da organização. Essa maneira agregada passa então a ser mais eficiente que a gestão individual dos riscos, das partes da organização ou de atividades. Como exemplo dessa proposição, podemos considerar a influência da elevação da taxa básica de juros de determinada economia sobre uma organização. Se ela possui segmentos ou negócios que podem ser negativamente afetados com a elevação dos juros (p. ex. sofrer aumentos de custo) e ao mesmo tempo tem outros segmentos que podem ter seus retornos alavancados com a elevação dos juros (p. ex. aumentar receitas), então uma gestão agregada dos riscos de aumento dessa taxa de juros é naturalmente mais eficaz que os esforços individuais

de seus segmentos ou negócios para protegerem-se dessa variável macroeconômica (Harrington et al., 2002).

Outra característica extensivamente exemplificada na literatura sobre GRC é sua capacidade de incluir os riscos relacionados às estratégias corporativas que a visão em silos não pode capturar. Por isso, a GRC tem características muito mais próximas ao planejamento estratégico da organização e mais apropriadas à visão mais distante de prazos e cenários (Aabo, Fraser, & Simkins, 2005; Bromiley et al., 2014).

Nesse contexto estratégico e de longo prazo, o *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) produziu o Modelo Integrado de Gestão de Riscos Corporativos, apresentado pela primeira vez em 2004. Ele representa um esforço para desenvolver e operacionalizar conceitos de gestão de riscos que funcionam alinhados aos objetivos da organização.

Para o COSO, risco é a possibilidade de que um evento tenha impacto nos objetivos, sendo o evento uma ocorrência tanto interna quanto externa. São definidas quatro classificações de objetivos: Estratégicos, Operacionais, de Comunicação e de Conformidade. Entretanto, para o COSO, risco é a dimensão negativa da incerteza, podendo essa também ser uma fonte de oportunidades (COSO, 2004; 2017).

Também a *International Organization for Standardization* (ISO) propõe uma visão sistêmica do modelo de Gestão de Riscos Corporativos através de suas normas 31000. Para a ISO, o risco é o efeito da incerteza no alcance dos objetivos da empresa e suas normas pretendem estabelecer um processo sistemático e lógico para tornar a gestão de riscos eficaz. Semelhante ao COSO, a ISO 31000 define risco como o "efeito da incerteza nos objetivos". Define ainda efeito como "um desvio em relação ao esperado", podendo ser este positivo ou negativo. Também define incerteza como "o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade" (ISO, 2009).

A Tabela 1, a seguir, apresenta as referências em Gestão de Riscos Corporativos relevantes para esta pesquisa e que formam a base teórica do MAM-GRC.

Tabela 1 – Principais referências em GRC que fundamentam a pesquisa

Fonte	Principais contribuições teóricas para a pesquisa
Baird & Thomas (1985)	Estudos do risco estratégico, definiram um modelo com componentes ambientais, setoriais, organizacionais, do tomador de decisão e de variáveis do problema.
March & Shapira (1987)	Gestores são insensíveis em calcular reais probabilidades; seus focos em metas desviam suas decisões; e consideram a tomada de riscos equivalentes a fazer apostas.
Ghoshal (1987)	Visão agregada de riscos, classificou quatro categorias: macroeconômico, político, competitivo, e de recursos. As quatro categorias são mutáveis ao longo do tempo.
Miller & Bromiley (1990)	Três fatores principais com efeito sobre os resultados corporativos: risco de fluxo de renda; de retorno das ações; e estratégico. Sugeriram novos trabalhos para melhor definir e medir risco.
Miller (1992)	Elaborou um modelo de risco integrado compilando teorias. Esse modelo teve propósito aos negócios internacionais.
Jorion (2000)	Três riscos a que as empresas estão expostas: risco do negócio, estratégico e financeiro.
Harrington et al. (2002)	A GRC é capaz de gerenciar uma carteira de riscos constituída de toda a empresa de forma mais eficiente que a gestão individual dos riscos, das atividades ou partes.
COSO (2004)	Modelo Integrado de Gestão de Riscos Corporativos alinhado aos objetivos organizacionais. É um dos modelos mais utilizados no mundo.
Aabo et al. (2005)	A GRC agrega também os riscos estratégicos que a fragmentação da Gestão Tradicional de Riscos não é capaz de capturar.
Deloitte (2005) [1]	As maiores perdas de valor estão relacionadas a eventos de baixa probabilidade, porem de alto impacto. Quatro categorias: estratégicos, operacionais, financeiros e externos.
RIMS (2006) [2]	GRC é uma disciplina de gestão estratégica que suporta a conquista dos objetivos de uma organização através da identificação de um espectro completo dos seus riscos e da gestão dos impactos combinados desses riscos.
Nocco & Stulz (2006)	Empresas de sucesso assumem mais riscos em suas atividades essenciais e buscam proteção para outras atividades. Gerir riscos na cadeia é uma vantagem comparativa.
Standard & Poor´s (2007) [3]	A GRC é uma abordagem que permite a gestores, acionistas e conselho decidir sobre quais riscos devem tomar ou não. Cria métodos para mudar o foco de custo/benefício para risco/retorno.
Gordon, Loeb, & Tseng (2009)	Índice para medir a efetividade da GRC das empresas baseado nos quatro pilares propostos pelo COSO: estratégia, operações, comunicação e conformidade.
Ojasalo (2009)	Modelo para gestão de riscos em empresas globalizadas com seis etapas: identificação do contexto; identificação dos riscos; análise dos riscos; avaliação dos riscos; mitigação dos riscos e monitoramento e melhoria.
ISO:31000 (ISO, 2009) [4]	Visão sistêmica do modelo de GRC como um processo lógico para tornar a gestão de riscos eficaz. Risco é o efeito da incerteza no alcance dos objetivos da empresa.
Aon (2010) [5]	Cinco níveis de maturidade de GRC. Compromisso da alta gestão e desenvolvimento de cultura de comprometimento de todos os stakeholders são fundamentais.
Pagach & Warr (2011)	Evidências de que as empresas adotam a GRC por motivações mais econômicas do que por exigências regulatórias.
Liesch, Welch, & Buckley (2011)	Concluíram que gestores não tem boa compreensão se estão administrando riscos ou incertezas.
Bromiley et al. (2014)	A GRC é mais alinhada ao planejamento estratégico e a visão de prazos e cenários mais distantes. Também envolve estimações e probabilidades que a GTR não pode considerar.

Gatzert & Martin (2015)	Revisão da literatura sobre GRC. A GRC tem impactos positivos em diversas métricas de performance. Os resultados são ainda mais positivos para as seguradoras.
Edmonds et al. (2015)	Escala de oito pontos para medir a qualidade da gestão de riscos das empresas, com base em quatro objetivos do modelo COSO sobre as responsabilidades da diretoria.
Choi et al. (2015)	Fizeram uma revisão da literatura entre 2000 e 2014 e apresentaram métodos utilizados para abordar a GRC de forma empírica.
Oliva (2016)	Modelo de maturidade no qual a GRC tem cinco níveis: insuficiente, contingencial, estruturado, participativo, sistêmico. A análise de riscos corporativos não é posicional, mas uma análise relacional da organização frente ao ambiente e seus agentes.
Viscelli, Beasley, & Hermanson (2016)	Investigou as responsabilidades do conselho de administração e identificou diversas oportunidades para futuras pesquisas.
COSO (2017)	Reforçou principalmente a ligação entre gestão de riscos e estratégia, atualizando o modelo de 2004 com a incorporação de características de estratégia, globalização, alta complexidade, novas tecnologias e transparência.
Florio & Leoni (2017)	Utilizou conceitos de Governança Corporativa da equivalente italiana da lei Sarbanes-Oxley em três níveis (conselho diretivo, comitê de risco e gestor de risco) para medir a maturidade da GRC.
ISO:31000 (ISO, 2018) [4]	Segunda edição da ISO 31000. Entre as principais atualizações está o papel da liderança, a maior iteratividade na gestão dos riscos e a revisão de processos.
Shad et al. (2019)	Incorpora o papel da sustentabilidade e seu efeito moderador no impacto da Gestão de Riscos Corporativos.
Oliva et al.(2022)	Aplica o conceito de ambiente de valor para avaliar riscos relacionados ao conhecimento disperso entre agentes de um sistema de inovação aberta. Exemplifica os tipos de relações entre agentes do ambiente de valor.

Notas: 1 Deloitte Touche Tohmatsu Ltd; **2** Risk and Insurance Management Society; **3** Standard & Poor´s Financial Services llc; **4** International Organization for Standardization; **5** Aon Risk Management Plc. **Fonte:** elaborado pelo autor a partir de Bution (2016).

Por diversas motivações, tais como o aumento da complexidade do ambiente de negócios e as diversas pressões dos stakeholders, as ameaças fora do escopo da corporação recentemente passaram a ter mais relevância na gestão de riscos das organizações, com consequente impacto na elaboração de suas estratégias (Bohnert et al., 2018). Essa realidade foi refletida na dilatação dos limites da GRC e promoveu revisões de diretrizes importantes.

É exemplo a nova "*Enterprise Risk Management - Integrating with Strategy and Performance*" do COSO, publicada em 2017 e que emenda a tradicional versão de 2004 adicionando ênfase na relação entre gestão de riscos e estratégia. Essa versão, representada pelo modelo da Figura 2, incorpora novas características de globalização, de alta complexidade do ambiente, das novas tecnologias e de maior transparência (COSO, 2017).

Figura 2 - Modelo COSO de GRC integrado à estratégia e desempenho

Fonte: COSO (2017, p. 6).

Nesse novo conceito apresentado pelo COSO em 2017, a estratégia empresarial é construída e implementada considerando riscos e recursos a partir da missão, visão e valores da organização (COSO, 2004, 2017). Essa construção difere da abordagem anterior em que a empresa define sua estratégia e então gerencia o que poderia afetá-la. Nesse novo paradigma há dois aspectos adicionais principais: a possibilidade de a estratégia não estar alinhada com a missão, visão e valor; e as implicações dos *trade-offs* entre as possíveis estratégias (COSO, 2017).

Seguindo a mesma tendência, a *International Organization for Standardization* (ISO) publicou em 2018 a segunda edição de sua norma para Gestão de Riscos Corporativos de 2009, a ISO 31.000. Entre as principais atualizações estão o papel da liderança e a maior preocupação com as iterações, ou interrelações, entre riscos na sua gestão (ISO, 2018). Do ponto de vista dos gestores, além do planejamento estratégico, a efetiva implementação da GRC em suas organizações depende de ações práticas. "*Strategy Execution Is the Key*" foi o jargão imortalizado pelos professores Lawrence Hrebiniak e William Joyce em 1984 (Hrebiniak & Joyce, 2008).

Em relação às práticas de gestão, no Brasil, a Fundação Nacional da Qualidade (FNQ) define:

> **Prática de gestão (ou prática gerencial):** Processo gerencial como efetivamente implementado pela organização. Atividades executadas regularmente com a finalidade de gerir uma organização, de acordo com os padrões de trabalho;
>
> **Processo de gestão (ou processo gerencial):** Processo de natureza gerencial, não operacional (FNQ, 2011, p. 76).

Com abrangência internacional, a ISO também se define prática pelo contexto de gestão de processos em sua norma 31001 conforme:

> **Prática:** tipo específico de atividade que contribui para a execução de um processo.
>
> **Processo:** conjunto de atividades inter-relacionadas ou interativas que transformam entradas em saídas.
>
> **Prática genérica:** atividade que, quando executada de forma consistente, contribui para o alcance de um atributo de processo especificado.
>
> **Processo definido:** processo implementado que é gerenciado e adaptado a partir do conjunto de processos padrão da organização de acordo com as diretrizes de adaptação da organização (ISO/IEC 33001:2015, p. 38, tradução nossa).

Diversos estudos dedicaram-se a explorar as melhores práticas relacionadas à gestão de riscos. Zhao et al. (2013) fez um esforço através de revisão de literatura e aplicação de questionário com 89 profissionais para compilar 66 melhores práticas de GRC, organizadas em 16 grupos. Os agrupamentos de Zhao et al. (2013), são:

1) *Existe comprometimento da alta gestão com a GRC.* Atividades que exemplificam esse comprometimento são: Uma política escrita de GRC é aprovada pelo conselho e pela alta administração e é divulgada a todos os funcionários; Um plano de GRC é desenvolvido e adaptado aos objetivos e contexto corporativos; Todas as tomadas de decisão relacionadas ao risco e práticas de GRC são consistentes com a política e o plano de GRC; O conselho e a alta

administração participam ativamente da GRC; O compromisso é contínuo e não é interrompido por mudanças no conselho ou na alta administração.

2) *Existe responsabilidade sobre os riscos.* Todo risco tem um "dono" ou "proprietário do risco". Atividades que exemplificam esse comprometimento são: Um executivo sênior dedicado, departamento autônomo ou comitê de nível de conselho assume a supervisão de risco e centraliza o gerenciamento de risco; Todos os funcionários participam ativamente do processo de GRC; Cada categoria de risco crítico tem um proprietário do risco que compreende totalmente os riscos que estão dentro do limite de responsabilidade do proprietário; Todos os proprietários de risco têm autoridade suficiente para supervisionar qualquer ação relacionada ao risco e aceitam responsabilidades claramente definidas para gerenciar os riscos; A autoridade e a responsabilidade dos proprietários do risco são compreendidas pelos funcionários em todos os níveis da empresa; A GRC é incorporada na análise de desempenho e avaliação dos proprietários de risco.

3) *Existe tolerância e apetite a risco bem definidos.* Atividades que exemplificam essa prática são: O apetite de risco é formal e claramente definido de acordo com a estratégia corporativa; O apetite pelo risco é comunicado a todos os funcionários da empresa; A tolerância ao risco para cada risco específico é formal e claramente definida de acordo com os objetivos corporativos; As diferenças entre a tolerância ao risco definida e os riscos reais são avaliadas regularmente; Os efeitos esperados das medidas de resposta ao risco são medidos em relação à tolerância ao risco.

4) *Existe uma cultura consciente dos riscos.* Atividades que exemplificam essa prática são: Uma cultura de consciência de risco é criada em toda a empresa e faz com que a equipe em todos os níveis tenha consciência de risco; Um clima de confiança é criado dentro da empresa e das equipes de projeto; A cultura de consciência de risco está completamente incorporada à cultura corporativa; Não há cultura de culpa nem rotinas defensivas na organização; O comportamento esperado dentro da organização é expresso de forma explicita e colabora para sustentar uma forte cultura de consciência de risco.

5) *Existem recursos suficientes para a GRC*. Atividades que exemplificam essa prática são: Os recursos são continuamente investidos na melhoria, por exemplo, do processo de gestão de risco, ferramentas, técnicas e habilidades do pessoal; Os recursos são alocados para a resposta ao risco com base nos resultados da análise de risco e na prioridade de risco; A empresa possui pessoal qualificado suficiente e conhecimento interno, habilidades e experiência para implementar a GRC; Consultores externos ou especialistas, se necessário, são usados para

reforçar e complementar conhecimentos e habilidades internas existentes sobre a GRC; Um conjunto abrangente de métricas é aplicado de forma consistente para medir o desempenho da GRC.

6) *Há eficiência na identificação, análise e resposta ao risco*. Atividades que exemplificam essa prática são: Uma empresa adota um processo de GRC formalizado e padronizado tanto nos níveis de projeto quanto de toda a empresa; As informações de risco coletadas são garantidas como relevantes e confiáveis; Ferramentas e técnicas qualitativas e/ou quantitativas de gestão de risco são utilizadas rotineiramente; A organização identifica de forma abrangente as fontes de risco, áreas de impactos e suas causas e impactos potenciais; A probabilidade de ocorrência e magnitude do impacto de todos os riscos identificados é analisada a fim de identificar a classificação de risco e a prioridade de gestão; A interdependência entre riscos de diferentes tipos é considerada e avaliada; A estratégia de resposta ao risco apropriada é escolhida considerando a significância do risco, apetite e tolerância ao risco, disponibilidade de recursos e comparações de custo *versus* benefício, bem como os objetivos da empresa; A resposta a riscos é projetada para lidar com riscos críticos em suas fontes.

7) *Os processos de GRC são dinâmicos e realimentados*. Atividades que exemplificam essa prática são: Os riscos novos e emergentes são identificados de forma consistente de maneira oportuna e proativa; As informações de risco são coletadas de várias fontes e atualizadas rotineiramente; As atividades de identificação, análise e resposta de riscos são continuamente monitoradas, revisadas e aprimoradas; O processo de GRC é claramente registrado para torná-lo conveniente para revisão e melhoria; Os riscos residuais, que permanecem após as medidas de resposta terem sido totalmente implementadas, são avaliados.

8) *A GRC é relacionada as oportunidades*. Atividades que exemplificam essa prática são: É amplamente reconhecido na empresa que as oportunidades são um aspecto dos riscos; As oportunidades são regularmente identificadas e exploradas durante o planejamento de gerenciamento de risco; As oportunidades são avaliadas regularmente, pesando os benefícios esperados e a probabilidade relevante contra as perdas potenciais e suas probabilidades; Oportunidades para a melhoria esperada do desempenho da empresa são ativamente buscadas por meio da GRC; A tomada de riscos da empresa está alinhada com suas competências essenciais e seu apetite de risco.

9) *Existe uma comunicação sobre riscos*. Atividades que exemplificam essa prática são: As informações de risco são comunicadas e compartilhadas de forma consistente entre os projetos e departamentos da empresa; As informações de risco crítico são relatadas ao conselho e à alta

administração de maneira periódica ou imediata, de acordo com a gravidade ou urgência do risco; Linhas de comunicação claras são estabelecidas para garantir que os gerentes, gestores de projeto e equipe da linha de frente sejam prontamente notificados sobre informações e decisões críticas da alta administração; Comentários e opiniões individuais de especialistas internos ou externos são incentivados durante o processo de GRC.

10) *A GRC tem uma linguagem comum*. Atividades que exemplificam essa prática são: A linguagem de risco explica claramente as terminologias e metodologias de gerenciamento de risco usadas na organização; A linguagem do risco é entendida e mantida por todos os funcionários de uma empresa; A linguagem do risco é usada de forma consistente em toda a comunicação dentro da empresa.

11) *Existe um sistema de informações gerenciais para a GRC*. (*Risk Management Information System* - RMIS). Atividades que exemplificam essa prática são: Um RMIS serve como uma plataforma para comunicação e relatório de risco, registra atividades de GRC, realiza a identificação e análise de risco e facilita a seleção de estratégias de resposta; Os funcionários em todos os níveis entendem claramente como aplicar o RMIS nas práticas de GRC; As funções do RMIS são totalmente utilizadas nas práticas de GRC.

12) *Há programas de treinamento para a GRC*. Atividades que exemplificam essa prática são: Os programas de treinamento formalizados garantem que a equipe em todos os níveis compreenda claramente a política de GRC, o processo de GRC e os benefícios potenciais do GRC, reduzindo assim o mal-entendido e a ansiedade sobre o GRC; Treinamento regular é fornecido à equipe para manter seu alto nível de conhecimento e habilidades relacionadas a GRC; Os programas de treinamento fazem a equipe aprender com os sucessos e fracassos de projetos anteriores e em andamento; O pessoal que é profissional ou experiente em GRC compartilha seus conhecimentos relativos a GRC com colaboradores menos experientes em programas de treinamento.

13) *Existem indicadores formais para riscos*. (*Key Risk Indicators* - KRIs). Atividades que exemplificam essa prática são: KRIs são identificados para todos os riscos críticos que uma empresa enfrenta; Os KRIs são continuamente revisados e atualizados; Os KRIs são monitorados e analisados regularmente pelos proprietários de risco; Os KRIs atuam como sinais de alerta antecipado do aumento da exposição ao risco em uma empresa.

14) *Existe integração entre a GRC e os processos da organização*. Atividades que exemplificam essa prática são: A administração de uma empresa considera consistentemente as

informações de risco, a tolerância e o apetite ao risco e as estratégias de resposta ao risco em todas as atividades de tomada de decisão, especialmente na tomada de decisão estratégica; O GRC está totalmente integrado em todos os processos de gestão e negócios diários; Os níveis de implementação das melhores práticas de GRC são avaliados periodicamente para identificar lacunas e melhorar as práticas de GRC.

15) *Definição de objetivos*. Os objetivos da empresa são claramente identificados e compreendidos pelos colaboradores em todos os níveis. Todos os objetivos têm medidas de desempenho e todas as medidas de desempenho estão ligadas aos objetivos. Desvios de planos ou expectativas são avaliados em relação aos objetivos corporativos e objetivos do projeto.

16) *Monitoramento, revisão e melhoria do planejamento da GRC*. Atividades que exemplificam essa prática são: A empresa monitora periodicamente o progresso da implementação de GRC em relação ao plano de GRC e seu desvio; A empresa revisa periodicamente se a estrutura, política e plano de GRC ainda são apropriados, de acordo com o contexto externo e interno da empresa; As decisões são tomadas para melhorar a estrutura, a política e o plano do GRC com base nos resultados do monitoramento e das revisões.

2.3. Modelos de maturidade em Gestão de Riscos Corporativos

Apesar de ter evoluído rapidamente, formas de avaliação da GRC estão em construção e, em geral, pesquisadores tem encontrado dificuldades para avaliar o nível de adoção ou mesmo se a Gestão de Riscos Corporativos é de fato empregada (Choi et al., 2016; Schiller & Prpich, 2013). Para Beasley, Clune, & Hermanson (2005), essa dificuldade surge porque as empresas raramente explicitam informações sobre seus planos futuros. Outra barreira tem sido os problemas de amostragem, decorrentes de informações raras ou não confiáveis, o que restringiu a maioria das pesquisas a poucos setores, notadamente à bancos e seguros (Gatzert & Martin, 2015).

Gatzert e Martin (2015) analisaram as publicações que pretenderam determinar uma medida ou avaliar o grau de implantação da GRC e encontraram dois caminhos de pesquisa, definidos principalmente pelas fontes de dados: subjetivos, através de *surveys* e entrevistas, e objetivos, através de fontes públicas de dados. São exemplos de pesquisas objetivas, com dados secundários, os trabalhos de McShane, Nair, & Rustambekov (2011), que utilizaram as notas de GRC da Standard & Poor´s, disponível apenas para empresas financeiras, de Razali, Yazid,

& Tahir (2011) e de Tahir & Razali (2011), que utilizaram um banco de dados públicos da Holanda, e de Gordon et al. (2009), que desenvolveram seu próprio índice de GRC.

Partindo de dados subjetivos e primários, Beasley et al. (2005) encontraram sete fatores relacionados à implementação de GRC e Wan Daud, Haron, & Nasir Ibrahim (2011) determinaram a adoção de GRC através de cinco níveis, de 'sem plano para implementar' até 'GRC em pleno funcionamento'. Ainda, Yaraghi & Langhe (2011) encontraram 19 fatores críticos de sucesso para a implementação da GRC e apontaram estratégia, estrutura organizacional e comunicação como os três mais importantes.

Em um nível mais abrangente que o grau de implementação, Hillson (1997) foi o precursor de um Modelo de Maturidade ao incorporar cultura, processo, experiência e aplicação em um modelo de quatro níveis, denominados: ingênuo, novato, normalizado e natural. Aparentemente, nos anos seguintes os modelos de maturidade evoluíram para cinco níveis (Oliva, 2016).

Explorando as capacidades de gestão, a *Risk and Insurance Management Society* (RIMS, 2006) propôs um modelo de cinco níveis, denominados: ad hoc, inicial, repetitivo, gerido e liderado. Ainda, von Känel et al. (2010) categorizaram os cinco níveis de maturidade em: ad hoc, básico, consistente, forte mas separado e integrado com desempenho ajustado ao risco.

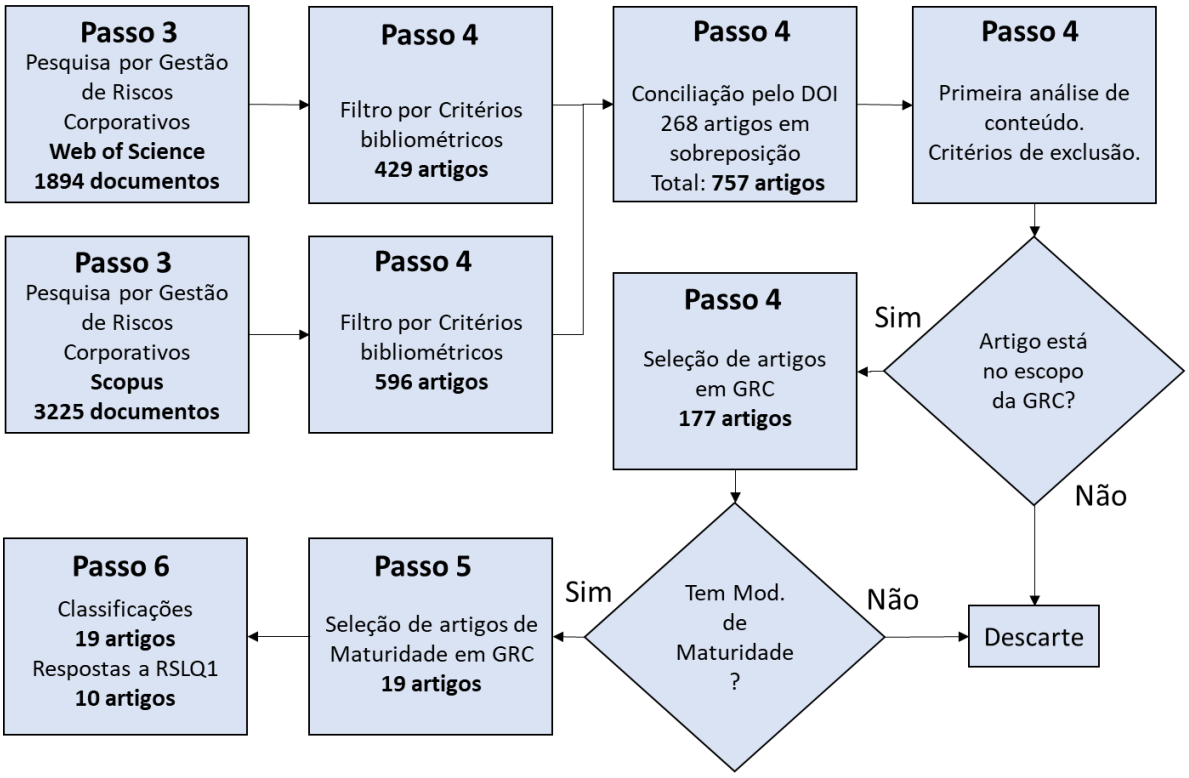
2.3.1. Resultados da Revisão Sistemática da Literatura sobre modelos de maturidade em Gestão de Riscos Corporativos

Conforme descrito anteriormente, uma Revisão Sistemática da Literatura (RSL) foi conduzida para identificar os modelos de maturidade em Gestão de Riscos Corporativos existentes bem como suas características conceituais e operacionais. Partindo de 1894 documentos encontrados na *Web of Science* e 3225 documentos encontrados na plataforma *Scopus*, foram identificados 19 artigos sobre Maturidade em Gestão de Riscos Corporativos.

Apesar de narrativas sobre Modelos de Maturidade e Gestão de Riscos Corporativos constarem nos textos dos 19 artigos selecionados, uma análise de conteúdo acurada revelou que em apenas dez deles a pesquisa de fato ocorreu com abordagem concordante com os conceitos da GRC. Nove artigos, apesar de mencionar a GRC, tratam riscos de forma setorizada, em silo, como gestão tradicional de riscos (Gatzert & Martin, 2015). A Figura 3 mostra o fluxograma e

os resultados quantitativos conforme os passos de 3 a 6, propostos por Petticrew & Roberts (2008) e descritas no Capítulo 3 - Metodologia.

Figura 3 – Resultados dos passos da RSL sobre modelos de maturidade em GRC



Notas: Passos conforme Petticrew & Roberts (2008): **3** Conduzir uma pesquisa abrangente da literatura para localizar estudos; **4** Filtrar verificando quais dos estudos aparentam cumprir os critérios de inclusão; **5** Analisar criticamente os estudos incluídos; **6** Sintetizar os estudos e evidenciar as heterogeneidades para conclusões. **Fonte:** elaborado pelo autor.

Dentre os nove artigos que não foram classificados como aderentes ao paradigma de GRC, sete são focados em projetos, com destaque para empresas do setor de construção. Alguns dentre esses sete artigos mencionam a possibilidade de estrapolação da gestão de riscos de um nível de projetos para o nível corporativo, argumentando que empresas desse perfil são formadas por um conjunto de projetos. Porém, nesses artigos, as metodologias empregadas não são capazes de capturar o nível corporativo das organizações estudadas e, mais ainda, os modelos resultantes são customizados para o setor.

Os dois artigos restantes dentre os nove não considerados como de Gestão de Riscos Corporativos fazem adaptações do modelo de Oliva (2016), utilizando recortes especificamente para a cadeia de valor de ônibus urbano e para *startups*.

2.3.2. Características dos modelos de maturidade em Gestão de Riscos Corporativos selecionados pela Revisão Sistemática da Literatura

Para responder à questão da revisão sistemática da literatura foram aplicadas as classificações de *Tipo de modelo*, *Forma de representação* e *Objetivo da apresentação do modelo* de acordo com a metodologia apresentada no Capítulo 3 – Metodologia. Vale adiantar esta questão:

RSL Q1: *Quais são os modelos de maturidade em Gestão de Riscos Corporativos existentes na literatura e quais suas características?*

Dentre os dez artigos que descrevem modelos de GRC, cinco são de Modelos de Maturidade, quatro de Modelos de Avaliação e um de meta-análise. Dentre os 4 Modelos de Avaliação, dois utilizaram dados da autoavaliação da RIMS e um artigo teve o propósito de apresentar um modelo multisetorial empregando uma *survey* de 15 perguntas na Tunísia. O artigo restante teve o propósito de aplicação e utilizou um questionário autodeclarativo de três perguntas diretas sobre o nível de maturidade em GRC das empresas pesquisadas.

Dentre os cinco Modelos de Maturidade encontrados em ERM, dois são teóricos e três empíricos. Ainda, dentre os cinco, dois são específicos para o setor de saneamento (sendo que dentre esses dois há o único que tem seguimento com validação e representação operacional), e apenas um modelo de maturidade teve base metodológica multisetorial: o modelo de Oliva (2016).

Em relação aos Modelos Operacionais, dentre os onze encontrados, cinco são de GRC. Entre os cinco de GRC, apenas dois chegaram a ser validados: um com dados do RIMS e um específico para o setor de saneamento. A Tabela 2 apresenta os dez artigos aderentes à Gestão de Riscos Corporativos e permite a melhor organização e visualização das descrições anteriores.

Tabela 2 – Artigos selecionados sobre modelos em Gestão de Riscos Corporativos

Artigo	Tipo de Modelo [A]	Objetivo quanto ao Modelo [B]	Forma de representação [C]	Setor e região	Método
Farrell & Gallagher (2019)	Avaliação	Validação	Operacional	Multisetor, diversos países	Empírico, quantitativo. 230 empresas que fizeram a autoavaliação do RIMS, com 5 níveis.
Mardessi & Ben Arab (2018)	Avaliação	Desenvolvimento	Operacional	Multisetor, Tunísia	Empírico, quantitativo. Survey, 15 perguntas (escala de 0 a 15) e 80 empresas respondentes.
Rubino (2018)	-	Meta-artigo	-	-	Teórico. Compara modelos dos *guidelines* de GRC.
Oliva (2016)	Maturidade	Desenvolvimento	Conceitual	Multisetor, Brasil.	Empírico, quantitativo. *Survey* com 18 questões, 168 empresas respondentes. 5 níveis definidos por clusters.
Farrell & Gallagher (2015)	Avaliação	Aplicação	Operacional	Multisetor, diversos países	Empírico, quantitativo. 225 empresas respondentes do RIMS. Porém com análise dicotômica (apenas 2 níveis) da autoavaliação do RIMS.
Beasley et al. (2015)	Avaliação	Aplicação	Operacional	Multisetor, EUA	Empírico, quantitativo. *Survey*, 3 perguntas (definido por autodeclaração) e 645 empresas respondentes.
von Känel et al. (2010)	Maturidade	Desenvolvimento	Conceitual	-	Teórico. Proposição teórica a partir da experiência dos autores na IBM.
MacGillivray et al. (2007a)	Maturidade	Desenvolvimento	Conceitual	Saneamento, 5 países.	Empírico, qualitativo. Painel com 16 experts. Adaptado especificamente para o setor de saneamento. Parte 1.
MacGillivray et al. (2007b)	Maturidade	Validação	Operacional	Saneamento, Reino Unido, Austrália e EUA.	Empírico, qualitativo. Estudo de 8 casos. Adaptado especificamente para o setor de saneamento. Parte 2.
Hillson (1997)	Maturidade	Desenvolvimento	Conceitual	-	Teórico. Primeiro a propor para GRC.

Notas: Referenciais teóricos: **A:** Modelo de Avaliação ou Modelo de Maturidade (Tarhan et al., 2016 ISO/IEC 33001:2015); **B:** Desenvolvimento, Aplicação, Validação ou Meta-artigos (Tarhan et al., 2016; Wendler, 2012); **C:** Modelo Conceitual ou Modelo Operacional (Echambadi et al., 2006; Gil, 2010; Mazzon & Berndt, 1978; Shah & Corley, 2006; Wacker, 1998). **Fonte:** Desenvolvido pelo autor.

Uma análise da Tabela 2 anterior permite concluir que, apesar de dezenove artigos relatarem que fizeram investigações sobre modelos de maturidade em gestão de riscos corporativos, apenas dez abordam riscos de forma corporativa pelos conceitos do COSO (2004, 2017) e ISO (2009; 2018). O problema mais comum é a estrapolação de modelos desenvolvidos para projetos sem a inclusão dos fatores estratégicos ou a superação dos silos necessários para abranger toda a corporação de forma integrada ou holística, caso de sete artigos.

A partir de um volume inicial de mais de cinco mil documentos cuidadosamente filtrados e conciliados em uma massa de 757 artigos de GRC, foram encontrados apenas cinco artigos que propõe modelos de maturidade para a GRC, dos quais quatro são teóricos ou específicos para setores, sendo o modelo de Oliva (2016) o único com fundamentação empírica e multisetorial.

2.3.3. O modelo de maturidade em Gestão de Riscos Corporativos proposto por Oliva (2016)

O Modelo de Maturidade em Gestão de Riscos Corporativos de Oliva (2016) é resultado de uma pesquisa primordialmente quantitativa e ancorada na Gestão de Riscos Corporativos (COSO, 2004, 2017; ISO, 2018; RIMS, 2006). Ela foi conduzida com especialistas e gestores em uma amostra de 243 empresas dentre as 1100 maiores empresas brasileiras de 2011. Esse modelo classifica a GRC em cinco níveis: (1) insuficiente; (2) contingencial; (3) estruturado; (4) participativo; e (5) sistêmico. A Tabela 3, a seguir, apresenta os níveis de maturidade propostos por esse modelo.

A Figura 4 apresenta o Modelo de Maturidade em Gestão de Riscos Corporativos de Oliva (2016) que expõe os ambientes de valor e de negócios e da companhia. No ambiente de negócios, principalmente suportado pela Nova Economia Institucional, há uma visão relacional dos agentes de forma que os riscos devem ser avaliados a partir da exposição dos objetivos corporativos a essas relações (Menard & Shirley, 2005; Richter, 2015).

Tabela 3 – Níveis de Maturidade em GRC definidos pelo modelo de Oliva (2016)

Nível 1 Gestão de Riscos Corporativos Insuficiente	Inclui empresas que tem pouco conhecimento dos riscos corporativos. Não há estrutura física ou conceitual dedicada aos riscos corporativos. A adoção de práticas de gestão de riscos ocorre de maneira não estruturada.
Nível 2 Gestão de Riscos Corporativos Contingencial	Envolve empresas que estão conscientes dos riscos a que estão expostas. As técnicas, ferramentas e métodos são grosseiramente utilizadas. A gestão de riscos é centralizada e caracterizada pelo baixo envolvimento dos funcionários em geral.
Nível 3 Gestão de Riscos Corporativos Estruturada	Envolvem companhias com alto grau de organização de processos relacionados à gestão de riscos. Há um uso mais intenso de técnicas, ferramentas e métodos.
Nível 4 Gestão de Riscos Corporativos Participativa	Inclui empresas com alto nível de conhecimento e organização que dizem respeito aos processos relativos à Gestão de Riscos Corporativos. A gestão de riscos é mais descentralizada. A comunicação é integral e parte importante da gestão de riscos. A Gestão de Riscos Corporativos é guiada pela maior parte dos funcionários.
Nível 5 Gestão de Riscos Corporativos Sistêmica	É o nível mais alto da classificação. Nesse nível as companhias têm uma gestão de riscos consciente, organizada e transparente. Essas empresas utilizam suporte externo de consultorias, parceiros e institutos de pesquisa para aperfeiçoar a gestão de riscos. Além do mais, a gestão de riscos da empresa inclui a avaliação do ambiente de valor, considerando que os riscos não respeitam os limites da empresa, eles são soberanos quanto aos limites da propriedade. Dessa forma, é esperado que a Gestão de Riscos Corporativos moderna transcenda suas práticas além dos limites da organização.

Fonte: Oliva (2016, p. 77-78). Tradução de Bution (2016).

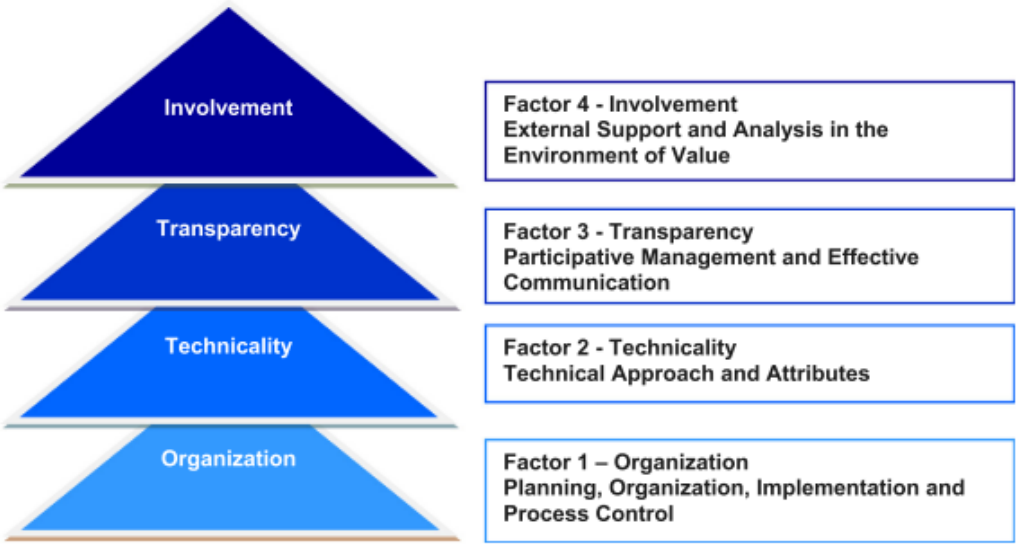
Figura 4 – Riscos Corporativos nos ambientes de valor e de negócios

Fonte: Oliva (2016, p.70, tradução nossa).

No ambiente de valor, suportado principalmente pelos conceitos da Cadeia de Valor, os agentes estão expostos a riscos relativos à destruição de valor (Oliva, 2016; Olson & Swenseth, 2014). Incorporando os três níveis ambientais em sua análise, Oliva (2016) encontrou quatro fatores explicativos para o nível de maturidade em gestão de riscos corporativos, que são: organizacional, de tecnicidade, de transparência e de envolvimento. Mais ainda, relacionou o desempenho de cada fator hierarquicamente, de forma que a evolução de nível de maturidade é explicada principalmente pelo desenvolvimento progressivo dos fatores.

A Figura 5 apresenta os fatores explicativos encontrados pelo autor com suas características progressivas, representadas pelo empilhamento de baixo para cima. Assim, um incremento de desempenho no fator organizacional é o maior responsável pela elevação da maturidade do nível 1 (insuficiente) para a maturidade de nível 2 (contingencial). Consecutivamente, um incremento de desempenho no fator de tecnicidade é o maior responsável pela elevação da maturidade do nível 2 (contingencial) para a maturidade de nível 3 (estruturado), e assim sucessivamente até a maior maturidade, de nível 5 (sistêmica).

Figura 5 – Fatores explicativos do Nível de Maturidade em GRC



Fonte: Oliva (2016, p.74).

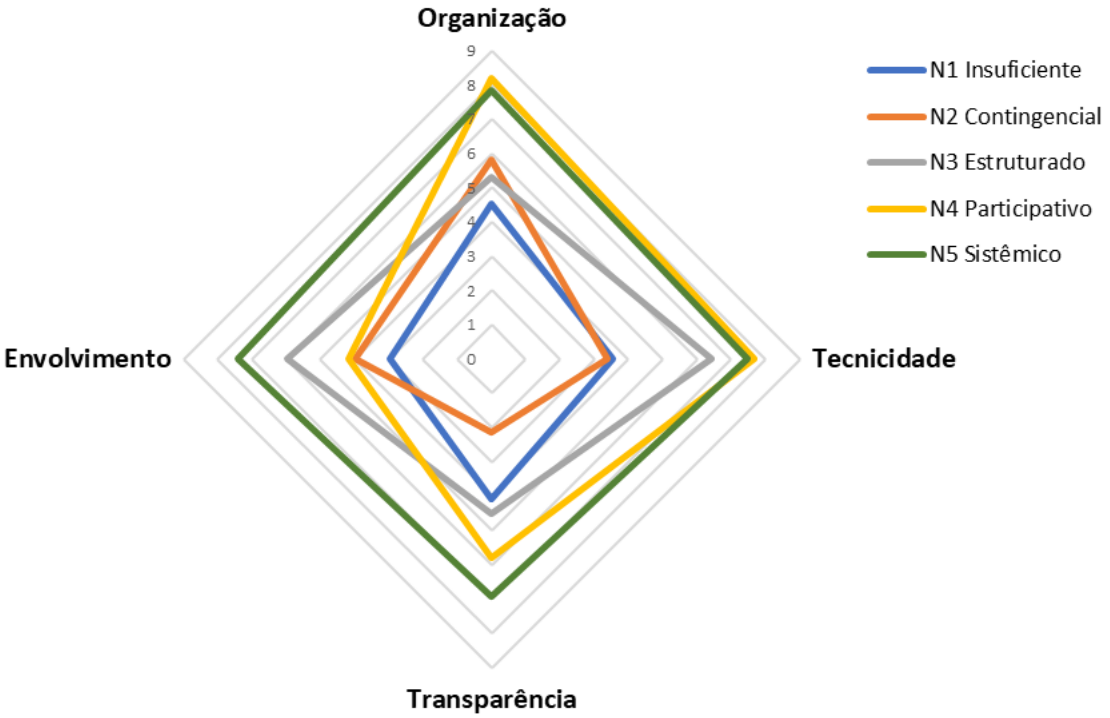
O primeiro fator, *organização*, representa o esforço dedicado pela organização para estruturar sua gestão de riscos, tais como planejar, organizar, implementar e controlar seu processo. O segundo fator, *tecnicidade*, envolve o desenvolvimento de atributos técnicos e incorpora a habilidade e implementação de métricas e técnicas qualitativas e quantitativas de suporte ao processo de gestão de riscos. O terceiro fator, *transparência*, tem a perspectiva de compartilhamento de informações e fluxo de comunicação para engajamento da organização.

Esse fator revela o quanto a empresa discute abertamente a gestão de riscos com seus colaboradores e os incluem para uma gestão participativa dos seus riscos.

O quarto e último fator é o envolvimento. Ele ultrapassa os limites da empresa e representa a habilidade em engajar também os agentes envolvidos em seu ambiente de valor. O fator envolvimento é uma das principais contribuições desse modelo e representa o poder de coordenação da empresa para que os riscos do seu ambiente de valor sejam gerenciados de forma orquestrada para melhor eficiência e efetividade.

Ao analisar as cargas fatoriais desses quatro fatores é possível observar o motivo pelo qual o autor identificou uma hierarquização entre eles. A Figura 6, a seguir, apresenta um gráfico das cargas obtidas por Oliva (2016) para cada nível de maturidade em Gestão de Riscos Corporativos do seu estudo. Uma análise dessa plotagem revela que a evolução dos níveis de maturidade em GRC parece ocorrer em espiral, do centro para a periferia, em sentido horário, de forma que cada fator contribui para a elevação do nível de maturidade a cada momento.

Figura 6 – Cargas dos fatores explicativos dos níveis de maturidade em Gestão de Riscos Corporativos identificados por Oliva (2016)



Fonte: Desenvolvido pelo autor com dados de Oliva (2016, p. 75).

É importante destacar que a progressividade dos fatores explicativos se dá pela maior influência de cada fator na elevação para o próximo nível de maturidade em GRC, entretanto, todos os fatores crescem em importância à medida em que o nível de maturidade em GRC também se eleva.

3. METODOLOGIA

Neste capítulo apresentam-se os *aspectos metodológicos* utilizados para determinar o tipo de pesquisa desta tese e o *caminho metodológico* percorrido para cumprir seus objetivos geral e específicos. O caminho metodológico apresenta uma divisão do método em etapas e assim organiza seu detalhamento.

3.1. Aspectos metodológicos e tipo de pesquisa

Considerando o problema de pesquisa desta tese e a orientação de seus objetivos específicos para a solução de problemas das organizações, trata-se de uma pesquisa *qualitativa* com paradigma de *pesquisa aplicada* (*Design Science Research*) desenhada predominantemente como um *estudo de caso múltiplo* (Aken, Berends, & Bij, 2012; Aken & Romme, 2009; Cooper & Schindler, 2014; Yin, 2013).

Para Aken, Berends, & Bij (2012), devido a sua orientação à solução de problemas, a *Design Science Research* tem as seguintes características:

> É direcionada por problemas de campo (não por problemas conceituais puros);
>
> Emprega a perspectiva do ator (e não a perspectiva do observador);
>
> É orientada a soluções (não apenas ao entendimento do problema); e
>
> Justifica os produtos da pesquisa com base em uma validação pragmática (se funciona ou não) (Aken, Berends, & Bij, 2012, p. 61, tradução nossa).

Para Lakatos & Marconi (2010), estudos qualitativos em sequência de quantitativos são importantes para capturar as formas de mudança dos fenômenos, que podem não ser contínuas como as conclusões quantitativas costumam apresentar. Dessa forma, este estudo pretende investigar nuances que geralmente passam despercebidas em análises quantitativas com agregações de práticas de gestão (Röglinger et al., 2012).

A utilização de estudo de caso múltiplo para fins desta pesquisa se justifica inicialmente porque os fenômenos estudados pertencem a vida real das atividades das empresas (Yin, 2013) e porque diferentes setores podem trazer especificidades mesmo sob a mesma base teórica (Oliva et al., 2018). Também, pela profundidade a que se deve chegar para alcançar elementos de análise sobre riscos e sua forma de gestão, sejam eles o de identificação de práticas de gestão

ou de ações pertinentes para elevar seu nível de maturidade (Federico Neto et al., 2018; Teberga et al., 2018; Bution et al.,2015).

Ainda, porque mesmo pesquisas com foco na resolução de problemas podem ser usadas para a geração de teorias explicativas (Aken, Berends, & Bij, 2012; Aken & Romme, 2009) e porque múltiplos casos permitem maior robustez de análise e maiores replicações teóricas e generalizações a partir de constatações e cruzamentos dos resultados dos casos (Cassell et al., 2018; Miles et al., 2014; Gil, 2002).

O principal instrumento de pesquisa de campo utilizado foi a *entrevista*, realizada em duas etapas distintas. Inicialmente, foram conduzidas entrevistas semiestruturadas com executivos experientes em gestão de riscos para auxiliar na consolidação dos elementos e das práticas de gestão de riscos mais importantes para determinar os níveis de maturidade em GRC. E assim cumprir os objetivos específicos 1 e 2 desta tese. E então, para assistir à elaboração do Modelo Operacional para Avaliação da Maturidade em Gestão de Riscos Corporativos (MAM-GRC), e assim cumprir o terceiro objetivo específico desta tese.

Em um segundo momento, foram conduzidas novas entrevistas com gestores das empresas estudadas para a aplicação do MAM-GRC em contextos reais de três organizações. Pretendeu-se assim conduzir uma pesquisa nos parâmetros sistemáticos do método científico para obter dados primários qualitativos e registrá-los em planilhas para compreender o fenômeno da aplicação do MAM-GRC nas grandes empresas brasileiras (Aken, Berends, & Bij, 2012; Aken & Romme, 2009).

Após a aplicação do MAM-GRC, um questionário anônimo foi aplicado com os mesmos gestores para avaliar a utilidade e aplicabilidade do modelo empregado. Entrevistas com roteiro semiestruturado são consideradas para estudos relativamente intensos e com número pequeno de unidades (Cooper & Schindler, 2014; Lakatos & Marconi, 2010). Enquanto o questionário, no caso desta pesquisa, permite ao entrevistado responder assertivamente e fornecer informações sem o viés do relacionamento com o entrevistador (Moser & Kalton, 2017).

Complementarmente, dados secundários foram somados nas diversas fases da pesquisa, inclusive os documentos indicados e disponibilizados pelos entrevistados, considerando a importância da contextualização e casuística de Yin (2010).

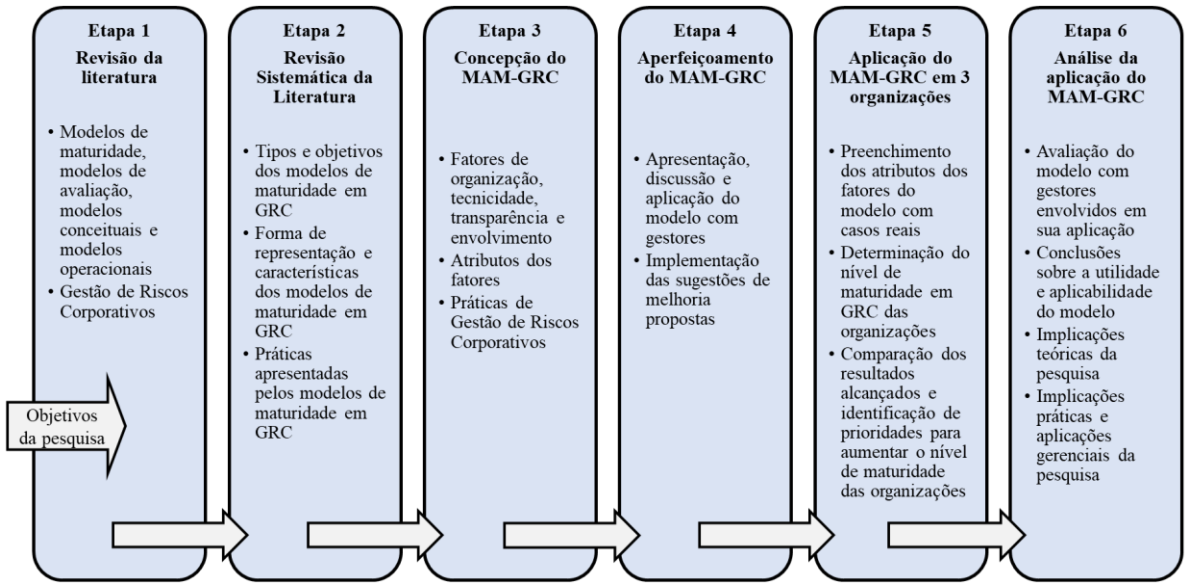
Finalmente, a análise deu-se a partir da teoria levantada, dos dados obtidos de forma primária com os documentos produzidos nas sessões com os entrevistados, e dos dados

secundários complementares (Aken, Berends, & Bij, 2012; Aken & Romme, 2009; Cooper & Schindler, 2014; Hsieh & Shannon, 2005; Sinkovics, 2018).

3.2. Caminho metodológico percorrido pela pesquisa

A fim de atingir seus objetivos geral e específicos, a pesquisa foi planejada e executada em seis etapas que, encadeadas e por vezes inter-relacionadas, constituem o caminho percorrido para sua realização. Este caminho está em linha com as premissas de validação de modelo de pesquisa, validação externa e de lógica para replicação da pesquisa qualitativa, como proposto por Yin (2010). A Figura 7 mostra o caminho metodológico da pesquisa e cumpre a função de ilustrar e organizar a apresentação de cada uma de suas etapas.

Figura 7 – Caminho metodológico com as etapas da pesquisa



Fonte: Elaborado pelo autor.

As etapas apresentadas estão detalhadas a seguir, organizadas em subitens correspondentes a figura anterior.

3.2.1. Etapa 1 – Revisão da literatura

A primeira etapa do caminho metodológico da pesquisa foi norteada pelo seu objetivo geral de analisar o nível de maturidade em GRC em grandes organizações, assim como pelos seus quatro objetivos específicos. Estes objetivos estão representados pela primeira da sequência de setas da Figura 7.

Dessa forma, a primeira revisão, sobre modelos de maturidade, pretendeu compreender seus antecedentes e sua evolução com aplicações na gestão das organizações. Também, teve o objetivo de levantar os tipos e classificações proeminentes de modelos de maturidade para suportar a próxima etapa do caminho metodológico: a revisão sistemática da literatura sobre modelos de maturidade em GRC.

Finalmente, nesta primeira etapa, também foram revisados os principais conceitos de Gestão de Riscos Corporativos e as contribuições acadêmicas, de consultorias, de reguladores e de órgãos normativos sobre o tema.

3.2.2. Etapa 2 – Revisão Sistemática da Literatura sobre modelos de maturidade em Gestão de Riscos Corporativos

A Revisão Sistemática de Literatura (RSL) é uma metodologia que permite chegar a conclusões razoavelmente claras a respeito do que é ou não conhecido sobre um tema científico. Ela é capaz de localizar pesquisas existentes, selecionar contribuições, analisar e sintetizar dados e organizar evidências (Denyer et al., 2008; Tranfield et al., 2003). Trata-se de uma alternativa ao método bola-de-neve de busca por referências, no qual uma bibliografia é composta através de investigações em série, usualmente seguindo o caminho das citações (Jalali & Wohlin, 2012).

Nesta segunda etapa do caminho metodológico da pesquisa, uma RSL foi conduzida principalmente para subsidiar três estágios importantes dessa tese:

> (1) Contextualização do problema de pesquisa a partir da identificação das lacunas na literatura de Gestão de Riscos Corporativos, como já apresentada desde a introdução desse trabalho;

(2) Levantamento de elementos de maturidade em Gestão de Riscos Corporativos através da identificação e classificação dos tipos, formas e objetivos dos modelos existentes na literatura.

(3) Constituição do corpo teórico para compor o Modelo Operacional de Avaliação da Maturidade em Gestão de Riscos Corporativos (MAM-GRC).

A principal vantagem da RSL advém do que seu nome intermediário representa. Sua característica "sistemática" confere aderência a um conjunto de métodos científicos, replicáveis e definidos *a priori*, que objetivam limitar e explicitar o erro sistemático, ou viés, na identificação, avaliação e síntese de todos os estudos relevantes para responder a uma questão específica (Fink, 2014; Petticrew & Roberts, 2008).

Petticrew & Roberts (2008) propuseram sete passos para a condução de uma revisão sistemática da literatura em ciências sociais, que são:

1. Definição clara da questão a que a revisão pretende responder, ou a hipótese que a revisão testará em consulta aos trabalhos anteriores.
2. Determinação dos tipos de estudo que precisam ser localizados para responder à questão anterior.
3. Conduzir uma pesquisa abrangente da literatura para localizar tais estudos.
4. Filtrar os resultados da pesquisa, isto é, verificar quais os estudos localizados e decidir quais aparentam cumprir os critérios de inclusão, quais precisam de maior análise e quais podem ser descartados.
5. Analisar criticamente os estudos incluídos.
6. Sintetizar os estudos e evidenciar as heterogeneidades de suas conclusões.
7. Disseminar os achados da revisão (Petticrew & Roberts, 2008, p. 27, tradução nossa)

Seguindo os passos de Petticrew & Roberts (2008), a RSL sobre Modelos de Maturidade em Gestão de Riscos Corporativos foi conduzida como melhor apresentada pela Tabela 4, a seguir. Para o primeiro passo, a questão de pesquisa foi definida por:

RSL Q1: *Quais são os Modelos de Maturidade em Gestão de Riscos Corporativos existentes na literatura e quais suas características?*

Tabela 4 – Passos da RSL sobre modelos de maturidade em GRC

Passo	Definições para a Revisão Sistemática da Literatura (RSL) aplicada
1.Questões que a RSL pretende responder.	RSL Q1: Quais são os Modelos de Maturidade em Gestão de Riscos Corporativos existentes na literatura e quais suas características?
2.Tipos de estudos localizados.	Artigos científicos que utilizem práticas de gestão para distinguir níveis ou mensurar a Gestão de Riscos Corporativos de organizações.
3.Pesquisa para localizar os estudos.	**Motores de busca:** Web of Science e Scopus. **Tema da pesquisa**: Gestão de Riscos Corporativos. **Palavras chave para GRC**: enterprise risk management ; enterpris* management of risk ; corporat* risk management ; corporat * management of risk ; total* risk management ; total* management of risk ; comprehensi* risk management ; comprehensi* management of risk ; strategic* risk management ; strategic* management of risk ; integrat* risk management ; integrat* management of risk ; global* risk management ; global* management of risk ; holistic* risk management ; holistic* management of risk ; complet* risk management ; complet* management of risk ; business risk management ; chief risk officer ; coso ; iso31000* ; iso 31000*. **Critérios de busca Web of Science:** Tópico do documento (TS); Intervalo de tempo: todos os anos. Bases de dados: SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH, ESCI. **Critérios de busca Scopus:** Título, resumo ou palavras-chave do documento (TITLE-ABS-KEY)
4.Filtrar resultados.	**Critérios bibliométricos de inclusão:** Artigos publicados em língua inglesa em periódicos revisados por pares (*journals*) de linha editorial correlata a Administração, em qualquer data. Categorias da Web of Science: BUSINESS FINANCE; MANAGEMENT; ECONOMICS; BUSINESS; SOCIAL SCIENCES INTERDISCIPLINARY; PUBLIC ADMINISTRATION. Área do assunto do Scopus: BUSINESS (SUBJAREA , "BUSI") **Critérios bibliométricos de exclusão:** Anais de congressos, livros, material jornalístico ou não indexados a um *Direct Object Identifier* (DOI). **Critérios de conteúdo para inclusão:** Artigos teóricos ou empíricos que empreguem práticas de gestão para distinguir níveis, mensurar ou modelar graus de Gestão de Riscos Corporativos. **Critérios de conteúdo para exclusão:** Temática estranha a Gestão de Riscos Corporativos conforme conceitos do COSO ou ISO 31000. Artigos que não abordem a Gestão de Riscos Corporativos através de práticas, modelos ou elementos de gestão.
5.Analisar os estudos incluídos. **6.Sintetizar e evidenciar as heterogeneidades.** **7.Disseminar.**	**Critérios bibliométricos**: Contextualizar o problema de pesquisa com métricas de publicações, colaborações e citações. **Critérios de conteúdo:** Formar o corpo de conhecimento em Modelos de Maturidade em Gestão de Riscos Corporativos para fundamentar a proposição do Modelo Operacional de Maturidade em Gestão de Riscos Corporativos.

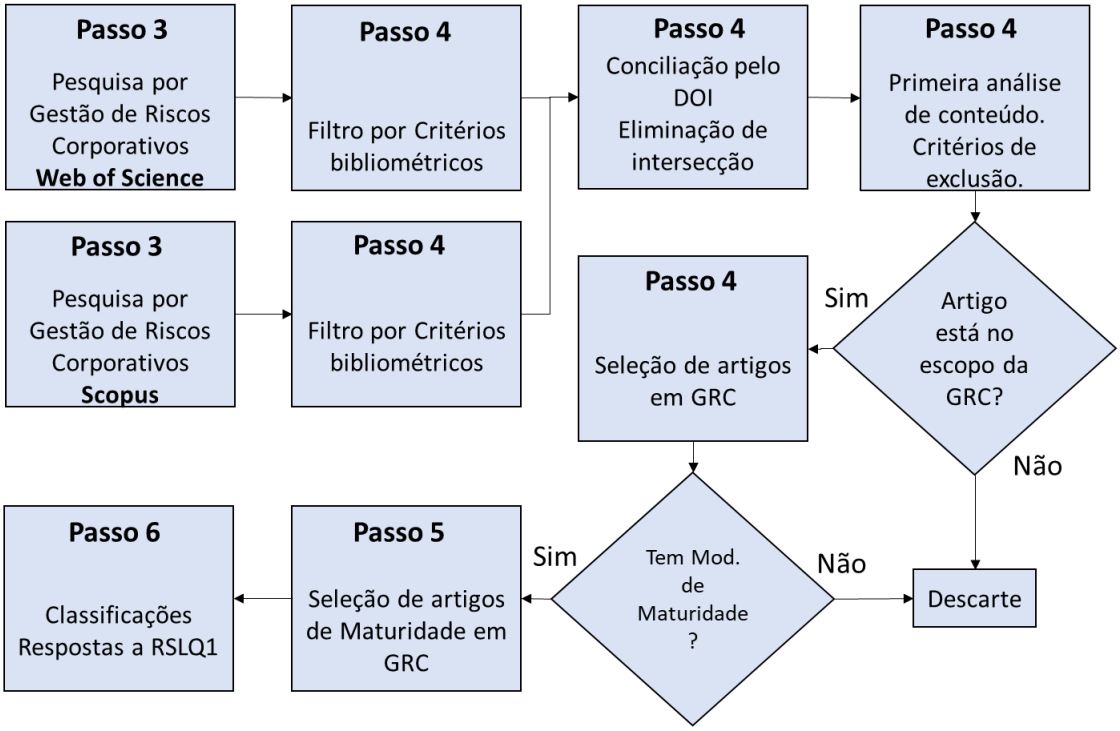
Fonte: Desenvolvido pelo autor a partir dos passos propostos por Petticrew & Roberts (2008)**.**

Para o segundo passo, foram pesquisados artigos científicos que utilizam práticas de gestão para distinguir níveis ou mensurar a GRC de organizações. Para o terceiro passo, foram utilizados os motores de busca do Clarivate Analytics Group, a *Web of Science*, e do Relx Group, o *Scopus*. Considerou-se que são complementares para as bases de dados mais relevantes às ciências sociais aplicadas, que o número de documentos pesquisados é relativamente pequeno para a capacidade computacional atual e que as publicações são relativamente recentes (Cobo et al., 2011; Wallin, 2005). Os resultados foram conciliados

através do *Direct Object Identifier* (DOI) para eliminação de duplicidades e composição de lista única de artigos (Crossref, 2019).

Nesse passo, um ponto de atenção surgiu ao considerarmos que o conceito de maturidade pode variar entre autores de tal modo que artigos poderiam não carregar a expressão "maturidade". Para contornar esse problema, foi conduzida uma pesquisa sobre *Gestão de Riscos Corporativos*, por ser este um tema mais abrangente e de denominação consolidada. Assim a seleção de "maturidade" foi transferida para o passo seguinte da RSL. Estas seleções podem ser melhor compreendidas através da Figura 8, onde combinações de métodos bibliométricos e de análise de conteúdo estão representadas em forma de fluxograma.

Figura 8 – Fluxograma do método da RSL sobre modelos de maturidade em GRC



Nota: A numeração dos passos refere-se aos passos propostos por Petticrew & Roberts (2008)**.** Fonte: Desenvolvido pelo autor.

Em relação à análise de conteúdo, trata-se de uma forma qualitativa, objetiva e ordenada de verificação de comunicação que pode ser aplicada a qualquer material simbólico (Hsieh & Shannon, 2005; Oliva et al., 2022; Seuring & Gold, 2012). Quanto aos métodos bibliométricos, Zupic & Čater (2015, p. 430, tradução nossa) explicam que:

> "Métodos bibliométricos permitem aos pesquisadores basear seus achados em dados bibliográficos agregados, produzidos por outros cientistas da área que expressam suas opiniões através de citações, colaborações e publicações. Quando esses dados são agregados e analisados, *insights* sobre a estrutura da área, redes de contatos e tópicos de interesse podem emergir."

Revisões Sistemáticas de Literatura são ferramentas valiosas para desobstruir caminhos congestionados pela superabundância de informações e possuem diversas vantagens sobre o método bola de neve. Entretanto, fatores subjetivos associados a critérios e filtros sempre existirão (Bar-Ilan, 2008). Para minimizá-los, duas medidas foram tomadas em relação às escolhas necessárias durante o processo: (1) os *trade-offs* e as escolhas decorrentes foram explicitados para possibilitar replicação e (2) foi preferida a qualidade, em termos de apresentação de práticas de gestão para distinguir níveis ou mensurar a Gestão de Riscos Corporativos de organizações, em detrimento da quantidade de artigos selecionados para análise final da literatura.

Para concluir esta segunda etapa do caminho metodológico da pesquisa, foram aplicadas as classificações da Tabela 5 para definir as características dos modelos de maturidade em Gestão de Riscos Corporativos.

Tabela 5 – Critérios para classificação dos artigos selecionados pela RSL

Classificação	Referenciais teóricos
Gestão de Riscos Corporativos *Em oposição à Gestão Tradicional de Riscos.*	COSO (2004, 2017); ISO 31000 (2018)
Tipo de modelo *Modelo de Maturidade* ou *Modelo de Avaliação*	Tarhan, Turetken, & Reijers (2016); ISO/IEC 33001:2015
Forma de representação *Modelo Conceitual* ou *Modelo Operacional*	Wacker (1998); Gil (2010); Mazzon & Berndt (1978); Echambadi, Campbell, & Agarwal (2006); Shah & Corley (2006)
Objetivo da apresentação do modelo *Desenvolvimento, Aplicação, Validação* ou *Meta-artigos*	Wendler (2012); Tarhan, Turetken, & Reijers (2016)

Fonte: desenvolvido pelos autores.

Dessa forma, os artigos selecionados pelos critérios bibliométricos e de análise de conteúdo foram analisados conforme os passos 5, 6 e 7 de Petticrew & Roberts (2008) à luz das classificações expostas pela Tabela 5, imediatamente anterior. Os resultados dessa revisão sistemática da literatura estão apresentados no Capítulo 2 – Referencial Teórico. Finalmente, essa compilação sobre o estado da arte em modelos de maturidade em GRC deu sustentação teórica para a composição do MAM-GRC, descrito na próxima etapa do caminho metodológico desta pesquisa.

3.2.3. Etapa 3 – Construção do MAM-GRC

O MAM-GRC foi então composto nesta terceira etapa do caminho metodológico percorrido pela pesquisa. A anterior Revisão Sistemática da Literatura sobre modelos de maturidade em GRC revelou que, dos cinco modelos de maturidade encontrados nessa área, quatro são teóricos ou foram desenhados para indústria específica, sendo o modelo de Oliva (2016) o único com fundamentação empírica e multisetorial.

Assim, o modelo conceitual de Oliva (2016) foi definido como principal ponto de partida para compor o modelo operacional proposto. Essa opção se justifica porque, inicialmente, ele tem origem na análise de grandes empresas brasileiras atuantes em diversos setores econômicos, logo tem menor propensão a vieses setoriais ou regionais (Spector et al., 2015; Tight et al., 2016).

Também, por sua metodologia quantitativa, adequada para ancorar subsequente investigação qualitativa (Echambadi et al., 2006; Shah & Corley, 2006). Ainda, pela sua consideração aos agentes externos à empresa focal na conceituação da Gestão de Riscos Corporativos e, finalmente, pela sua característica conceitual, que implica na possibilidade de desenvolvimento em direção à operacionalização (Gil, 2010; Wacker, 1998).

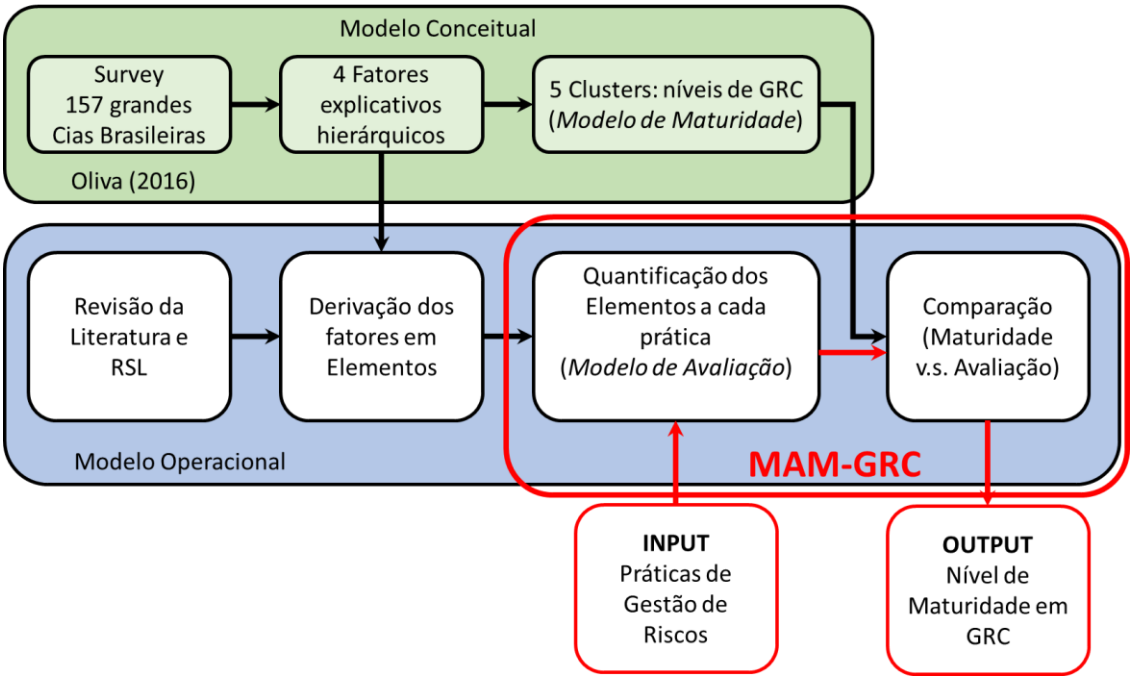
O modelo de Oliva (2016) foi construído sobre conceitos da Nova Economia Institucional (Menard & Shirley, 2005; Richter, 2015), da Cadeia de Valor (Oliva et al., 2014; Olson & Swenseth, 2014) e da Gestão de Riscos Corporativos (COSO, 2004, 2017; ISO, 2018; RIMS, 2006). Ao contrário dos modelos de maturidade baseados em processos de negócios, o autor definiu seus cinco níveis de maturidade a partir da agregação em clusters das 157 companhias pesquisadas.

A *survey* aplicada por Oliva (2016) foi reduzida a quatro fatores explicativos das práticas que indicaram o nível de maturidade em GRC. Esses fatores, ainda, puderam ser ordenados quanto aos seus pesos relativos para a posterior identificação de cinco agrupamentos, ou *clusters*. Os agrupamentos resultantes foram então caracterizados de acordo com seu nível de maturidade em GRC, como detalhado na revisão da literatura exposta no Capítulo 2. Assim, esta tese emprega os cinco agrupamentos do *modelo conceitual* de Oliva (2016) como um *modelo de maturidade* contra o qual o *modelo de avaliação* desenvolvido nesta tese pode ser comparado, para então determinar o nível de maturidade em GRC da organização avaliada.

De forma simples, pode-se comparar o modelo aqui proposto (MAM-GRC) como o mecanismo de avaliação da GRC em uma organização, enquanto o modelo de Oliva (2016)

serve como padrão contra o qual a avaliação é aferida. A Figura 9 apresenta o esquema empregado para desenvolver o MAM-GRC e assim operacionalizar o modelo de Oliva (2016).

Figura 9 – Desenvolvimento do MAM-GRC



Fonte: Desenvolvido pelo autor.

Na figura anterior, observa-se em verde o caminho metodológico da pesquisa quantitativa de Oliva, publicada em 2016, destacado em azul o modelo operacional que é o escopo desta tese e, em vermelho, o MAM-GRC. O processo de operacionalização do modelo de Oliva (2016), representado pela cor azul, ocorre, principalmente, pela derivação dos fatores explicativos para o nível de maturidade em GRC encontrados pelo autor. Vale revisitar esses fatores, que são: (F1) organização; (F2) tecnicidade; (F3) transparência; e (F4) envolvimento.

A racionalidade por trás da utilização desses fatores reside no fato de que eles são, grosso modo, a aglutinação das questões aplicadas pelo autor em sua *survey*, obtida através de uma análise fatorial com explicação total da variância de 80,75%. Assim, uma base teórica foi empregada para derivar cada um dos fatores em três elementos formativos, gerando assim um modelo de avaliação de doze elementos quantificáveis. A determinação desses elementos contribui para o alcance do terceiro objetivo específico da pesquisa.

Para colocar o MAM-GRC em prática e avaliar a maturidade em GRC de uma organização, deve-se iniciar pelo levantamento de suas práticas de GRC. Essas práticas adentram o MAM-GRC pelo fluxo representado em vermelho (*input*). Uma vez que as práticas são quantificadas em doze elementos, cada fator é calculado pela média aritmética de seus três

elementos correspondentes. Os valores obtidos para cada fator são então comparados aos valores dos fatores dos agrupamentos encontrados por Oliva (2016).

A partir dos valores apresentados por Oliva (2016), e seguindo uma lógica de restrições e gargalos (Şimşit et al., 2014), os determinantes de cada nível de maturidade foram identificados para compor uma *tabela determinante de nível* ajustada para uma escala de 0 a 1, como mostra a Tabela 6. Com ela, o fluxo de avaliação em vermelho segue para sua saída (*output*), ou seja, a caracterização da organização em um dos cinco níveis de maturidade em GRC.

Tabela 6 – Tabela determinante dos níveis de maturidade em GRC

Nível de Maturidade	**Valores dos fatores** (de 0 a 1)			**Características determinantes dos níveis**
	Média	Máximo	Desvio padrão	
Nível 1 Insuficiente	≤ 0,6	indiferente	< 0,1	No nível insuficiente, todos os fatores são proporcionalmente baixos. Logo, tanto a média de valor dos fatores como sua variância é pequena. Este nível tem como característica média baixa e desvio padrão baixo.
Nível 2 Contingencial	≤ 0,6	Organização	≥ 0,1	No nível contingencial, a média de valor dos fatores ainda é baixa. Entretanto, o fator organização se destaca como o de maior valor. O salto do fator organização aumenta, proporcionalmente, a variância entre fatores. Este nível tem como características a média entre fatores menor que 6, com desvio padrão alto e fator organização com maior valor.
Nível 3 Estruturado	> 0,6 e ≤ 0,7	Tecnicidade	~ 0,1	No nível estruturado, a média de valor dos fatores aumenta em relação ao nível anterior e o fator tecnicidade se destaca. Como o fator tecnicidade é acumulativo ao de organização, a variância pode aumentar. Este nível tem como características média entre fatores acima de 6 e fator tecnicidade como o de maior valor.
Nível 4 Participativo	> 0,7 e ≤ 0,8	Indiferente	≥ 0,1	No nível participativo, a média de valor dos fatores aumenta em relação ao nível anterior, mas todos os fatores permanecem desbalanceados. Alguns fatores podem ter valores inferiores ao do nível estruturado. Logo, a variância é alta. Este nível tem como características a média entre fatores acima de 7 com desvio padrão alto.
Nível 5 Sistêmico	> 0,8	indiferente	< 0,1	No nível sistêmico, todos os fatores são altos. Assim, a variância entre eles é pequena. Este nível tem como características a média entre fatores acima de 7 com desvio padrão baixo.

Nota: Tabela ajustada para uma escala de 0 a 1. Fonte: Desenvolvida pelo autor.

A Tabela 7 sintetiza a derivação dos quatro fatores de Oliva (2016) em seus doze elementos formativos, também resumindo a base teórica empregada para a construção deste modelo de avaliação. Para tanto, foram empregadas as principais práticas de gestão de riscos apontadas na literatura, principalmente a partir dos trabalhos de Zhao, Hwang, & Low (2013), Kaplan & Mikes (2016), Mardessi & Bem Arab (2018), Yeo & Ren (2009) e Oliva et al (2022).

Tabela 7 – Síntese dos Elementos de avaliação de GRC, seus fatores originais e base teórica empregada

<table>
<tr><td colspan="2">Fator 1 – Organização. É o esforço dedicado pela empresa para estruturar sua gestão de riscos, tais como planejar, organizar, implementar e controlar a forma como os riscos serão geridos. Exemplos: definições de pessoas e funções específicas, formas de mandato e reporte, instaurações de comitês, projetos de implementação etc.</td></tr>
<tr><td>Principais práticas relacionadas

A empresa se esforça para manter uma estrutura para planejar, organizar, implementar e controlar sua gestão de riscos. [A]
Existe uma política de GRC escrita e documentada para toda a organização. [B]
A empresa tem um nível de controle suficiente de seus riscos. [A]
Os processos relacionados a risco são planejados, executados e gerenciados de forma racional. [A]
Os processos relacionados a risco são revistos com frequência. [A]
A política de gestão de riscos é desenvolvida e adaptada para o contexto e objetivo da empresa. [B]
Os processos relacionados a risco são contínuos e não são interrompidos por mudanças no alto escalão. [B]
Existe um alto executivo, um departamento dedicado ou um comitê no nível do conselho administrativo encarregado de centralizar a gestão de riscos. [B]
O apetite a risco é formalmente e claramente definido de acordo com a estratégia da empresa. [B]
São investidos recursos de forma contínua para manter uma estrutura capaz de organizar, implementar e controlar a gestão de riscos. [B]
A empresa faz reuniões ou mantem formulários de autoavaliação para identificar, avaliar e priorizar riscos. [C]
Os processos relacionados a risco são capazes de identificar e avaliar riscos novos ou emergentes. [D]
Existe um plano estruturado de resposta para riscos que ultrapassam o nível aceitável (apetite a risco) da empresa. [D]
A gestão de riscos faz parte da atividade diária de tomada de decisões da organização. [A]</td><td>Elementos Fator 1

F1.E1. Recursos dedicados. A prática tem alocação de recursos físicos e financeiros suficientes para a sua execução contínua, em longo prazo e sem interrupção.

F1.E2. Estrutura organizacional. A prática tem uma estrutura humana com pessoas definidas, funções específicas, formas de mandato e reporte que incorporam indicadores de gestão de riscos na avaliação de desempenho dos colaboradores.

F1.E3. Estrutura Conceitual. A prática é claramente descrita em suas funções e limites e é documentada como um processo, guia e/ou política para a Gestão de Riscos Corporativos.</td></tr>
<tr><td colspan="2">Fator 2 – Tecnicidade. É o desenvolvimento de atributos técnicos para suportar a gestão de riscos. Exemplos: indicadores (tanto qualitativos quanto quantitativos), implantações de sistemas, desenvolvimento e uso de ferramentas, etc.</td></tr>
<tr><td>Principais práticas relacionadas

Os riscos são medidos quantitativamente. [A]
Existe uma cultura de avaliação de riscos na gestão da empresa. [A]
As diferenças entre o apetite e tolerância a riscos da empresa e sua real exposição são medidos com frequência. [B]
A gestão de riscos é incorporada à avaliação de desempenho dos colaboradores que tomam decisões. [B]
São investidos recursos de forma contínua para manter e atualizar métricas e técnicas qualitativas e quantitativas de suporte ao processo de gestão de riscos. [B]
As informações coletadas sobre riscos são verificadas quanto a sua veracidade e relevância. [B]
A empresa é capaz de identificar e medir a interdependência e interação entre os riscos a que está exposta. [B]
As informações sobre riscos são coletadas de diversas fontes distintas e atualizadas rotineiramente. [B]
O processo de gestão de riscos é registrado e de fácil acesso a revisão e melhoria. [B]</td><td>Elementos Fator 2

F2.E1. Eficiência de Indicadores. A prática possui indicadores quantitativos ou qualitativos suficientes, relevantes, coletados de fontes distintas e que podem ser verificados quanto a sua veracidade e relevância.

F2.E2. Regularidade. A prática tem sua relevância e suas métricas revistas com periodicidade compatível com a velocidade de mudança do setor ou negócio.</td></tr>
</table>

Existe um sistema de informação específico para a gestão de riscos. [A] *Key Risk Indicators* (KRIs) são continuamente revisados e atualizados. [B] As ferramentas utilizadas para identificar, avaliar e priorizar riscos são consideradas relevantes pelos gestores da organização. [C]	**F2.E3. Sistema de Inteligência.** A prática está vinculada, alimenta ou é alterada por um processo capaz de identificar sua interdependência ou interação com outras práticas e oferecer um diagnóstico para avaliar riscos, priorizar ações e antecipar cenários.
Fator 3 – Transparência. É o compartilhamento de informações e a capacidade de discutir abertamente a gestão de riscos com colaboradores para promover o engajamento e a participação na gestão de riscos. Exemplos: Boletins periódicos, reuniões abertas, disponibilidade de material para consulta, canal de comunicação para reporte de riscos, etc.	
Principais práticas relacionadas	**Elementos Fator 3**
Existem reuniões e eventos frequentes para discutir os riscos da empresa. [A] A gestão de riscos da empresa é descentralizada. [A] As decisões sobre riscos em todos os níveis hierárquicos são integralmente baseadas na política de GRC da empresa. [B] Todos na empresa efetivamente participam da gestão de riscos. [B] O apetite a risco e a tolerância a riscos é formalmente e claramente comunicada a todos os colaboradores. [B] Oportunidades são regularmente identificadas e exploradas durante o planejamento de gestão de riscos. [B] É de conhecimento de todos na empresa que oportunidades são um aspecto dos riscos. [B] Comentários individuais são encorajados e considerados no processo de gestão de riscos. [B] Existe uma linguagem comum sobre riscos que é utilizada por todos na comunicação sobre riscos. [B] Todos na empresa utilizam o sistema de informações sobre riscos. [A] Os treinamentos regulares asseguram que todos os níveis entendem o processo e os benefícios da GRC. [A] Os colaboradores experientes em GRC dividem seus conhecimentos com colaboradores mais novos. [B] Os colaboradores compreendem os benefícios da GRC. [E] São investidos recursos de forma contínua para manter o compartilhamento de informações e o fluxo de comunicação para engajamento da organização na gestão de riscos. [A]	**F3.E1. Permeabilidade na Estrutura.** A prática é conhecida por todos os colaboradores, é reconhecida como importante para a gestão de riscos e seus benefícios são compreendidos por todos na organização. Conceito *top- down*. **F3.E2. Consciência para oportunidades.** A prática é capaz de envolver colaboradores no aspecto positivo da gestão de riscos, identificar e comunicar oportunidades a serem exploradas. **F3.E3. Iniciativa vigilante.** A prática é capaz de incorporar a tolerância a riscos da empresa e de identificar e comunicar riscos de baixo para cima na hierarquia. Conceito *bottom-up*.
Fator 4 – Envolvimento. É a habilidade de engajar também os agentes envolvidos nos ambientes de fora da empresa. Representa o poder de coordenação da empresa para que a gestão dos riscos relativos a seus ambientes de valor e de negócios seja otimizada. Exemplos: Gestão compartilhada com fornecedores, clientes, e outros agentes para os riscos de destruição de valor (i.e. imagem ou operação) e do ambiente comum de negócios (i.e. político ou ambiental).	
Principais práticas relacionadas	**Elementos Fator 4**
Existe suporte externo, como consultoria ou universidade, para a gestão de riscos. [A] Existe uma linguagem comum sobre riscos entre os agentes do ambiente de valor (i.e. fornecedores, clientes e outros agentes). [B] As alianças estratégicas, cooperações ou parcerias tem canal formal de comunicação sobre riscos. [E] A política de GRC escrita e documentada inclui riscos de agentes que estão fora do ambiente da organização, tais como fornecedores e clientes. [F]	**F4.E1. Suporte Externo.** A prática envolve suportes externos tais como consultoria, universidade ou outros parceiros para contribuir com seu desenvolvimento, aplicação e melhoria. **F4.E2. Liderança dos agentes.** A prática define o padrão e a linguagem nas relações com agentes fora do

Os processos para identificar, avaliar e priorizar riscos contemplam as relações entre agentes do ambiente de valor. [F] A empresa é capaz de identificar e medir a interdependência e interação entre seus riscos internos e os do ambiente de valor. [F] Os colaboradores compreendem que os agentes da cadeia de valor são fontes de risco. [F] Existem KRIs relativos a agentes externos a organização que são considerados confiáveis e relevantes. [F]	ambiente da organização de forma que os outros agentes do ambiente de valor reconhecem sua liderança. **F4.E3. Interação no Ambiente de Valor.** A prática é capaz de identificar e avaliar a interdependência e interação entre seus riscos internos e os de agentes externos. Com isso, oferecer um diagnóstico para priorizar ações e antecipar cenários na cadeia de valor.

Notas: A Oliva (2016); **B** Zhao, Hwang, & Low (2013); **C** Kaplan & Mikes (2016); **D** Mardessi & Bem Arab (2018); **E** Yeo & Ren (2009); **F** Oliva et al (2022). **Fonte:** Desenvolvido pelo autor.

3.2.4. Etapa 4 – Aperfeiçoamento do MAM-GRC

Nesta quarta etapa do caminho metodológico da pesquisa, o modelo desenvolvido na etapa anterior foi apresentado a gestores experientes. O objetivo foi melhorar o modelo a partir de discussões contextualizadas sobre sua aplicação e atingir a melhor versão do MAM-GRC. Estas discussões envolveram pontos tais como o nível de compreensão do modelo pelos executivos, a simulação de sua aplicação nas diferentes realidades dos envolvidos e, principalmente, a coleta de dúvidas e sugestões relacionadas a sua aplicação.

A Tabela 8 apresenta em forma de lista os profissionais que gentilmente colaboraram e contribuíram com suas experiências em diversos pontos importantes para a evolução do modelo.

Tabela 8 – Profissionais que colaboraram para o aperfeiçoamento do MAM-GRC

Ordem	Setor de atuação	Função principal	Experiências relacionadas à gestão de riscos	Anos de experiência
1	Consultoria	Consultor	Gestão da inovação, startup e empreendedorismo	31
2	Publicidade	Gerente	Marketing digital	9
3	Tecnologia industrial	Co-Fundador	Startup e empreendedorismo	15
4	Banco	Conselheiro	Governança corporativa	25
5	Banco	Gerente	Gestão comercial e de carteira de clientes	13
6	Construção civil	Consultor	Gestão de projetos	22
7	Banco	Coordenador	Gestão de Crédito e detecção de fraude	6
8	Mineração	Gerente	Soluções de TI e indústria de base	14
9	Indústria ótica	Analista	Logística e gestão de imagem no pós-vendas	6
10	Indústria alimentícia	Gerente	Gestão de projetos e processos de negócios	24
11	Infraestrutura de TI	Gerente	Gestão de processos de negócios	8
12	Varejo	Diretor	Gestão da cadeia de suprimentos	15
13	Fintech	Sócio	Gestão de carteira de crédito, recuperação e cobrança	8
14	Banco	Gerente	Segurança da Informação, cyber segurança e gestão de riscos cibernéticos	5
15	Universidade	Pesquisador	Desempenho organizacional	5
16	Banco	Gerente	Gestão de projetos de TI	12
17	Banco	Gerente	Auditoria interna	10
18	Indústria química	Gerente	Gestão de TI e infraestrutura regional	25
19	Agronegócio	Gerente	Gestão de riscos e controles internos	12
20	Saúde	Gerente	Gestão da inovação	11
21	Atacadista	Diretor	Gestão comercial e vendas públicas	8
22	Construção civil	Diretor	Gestão de operações	13
23	Energia	Gerente	Controles internos, auditoria e compliance	15
24	Agronegócio	Gerente	Gestão da qualidade e segurança	27
25	Associação / Instituto	Diretor	Compliance	26
26	Banco	Gerente	Gestão comercial e de novos negócios	12
27	Indústria setor elétrico	Gerente	Gestão comercial e de projetos de aplicação	7

Fonte: Desenvolvido pelo autor

As entrevistas foram conduzidas de forma individual ou em grupo de no máximo quatro profissionais, conforme conveniência, entre os meses de fevereiro de 2020 e junho de 2021. Ao todo 11 sessões de videoconferência, com duração média de 1h45, foram realizadas com 27 profissionais estabelecidos em diversas cidades brasileiras. Alguns profissionais se dispuseram a participar de mais de uma sessão.

Vale destacar que esta pesquisa foi realizada durante um período de isolamento social recomendado pelas autoridades de saúde devido à pandemia de Covid-19. Além das sessões de discussão do modelo, uma linha direta de comunicação com os profissionais foi estabelecida para o caso de haver eventuais dúvidas sobre as sugestões propostas.

Durante as sessões, o modelo de avaliação concebido na etapa 3 do caminho metodológico da pesquisa foi apresentado aos gestores. Um roteiro semiestruturado foi empregado para conduzir as discussões e as respostas ao roteiro foram reavaliadas e paulatinamente incorporadas ao modelo. O roteiro para a condução das sessões de entrevista consistiu nos seguintes tópicos iniciais:

- Após a apresentação do modelo, está claro o conceito de levantamento de práticas de gestão de riscos para determinar a maturidade na Gestão de Riscos Corporativos? Como podemos ser mais claros?
- Após a apresentação do modelo, está claro o conceito de 4 fatores (organização, tecnicidade, transparência e envolvimento) para determinar a maturidade na Gestão de Riscos Corporativos? Como podemos ser mais claros?
- Os exemplos de práticas de gestão de riscos apresentados no modelo são úteis para identificar as práticas de gestão de riscos da sua empresa? Existem práticas que você considera importantes e que não estão contempladas entre as apresentadas?
- Todos os 4 fatores (organização, tecnicidade, transparência e envolvimento) apresentados no modelo se aplicam de alguma maneira ou em algum grau a sua empresa? Há outros fatores além dos apresentados no modelo?
- Você acredita que os 12 Elementos apresentados são capazes de distinguir os 4 fatores? Você tem alguma sugestão?
- Você acredita que ao atribuir notas de 0 a 10 para os 12 elementos do modelo podemos medir os fatores na sua empresa?

- Você acredita que o modelo, após implementarmos as sugestões que conversamos, será capaz de medir o nível de maturidade em GRC de sua empresa? O mesmo vale para seu setor?

O MAM-GRC, resultante desta quarta etapa do caminho metodológico da pesquisa, foi desenhado em forma de planilha eletrônica Excel. Esta ferramenta foi projetada para ser preenchida com as informações da organização em avaliação (i.e. *input*), embutir a lógica do modelo, e exibir o resultado em forma de *dashboard* (i.e. *output*).

Além disso, a ferramenta foi desenvolvida para facilitar a identificação de quais práticas a gestão deve priorizar para aumentar o seu nível de maturidade em GRC. Esta lógica de identificação contribui para o cumprimento do quarto objetivo específico desta tese. Após diversas interações e implementações de sugestões, a planilha final desta etapa é apresentada no Capitulo 4 – Resultados.

3.2.5. Etapa 5 – Aplicação do MAM-GRC em diferentes organizações

Nesta quinta etapa do caminho metodológico da pesquisa, o MAM-GRC concebido e aperfeiçoado nas etapas anteriores foi aplicado em três organizações. Os objetivos principais destas aplicações foram, inicialmente, o de observar o emprego do modelo em contextos reais, os quais naturalmente incluem premissas particulares das organizações, e assim subsidiar uma avaliação de sua aplicabilidade (Albliwi et al., 2014; Tarhan et al., 2016).

Também, o de promover uma oportunidade para descrever o processo de aplicação do MAM-GRC e consequentemente servir de ilustração, ou de guia de aplicação, para gestores e pesquisadores, colaborando para um impacto real da pesquisa (Doyle, 2018; Oliva et al., 2022). Finalmente, o de capturar suas limitações e pontos passíveis de desenvolvimento (Carmona et al., 2017; Rohloff, 2011).

Em relação à aplicação de modelos em casos reais, de Jongh et al. (2017) considera que:

> Tão logo o paradigma do modelo seja concebido, o modelo precisa ser avaliado em termos de sua aplicabilidade ao problema que está sendo resolvido, e o conjunto de premissas associado ao modelo precisa ser verificado em termos de sua validade no contexto particular (de Jongh et al., 2017, p. 3, tradução nossa).

Para esta aplicação os casos foram selecionados de forma não probabilística através de três critérios principais:

I. Que as organizações fossem brasileiras e de grande porte, ou seja, com origem e sede corporativa no Brasil, mesmo que com subsidiárias no exterior. Este critério foi adotado principalmente porque o modelo teórico de Oliva (2016), operacionalizado nesta tese, partiu de uma amostra das maiores empresas brasileiras. Assim, este critério evita vieses de porte e de localização.

II. Que as organizações fossem de setores distintos, uma vez que os resultados da Revisão Sistemática da Literatura apontaram uma lacuna quanto a aplicação de modelos em diferentes indústrias. Também porque a diversidade de organizações, inclusive quanto a origem do investimento, é relevante para a observação da aplicação do modelo em diferentes contextos (Spector et al., 2015; Tight et al., 2016).

III. Que as organizações inicialmente apresentassem indícios de diferentes níveis de maturidade em GRC, para aproveitar a diversidade. Isto porque os modelos de maturidade são constituídos de características incrementais de gestão e de competências cumulativas, logo organizações mais maduras condensam também as práticas dos níveis de maturidade pelos quais já passaram (Albliwi, Antony, & Arshed, 2014; Carmona et al., 2017; Oliva, 2014).

A partir desses três critérios, o MAM-GRC foi aplicado em três organizações consolidadas e de destaque em seus setores: uma organização do setor de aviação, uma organização do setor de óleo, gás e biocombustíveis; e uma organização de interesse à saúde. No Capitulo 4 – Resultados, estão descritos os casos e as características dessas organizações, bem como os modelos, operacionalizados em forma de planilhas preenchidas.

3.2.6. Etapa 6 – Análises de utilidade e aplicabilidade do MAM-GRC

Nesta sexta e última etapa do caminho metodológico da pesquisa, o MAM-GRC foi reavaliado, após sua aplicação em três casos reais. Esta reavaliação teve o objetivo de complementar a etapa anterior para subsidiar conclusões sobre a utilidade e aplicabilidade do

modelo, bem como suas implicações práticas e aplicações gerenciais. Para Gass (1983), o modelo deve, em última instância, ser ajuizado *se* e *como* pode ser usado como auxílio à tomada de decisão.

Para isso, foi aplicado um questionário aos envolvidos na aplicação do modelo aos casos. A finalidade deste instrumento de pesquisa adicional foi colher informações complementares sobre a opinião dos indivíduos que vivenciaram a aplicação do MAM-GRC ou estiveram comprometidos com o preenchimento das planilhas que operacionalizaram o modelo. A íntegra do questionário segue nesta tese como Anexo II.

O questionário foi distribuído e aplicado por meio de ferramenta eletrônica, com resposta anônima. A tecnologia empregada foi a plataforma de formulários do Google. Os inquiridos foram informados de que suas respostas seriam analisadas de forma agregada e de que seria impossível identificar as respostas individuais. Como as perguntas pretendiam desafiar o modelo aplicado, o principal propósito para a aplicação de um questionário em detrimento de um novo contato foi o de reduzir a tendencia de respostas concordantes com o entrevistador (Moser & Kalton, 2017).

As principais bases teóricas para a formulação do questionário foram os critérios de avaliação, utilidade, confiança e documentação de Gass (1983), e os atributos de transparência (i.e. que seja possível ver como o modelo é construído) e validação (i.e. o quão bem ele reproduz a realidade) de Eddy et al. (2012).

4. RESULTADOS

Este capítulo apresenta os resultados das etapas organizadas pelo caminho metodológico da pesquisa, que compreendem o produto do aperfeiçoamento com profissionais do modelo operacional para avaliação da maturidade em GRC, os desfechos de sua aplicação em organizações reais e a apuração de sua utilidade e aplicabilidade.

É importante destacar que a pesquisa não pretendeu estudar características específicas das organizações e que os profissionais que gentilmente cederam seu tempo e dedicação contribuíram com suas experiências pessoais e profissionais. Nenhuma informação privada ou desconhecida de especialistas nos setores econômicos representados foi necessária para atingir os resultados que seguem.

4.1. Resultados da etapa de aperfeiçoamento do MAM-GRC

Esta seção descreve os resultados obtidos a partir das entrevistas com gestores experientes em gestão de riscos que, ao final, culminaram em uma ferramenta prática, em forma de planilha, que pode ser diretamente aplicada para avaliação da maturidade em GRC nas organizações. Mais ainda, após a avaliação, a ferramenta também é capaz de informar executivos sobre ações gerenciais mais imediatas para aumentar o nível de maturidade em GRC de suas organizações.

Inicialmente, os *insights* dos profissionais apontaram a necessidade de separação entre práticas de gestão de riscos específicas das realidades de cada setor ou organização, e de práticas de gestão de riscos comuns entre organizações. Em outras palavras, a partir das discussões em torno das práticas compiladas da literatura, e considerando as experiências de cada profissional, foi identificada a necessidade de haver uma lista de *práticas genéricas de Gestão de Riscos Corporativos* para que servissem de base para que *práticas específicas da organização para a Gestão de Riscos Corporativos* pudessem ser identificadas ou modificadas a partir de uma compilação inicial.

Este resultado está em linha com diversas pesquisas sobre a adaptação de modelos, tais como a de Heckmann et al. (2015), que obtiveram heterogeneidade e separação entre características principais e específicas ao estudarem cadeias de suprimentos, e de Zou et al.

(2010), que encontraram atributos específicos para a indústria de construção e que diferem dos principais apontados pela literatura.

Neste sentido, uma linguagem comum foi apresentada e discutida a partir das definições de *prática de gestão* e *processo de gestão*, da Fundação Nacional da Qualidade, e das definições de *prática genérica* e de *processo definido* da ISO (FNQ, 2011; ISO/IEC 33001:2015). Assim, a concepção adotada para estabelecer uma linguagem comum sobre prática de gestão de riscos no modelo foi:

Prática de gestão de riscos é um conjunto de atividades inter-relacionadas ou interativas, de natureza gerencial, relacionada a riscos e implementada pela organização de forma regular.

Definições:

- Conjunto de atividades inter-relacionadas ou interativas é o mesmo que um processo de gestão.
- Atividade regular é uma atividade que ocorre de forma contínua ou periódica.
- Natureza gerencial reflete as funções administrativas, frequentemente definidas pelas funções de planejar, organizar, dirigir e controlar, pelos *trade-offs* relacionados à eficiência e eficácia, pelas relações entre recursos escassos, problemas e objetivos ou pela função de equacionar conflitos: escolher, priorizar e selecionar.
- Risco é a possibilidade de que um evento tenha impacto negativo nos objetivos, sendo o evento uma ocorrência tanto interna quanto externa.

Corolário:

- Portanto, uma prática de gestão de riscos é um processo de gestão e por isso geralmente, mas não obrigatoriamente, caracteriza mais de uma atividade.
- Portanto, uma prática de gestão de riscos deve estar relacionada à administração da organização.
- Portanto, uma prática de gestão de riscos não pode ser apenas ocasional, contingente ou extraordinária.
- Portanto, uma prática de gestão de riscos deve estar relacionada aos objetivos da organização.

Ainda assim, os profissionais perceberam a necessidade de eventualmente adaptar as práticas definidas como genéricas, uma vez que algumas delas podem não fazer sentido em casos específicos. Os resultados destas discussões corroboram os encontrados por Zhao &

Singhaputtangkul (2016), que aplicaram um questionário com 35 gestores e concluíram que as características específicas das organizações precisam ser consideradas, mas as práticas generalistas de GRC precisam ser customizadas pela alta gestão.

Com relação às práticas genéricas de Gestão de Riscos Corporativos, optou-se por adotar 15 dos 16 conjuntos de melhores práticas compiladas por Zhao et al. (2013). O conjunto excluído, que se refere ao 15º conjunto do trabalho dos autores e versa sobre estabelecimento dos objetivos, foi considerado não aderente ao propósito deste modelo porque todas as práticas devem estar relacionadas aos objetivos da organização (Oliva, 2016; Oliva et al., 2022).

Vale recuperar que as práticas inicialmente relacionadas a esses fatores, ou seja, as originadas na literatura e apresentadas aos executivos, estão integralmente elencadas na Etapa 3 do Capitulo 3 - Metodologia. Como resultado, as *práticas genéricas de Gestão de Riscos Corporativos* consolidadas para compor o MAM-GRC são:

1) Existe comprometimento da alta gestão com a GRC.
2) Existe responsabilidade sobre os riscos (todo risco tem um gestor).
3) Existe tolerância e apetite a risco bem definidos.
4) Existe uma cultura consciente dos riscos.
5) Existem recursos suficientes para a GRC.
6) Há eficiência na identificação, análise e resposta ao risco.
7) Os processos de GRC são dinâmicos e realimentados.
8) A GRC é relacionada a oportunidades.
9) Existe uma comunicação sobre riscos.
10) A GRC tem uma linguagem comum.
11) Existe um sistema de informações gerenciais para a GRC.
12) Há programas de treinamento para a GRC.
13) Existem indicadores formais para riscos.
14) Existe integração entre a GRC e os processos da organização.
15) Monitoramento, revisão e melhoria do planejamento da GRC.

A partir dessa lista de práticas, uma tabela foi desenvolvida para facilitar a identificação das *práticas específicas da organização para a Gestão de Riscos Corporativos*. Os executivos entrevistados sugeriram e demonstraram maior facilidade para compreender uma ferramenta em forma de planilha com as definições necessárias e distinção dos fatores. Os fatores organização, tecnicidade, transparência e envolvimeto se mostraram importantes para guiar

uma distribuição equânime de práticas. A Figura 10 apresenta a Planilha 1, desenvolvida para registrar o resultado da contextualização entre práticas genéricas e específicas de GRC nas organizações.

Figura 10 – Planilha 1: identificação de práticas de GRC específicas da organização

Práticas de Gestão de Riscos Corporativos		
Prática de gestão de riscos é um conjunto de atividades inter-relacionadas ou interativas, de natureza gerencial, relacionada a riscos e implementada pela organização de forma regular. *Definições importantes a serem consideradas para a identificação das práticas de gestão de riscos:* **Conjunto de atividades inter-relacionadas ou interativas** é o mesmo que um processo de gestão. **Atividade regular** é uma atividade que ocorre de forma contínua ou periódica. **Natureza gerencial** reflete as funções administrativas, frequentemente definidas pelas funções de planejar, organizar, dirigir e controlar, pelos trade-offs relacionados à eficiência e eficácia, pelas relações entre recursos escassos, problemas e objetivos ou pela função de equacionar conflitos: escolher, priorizar e selecionar. **Risco** é a possibilidade de que um evento tenha impacto nos objetivos, sendo o evento uma ocorrência tanto interna quanto externa. *Implicações:* Uma prática de gestão de riscos é um processo e por isso geralmente, mas não obrigatoriamente, caracteriza mais de uma atividade. Uma prática de gestão de riscos deve estar relacionada à administração da organização. Uma prática de gestão de riscos não pode ser apenas ocasional, contingente ou extraordinária. Uma prática de gestão de riscos deve esta relacionada aos objetivos da organização.		
Efetividade		
Efetividade é a capacidade que a prática de gestão de riscos tem de produzir e manter na organização, através das atividades compatíveis com sua finalidade, um efeito real tal como o esperado. A efetividade de uma prática de GRC deve medir o quanto ela tem sucesso no seu resultado, ou se "está ou não funcionando".		
Fator 1 - Organização riscos serão geridos.		**Efetividade (1 a 10)**
Como a empresa se estrutura para realizar sua gestão de riscos? O que/Como/Onde/De qual forma se organiza para realizar atividades tais como planejamento, organização, implementação e controle da gestão de riscos corporativos?		
Prática Ex.	Um Comitê de Gestão de Riscos Corporativos, formado por diretores de diversas unidades e liderado pelo vice-presidente conduz o processo de planejamento, organização, implementação e controle da gestão de riscos corporativos, reunindo-se periodicamente para planejar novas ações e acompanhar a implementação das ações anteriormente planejadas.	-
Prática 1		
Prática 2		
Prática n	inserir quantas linhas forme necessárias	
Fator 2 - Tecnicidade É o desenvolvimento de atributos técnicos para suportar a gestão de riscos.		**Efetividade (1 a 10)**
Como a empresa implementa técnicas qualitativas e/ou quantitativas de suporte ao processo de gestão de riscos? O que/Como/Onde/De qual forma desenvolve e/ou aplica atributos técnicos tais como métricas, indicadores, habilidades, frequências, etc?		
Prática Ex.	A avaliação anual dos líderes contempla, dentre os indicadores de desempenho, indicadores específicos de gestão de riscos que são considerados para a progressão de carreira.	-
Prática n		
Prática n		
Prática n	inserir quantas linhas forme necessárias	
Fator 3 - Transparência É o compartilhamento de informações e a capacidade de discutir abertamente a gestão de riscos com colaboradores para promover o engajamento e a participação na gestão de riscos.		**Efetividade (1 a 10)**
que/Como/Onde/De qual forma a empresa discute abertamente a gestão de riscos com seus colaboradores e os inclui para uma gestão participativa dos seus riscos?		
Prática Ex.	O presidente da empresa participa de eventos, cita casos e demonstra, pelo exemplo, comprometimento com a Gestão de Riscos Corporati	-
Prática n		
Prática n		
Prática n	inserir quantas linhas forme necessárias	
Fator 4 - Envolvimento É a habilidade de engajar também os agentes envolvidos nos ambientes exteriores à empresa. Representa o poder de coordenação da empresa para que a gestão dos riscos relativos a seus ambientes de valor e de negócios seja otimizada.		**Efetividade (1 a 10)**
Como a empresa faz para envolver os agentes do seu ambiente de valor na gestão de riscos? O que/Como/Onde/De qual forma a empresa é capaz de engajar também outros agentes envolvidos em seu ambiente de valor para tornar a gestão de riscos mais eficiente e eficaz?		
Prática Ex.	A avaliação de novos clientes inclui uma avaliação de riscos que tem seu resultado discutido para a elaboração de um plano mútuo de mel	-
Prática n		
Prática n		
Prática n	inserir quantas linhas forme necessárias	

Fonte: Desenvolvido pelo autor.

A Planilha 1 apresenta a primeira de duas planilhas desenvolvidas a partir das entrevistas com os profissionais para o aperfeiçoamento do MAM-GRC. Os executivos envolvidos neste processo contribuíram com *insights* importantes para a conclusão desta etapa, principalmente quanto a sua forma de apresentação em planilha única, quanto a necessidade de haver definições

de conceitos na própria planilha, quanto a forma como estes conceitos foram incluídos na planilha e, finalmente, quanto a necessidade de haver exemplos para as práticas de GRC.

Um ponto importante sobre a ferramenta desenvolvida para identificar as práticas de GRC é que gestores revelaram a existência de práticas de gestão que, apesar de existirem em suas organizações, estão em vias de implementação ou, mesmo após terem sido consideradas implementadas, não geram resultados tal como o planejado. Esta constatação alimentou discussões sobre o limiar assumido por cada gestor para considerar se uma prática deveria ser listada na planilha. Nesta etapa, ao discutirem sobre práticas de suas organizações, gestores mencionaram práticas com rótulos tais como "não merece ser considerada", "existe, mas não funciona" ou "vamos nos concentrar nas práticas principais".

Como solução para este problema, foi implementada uma medida de efetividade para cada prática de GRC identificada. A medida de efetividade foi considerada importante e suficiente para que profissionais mais críticos, ou aqueles que tendem a identificar apenas práticas "que funcionam", pudessem ficar mais livres para listar práticas "que funcionam parcialmente ou não funcionam", nesse caso atribuindo valor máximo de efetividade para a prática que "funciona" perfeitamente e valores proporcionalmente mais baixos para a efetividade das que "funcionam" menos.

Esta lógica também se mostrou útil para que gestores com perfil mais minucioso, e que tendem a elencar mais práticas, pudessem avaliar a importância das práticas reportadas e, por consequência, reavaliar a extensão da lista composta. Nesse sentido, a avaliação da efetividade também serviu como guia aos entrevistados para que pudessem decidir quais práticas incluiriam na Planilha 1.

Para determinar uma linguagem comum de efetividade foram empregados os conceitos de *capacidade*, *maturidade organizacional*, *medição de processo* e de *desempenho de processo* da ISO 33001, bem como os de *prática de gestão* e de *processo de gestão* da Fundação Nacional da Qualidade (FNQ, 2011; ISO/IEC 33001:2015). Dessa forma, efetividade foi definida, discutida e operacionalizada na planilha de identificação de práticas de GRC (Planilha 1) como:

Efetividade é a capacidade que a prática de gestão de riscos tem de produzir e manter na organização, através das atividades compatíveis com sua finalidade, um efeito real tal como o esperado.

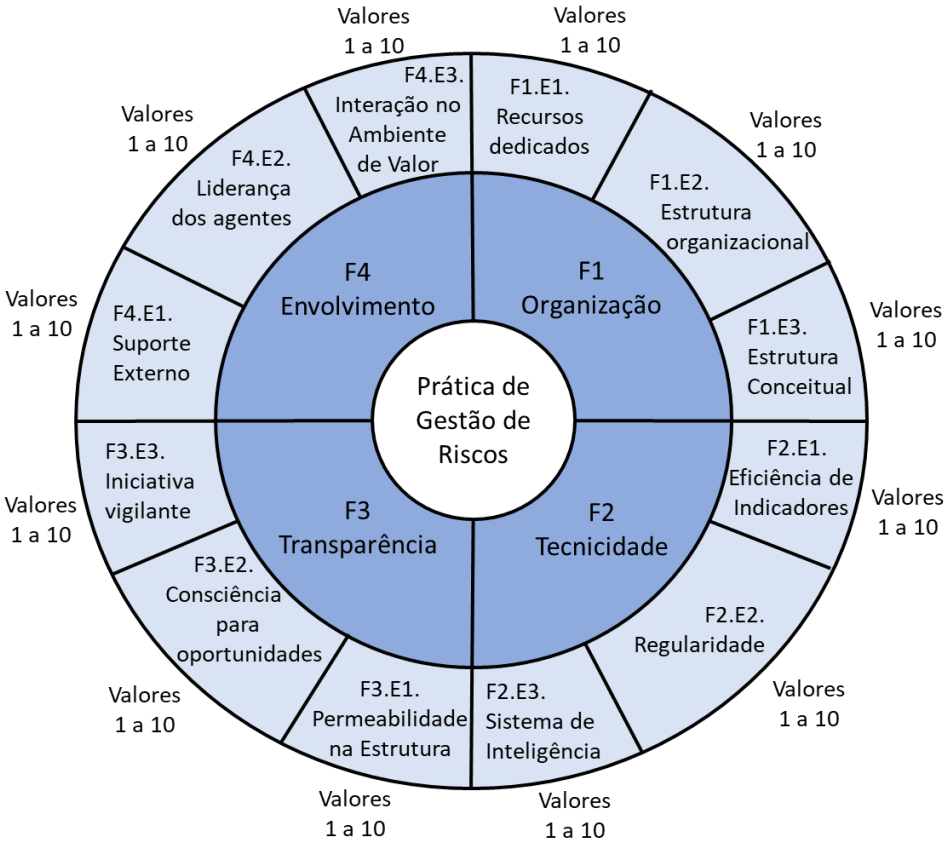
Objetivo prático: *A efetividade de uma prática de GRC deve medir o quanto ela tem sucesso no seu resultado, ou se "está ou não funcionando".*

Ao final desta etapa os entrevistados reconheceram que a ferramenta desenvolvida poderia ser aplicada em seus negócios, mesmo considerando as diversas indústrias nas quais possuem experiências. Para a maioria deles, as 15 práticas genéricas de GRC puderam ser adaptadas às realidades de suas organizações por meio da Planilha 1.

Após operacionalizar a identificação de práticas de GRC, uma segunda planilha foi desenvolvida para operacionalizar a ponderação dos 12 elementos desenvolvidos a partir da literatura e, assim, atribuir valores para os quatro fatores base do modelo. Os doze elementos compostos a partir da literatura estão melhor apresentados na Etapa 3 do Capitulo 3 - Metodologia.

Inicialmente, os elementos foram apresentados em forma de um modelo circular para explicar a atribuição de valores em uma escala de 1 a 10. A Figura 11 exibe a escala que caracteriza os fatores de cada prática de gestão de riscos.

Figura 11 – Mensuração das práticas de GRC por meio de doze elementos



Fonte: Desenvolvido pelo autor.

Ainda que a literatura acumule diversas discussões sobre as propriedades das escalas, os gestores envolvidos nesta etapa consideraram a escala ordinal adotada, de 1 a 10, intuitiva e de fácil aplicação tanto para a *efetividade* quanto para os *elementos* de GRC (Bearden et al., 2001; Michell, 1986). Através dessa ferramenta, cada prática de GRC identificada pela Planilha 1 pôde ser então mensurada de acordo com os quatro fatores de Oliva (2016).

Foi considerado o paradigma formativo de composição para os fatores, pelo qual cada um dos três elementos correspondentes contribui igualmente para a mensuração de cada fator, bem como a capacidade de compreensão dos envolvidos e a parcimônia no método de cálculo do valor final (Bearden et al., 2001; Churchill, 1979; 1994). Assim, o critério adotado para a mensuração de cada fator foi a média simples dos elementos, ponderada pela efetividade de cada prática. Através desse método, a fórmula adotada para o cálculo dos fatores de cada prática é:

$$\textbf{Fator}_{i} = \{ [(\textbf{Fator}_{i}\ \textbf{Elemento1} + \textbf{Fator}_{i}\ \textbf{Elemento2} + \textbf{Fator}_{i}\ \textbf{Elemento3}) / 3] \ .\ \textbf{Efetividade}_{i} \} / 100$$

(Fórmula 1)

Onde:

i é um número Natural de 1 a 4 e representa cada um dos quatro fatores de Oliva (2016).

Fator $_{i}$ é um número Racional que assume valores entre 0 e 1.

Uma segunda planilha, denominada *Planilha 2*, foi desenvolvida para implementar o cálculo dos fatores. A Figura 12 apresenta a Planilha 2. Nela, as práticas de GRC e a efetividade atribuída a cada prática são transportadas da Planilha 1. Uma vez que as práticas de GRC estão dispostas nas linhas, as colunas da Planilha 2 estão prontas para receber os valores de cada elemento.

Figura 12 – Planilha 2: avaliação dos elementos das práticas de GRC específicas da organização

	ELEMENTOS												
	Fator 1 - Organização			**Fator 2 - Tecnicidade**			**Fator 3 - Transparência**			**Fator 4 - Envolvimento**			
	É o esforço dedicado pela empresa para estruturar sua gestão de riscos, tais como planejar, organizar, implementar e controlar a forma como os riscos serão geridos. Exemplos: definições de pessoas e funções específicas, formas de mandato e reporte, instaurações de comitês, projetos de implementação etc.			É o desenvolvimento de atributos técnicos para suportar a gestão de riscos. Exemplos: indicadores (tanto qualitativos quanto quantitativos), implantações de sistemas, desenvolvimento e uso de ferramentas, etc.			É o compartilhamento de informações e a capacidade de discutir abertamente a gestão de riscos com colaboradores para promover o engajamento e a participação na gestão de riscos. Exemplos: Boletins periódicos, reuniões abertas, disponibilidade de material para consulta, canal de comunicação para reporte de riscos, etc.			É a habilidade de engajar também os agentes envolvidos nos ambientes exteriores à empresa. Representa o poder de coordenação da empresa para que a gestão dos riscos relativos a seus ambientes de valor e de negócios seja otimizada. Exemplos: Gestão compartilhada com fornecedores, clientes e outros agentes para os riscos de destruição de valor (p. ex. imagem ou operação) e do ambiente comum de negócios (p. ex. político ou ambiental).			
	F1.E1. Recursos dedicados	**F1.E2. Estrutura organizacional**	**F1.E3. Estrutura Conceitual**	**F2.E1. Eficiência de Indicadores**	**F2.E2. Regularidade**	**F3.E3. Sistema de Inteligência**	**F3.E1. Permeabilidade na Estrutura**	**F3.E2. Consciencia para oportunidades**	**F3.E3. Iniciativa vigilante**	**F4.E1. Suporte Externo**	**F4.E2. Liderança dos agentes**	**F4.E3. Interação no Ambiente de Valor**	**EFETIVIDADE ATRIBUÍDA (1 a 10)**
PRÁTICAS Planilha 1	A prática tem alocação de recursos físicos e financeiros suficientes para a sua execução contínua, em longo prazo e sem interrupção.	A prática tem uma estrutura humana com pessoas definidas, funções específicas, formas de mandato e reporte que incorporam indicadores de gestão de riscos na avaliação de desempenho dos colaboradores.	A prática é claramente descrita em suas funções e limites e é documentada como um processo, guia e/ou política para a Gestão de Riscos Corporativos.	A prática possui indicadores quantitativos ou qualitativos suficientes, relevantes, coletados de fontes distintas e que podem ser verificados quanto a sua veracidade e relevância.	A prática tem sua relevância e suas métricas revistas com periodicidade compatível com a velocidade de mudança do setor ou negócio.	A prática está vinculada, alimenta ou é alterada por um processo capaz de identificar sua interdependência ou interação com outras práticas e oferecer um diagnóstico para avaliar riscos, priorizar ações e antecipar cenários.	(top down) A prática é conhecida por todos os colaboradores, é reconhecida como importante para a gestão de riscos e seus benefícios são compreendidos por todos na organização.	A prática é capaz de envolver colaboradores no aspecto positivo da gestão de riscos, identificar e comunicar oportunidades a serem exploradas.	(bottom-up) A prática é capaz de incorporar a tolerância a riscos da empresa e de identificar e comunicar riscos de baixo para cima na hierarquia.	A prática envolve suportes externos tais como consultoria, universidade ou outros parceiros para contribuir com seu desenvolvimento, aplicação e melhoria.	A prática define o padrão e a linguagem nas relações com agentes fora do ambiente da organização de forma que os outros agentes do ambiente de valor reconhecem sua liderança.	A prática é capaz de identificar e avaliar a interdependência e interação entre seus riscos internos e os de agentes externos. Com isso, oferecer um diagnóstico para priorizar ações e antecipar cenários na cadeia de valor.	
Prática 1													
Prática 2													
Prática 3													
Prática n													
Acrescetar tantas linhas quanto necessário													

Fonte: Desenvolvido pelo autor.

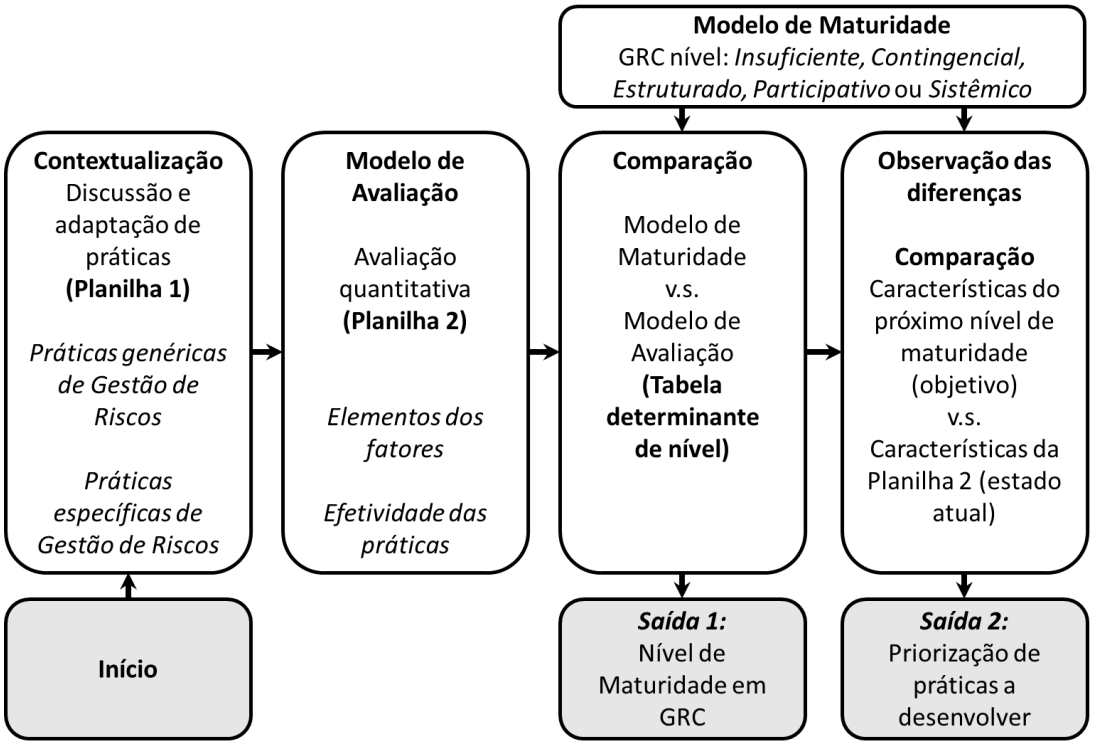
4.2. Resultados da etapa de aplicação do MAM-GRC

Esta seção descreve a forma como o Modelo Operacional para Avaliação da Maturidade em Gestão de Riscos Corporativos (MAM-GRC), concebido e aperfeiçoado nas seções anteriores, pode ser utilizado em uma organização. Para isso, define um fluxo para sua aplicação e apresenta os resultados obtidos em três casos reais. Além de cumprir com os objetivos propostos pela pesquisa, esta forma de apresentação, que inclui um "modo de aplicação", também pretende ilustrar a maneira como pesquisadores e executivos podem utilizar o MAM-GRC, e assim promover um impacto real à pesquisa (Doyle, 2018; Oliva et al., 2022).

4.2.1. Modo de aplicação do MAM-GRC em organizações

A seguir é demonstrada a forma como o MAM-GRC pode ser utilizado em uma organização, tanto para avaliar o nível de maturidade em GRC, como para auxiliar a tomada de decisões sobre a priorização de ações de desenvolvimento da GRC. Para melhor visualização, a Figura 13 demonstra seu fluxo de aplicação.

Figura 13 - Fluxo de aplicação do MAM-GRC em organizações



Fonte: Desenvolvido pelo autor.

Seguindo o fluxo de aplicação proposto, o **início** e a **contextualização** do modelo ocorrem com a utilização das práticas genéricas de GRC como guia para identificar e adaptar as práticas específicas de GRC da organização. Para isso é empregada a *Planilha 1*. Neste sentido, o modelo proposto permite uma adaptação ao ambiente de valor de cada organização investigada (Federico Neto et al., 2018; F. L. Oliva et al., 2022).

Vale recuperar da quinta etapa do caminho metodológico da pesquisa que o propósito da aplicação em casos é investigar a operacionalização do modelo, ou seja, examinar a utilização das planilhas desenvolvidas em contextos reais, os quais naturalmente incluem premissas particulares das organizações (Albliwi et al., 2014; Tarhan et al., 2016).

Em seguida, o **modelo de avaliação** consiste na aplicação da *Planilha 2*, com atribuição de valores e cálculo dos fatores através da *Fórmula 1*. O resultado desta análise passa então à **comparação**, quando a *tabela determinante de nível* é empregada para relacionar os valores obtidos para os fatores (i.e. o modelo de avaliação) aos níveis de maturidade em GRC (i.e. o modelo de maturidade). Esta abordagem está em linha com as definições da ISO (2015) e com Tarhan et al. (2016), que consideram que um modelo de maturidade tem a intenção de servir como um modelo de referência para ser comparado, enquanto um modelo de avaliação permite medir o estado atual.

Uma vez determinado o nível de maturidade em GRC da organização avaliada, ocorre a **saída 1.** A partir da **saída 1**, portanto conhecendo o estado atual da organização, é possível utilizar o **modelo de maturidade** para analisar as características necessárias para atingir o nível imediatamente superior ao alcançado. Neste momento, faz então sentido um estudo reverso do **modelo de avaliação**, ou seja, dos valores distribuídos pela *Planilha 2* para uma **observação das diferenças** entre o estado atual e o desejado.

Para Tarhan e seus coautores, “As descobertas de uma avaliação de processo são normalmente utilizadas para revelar as lacunas em relação ao modelo, o qual, então, serve de partida para o desenvolvimento de um plano para a melhoria do processo” (Tarhan et al., 2016, p. 129, tradução nossa).

Considerando o objetivo desta tese, a **Saída 1** desempenha o terceiro objetivo específico, que é o de propor um modelo operacional para avaliar a maturidade em GRC, ou seja, de apresentar um modelo adaptável ao contexto de cada organização e capaz de determinar seu nível de maturidade em GRC. Já a **Saída 2** atinge o quarto objetivo específico, que é o de

identificar as ações gerenciais pertinentes para elevar, a cada nível, a maturidade em GRC das organizações avaliadas pelo modelo.

4.2.2. Descrição dos casos selecionados

O fluxo de aplicação do MAM-GRC foi empregado em três casos. Além de ilustrativos, a fase de aplicação também teve o objetivo de capturar suas limitações e pontos passíveis de desenvolvimento (Carmona et al., 2017; Rohloff, 2011). Assim, as organizações estudadas foram:

Organização logística do setor de óleo, gás e biocombustíveis.

A primeira aplicação foi realizada em uma empresa do setor logístico, especializada em atender clientes da indústria de óleo, gás e biocombustíveis. Suas operações envolvem a prestação de diversos serviços característicos dessa indústria global, tais como a construção, manutenção e operação de dutos e terminais, tanto marítimos quanto terrestres, e de embarcações próprias ou de terceiros, para explorar o mercado de transporte, apoio marítimo e armazenamento de petróleo e seus derivados, petroquímicos, biocombustíveis, gases e fertilizantes.

Trata-se de uma multinacional consolidada no final dos anos 1990 como sociedade anônima de capital fechado. Sua atuação é internacional em diversos modais de transporte, tais como dutos, embarcações, terminais, ferroviário, rodoviário e multimodal. Considerando o ano de 2021 e os anos imediatamente anteriores, sua receita de serviços prestados tem ordem de 2 bilhões de dólares norte-americanos, sendo a Petrobras a maior cliente no Brasil. Suas operações envolvem o transporte anual médio da ordem de 650 milhões de m^3 de produtos para seus clientes.

Quanto ao início, contextualização e sequência do fluxo de aplicação do MAM-GRC, como qualquer negócio, a empresa está exposta a diversos riscos, sendo o ambiental, operacional, de segurança e saúde, financeiro e de imagem os mais típicos do setor em que atua. Especificamente sobre esta companhia, a gestão de riscos foi potencializada nos últimos anos para contribuir com uma mudança organizacional importante, caracterizando um estado atual acima da média internacional do setor, corroborado por diversos prêmios internacionais. Essa

gestão é regida por uma política de gestão de riscos aprovada pelo conselho de administração e que estabelece princípios, diretrizes e metodologias avançadas para a gestão de riscos, em especial para as estruturas e metodologias de identificação, análise, tratamento, monitoramento e comunicação dos riscos.

A empresa segue padrões estabelecidos pelos reguladores brasileiros e internacionais para as sociedades anônimas e dispõe de estrutura própria e profissionais qualificados distribuídos entre as três linhas de atuação em riscos, ou de defesa. Para a aplicação do MAM-GRC, foram envolvidos dois gestores seniores dessa estrutura, responsáveis pela gestão de riscos da organização e com mais de dez anos de experiência cada, considerando a trajetória profissional na organização e no setor. Além deles, também um consultor com mais de 20 anos de experiência no setor de transporte de óleo, gás e biocombustíveis foi entrevistado. Vale notar que não foram necessárias informações que não fossem, de alguma forma, públicas para os agentes que acompanham o setor e o mercado.

Foram realizadas três entrevistas em forma de reunião remota, via videoconferência e com a participação conjunta dos três colaboradores, com duração média de 1 hora e 45min cada entre os meses de abril e novembro de 2021. Durante as reuniões, as Planilhas 1 e 2 foram apresentadas, discutidas e preenchidas conforme a sequência planejada: inicialmente a Planilha 1 para a identificação das práticas de gestão de riscos e suas notas de efetividade e então a Planilha 2, para a atribuição de notas aos doze elementos do modelo.

Em relação à **contextualização** e a identificação das práticas de gestão de riscos, foram considerados os processos já mapeados pela estrutura de gestão de riscos existente, uma vez que tais práticas já haviam sido objeto de estudo interno da organização. Também, ficou claro neste ponto da pesquisa que um levantamento de práticas em um nível mais granular de análise seria inviável, tanto pelo tamanho e diversificação de atividades da empresa, quanto pelo tempo de dedicação disponibilizado pelos profissionais envolvidos.

Dessa forma, organizamos as práticas de gestão de riscos da empresa de maneira a convergirem para as 15 práticas genéricas de Gestão de Riscos Corporativos do modelo. Este mecanismo mostrou-se bastante útil, uma vez que quase todas as principais práticas de gestão de riscos da organização puderam ser aglomeradas dentre as 15 propostas. Uma implicação direta dessa fase da aplicação do modelo é o reforço aos resultados da fase anterior, de aperfeiçoamento do modelo, quando profissionais experientes de diversos setores concordaram que as 15 práticas elencadas seriam capazes de abranger, em um nível mais genérico, a maioria das práticas mais específicas de GRC. Para os entrevistados, a mensuração da efetividade das

práticas mostrou-se útil e até mesmo intuitiva para a tomada de decisão sobre a inclusão ou exclusão da prática na Planilha 1.

Após o processo de preenchimento da Planilha 1, ou **contextualização**, as práticas foram então transpostas para a Planilha 2, ou seja, para o **modelo de avaliação**. Neste momento os doze elementos utilizados para avaliar as práticas de gestão de riscos foram apresentados e discutidos. Esta etapa tomou o maior tempo das entrevistas e, dentre as discussões, diversas anotações passaram a ser feitas pelos próprios entrevistados diretamente na planilha. Esta funcionalidade não havia sido prevista no modelo, porém mostrou-se bastante útil. A próxima seção consolida as avaliações da organização logística do setor de óleo, gás e biocombustíveis e determina sua maturidade em GRC.

Organização industrial do setor de aviação.

A segunda aplicação do MAM-GRC foi realizada em uma empresa brasileira do setor de aviação, especializada em atender clientes particulares, companhias aéreas e a indústria de defesa. Suas operações principais envolvem atividades relacionadas direta ou indiretamente ao projeto, montagem, teste, homologação, comercialização e manutenção de aeronaves. Além disso, também desenvolvem atividades de fabricação e comercialização de equipamentos, materiais, sistemas, software, acessórios e componentes para os setores de defesa, segurança e energia, e realizam atividades técnicas e a prestação de serviços relacionados a essas áreas.

Trata-se de uma multinacional consolidada em meados dos anos 1990 como sociedade anônima de capital aberto, listada em bolsa de valores, e que desde então passou por diversas reestruturações societárias que a elevaram aos níveis mais altos de governança corporativa. Seu setor econômico é naturalmente internacionalizado e a empresa conta com subsidiárias em diversos países para compor uma cadeia global de produtos e serviços de alto valor agregado.

Como consequência de sua inserção internacional, no Brasil a empresa é uma grande importadora e exportadora. Considerando o ano de 2021 e os anos imediatamente anteriores, sua receita anual média tem ordem de 4 bilhões de dólares norte-americanos e suas operações têm envolvido um estoque de contratos futuros da ordem de 16 bilhões de dólares norte-americanos em produtos e serviços nos diversos segmentos em que atua.

Quanto ao início, contextualização e sequência do fluxo de aplicação do MAM-GRC, os riscos inerentes aos produtos e serviços do setor são bastante dependentes dos ciclos econômicos internacionais. A concorrência é altamente competitiva e não é incomum a

interferência de governos no mercado. Tais características dessa indústria podem contingenciar planos de longo prazo e caracterizar riscos estratégicos tanto regionais quanto globais.

Especificamente sobre esta companhia, além de manter a tradição na gestão de riscos operacionais e relacionados à qualidade, demandada pela própria indústria, teve sua gestão de riscos aprimorada nos últimos anos. Isso ocorreu, principalmente, tanto pela elevação das expectativas de seus stakeholders, notavelmente reguladores e investidores, como pela capacidade desenvolvida e o conhecimento acumulado para vislumbrar cenários e gerir riscos novos e emergentes. Assim, as principais classes de risco da companhia são os estratégicos, regulatórios, operacionais, financeiros e cibernéticos.

A gestão de riscos da organização é orientada por princípios e diretrizes alinhados a seu planejamento estratégico, emprega metodologias avançadas, é guiada por uma política de gestão de riscos aprovada pelo conselho de administração e é executada por meio de uma estrutura organizacional que conta com profissionais experientes. Para a aplicação do MAM-GRC foram envolvidos três desses profissionais qualificados, com média de experiência superior a dez anos entre os dedicados à cadeia de valor da aviação e a esta organização.

Os colaboradores possuem conhecimentos acumulados em diversas funções, com consequentes pontos de vista que vão desde a gestão de operações, que envolvem mais “donos de risco”, à gestão estratégica, que incluem as 2ª e 3ª linhas de atuação em riscos. É importante recuperar que, assim como para todas as entrevistas e pelo próprio objetivo da pesquisa, não foram necessárias informações que de alguma forma já não tivessem sido divulgadas ao setor ou ao mercado, ou seja, que não fossem de alguma maneira públicas.

Foram realizadas três entrevistas remotas, por videoconferência, no período de abril a junho de 2020, com participações individuais dos colaboradores. Como planejado para a aplicação do MAM-GRC, as entrevistas foram iniciadas com a apresentação, discussão e preenchimento da Planilha 1 (**contextualização**). Após essa fase, a Planilha 2 foi então apresentada para preenchimento (**modelo de avaliação**). Por limitações tais como o tamanho da organização e a disponibilidade dos profissionais, as planilhas preenchidas pelo primeiro entrevistado foram disponibilizadas para o segundo, e, de forma sucessiva e acumulativa, para o terceiro.

Dessa forma as planilhas foram completadas com *insights* dos três profissionais, sendo que o terceiro gentilmente empenhou-se em discutir e consolidar as práticas identificadas e os

valores a elas atribuídos. A próxima seção consolida as avaliações da organização industrial do setor de aviação e determina sua maturidade em GRC.

Organização pública de interesse à saúde.

A terceira aplicação do modelo operacional para avaliação da maturidade em GRC foi realizada em uma organização pública de interesse à saúde que colabora com a Agência Nacional de Vigilância Sanitária e com as secretarias de saúde estaduais e municipais. Suas atividades principais envolvem ensino, pesquisa e desenvolvimento de tecnologias de laboratório para controlar a qualidade de produtos, insumos, ambientes e serviços. Também realiza análise laboratorial e expedição de laudos técnicos para o registro, comercialização, importação e exportação de alimentos, cosméticos, saneantes, medicamentos, vacinas, sangue e seus derivados, e outras substâncias relacionadas à saúde.

Trata-se de uma instituição federal criada no início dos anos 1980 como parte de uma grande estrutura vinculada ao Ministério da Saúde e fornecedora de produtos estratégicos para o Sistema Único de Saúde. Sua atuação é bastante específica na vigilância sanitária e muitos dos serviços prestados são únicos no Brasil.

Para desenvolver suas atividades, a organização é intensiva em infraestrutura laboratorial, tecnologia e conhecimento. Possui instalações laboratoriais com mais de 10 mil m^2 operados por quase 500 profissionais qualificados. Com a pandemia de Covid-19, o mundo viveu e vem enfrentando o maior desafio sanitário, humanitário, social e econômico do século XXI e a organização desempenhou e vem desempenhando uma contribuição fundamental na resposta ao enfrentamento da doença.

Quanto ao início, contextualização e sequência do fluxo de aplicação do MAM-GRC, e considerando os objetivos da organização e suas atividades-fim, seus principais riscos estão associados à qualidade e confiabilidade dos serviços prestados, à segurança e saúde das pessoas e da sociedade, aos processos e às garantias orçamentarias para a manutenção de suas atividades. Por se tratar de instituição federal, está incluída no contexto da Instrução Normativa nº 01/2016, que tornou obrigatória a adoção de práticas relacionadas à gestão de riscos, aos controles internos e à governança a todos os órgãos e entidades do Poder Executivo Federal.

Nesse contexto federal, embora riscos venham sendo geridos com sucesso de forma coincidente aos processos desde a criação da instituição, uma política de gestão de riscos foi aprovada nos últimos anos e associada à integridade e aos controles internos. Como

consequência de sua implementação, uma estrutura dedicada à GRC foi mais recentemente estabelecida.

Para a aplicação do Modelo Operacional para Avaliação da Maturidade em Gestão de Riscos Corporativos (MAM-GRC), foram entrevistados três profissionais envolvidos nessa implementação, via videoconferência, entre março e junho de 2021. Vale destacar que não foram necessárias informações classificadas ou sensíveis sobre a organização, e que não fossem de conhecimento público, para a condução dessa aplicação.

Assim como para a organização logística do setor de óleo, gás e biocombustíveis, os três profissionais participaram em conjunto de duas reuniões, com duração média de duas horas cada. Um dos entrevistados participou ainda de uma terceira reunião, na qual gentilmente colaborou para a organização das informações e discussões sobre o modelo.

Foram apresentadas as duas planilhas em sequência, referentes à operacionalização do modelo, e preenchidos os campos de práticas de gestão de riscos (Planilha 1 e **contextualização**), suas atribuições de efetividade e as notas referentes aos 12 elementos que caracterizam os fatores determinantes da maturidade em GRC (Planilha 2 e **modelo de avaliação**). A próxima seção consolida as avaliações da organização pública de interesse à saúde e determina sua maturidade em GRC.

4.2.3. Avaliação da maturidade em Gestão de Riscos Corporativos e proposição de ações nos casos selecionados

Por meio das entrevistas com as organizações e seguindo o fluxo de aplicação do MAM-GRC, foram então obtidos os valores necessários para avaliar seus níveis de maturidade em GRC. A Tabela 9 apresenta os valores coletados nesta fase do fluxo de aplicação do modelo com os casos estudados.

Tabela 9 – Aplicação do MAM-GRC nas organizações avaliadas

Prática / Organização	Modelo de avaliação – Planilha 2												Efetividade
	F1. Organização			F2. Tecnicidade			F3. Transparência			F4. Envolvimento			
	F1. E1.	**F1. E2.**	**F1. E3.**	**F2. E1.**	**F2. E2.**	**F3. E3.**	**F3. E1.**	**F3. E2.**	**F3. E3.**	**F4. E1.**	**F4. E2.**	**F4. E3.**	
P1) Existe comprometimento da alta gestão com a GRC.													
Org. A	10	10	10	10	10	10	10	10	10	10	10	10	10
Org. B	9	10	10	9	9	7	8	8	8	10	7	7	10
Org. C	9	8	8	3	3	4	6	5	8	5	2	3	7
P2) Existe responsabilidade sobre os riscos (todo risco tem um gestor).													
Org. A	10	10	10	10	10	10	10	10	10	10	10	10	10
Org. B	10	10	9	9	8	9	8	7	8	10	7	7	9
Org. C	8	8	9	6	2	2	6	4	4	3	2	3	5
P3) Existe tolerância e apetite a risco bem definidos.													
Org. A	10	10	10	10	10	10	10	10	10	10	10	10	10
Org. B	10	10	9	9	9	8	8	7	10	9	7	7	8
Org. C	9	8	9	5	1	2	5	6	4	4	2	2	4
P4) Existe uma cultura consciente dos riscos.													
Org. A	10	10	10	10	10	10	10	9	10	10	10	10	10
Org. B	10	10	9	10	8	8	7	10	10	8	7	7	9
Org. C	8	9	6	6	5	5	4	4	5	5	3	3	4
P5) Existem recursos suficientes para a GRC.													
Org. A	10	10	10	10	10	10	10	10	10	10	10	10	10
Org. B	10	10	10	9	9	8	10	10	10	10	7	7	9
Org. C	9	8	9	4	4	5	8	6	7	5	4	2	6
P6) Há eficiência na identificação, análise e resposta ao risco.													
Org. A	10	10	10	10	10	10	10	10	10	9	10	10	10
Org. B	10	10	10	10	8	10	10	7	10	9	9	9	9
Org. C	8	6	4	4	3	3	8	8	8	4	2	2	3
P7) Os processos de GRC são dinâmicos e realimentados.													
Org. A	10	10	10	10	10	10	10	10	10	10	10	10	10
Org. B	9	10	10	8	8	7	7	7	7	7	5	5	8
Org. C	6	5	7	3	4	6	8	8	9	5	3	1	3
P8) A GRC é relacionada a oportunidades.													
Org. A	10	10	10	10	10	10	10	10	10	10	10	10	10
Org. B	9	9	8	8	7	7	7	7	5	7	5	5	8
Org. C	8	8	8	5	4	5	7	8	5	6	5	5	4
P9) Existe uma comunicação sobre riscos.													
Org. A	10	10	10	10	10	10	10	10	10	10	10	10	10
Org. B	10	10	10	7	10	7	10	10	7	10	7	7	9
Org. C	8	7	7	5	4	5	5	4	8	10	8	8	6
P10) A GRC tem uma linguagem comum.													
Org. A	10	10	10	10	10	10	10	10	10	10	10	10	10
Org. B	10	10	10	7	10	7	7	10	5	9	7	7	8
Org. C	6	8	6	5	4	6	5	8	9	3	4	2	6
P11) Existe um sistema de informações gerenciais para a GRC.													
Org. A	10	10	10	10	10	10	10	10	10	10	10	10	10
Org. B	10	10	10	9	9	7	8	10	7	8	5	5	7
Org. C	8	7	9	6	5	6	9	8	8	4	3	3	3
P12) Há programas de treinamento para a GRC.													
Org. A	10	10	10	10	10	10	10	10	10	10	10	10	10
Org. B	10	10	10	10	10	10	10	10	7	9	5	5	8
Org. C	8	7	8	4	2	3	9	7	7	5	5	5	5
P13) Existem indicadores formais para riscos.													
Org. A	10	10	10	10	10	10	10	10	10	10	10	10	10
Org. B	10	10	10	10	10	10	10	7	7	10	5	5	8
Org. C	8	8	9	5	6	7	7	6	6	4	1	1	2

Prática / Organização	Modelo de avaliação – Planilha 2												Efetividade
	F1. Organização			F2. Tecnicidade			F3. Transparência			F4. Envolvimento			
	F1. E1.	**F1. E2.**	**F1. E3.**	**F2. E1.**	**F2. E2.**	**F3. E3.**	**F3. E1.**	**F3. E2.**	**F3. E3.**	**F4. E1.**	**F4. E2.**	**F4. E3.**	
P14) Existe integração entre a GRC e os processos da organização.													
Org. A	10	10	10	10	10	10	10	10	10	10	10	10	9
Org. B	9	9	8	9	10	8	7	7	7	7	5	5	9
Org. C	6	7	7	6	7	6	4	6	5	5	10	2	2
P15) Monitoramento, revisão e melhoria do planejamento da GRC.													
Org. A	10	10	10	10	10	10	10	10	10	10	10	10	9
Org. B	9	9	8	9	9	8	7	7	5	7	5	5	9
Org. C	7	7	7	5	6	4	4	5	5	4	5	2	2

Fonte: Elaborado pelo autor.

Para determinar os valores atribuídos às práticas genéricas de GRC do modelo de avaliação, foram identificadas, discutidas e conciliadas diversas práticas específicas de GRC. O Anexo II apresenta uma lista das práticas identificadas nesta fase da pesquisa.

A partir dos valores atribuídos aos doze elementos e a cada uma das quinze práticas genéricas de GRC, foi então possível calcular os fatores organização, tecnicidade, transparência e envolvimento para cada organização. O cálculo dos fatores é determinado pela média simples dos elementos, ponderada pela efetividade de cada prática, de acordo com a Fórmula 1, já apresentada. A Figura 14 apresenta os fatores calculados de acordo com o modelo aplicado para cada organização.

Figura 14 – Fatores calculados para as organizações avaliadas

Fonte: Elaborado pelo autor.

A partir dos fatores calculados, e dando sequência ao fluxo de aplicação do MAM-GRC, a fase de **comparação** determinou em qual dos cinco níveis de maturidade a organização pôde ser classificada. Para isso, empregou a **tabela determinante de nível**, desenvolvida para classificar os níveis de maturidade em GRC e apresentada no Capítulo 3 - Metodologia. Os resultados dessa comparação estão apresentados na Tabela 10.

Tabela 10 – Resultados do MAM-GRC para as organizações avaliadas (Saída 1)

Organização avaliada	**Média** (critério)	**Maior fator** (critério)	**Desvio Padrão** (critério)	**Nível de GRC Classificado**
Organização A	**0,985** (> 0,8)	**Todos** (indiferente)	**0,006** (< 0,1)	Nível 5 Sistêmico
Organização B	**0,712** (>0,7 e ≤ 0,8)	**Organização** (indiferente)	**0,011** (≥ 0,1)	Nível 4 Participativo
Organização C	**0,480** (≤ 0,6)	**Organização** (Organização)	**0,152** (≥ 0,1)	Nível 2 Contingencial

Fonte: Elaborado pelo autor.

Dando sequência ao fluxo de aplicação do MAM-GRC, após obter os níveis de maturidade em GRC para as organizações, é possível realizar a **observação das diferenças** entre seus estados atual e desejado. Nesse passo, ocorre novamente a comparação entre o MAM-GRC, que é um modelo de avaliação, e um padrão, que é o modelo de maturidade de Oliva (2016).

Também nesta última etapa da aplicação do MAM-GRC, em direção à sua Saída 2, é realizada uma revisão crítica dos valores atribuídos às práticas de GRC, aos elementos e aos fatores que compõem o modelo. A Tabela 11 apresenta as prioridades de ação identificadas para cada organização através do MAM-GRC, que caracteriza a Saída 2 do fluxo de aplicação do modelo.

Tabela 11 – Aplicação do MAM-GRC para priorizar ações de elevação do nível de maturidade em GRC (Saída 2)

Org. A	**Nível atual**	**Próximo nível**	**Priorizar**
	Sistêmico	Manutenção	**Fator:** todos. **Elementos:** F3E3. **Práticas:** 14 e 15
	Ações gerenciais mais imediatas: Investir na manutenção dos níveis alcançados e na antecipação de eventos que possam prejudicar a efetividade das práticas identificadas. Priorizar ações para evoluir em consciência para oportunidades e nas práticas genéricas de GRC com menores avaliações de efetividade, como a prática 14 e a prática 15.		
Org. B	**Nível atual**	**Próximo nível**	**Priorizar**
	Participativo	Sistêmico	**Fator:** Envolvimento. **Elementos:** F3E1, F3E3. **Práticas:** 7, 8, 10, 11, 12 e 13.
	Ações gerenciais mais imediatas: Investir em ações para aumentar o suporte externo para a evolução da GRC, a liderança da organização na GRC para com os agentes que se relaciona e aumentar sua interação no ambiente de valor. Priorizar ações focadas nos elementos que receberam baixa avaliação, tais como para aumentar a permeabilidade da GRC na estrutura e promover a iniciativa vigilante em relação a riscos. Ainda, priorizar as práticas genéricas de GRC com menores avaliações de efetividade, principalmente a prática 11.		
Org. C	**Nível atual**	**Próximo nível**	**Priorizar**
	Contingencial	Estruturado	**Fator:** Tecnicidade. **Elementos:** F2E1, F2E2, F2E3**.** **Práticas:** 13, 14, 15, 6, 7 e 11.
	Ações gerenciais mais imediatas: Investir em ações para aumentar a eficiência de indicadores de riscos e dos sistemas de inteligência para a GRC, bem como para aumentar a regularidade da reavaliação desses indicadores e sistema. Priorizar ações focadas nas práticas genéricas de GRC com menores avaliações de efetividade, principalmente as práticas 13, 14 e 15.		

Fonte: Desenvolvido pelo autor.

Finalmente, neste último passo os gestores podem se beneficiar de um retorno aos critérios do MAM-GRC para verificar as prioridades de ação para elevar o nível de maturidade da GRC de suas organizações.

4.3. Resultados da etapa de análises de utilidade e aplicabilidade do MAM-GRC

Nesta sexta e última etapa do caminho metodológico da pesquisa o MAM-GRC foi avaliado, através de um questionário, pelos profissionais envolvidos no seu processo de aplicação em casos reais. A intenção foi analisar, pelo ponto de vista dos executivos, se o modelo pode ser utilizado para auxiliar a tomada de decisões. A íntegra do questionário segue nesta tese como Anexo I.

Vale recuperar do Capítulo 3 - Metodologia, que as fundamentações teóricas envolvidas nesta etapa são os critérios de avaliação, utilidade, confiança e documentação de Gass (1983) e os atributos de transparência e validação de Eddy et al. (2012). Ou seja, que possa ser possível compreender como o MAM-GRC foi construído e que ele seja capaz de reproduzir a realidade.

Ao todo, oito profissionais completaram o questionário. Todos responderam que o modelo pôde ser adequadamente compreendido, considerando as Planilha 1 e 2 e seus textos explicativos tanto para o levantamento de práticas de GRC quanto para determinar a maturidade em GRC de suas organizações.

Os profissionais também foram unânimes em responder que os quatro fatores apresentados no MAM-GRC são, de alguma forma, aplicáveis às suas organizações. E que a determinação do nível de maturidade em GRC através dele é aplicável em sua organização e no seu setor. Todos também responderam que tanto a estrutura quanto as variáveis utilizadas (termos, características e valores) estão coerentes com os objetivos do modelo, e que suas limitações foram compreendidas.

Entretanto, embora todos os respondentes acreditem que o MAM-GRC possa ser compreensível, plausível e acessível para técnicos no assunto, tais como gestores e analistas de riscos, um executivo respondeu que não acredita que profissionais não envolvidos com a gestão de riscos possam aplicá-lo: "*Pode ser que a pessoa não tenha interesse no assunto, ou tenha dificuldade de aprender, ou que nunca ouviu falar de algum termo.*"

Além disso, um respondente reportou dificuldade para aplicar a efetividade das práticas de GRC em escala de 1 a 10. Ao considerar sua sugestão, ficou claro que sua resposta estava relacionada a práticas com níveis baixos de efetividade: "*não faz sentido ter uma nota alta em Efetividade se as notas são baixas ou médias nas práticas*".

Considerando a forma como o modelo deve ser aplicado, em casos como este a prática poderia ter sido excluída do modelo na fase de contextualização. Ainda assim, a observação de que pode existir uma correlação entre os valores da efetividade e os dos elementos que compõem os fatores é bastante plausível e deve ser considerada para estudos futuros.

Metade dos profissionais que responderam à pesquisa concordaram totalmente que as atribuições de notas, de 1 a 10, para valorar o modelo de análise, ficaram claras. Por outro lado, a outra metade concordou apenas parcialmente com esta afirmação. As sugestões dos quatro respondentes que concordaram parcialmente convergem para a utilização de uma escala qualitativa: "*Talvez usar uma definição da performance (Otima, Boa, Ruim, etc) que corresponderia a uma nota ou um range de notas*." De fato, este pode ser um ponto importante a ser considerado em novas aplicações do MAM-GRC e por futuras pesquisas.

Avaliando que na etapa de aplicação do MAM-GRC foram envolvidos três profissionais em cada uma das três organizações estudadas, e que todos se comprometeram e dedicaram seu tempo e conhecimento à pesquisa, um retorno de oito questionários pode ser considerado um sucesso nessa etapa adicional.

Enfim, o propósito da aplicação desta nova camada de pesquisa, em forma de questionário, não foi o de produzir análises quantitativas, mesmo porque o número de respondentes é pequeno para que possam ser extraídas análises estatísticas. Ainda assim, as evidências encontradas nesta última etapa do caminho metodológico da pesquisa corroboram para inferir que o modelo desenvolvido é transparente, útil e razoável aos olhos dos profissionais que o aplicaram.

5. CONSIDERAÇÕES FINAIS

A pesquisa apresentada nesta tese teve início com a identificação de que não há na academia, no campo da Gestão de Riscos Corporativos (GRC), um modelo de avaliação de maturidade que tenha base teórica e empírica com espectro largo o suficiente para ser aplicado em diversos setores.

A partir desta constatação, decorrente de uma Revisão Sistemática da Literatura (RSL), um problema de pesquisa geral e quatro problemas específicos foram delineados para desenvolver e apresentar um modelo com essas características. Tratou-se, portanto, de um esforço para disponibilizar um modelo de maturidade pronto para ser aplicado em uma organização e, assim, contribuir com propósitos de pesquisadores e executivos.

O resultado é que, por meio de um planejamento metodológico e de sua execução através dos objetivos traçados, esta tese pesquisou, desenvolveu, aplicou e avaliou o Modelo Operacional para Avaliação da Maturidade em Gestão de Riscos Corporativos, ou simplesmente MAM-GRC.

Este quinto capítulo discute, nas seções seguintes, como os aspectos metodológicos foram executados e como os objetivos de pesquisa propostos foram atingidos. Além disso, discorre sobre as contribuições teóricas e práticas dos resultados encontrados e sobre as limitações da pesquisa e sugestões para estudos futuros.

5.1. Atendimento aos objetivos da pesquisa e aos aspectos metodológicos

Esta pesquisa teve como objetivo geral analisar o nível de maturidade em Gestão de Riscos Corporativos em grandes organizações. Para cumprir este objetivo, quatro objetivos específicos foram determinados: (1) identificar as práticas de gestão de riscos essenciais para avaliar o nível de maturidade em GRC; (2) determinar elementos de GRC suficientes para definir níveis de maturidade em GRC; (3) propor um modelo operacional para avaliar a maturidade em GRC; e (4) identificar as ações gerenciais pertinentes para elevar, a cada nível, a maturidade em GRC das organizações avaliadas pelo modelo.

Para que estes objetivos pudessem ser atingidos, uma sequência normativa de seis etapas foi planejada e denominada ‘caminho metodológico da pesquisa’. A primeira destas etapas foi

uma revisão da literatura sobre modelos de maturidade e GRC para suportar uma segunda etapa de revisão sistemática da literatura.

Na segunda etapa do caminho metodológico da pesquisa, uma seleção criteriosa a partir de mais de cinco mil documentos das bases *Scopus* e *Web of Science* foi realizada. O escopo da RSL foi identificar e classificar os modelos de maturidade em GRC existentes na literatura para extrair as práticas de GRC e seus atributos de maturidade. Na sequência, a terceira etapa empregou o corpo do conhecimento compilado pela RSL para conceber a primeira versão do MAM-GRC. Nesta versão o modelo era, ainda, fruto apenas de pesquisa teórica.

A quarta etapa do caminho metodológico da pesquisa envolveu entrevistas com 27 profissionais experientes em gestão de riscos de diversos setores. Nesta etapa ocorreu a primeira investigação empírica pela qual o modelo, até então teórico, foi aperfeiçoado e operacionalizado em uma nova versão. A versão resultante do MAM-GRC tem a forma de duas planilhas de trabalho. A Planilha 1 traz as práticas de gestão de riscos essenciais para adaptá-las a cada organização e a Planilha 2 contém os elementos suficientes para definir níveis de maturidade em GRC. Dessa forma, os objetivos específicos 1 e 2 foram atendidos com a conclusão desta quarta etapa.

Em seguida, na quinta etapa, o MAM-GRC aperfeiçoado teve suas duas planilhas aplicadas em três organizações por meio de uma segunda investigação empírica. Três profissionais de cada organização contribuíram para o preenchimento das planilhas com dados reais e um nível de maturidade em GRC foi encontrado para cada uma delas. Ainda nesta etapa, uma análise reversa e comparativa do MAM-GRC foi realizada para identificar as prioridades de ação para incrementar a GRC de cada organização avaliada. Assim, os objetivos específicos 3 e 4 foram atendidos com a conclusão desta quarta etapa.

Na sexta etapa do caminho metodológico da pesquisa o MAM-GRC foi avaliado por meio de um questionário anônimo. Esta terceira fase empírica serviu para concluir sobre a utilidade e aplicabilidade do MAM-GRC, além de apontar impressões sobre sua aplicação gerencial e corroborar o objetivo geral desta tese.

Finalmente, considerando as relações entre os objetivos específicos traçados e o método empregado em etapas, o objetivo principal desta tese foi atendido ao fim da sexta e última etapa do caminho metodológico da pesquisa.

5.2. Contribuições teóricas

O estudo desenvolvido e realizado nesta tese produz algumas contribuições teóricas, sobretudo pertinentes a área da GRC, mas também relacionadas aos modelos de maturidade e suas aplicações na gestão de organizações.

Inicialmente, contribui para futuros trabalhos de pesquisadores que demandam uma estrutura para qualificar ou medir a GRC de organizações de indústrias fora do *mainstream* de estudos em GRC ou entre setores. Como apresentado no Capítulo 2 - Referencial Teórico, existe uma concentração de formas empregadas para quantificar a GRC no setor de serviços financeiros, notavelmente divididas entre aquelas que empregam dados primários e secundários.

Evidentemente, cada *framework* possui suas aplicações e limitações e o modelo aqui apresentado pode ser bastante útil a pesquisas que pretendam abordar a GRC entre casos, especificamente às com intenção de comparar a GRC com outros fenômenos e, como notado, fora dos setores mais convencionais. Mais ainda, para estudos futuros que pretendam inclui o paradigma de ambiente de valor, que considera os agentes e suas relações, e em suas avaliações de GRC.

Outras contribuições deste estudo estão relacionadas a evolução do modelo de maturidade de GRC de Oliva (2016) em direção à sua aplicação. Enquanto a maioria dos modelos de maturidade em negócios, e em especial em GRC, são baseados em capacidades teóricas mínimas, este modelo se distingue por ter sido obtido a partir de dados empíricos. Mais ainda, também se destaca por considerar o ambiente de valor e os agentes externos à organização para a GRC. Dessa forma, esta tese apresenta, dentro de seus limites, uma extensão operacional do modelo de Oliva (2016).

Nesse contexto de operacionalização, há uma contribuição intrínseca a concepção dos elementos e fatores que compõem o MAM-GRC. A sustentação teórica que subsidia a criação dos doze elementos distintivos de fatores de GRC pode ser útil a pesquisadores que pretendam consolidar práticas de gestão relacionadas ou distintivas de GRC. Esta mesma contribuição advém da forma como a efetividade dos fatores é considerada. Mesmo a metodologia utilizada para a transformação do modelo de maturidade em modelo de avaliação pode ser útil a pesquisas com este mesmo desafio.

Mais distante da GRC, há também efeitos pertinentes aos modelos de maturidade em gestão de processos de negócios. Pesquisas que envolvam estes modelos podem reconhecer nesta tese contribuições para organizar suas características e colher frutos da estrutura conceitual apresentada para classificá-los. Tais caracterizações de modelos de maturidade aplicados à gestão de negócios revelaram-se bastante dispersas na literatura e, por isso, foram necessários arranjos para subsidiar a criação do MAM-GRC. Entretanto, as distinções entre modelos de maturidade e de avaliação, entre modelos conceituais e operacionais, e entre os tipos de estudos relacionados aos modelos podem ser aplicáveis não apenas à GRC, mas à diversas áreas da administração.

Especificamente sobre os modelos de maturidade em GRC, os resultados da RSL contribuem para apresentar o estado da arte em modelos de maturidade e de avaliação. Uma constatação e consequente contribuição conceitual é que, em GRC, apresentações de modelos fundem teorias de maturidade, de avaliação e de gestão de negócios por processos, de forma que pesquisadores tem dificuldade para compreender, a cada modelo publicado, *se* e *como* podem ser aplicados à realidade das empresas. Mais ainda, o quanto são aderentes aos conceitos holísticos de GRC ou mantém os silos da gestão tradicional de riscos.

Em relação ao avanço das pesquisas em GRC, esta tese apresenta uma contribuição para expandir o entendimento de sua aplicação em setores diferentes daqueles de sua origem. Ao empregar uma abordagem qualitativa e o estudo de três casos, a pesquisa viabiliza a contextualização e investigação da GRC com evidências que normalmente são tradas de forma superficial pelos estudos quantitativos. Esta contribuição é corroborada pela própria literatura da área, que com frequência menciona sugestões para que futuras pesquisas sejam realizadas em diferentes setores.

Finalmente, esta tese também colabora para a discussão e melhor conhecimento do limite da GRC em relação ao ambiente externo à organização. Há suporte na literatura recente de que a GRC deve transcender suas ações além dos limites da organização. Entretanto, esse limite ainda não é bem definido e as fronteiras da GRC têm sido discutidas quanto à capacidade de alcance aos stakeholders e agentes externos. Esta pesquisa corrobora com esta fronteira ao considerar que, no MAM-GRC, o nível mais alto de maturidade em GRC é dado pelo *nível sistêmico* do modelo de Oliva (2016). Para ser classificada neste nível, a gestão de riscos da empresa deve incluir a avaliação do seu ambiente de valor e considerar que os riscos não respeitam os limites da empresa.

5.3. Implicações gerenciais

Esta tese apresenta alguns resultados que podem ser diretamente aplicados por executivos em suas organizações. Tais resultados são corroborados tanto pelo objetivo de operacionalizar um modelo de maturidade em GRC, quanto pelos métodos empregados de adaptação, aplicação e validação do modelo com especialistas profissionais e casos reais.

A primeira contribuição prática é que o MAM-GRC pode ser empregado pelas organizações como instrumento de avaliação em GRC pelo paradigma de ambiente de valor. Este paradigma, que compreende os agentes, suas formas de relação com a organização e os riscos que emanam de tais relações, pode ser bastante útil para identificar riscos até então não alcançados pela visão tradicional de processos.

Logo, mesmo organizações com políticas de GRC eficientemente implementas podem potencialmente extrair benefícios da aplicação do MAM-GRC. Isso porque executivos podem, na aplicação deste modelo, acessar riscos e formas de tratamento não mapeados por outros modelos de capacidades ou ferramentas de gestão de riscos já empregadas.

Outra contribuição é a própria forma com que esta tese expõe o MAM-GRC. Além de manter o foco na descrição do método e na análise dos resultados, esta pesquisa também apresenta uma seção sobre a maneira de aplicá-lo, especificamente no Capítulo 4 – Análise de Resultados. O objetivo foi exibir de forma prática, com auxílio de figura e sequência de passos, um texto similar a um manual de aplicação do MAM-GRC.

Neste manual estão indicadas as duas planilhas que operacionalizam o modelo, a fórmula de cálculo do valor dos fatores e a tabela necessária para comparar o resultado e determinar o nível de maturidade em GRC da organização avaliada. Esta forma de apresentação permite que o MAM-GRC possa ser empregado diretamente por profissionais da organização como forma de autoavaliação da maturidade em GRC e de consideração do ambiente de valor.

Finalmente, uma implicação gerencial importante é a possibilidade de utilização do modelo para priorizar ações de desenvolvimento da GRC. A aplicação do MAM-GRC exige que executivos naturalmente discutam suas práticas de gestão de riscos e que façam o cruzamento das práticas selecionadas com ponderações de doze elementos distintivos de GRC. Este método de avaliação, seguido da comparação com o modelo de maturidade de Oliva (2016), permite evidenciar os pontos de vulnerabilidade da organização em GRC e assim guiar a construção de um plano de ação para alcançar o próximo nível de maturidade em GRC.

5.4. Limitações e sugestões para estudos futuros

Evidentemente, o estudo aqui apresentado possui limitações e novas pesquisas podem completá-lo. Cumprir a sequência metodológica já constituiu um desafio e, além disso, atingir o compromisso duplo de promover avanços teóricos e práticos exigiu a adoção de algumas convenções, as quais podem ser melhor desenvolvidas em estudos subsequentes.

As primeiras limitações estão associadas ao caminho metodológico da pesquisa e a forma como o modelo conceitual inicial foi adaptado. Algumas características importantes do modelo surgiram nesta etapa, como a definição de efetividade para as práticas de GRC e a aplicação em forma de duas planilhas sequenciais.

Apesar de ter contado com a disponibilidade e colaboração de 27 profissionais experientes nesta etapa, o questionário final de avaliação apontou que a implementação da efetividade em casos reais pode ser aprimorada. Uma sugestão muito pertinente, discutida *ex-post*, envolve a mudança de escala, de um a dez, para uma escala qualitativa. Nesse contexto, sugere-se novas pesquisas para implementar uma escala de avaliação e priorização de práticas de gestão de riscos que produzam efeitos melhores aos alcançados.

Ainda quanto ao caminho metodológico, também a etapa de aplicação do MAM-GRC é limitada aos resultados dos três casos estudados. Os modelos de avalição associados à maturidade, assim como diversos modelos de processos de gestão, são aprimorados a medida em que são implementados. Logo, é preciso reconhecer que o MAM-GRC está em sua infância e poderá adquirir maturidade a medida em que acumular mais casos, aplicações e diagnósticos prestados. Como consequência direta dessa constatação, sugerem-se novos estudos que apliquem o MAM-GRC e incorporem melhorias.

Um outro ponto importante sobre este estudo é que, embora ele apresente uma lista de 15 práticas genéricas de GRC, o MAM-GRC foi desenvolvido como um modelo aberto. Isto significa que ele foi concebido para ser capaz de acomodar práticas de gestão de riscos além de uma lista fechada, o que implica em algumas vantagens, mas também limitações. Há alguns pontos de atenção sobre esta proposição.

Primeiro, o MAM-GRC é adaptável a organizações de diferentes setores porque permite customizar as práticas genéricas a diferentes contextos e particularidades. Entretanto, sua operacionalização é dependente da qualidade das práticas selecionadas e adaptadas. A consequência direta é que o resultado, ou o nível de maturidade em GRC da organização

avaliada, é tão confiável quanto a qualidade da contextualização das práticas iniciais. Logo, pesquisas que possam contribuir para esta avaliação da adaptação de práticas ou de suas formas de customização podem incrementar consideravelmente a eficácia do MAM-GRC.

Segundo, esta pesquisa e o MAM-GRC como proposto não apresentam uma forma de avaliar a qualidade dessa contextualização de práticas. Durante a etapa metodológica de aplicação em organizações reais ficou claro que o empenho dos gestores e o envolvimento com a destilação das práticas específicas da organização são fundamentais. Mais ainda, que o tempo de dedicação é compreensivelmente proporcional ao tamanho da organização e ao nível de granularidade que gestores pretendem dar a avaliação. Dessa forma, investigações quanto ao nível de aplicação do MAM-GRC e ao seu desempenho em diversos níveis de análise podem ser muito contributivas ao modelo.

Finalmente, as análises de utilidade e aplicação do MAM-GRC foram conduzidas por meio de questionário anônimo. Embora seja esta uma terceira coleta de dados primários da pesquisa, as oito respostas não podem ser extrapoladas e devem ser limitadas aos contextos específicos das três aplicações do MAM-GRC. Sugere-se que novas pesquisas de validação sejam conduzidas em paralelo a correntes aplicações.

6. REFERÊNCIAS

Aabo, T., Fraser, J. R. S., & Simkins, B. J. (2005). The Rise and Evolution of the Chief Risk Officer: Enterprise Risk Management at Hydro One. *Journal of Applied Corporate Finance*, *17*(3), 62–75. Doi:10.1111/j.1745-6622.2005.00045.x

Aken, J. E. van, Berends, H., & Bij, H. (2012). *Problem solving in organizations: A methodological handbook for business and management students*. Cambridge University Press.

Aken, J. E. van, & Romme, G. (2009). Reinventing the future: adding design science to the repertoire of organization and management studies. *Organization Management Journal*, *6*(1), 5–12. Doi: 10.1057/omj.2009.1

Albliwi, S. A., Antony, J., & Arshed, N. (2014). Critical literature review on maturity models for business process excellence. *2014 IEEE International Conference on Industrial Engineering and Engineering Management*, *2015-Janua*, 79–83. Doi:10.1109/IEEM.2014.7058604

Aon. (2010). *Global Enterprise Risk Management Survey 2010*. Disponível em: https://www.aon.com/attachments/2010_Global_ERM_Survey.pdf

Arena, M., Arnaboldi, M., & Palermo, T. (2017). The dynamics of (dis)integrated risk management: A comparative field study. *Accounting, Organizations and Society*, *62*, 65–81. Doi:10.1016/j.aos.2017.08.006

Baird, I., & Thomas, H. (1985). Toward a contingency model of strategic risk taking. *The Academy of Management Review*, *10*(2), 230–243. Doi:10.2307/257965

Bar-Ilan, J. (2008). Informetrics at the beginning of the 21st century-A review. *Journal of Informetrics*, *2*(1), 1–52. Doi:10.1016/j.joi.2007.11.001

Bearden, W., Netemeyer, R., & Haws, K. (2001). *Handbook of Marketing Scales: Multi-Item Measures for Marketing and Consumer Behavior Research* (p. 177). SAGE Publications.

Beasley, M., Branson, B., & Pagach, D. (2015). An analysis of the maturity and strategic impact of investments in ERM. *Journal of Accounting and Public Policy*, *34*(3), 219–243. Doi:10.1016/j.jaccpubpol.2015.01.001

Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, *24*(6), 521–531. Doi:10.1016/j.jaccpubpol.2005.10.001

Bohnert, A., Gatzert, N., Hoyt, R. E., & Lechner, P. (2018). The drivers and value of enterprise risk management: evidence from ERM ratings. *European Journal of Finance*. Doi:10.1080/1351847X.2018.1514314

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2014). Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning*, *48*(4), 265–276. Doi:10.1016/j.lrp.2014.07.005

Bryman, A. (2008). *Social Research Methods* (3rd ed). Oxford University Press.

Burke, W. W. (1985). Leaders: The strategies for taking charge, by Warren Bennis and Burt Nanus. New York: Harper & Row, 1985, 244 pp., $19.95. *Human Resource Management*, *24*(4), 503–508. Doi:10.1002/hrm.3930240409

Bution, J. L., Masiero, G., & Oliva, F. L. (2015). The systematic risk of the Brazilian textile industry: Consequences of their increasing international exposure . *International Proceedings of Economics Development and Research*, *85*(1). Disponível em: http://www.ipedr.com/vol85/017-R016.pdf

Bution, J. L. (2016). *Análise da relação entre grau de internacionalização e nível de maturidade em gestão de riscos corporativos*. Dissertação de Mestrado, Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo. doi:10.11606/D.12.2017.tde-20122016-111322.

Carmona, J., Engels, G., Kumar, A., Aalst, W. M. P. Van Der, Mylopoulos, J., Rosemann, M., Shaw, M. J., & Szyperski, C. (2017). Elements for Tailoring a BPM Maturity Model to Simplify its Use. Em J. Carmona, G. Engels, & A. Kumar (Orgs.), *Business Process Management Forum* (Vol. 297, p. 3–18). Springer International Publishing. Doi:10.1007/978-3-319-65015-9

Cassell, C., Cunliffe, A., & Grandy, G. (2018). The SAGE Handbook of Qualitative Business and Management Research Methods: Methods and Challenges. Em *SAGE Publications Ltd* (Vol. 1, Issue 4). SAGE Publications Ltd. Doi:10.4135/9781526430236

Choi, Y., Ye, X., Zhao, L., & Luo, A. C. (2016). Optimizing enterprise risk management: a literature review and critical analysis of the work of Wu and Olson. *Annals of Operations Research*, *237*(1–2), 281–300. Doi:10.1007/s10479-015-1789-5

Choi, Y., Ye, X., Zhao, L., & Luo, AmandaC. (2015). Optimizing enterprise risk management: a literature review and critical analysis of the work of Wu and Olson. *Annals of Operations Research*, 1–20. Doi:10.1007/s10479-015-1789-5

Churchill, G. A. (1979). A Paradigm for Developing Better Measures of Marketing Constructs. *Journal of Marketing Research*, *16*(1), 64. Doi:10.2307/3150876

Churchill Jr., G. A. (1994). Attitude Measurement. Em *Marketing Research* (p. 824).

Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., & Herrera, F. (2011). Science mapping software tools: Review, analysis, and cooperative study among tools. *Journal of the American Society for Information Science and Technology*, *62*(7), 1382–1402. Doi:10.1002/asi.21525

Cooper, D. R., & Schindler, P. S. (2014). Business Research Methods. Twelfth Edition. Em *Business Research Methods*.

COSO. Committee of Sponsoring Organizations of the Treadway Commission (2017). *Enterprise Risk Management Integrating with Strategy and Performance*. Disponível em: https://www.coso.org/

COSO. Committee of Sponsoring Organizations of the Treadway Commission (2004). Enterprise Risk Management — Integrated Framework. *New York*, *3*(September), 1–16. Disponível em: https://www.coso.org/

Crosby, P. B. (1979). *Quality is free: the art of making quality certain*. McGraw-Hill.

Crossref. (2019). *Crossref*. https://www.crossref.org

de Jongh, P. J. R., Larney, J., Mare, E., van Vuuren, G. W., & Verster, T. (2017). A proposed best practice model validation framework for banks. *South African Journal of Economic and Management Sciences*, *20*(1). Doi:10.4102/sajems.v20i1.1490

Deloitte. Deloitte Touche Tohmatsu Limited (2005). Disarming the Value Killers. *PR Newswire*, Disponível em: https://www2.deloitte.com/us/en/insights/topics/risk-management/disarming-the-value-killers-a-risk-management-study.html

Denyer, D., Tranfield, D., & van Aken, J. E. (2008). Developing Design Propositions through Research Synthesis. *Organization Studies*, *29*(3), 393–413. Doi:10.1177/0170840607088020

Dionne, G. (2013). Risk Management: History, Definition, and Critique. *Risk Management and Insurance Review*, *16*(2), 147–166. Doi:10.1111/rmir.12016

Doyle, J. (2018). Reconceptualising research impact: reflections on the real-world impact of research in an Australian context. *Higher Education Research and Development*, *37*(7). Doi:10.1080/07294360.2018.1504005

Echambadi, R., Campbell, B., & Agarwal, R. (2006). Encouraging best practice in quantitative management research: An incomplete list of opportunities. *Journal of Management Studies*, *43*(8), 1801–1820. Doi:10.1111/j.1467-6486.2006.00660.x

Eddy, D. M., Hollingworth, W., Caro, J. J., Tsevat, J., McDonald, K. M., & Wong, J. B. (2012). Model transparency and validation: A report of the ISPOR-SMDM modeling good research practices task force-7. *Medical Decision Making*, *32*(5). Doi:10.1177/0272989X12454579

Edmonds, C. T., Edmonds, J. E., Leece, R. D., & Vermeer, T. E. (2015). Do risk management activities impact earnings volatility? *Research in Accounting Regulation*, *27*(1), 66–72. Doi:10.1016/j.racreg.2015.03.008

Farrell, M., & Gallagher, R. (2015). The Valuation Implications of Enterprise Risk Management Maturity. *Journal of Risk and Insurance*, *82*(3), 625–657. Doi:10.1111/jori.12035

Farrell, M., & Gallagher, R. (2019). Moderating influences on the ERM maturity-performance relationship. *Research in International Business and Finance*, *47*(November 2018), 616–628. Doi:10.1016/j.ribaf.2018.10.005

Federico Neto, P., Santos, R. F., & Oliva, F. L. (2018). Enterprise risk management in the bus market of the city of São Paulo. *Benchmarking: An International Journal*. Doi:10.1108/BIJ-03-2018-0053

Fink, A. (2014). *Conducting Research Literature Reviews: From the Internet to Paper*. SAGE Publications. Doi:10.1002/nha3.10270

Florio, C., & Leoni, G. (2017). Enterprise risk management and firm performance: The Italian case. *The British Accounting Review*, *49*(1), 56–74. Doi:10.1016/j.bar.2016.08.003

FNQ, Fundação Nacional da Qualidade (2011). *Critérios rumo à excelência: Avaliação e diagnóstico da gestão organizacional* (6º ed). Disponível em: fnq.org.br

Gass, S. I. (1983). DECISION-AIDING MODELS: VALIDATION, ASSESSMENT, AND RELATED ISSUES FOR POLICY ANALYSIS. *Operations Research*, *31*(4). Doi:10.1287/opre.31.4.603

Gatzert, N., & Martin, M. (2015). Determinants and Value of Enterprise Risk Management: Empirical Evidence From the Literature. *Risk Management and Insurance Review*, *18*(1), 29–53. Doi:10.1111/rmir.12028

Ghoshal, S. (1987). Global Strategy: An Organizing Framework. *Strategic Management Journal*, *08*(05), 425–440. Doi:10.1002/ppul.21321

Gil, A. C. (2002). *Como elaborar projetos de pesquisa* (4º ed). Atlas.

Gil, A. C. (2010). Métodos e técnicas de pesquisa social. Em *Métodos e técnicas de pesquisa social*. Atlas.

Gordon, L. A., Loeb, M. P., & Tseng, C.-Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy*, *28*(4), 301–327. Doi:10.1016/j.jaccpubpol.2009.06.006

Grace, M. F., Leverty, J. T., Phillips, R. D., & Shimpi, P. (2015). The value of investing in enterprise risk management. *Journal of Risk and Insurance*, *82*(2), 289–316. Doi:10.1111/jori.12022

Hagigi, M., & Sivakumar, K. (2009). Managing diverse risks: An integrative framework. *Journal of International Management*, *15*(3), 286–295. Doi:10.1016/j.intman.2009.01.001

Hahn, G. J., & Kuhn, H. (2012). Value-based performance and risk management in supply chains: A robust optimization approach. *International Journal of Production Economics*, *139*(1), 135–144. Doi:10.1016/j.ijpe.2011.04.002

Hammer, M., & Champy, J. (1993). Reengineering the corporation: A manifesto for business revolution. Em *Business Horizons*. Doi:10.1016/S0007-6813(05)80064-3

Harrington, S. E., Niehaus, G., & Risko, K. J. (2002). Enterprise Risk Management: the case of United Grain Growers. *Journal of Applied Corporate Finance*, *14*(4), 71–81. Doi:10.1111/j.1745-6622.2002.tb00450.x

Heckmann, I., Comes, T., & Nickel, S. (2015). A critical review on supply chain risk – Definition, measure and modeling. *Omega*, *52*, 119–132. Doi:10.1016/j.omega.2014.10.004

Hillson, D. A. (1997). Towards a risk maturity model. *The International Journal of Project & Business Risk Management*, *1*(1), 35–45.

Hoyt, R. E., & Liebenberg, A. P. (2011). The Value of Enterprise Risk Management. *Journal of Risk and Insurance*, *78*(4), 795–822. Doi:10.1111/j.1539-6975.2011.01413.x

Hrebiniak, L. G., & Joyce, W. F. (2008). Implementing Strategy: An Appraisal and Agenda for Future Research. Em *The Blackwell Handbook of Strategic Management*. Doi:10.1111/b.9780631218616.2006.00023.x

Hsieh, H., & Shannon, S. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, *15*(9), 1277–1288. Doi:10.1177/1049732305276687

Humphrey, W. S. (1989). *Managing the Software Process*. Addison-Wesley.

IRM. Institute of Risk Management (2018). A Risk Practitioners Guide to ISO 31000 : 2018. *Institute of Risk Management*, 20. Disponível em: https://www.theirm.org/media/6907/irm-report-iso-31000-2018-v2.pdf

ISACA. Information Systems Audit and Control Association (2019). COBIT 2019 Framework: Introduction and Methodology. ISBN: 978-1604206449.

ISO. International Organization for Standardization. (2009). ISO/IEC 31010:2009 Risk management - Risk assessment techniques. *Risk Management*, *31010*, 92. Disponível em: https://www.iso.org/standard/72140.html

ISO. International Organization for Standardization (2009). *Risk Management - Principles and Guidelines*. Disponível em: https://www.iso.org/standard/43170.html

ISO. International Organization for Standardization (2018). *International Standard ISO 31000 Risk management — Guidelines*. Disponível em: https://www.iso.org/standard/65694.html

ISO/IEC 33001:2015 Information technology — Process assessment — Concepts and terminology, (2015). Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:33001:ed-1:v1:en

Jalali, S., & Wohlin, C. (2012). Systematic literature studies. *ESEM'12*, 29. Doi:10.1145/2372251.2372257

Jorion, P. (2000). Risk management lessons from Long-Term Capital Management. *European Financial Management*, *6*(3), 277–300. Doi:10.1111/1468-036X.00125

Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. Em *Harvard Business Review*. Doi:10.1080/14783360802264061

Kaplan, R. S., & Mikes, A. (2016). Risk Management-the Revealing Hand. *Journal of Applied Corporate Finance*, *28*(1), 8–18. Doi:10.1111/jacf.12155

Khan, M. J., Hussain, D., & Mehmood, W. (2016). Why do firms adopt enterprise risk management (ERM)? Empirical evidence from France. *Management Decision*, *54*(8), 1886–1907. Doi:10.1108/MD-09-2015-0400

Kloman, H. F. (1976). The risk management revolution. *Fortune, July*.

Kloman, H. F. (1992). Rethinking risk management. *Geneva Papers on Risk and Insurance. Issues and Practice*, 299–313.

Lakatos, E. M., & Marconi, M. de A. (2010). *Fundamentos de metodologia científica* (7º ed). Altas.

Liesch, PeterW., Welch, LawrenceS., & Buckley, Peter J. (2011). Risk and Uncertainty in Internationalisation and International Entrepreneurship Studies: Review and concept development. *Management International Review*, *51*(6), 851–873. Doi:10.1007/s11575-011-0107-y

MacGillivray, B. H., Sharp, J. v., Strutt, J. E., Hamilton, P. D., & Pollard, S. J. T. (2007a). Benchmarking Risk Management Within the International Water Utility Sector. Part I: Design

of a Capability Maturity Methodology. *Journal of Risk Research*, *10*(1), 85–104. Doi:10.1080/13669870601011183

MacGillivray, B. H., Sharp, J. v., Strutt, J. E., Hamilton, P. D., & Pollard, S. J. T. (2007b). Benchmarking Risk Management Within the International Water Utility Sector. Part II: A Survey of Eight Water Utilities. *Journal of Risk Research*, *10*(1), 105–123. Doi:10.1080/13669870601011191

Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management strategies. *International Journal of Physical Distribution & Logistics Management*, *38*(3), 192–223. Doi:10.1108/09600030810866986

March, J. G., & Shapira, Z. (1987). Managerial Perspectives on Risk and Risk Taking. *Management Science*, *33*(11), 1404–1418. Doi:10.1287/mnsc.33.11.1404

Mardessi, S. M., & Ben Arab, S. D. (2018). Determinants of ERM implementation: the case of Tunisian companies. *Journal of Financial Reporting and Accounting*, *16*(3), 443–463. Doi:10.1108/JFRA-05-2017-0044

Mazzon, J. A., & Berndt, A. P. P.-S. P. (1978). *Formulação de um modelo de avaliação e comparação de modelos de marketing* [Universidade de São Paulo]. https://repositorio.usp.br/item/000714783

McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does Enterprise Risk Management Increase Firm Value? *Journal of Accounting, Auditing & Finance*, *26*(4), 641–658. Doi:10.1177/0148558X11409160

Menard, C., & Shirley, Mary. M. (2005). The Handbook of New Institutional Economics. Springer. ISBN: 978-3540776604.

Michell, J. (1986). Measurement Scales and Statistics. A Clash of Paradigms. *Psychological Bulletin*, *100*(3), 398–407. Doi:10.1037/0033-2909.100.3.398

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). Qualitative Data Analysis: A Methods Sourcebook. Third Edition. Em *The SAGE Handbook of Applied Social Research Methods*.

Miller, K. D. (1992). A framework for integrated risk management in international business. *Journal of International Business Studies*, *23*(2), 311–331. http://www.jstor.org/stable/10.2307/154903

Miller, K. D., & Bromiley, P. (1990). Strategic Risk and Corporate Performance: An Analysis of Alternative Risk Measures. *The Academy of Management Journal*, *33*(4), 756. Doi:10.2307/256289

Moser, C. A., & Kalton, G. (2017). Survey Methods in Social Investigation. Em *Survey Methods in Social Investigation*. Doi:10.4324/9781315241999

Nocco, B. W., & Stulz, R. M. (2006). Enterprise Risk Management: Theory and Practice. *Journal of Applied Corporate Finance*, *18*(4), 8–20. Doi:10.1111/j.1745-6622.2006.00106.x

Nolan, R. L. (1979). Managing the crises in data processing. *Harvard Business Review*.

Ojasalo, J. (2009). A model of risk management in globalizing companies. *The Business Review*, *13*(1), 200–210.

Oliva, F. L. (2014). Knowledge management barriers, practices and maturity model. *Journal of Knowledge Management*, *18*(6), 1053–1074. Doi:10.1108/JKM-03-2014-0080

Oliva, F. L. (2016). A maturity model for enterprise risk management. *International Journal of Production Economics*, *173*, 66–79. Doi:10.1016/j.ijpe.2015.12.007

Oliva, F. L., Paza, A. C. T., Bution, J. L., Kotabe, M., Kelle, P., Vasconcellos, E. P. G. de, Grisi, C. C. de H. e, Almeida, M. I. R. de, & Fischmann, A. A. (2022). A model to analyze the knowledge management risks in open innovation: proposition and application with the case of GOL Airlines. *Journal of Knowledge Management*, *26*(3), 681–721. Doi:10.1108/JKM-11-2020-0809

Oliva, F. L., Semensato, B. I., Prioste, D. B., Winandy, E. J. L., Bution, J. L., Couto, M. H. G., Bottacin, M. A., Mac Lennan, M. L. F., Teberga, P. M. F., Santos, R. F., Singh, S. K., da Silva, S. F., & Massaini, S. A. (2018). Innovation in the main Brazilian business sectors: characteristics, types and comparison of innovation. *Journal of Knowledge Management*, *23*(1), 135–175. Doi:10.1108/JKM-03-2018-0159

Oliva, F. L., C. Sobral, M., Damasceno, F., Janny Teixeira, H., Cláudio de Hildebrand e Grisi, C., Américo Fischmann, A., & Aparecido dos Santos, S. (2014). Risks and strategies in a Brazilian innovation – flexfuel technology. *Journal of Manufacturing Technology Management*, *25*(6), 916–930. Doi:10.1108/JMTM-11-2012-0105

Oliva, F. L., Sobral, M. C., Santos, S. A. dos, Almeida, M. I. R. de, & Grisi, C. C. de H. e. (2011). Measuring the probability of innovation in technology-based companies. *Journal of Manufacturing Technology Management*, *22*(3), 365–383. Doi:10.1108/17410381111112729

Olson, D. L., & Swenseth, S. R. (2014). Trade-offs in Supply Chain System Risk Mitigation. *Systems Research and Behavioral Science*. Doi:10.1002/sres.2299

Paape, L., & Speklé, R. F. (2012). The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study. *European Accounting Review*, *21*(3), 533–564. Doi:10.1080/09638180.2012.661937

Pagach, D., & Warr, R. (2011). The Characteristics of Firms That Hire Chief Risk Officers. *Journal of Risk and Insurance*, *78*(1), 185–211. Doi:10.1111/j.1539-6975.2010.01378.x

Petticrew, M., & Roberts, H. (2008). Systematic Reviews in the Social Sciences. Em *Systematic Reviews in the Social Sciences*. Blackwell Publishing. Doi:10.1002/9780470754887

Razali, A. R., Yazid, A. S., & Tahir, I. M. (2011). The determinants of enterprise risk management (ERM) practices in Malaysian public listed companies. *Journal of Social and Development Sciences*, *1*(5), 202–207.

Richter, R. (2015). Essays on new institutional economics. Em *Essays on New Institutional Economics*. Doi:10.1007/978-3-319-14154-1

RIMS. The risk management society (2006). *RIMS Risk Maturity Model (RMM) for Enterprise Risk Management*. Disponível em: http://www.rims.org/RMM

RIMS. (2011). *An overview of widely used risk management standards and guidelines*. Executive Report on Widely Used Standards and Guidelines. Disponível em: https://www.rims.org/resources

RIMS, & Logic Manager. (2014). *ERM Program Audit Guide: RIMS Risk Maturity Model*. Disponível em: https://www.rims.org/resources

Röglinger, M., Pöppelbuß, J., & Becker, J. (2012). Maturity models in business process management. *Business Process Management Journal*, *18*(2), 328–346. Doi:10.1108/14637151211225225

Rohloff, M. (2011). Advances in business process management implementation based on a maturity assessment and best practice exchange. *Information Systems and E-Business Management*, *9*(3), 383–403. Doi:10.1007/s10257-010-0137-1

Rubino, M. (2018). A Comparison of the Main ERM Frameworks: How Limitations and Weaknesses can be Overcome Implementing IT Governance. *International Journal of Business and Management*, *13*(12), 203. Doi:10.5539/ijbm.v13n12p203

Schiller, F., & Prpich, G. (2013). Learning to organise risk management in organisations: what future for enterprise risk management? *Journal of Risk Research*, *17*(8), 999–1017. Doi:10.1080/13669877.2013.841725

Seuring, S., & Gold, S. (2012). Conducting content-analysis based literature reviews in supply chain management. *Supply Chain Management*, *17*(5), 544–555. Doi:10.1108/13598541211258609

Shad, M. K., Lai, F.-W., Fatt, C. L., Klemeš, J. J., & Bokhari, A. (2019). Integrating sustainability reporting into enterprise risk management and its relationship with business performance: A conceptual framework. *Journal of Cleaner Production*, *208*, 415–425. Doi:10.1016/j.jclepro.2018.10.120

Shah, S. K., & Corley, K. G. (2006). Building better theory by bridging the quantitative-qualitative divide. *Journal of Management Studies*, *43*(8), 1821–1835. Doi:10.1111/j.1467-6486.2006.00662.x

Şimşit, Z. T., Günay, N. S., & Vayvay, Ö. (2014). Theory of Constraints: A Literature Review. *Procedia - Social and Behavioral Sciences*, *150*, 930–936. Doi:10.1016/j.sbspro.2014.09.104

Sinkovics, N. (2018). Pattern Matching in Qualitative Analysis. Em *The SAGE Handbook of Qualitative Business and Management Research Methods: Methods and Challenges* (p. 468–484). SAGE Publications Ltd. Doi:10.4135/9781526430236.n28

Soltanizadeh, S., Abdul Rasid, S. Z., Mottaghi Golshan, N., & Wan Ismail, W. K. (2016). Business strategy, enterprise risk management and organizational performance. *Management Research Review*, *39*(9), 1016–1033. Doi:10.1108/MRR-05-2015-0107

Spector, P. E., Liu, C., & Sanchez, J. I. (2015). Methodological and Substantive Issues in Conducting Multinational and Cross-Cultural Research. *Annual Review of Organizational Psychology and Organizational Behavior*, *2*(1), 101–131. Doi:10.1146/annurev-orgpsych-032414-111310

Standard & Poor´s. (2007). *A Roadmap For Evaluating Financial Institutions ERM Practices*. *1*, 1–11. Disponível em: www.standardandpoors.com/ratingsdirect

Tahir, I. M., & Razali, a. R. (2011). The Relationship Between Enterprise Risk Management (ERM) and Firm Value: Evidence From Malaysian Public Listed Companies. *International Journal of Economics and Management Sciences*, *1*(2), 32–41.

Tarhan, A., Turetken, O., & Reijers, H. A. (2016). Business process maturity models: A systematic literature review. *Information and Software Technology*, *75*, 122–134. Doi:10.1016/j.infsof.2016.01.010

Teberga, P. M. F., Oliva, F. L., & Kotabe, M. (2018). Risk analysis in introduction of new technologies by start-ups in the Brazilian market. *Management Decision*, *56*(1), 64–86. Doi:10.1108/MD-04-2017-0337

The Economist. (2019). Vale and the aftermath of a devastating dam failure. *The Economist*, 61–62. Disponível em: https://www.economist.com/business/2019/03/09/vale-and-the-aftermath-of-a-devastating-dam-failure

Tight, M., Symonds, P., & Symonds, P. M. (2016). The Case Study as a Research Method. Em *Case Studies* (p. 15–15). SAGE Publications Ltd. Doi:10.4135/9781473915480.n2

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management*, *14*, 207–222. Doi:10.1111/1467-8551.00375

Van Looy, A. (2014). *Business Process Maturity*. Springer International Publishing. Doi:10.1007/978-3-319-04202-2

Viscelli, T. R., Beasley, M. S., & Hermanson, D. R. (2016). Research Insights About Risk Governance. *SAGE Open*, *6*(4), 215824401668023. Doi:10.1177/2158244016680230

vom Brocke, J., Schmiedel, T., Recker, J., Trkman, P., Mertens, W., & Viaene, S. (2014). Ten principles of good business process management. *Business Process Management Journal*, *20*(4), 530–548. Doi:10.1108/BPMJ-06-2013-0074

von Känel, J., Cope, E. W., Deleris, L. A., Nayak, N., & Torok, R. G. (2010). Three key enablers to successful enterprise risk management. *IBM Journal of Research and Development*, *54*(3), 231–245. Doi:10.1147/JRD.2010.2043973

Wacker, J. G. (1998). A definition of theory: research guidelines for different theory-building research methods in operations management. *Journal of Operations Management*, *16*(4), 361–385. Doi:10.1016/S0272-6963(98)00019-9

Wallin, J. A. (2005). Bibliometric Methods: Pitfalls and Possibilities. *Basic & Clinical Pharmacology & Toxicology*, *97*(5), 261–275. Doi:10.1111/j.1742-7843.2005.pto_139.x

Wan Daud, W. N., Haron, H., & Nasir Ibrahim, D. (2011). The Role of Quality Board of Directors in Enterprise Risk Management (ERM) Practices: Evidence from Binary Logistic Regression. *International Journal of Business and Management*, *6*(12), 205–211. Doi:10.5539/ijbm.v6n12p205

Weber, Y., & Tarba, S. Y. (2014). Strategic Agility: A State of the Art Introduction to the Special Section on Strategic Agility. *California Management Review*, *56*(3), 5–12. Doi:10.1525/cmr.2014.56.3.5

Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. *Information and Software Technology*, *54*(12), 1317–1339. Doi:10.1016/j.infsof.2012.07.007

Yaraghi, N., & Langhe, R. G. (2011). Critical success factors for risk management systems. *Journal of Risk Research*, *14*(5), 551–581. Doi:10.1080/13669877.2010.547253

Yeo, K. T., & Ren, Y. (2009). Risk management capability maturity model for complex product systems (CoPS) projects. *Systems Engineering*, *12*(4), 275–294. Doi:10.1002/sys.20123

Yin, R. K. (2013). Case Study Research: Design and Methods. Em *Sage Publications Inc.* (5th ed).

Zhao, X., Hwang, B.-G., & Low, S. P. (2013). Developing Fuzzy Enterprise Risk Management Maturity Model for Construction Firms. *Journal of Construction Engineering and Management*, *139*(9), 1179–1189. Doi:10.1061/(ASCE)CO.1943-7862.0000712

Zhao, X., & Singhaputtangkul, N. (2016). Effects of Firm Characteristics on Enterprise Risk Management: Case Study of Chinese Construction Firms Operating in Singapore. *Journal of Management in Engineering*, *32*(4), 05016008. Doi:10.1061/(ASCE)ME.1943-5479.0000434

Zou, P. X. W., Chen, Y., & Chan, T.-Y. (2010). Understanding and Improving Your Risk Management Capability: Assessment Model for Construction Organizations. *Journal of Construction Engineering and Management*, *136*(8), 854–863. Doi:10.1061/(ASCE)CO.1943-7862.0000175

Zupic, I., & Čater, T. (2015). Bibliometric Methods in Management and Organization. *Organizational Research Methods*, *18*(3), 429–472. Doi:10.1177/1094428114562629

7. ANEXOS

ANEXO I- Questionário pós aplicação do Modelo Operacional para Avaliação da Maturidade em Gestão de Riscos Corporativos (MAM-GRC)

Este Anexo I apresenta a íntegra do questionário aplicado na sexta etapa do caminho metodológico da pesquisa.

Seção 01 – Práticas de Gestão de Riscos

- Está claro o conceito de levantamento de práticas de gestão de riscos para determinar a maturidade na Gestão de Riscos Corporativos?
    - Sim.
    - Não.
- A partir dos textos explicativos do modelo sobre a forma de identificar uma prática de gestão de riscos, você consegue identificá-las na sua empresa?
    - Sim. (Próxima Seção 03)
    - Não. (Próxima Seção 02)

Seção 02 – Conte-me mais!

- Por que você sente dificuldades em identificar práticas de gestão de riscos em sua empresa a partir dos textos explicativos do modelo? (Próxima Seção 03)

Seção 03 – Práticas de Gestão de Riscos

- Os exemplos de práticas de gestão de riscos apresentados no modelo foram úteis para a identificação das práticas de gestão de riscos da sua empresa?
    - Sim. (Próxima Seção 05)
    - Não (Próxima Seção 04)

Seção 04 – Conte-me mais!

- Por que os exemplos de práticas apresentados no modelo não foram úteis para a identificação das práticas de gestão de riscos da sua empresa? (Próxima Seção 05)

Seção 05 – Práticas de Gestão de Riscos

- As práticas apresentadas como “melhores práticas” (as que já vieram listadas na planilha) foram úteis na aplicação do modelo em sua empresa?
    - Sim. (Próxima Seção 07)
    - Não. (Próxima Seção 06)

Seção 06 – Conte-me mais!

- Por que as “melhores práticas” apresentadas (as que já vieram listadas na planilha) não foram úteis para a aplicação do modelo na sua empresa? (Próxima Seção 07)

Seção 07 – Práticas de Gestão de Riscos

- Dentre as práticas apresentadas como “melhores práticas” (as que já vieram listadas na planilha) estão contempladas as práticas de gestão de riscos mais adequadas ao seu setor?
    - Concordo totalmente. As “melhores práticas” de gestão de riscos apresentadas (as que já vieram listadas na planilha) contém todas as que considero mais importantes em meu setor. (Próxima Seção 09)
    - Concordo parcialmente. Apenas algumas das que considero “melhores práticas” de gestão de riscos do meu setor estão entre as apresentadas como “melhores práticas” no modelo (as que já vieram listadas na planilha). (Próxima Seção 08)
    - Discordo. Nenhuma das que considero “melhores práticas” de gestão de riscos no meu setor estão entre as apresentadas como “melhores práticas” no modelo (as que já vieram listadas na planilha). (Próxima Seção 08)

Seção 08 – Conte-me suas sugestões!

- Quais práticas de gestão de riscos não contempladas entre as “melhores práticas” apresentadas no modelo você considera importantes em seu setor? Quais você incluiria na planilha? (Próxima Seção 09)

Seção 09 – Fatores

    - Sim.
    - Não.
- A partir dos textos explicativos sobre os 4 fatores (organização, tecnicidade, transparência e envolvimento), você consegue caracterizar as práticas identificadas na sua empresa?
    - Sim. (Próxima Seção 11)
    - Não. (Próxima Seção 10)

Seção 10 – Conte-me mais!

- Por que você sente dificuldades em caracterizar as práticas identificadas em sua empresa a partir dos textos explicativos sobre os 4 fatores (organização, tecnicidade, transparência e envolvimento)? (Próxima Seção 11)

Seção 11 – Fatores

- Todos os 4 fatores (organização, tecnicidade, transparência e envolvimento) apresentados no modelo se aplicam de alguma maneira ou em algum grau a sua empresa?
    - Sim. (Próxima Seção 13)
    - Não (Próxima Seção 12)

Seção 12 – Conte-me mais!

- Quais dos 4 fatores (organização, tecnicidade, transparência e envolvimento) do modelo não se aplicam a sua empresa? (Próxima Seção 13)

Seção 13 – Fatores

- Há outros fatores além dos apresentados no modelo (organização, tecnicidade, transparência e envolvimento) que você entende que se aplicariam ao seu setor?

- Sim. (Próxima Seção 15)
- Não. (Próxima Seção 14)

Seção 14 – Conte-me mais!

- Qual(is) fator(es) não apresentados no modelo você identificou que seriam aplicáveis ao seu setor? (Próxima Seção 15)

Seção 15 – Fatores

- Estão claras as ponderações apresentadas no modelo (notas com valores de 0 a 10 que devem ser preenchidos para cada fator na planilha)?
  - Concordo totalmente. Estão claras todas as notas de 0 a 10 que devem ser preenchidas para cada fator no modelo. (Próxima Seção 17)
  - Concordo parcialmente. Estão claras apenas algumas das notas de 0 a 10 que devem ser preenchidas para cada fator no modelo. (Próxima Seção 16)
  - Discordo. Nenhuma das notas que devem ser preenchidas para cada fator no modelo estão claras para mim. (Próxima Seção 16)

Seção 16 – Conte-me suas dúvidas!

- Quanto à caracterização dos fatores através das notas de 0 a 10 nas colunas da planilha, quais foram suas dúvidas? (Próxima Seção 17)

Seção 17 – Efetividade da prática de Gestão de Riscos

- Está claro o conceito de Efetividade (intensidade do resultado atingido pela prática de gestão de riscos) listada no modelo para determinar a maturidade em Gestão de Riscos Corporativos?
  - Sim.
  - Não.
- A partir dos textos explicativos sobre a Efetividade (intensidade do resultado atingido pela prática de gestão de riscos), você consegue determinar a efetividade das práticas identificadas na sua empresa?
  - Sim. (Próxima Seção 19)
  - Não. (Próxima Seção 18)

Seção 18 – Conte-me mais!

- Por que você sente dificuldades em determinar a Efetividade das práticas de gestão de riscos identificadas em sua empresa? (Próxima Seção 19)

Seção 19 – Efetividade da prática de Gestão de Riscos

- Você acredita que a identificação do nível de efetividade das práticas de gestão de riscos são aplicáveis de alguma maneira ou em algum grau a sua empresa?
  - Sim. (Próxima Seção 21)
  - Não (Próxima Seção 20)

Seção 20 – Conte-me mais!

- Por que você não acredita que a Efetividade das práticas de gestão de riscos (intensidade do resultado atingido pela prática de gestão de riscos) pode ser aplicável a sua empresa? (Próxima Seção 21)

Seção 21 – Efetividade da prática de Gestão de Riscos

- Você acredita que a identificação do nível de efetividade das práticas de gestão de riscos são aplicáveis de alguma maneira ou em algum grau a seu setor?
    - Sim. (Próxima Seção 23)
    - Não (Próxima Seção 22)

Seção 22 – Conte-me mais!

- Por que você não acredita que a Efetividade das práticas de gestão de riscos (intensidade do resultado atingido pela prática de gestão de riscos) pode ser aplicável em seu setor? (Próxima Seção 23)

Seção 23 – Efetividade da prática de Gestão de Riscos

- Estão claras as ponderações apresentadas no modelo para a determinação da Efetividade (notas com valores de 0 a 10 para a efetividade)?
    - Concordo totalmente. Estão claras as notas de 0 a 10 preenchidas para determinar a efetividade de todas as práticas de gestão de riscos listadas. (Próxima Seção 25)
    - Concordo parcialmente. Estão claras as notas de 0 a 10 preenchidas para determinar a efetividade de apenas algumas práticas de gestão de riscos. (Próxima Seção 24)
    - Discordo. Nenhuma das notas que devem ser preenchidas para determinar a efetividade de cada prática de gestão de riscos estão claras para mim. (Próxima Seção 24)

Seção 24 – Conte-me suas dúvidas!

- Quanto determinação da efetividade das práticas listadas, considerando efetividade como o grau de intensidade do resultado por ela atingido, quais foram as dúvidas encontradas? (Próxima Seção 25)

Seção 25 – Nível de Maturidade da Gestão de Riscos

- Está claro o conceito de Nível de Maturidade em Gestão de Riscos Corporativos?
    - Sim.
    - Não.
- A partir dos textos explicativos, você consegue determinar o Nível de Maturidade em Gestão de Riscos Corporativos na sua empresa?
    - Sim. (Próxima Seção 27)
    - Não. (Próxima Seção 26)

Seção 26 – Conte-me mais!

- Por que você sente dificuldades em determinar o Nível de Maturidade em Gestão de Riscos Corporativos em sua empresa? (Próxima Seção 27)

Seção 27 – Nível de Maturidade da Gestão de Riscos

- Você acredita que a determinação do Nível de Maturidade em Gestão de Riscos Corporativos é aplicável a sua empresa?
    - Sim. (Próxima Seção 29)
    - Não (Próxima Seção 28)

Seção 28 – Conte-me mais!

- Por que você não acredita que a determinação do Nível de Maturidade em Gestão de Riscos Corporativos pode ser aplicável a sua empresa? (Próxima Seção 29)

Seção 29 – Nível de Maturidade da Gestão de Riscos

- Você acredita que a determinação do Nível de Maturidade em Gestão de Riscos Corporativos através do modelo utilizado é aplicável a seu setor?
    - Sim. (Próxima Seção 31-fim)
    - Não (Próxima Seção 30)

Seção 30 – Conte-me mais!

- Por que você não acredita que a determinação do Nível de Maturidade em Gestão de Riscos Corporativos através do modelo utilizado pode ser aplicável a seu setor? (Próxima Seção 31-fim)

ANEXO II – Práticas de Gestão de Riscos Corporativos específicas das organizações estudadas

Este Anexo II apresenta as práticas de Gestão de Riscos Corporativos específicas das organizações estudadas e que foram conciliadas às práticas de Gestão de Riscos Corporativos genéricas ao longo do processo de contextualização.

Organização

- A organização possui um comitê de Gestão de Riscos Corporativos implantado e possui uma área dedicada à Gestão de Riscos, ligada diretamente à vice-diretoria de gestão.
- O Comitê de Gestão de Riscos Corporativos é formado por membros de diversas áreas, sendo um externo, conforme previsto no estatuto social.
- A equipe de risco conduz a matriz e lidera as análises, apresentando e validando com os vice-presidentes.
- Conceito de avaliação e gerenciamento de incertezas e riscos enfrentados pela organização por meio de um enfoque estruturado de controles que alinha estratégia, processos, pessoas, tecnologia e conhecimentos, objetivando a preservação e criação de valores aos stakeholders.
- A organização estabeleceu um plano específico para a gestão de riscos com horizonte de dois anos.
- Como uma das principais referências de estrutura integrada de Gestão de Riscos e Controles Internos, a organização busca seguir as diretrizes estabelecidas pelo COSO 2013 e COSO ERM II (Enterprise Risk Management).
- A política de gerenciamento de risco da organização foi estabelecida pela Diretoria e aprovada pelo Conselho de Administração. O Comitê de Gestão Financeira auxilia a Diretoria Financeira.
- Na política de gerenciamento de risco da organização, os riscos de mercado são protegidos quando não têm contrapartida nas operações da organização ou quando é considerado necessário suportar a estratégia corporativa.

Tecnicidade

- Existe um plano de ação para implementação de métricas de GRC.
- A Política de Gestão de Riscos Corporativos abrange a organização e suas controladas que, direta ou indiretamente, participam do processo de gestão de risco considerando o horizonte de curto e longo prazos.
- A gestão integrada de riscos é aplicada às vice-presidências e/ou a qualquer área da organização que deseje utilizar as ferramentas disponibilizadas pela área de riscos e

controles internos como suporte à condução de seus processos de forma a buscar redução da exposição aos riscos, internos ou externos, inerentes aos negócios da organização e que os mesmos sejam identificados, priorizados, avaliados e mitigados.

- A organização possui políticas específicas para tratar os riscos das operações financeiras e o desdobramento de eventos cujas consequências possam colocar em risco a continuidade das operações.
- Está prevista a avaliação qualitativa da eficácia dos controles internos existentes.
- Ferramentas de análise de riscos existem e são customizadas para diversas áreas, porém com consolidação de informações.
- Está prevista a realização de análise qualitativa de riscos com uso de avaliações de probabilidade e impacto e elaboração da matriz de riscos da organização.
- A auditoria interna é responsável por avaliar a suficiência e a eficácia dos controles operacionais e de gestão, verificar a adequação dos processos de identificação e o gerenciamento dos riscos e avaliar a eficácia dos controles relacionados à sua gestão, a gestão contábil e a geração de relatórios financeiros.

Transparência

- A organização executa uma prática de *mentoring* para se manter o conhecimento e, consequentemente, as transferências e difusão de práticas relacionadas à GRC
- A organização divulga anualmente e trimestralmente os resultados ao conselho e acionistas.
- Existe segregação de funções na gestão das contratações para mitigando os riscos relacionados a concentração de decisões e possíveis desvios dos desvios do padrão esperado.
- As áreas de riscos e de controles internos realiza o reporte de suas atividades, resultados e planos de ação para o Conselho de Administração, Conselho Fiscal e Comitê de Auditoria e Riscos.
- As equipes sabem de forma transparente quais são os riscos que impactam as suas atividades e sua área para atuar como *gatekeeper* e mitigá-los ou evitá-los.
- A organização tem uma cultura de responsabilização e de cuidado com os processos, que se estende à gestão de riscos.
- As áreas de riscos e de controles internos trabalham de forma colaborativa com a área de auditoria interna e compliance para alinhar os riscos, planos de ação e evitar sobreposições de atividades.

Envolvimento

- A organização faz a avaliação de todos os agentes, analisando fatores que definam graus de riscos nas relações para tomar decisões. Práticas relacionadas a essas decisões são as definições de processos internos, documentos ou cláusulas contratuais que deverão estar contidas em determinada relação com agentes para mitigar ou evitar riscos.

- A organização possui uma vice-diretoria dedicada à qualidade, com processos mapeados e POPs específicos para as atividades, de modo a mitigar os riscos de conformidade técnica.
- Níveis aceitáveis são definidos. Os riscos relacionados aos objetivos estratégicos da organização (i.e., estabelecimento do Contexto) são identificados e priorizados para assegurar que quaisquer materializações que venham a ocorrer sejam conhecidas previamente e geridas em um nível aceitável.
- A organização oferece treinamentos e capacitações em gestão de riscos.
- A organização provê treinamentos de processos, condutas, códigos de ética e compliance aos parceiros de negócios, fornecedores e outros agentes.
- Os contratos são acompanhados na sua execução para que não haja interrupções na prestação de serviços.
- Práticas relacionadas à Biossegurança são ostensivas (comunicação, acompanhamento dos resíduos da origem ao destino)
- Existem canais de comunicação abertos para que todos na organização possam ter acesso aos códigos de ética e compliance e possam opinar ou denunciar desvios do padrão esperado.
- A organização mapeia os riscos para os contratos.
- A organização impõe a obrigatoriedade de cláusulas contratuais de conformidade ética e fiscal para os contratados.