

**UNIVERSIDADE MUNICIPAL DE SÃO CAETANO DO SUL
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO**

Leonardo Santicioli

**MENSURAÇÃO DA MATURIDADE DA GESTÃO DE RISCOS EM COMPANHIAS
ABERTAS DOS SEGMENTOS FINANCEIRO E VAREJO**

**São Caetano do Sul
2023**

LEONARDO SANTICIOLI

**MENSURAÇÃO DA MATURIDADE DA GESTÃO DE RISCOS EM COMPANHIAS
ABERTAS DOS SEGMENTOS FINANCEIRO E VAREJO**

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Administração da Universidade Municipal de São Caetano do Sul como requisito para obtenção do título de Mestre em Administração.

Área de Concentração: Gestão e Regionalidade

Orientador: Prof. Dr. Sérgio Feliciano Crispim

**São Caetano do Sul
2023**

SANTICIOLI, Leonardo.

Mensuração da Maturidade da Gestão de Riscos em Companhias Abertas dos Segmentos Financeiro e Varejo / Leonardo Santicioli – São Caetano do Sul – USCS - 2023.

143 f.

Orientador: Prof. Dr. Sérgio Feliciano Crispim

Dissertação (Mestrado) – USCS, Universidade Municipal de São Caetano do Sul, Programa de Mestrado em Administração, 2023.

1. Riscos Corporativos 2. Modelos de maturidade de risco 3. Gestão de Riscos I. Crispim, Sérgio. II. Mensuração da Maturidade da Gestão de Risco em Companhias Abertas dos Segmentos Financeiro e Varejo.

Reitor da Universidade Municipal de São Caetano do Sul

Prof. Dr. Leandro Campi Prearo

Pró-Reitora de Pós-graduação e Pesquisa

Profa. Dra. Maria do Carmo Romeiro

Gestor do Programa de Pós-graduação em Administração

Prof. Dr. Eduardo de Camargo Oliva

Dissertação de Mestrado aprovada em 07/12/2023 pela Banca Examinadora constituída pelos professores:

Prof. Dr. Sérgio Feliciano Crispim

(Orientador – Universidade Municipal de São Caetano do Sul)

Prof. Dr. Silvio Augusto Minciotti

(Universidade Municipal de São Caetano do Sul)

Prof. Dr. José Roberto Ferreira Savoia

(Universidade de São Paulo)

Dedico este trabalho aos meus pais Leonilda e Humberto. Seu amor e entrega foram essenciais para que eu chegasse aqui. Dedico também à minha esposa Bruna, amor e parceira permanente desta caminhada e aos meus filhos Davi e Gabriel, encontro especial desta existência.

Agradeço imensamente a Deus – presença permanente nos meus dias; cuja misericórdia me possibilitou mais do que eu poderia e mais do que mereço.

Agradeço aos professores do Programa de Pós-Graduação em Administração da Universidade Municipal de São Caetano do Sul, por viabilizarem a realização desta pesquisa. Em particular, registro meu agradecimento ao Prof. Dr. Sérgio Feliciano Crispim, meu mestre há quase 20 anos e orientador deste trabalho, pela inspiração, dedicação e partilha. Carregarei seu exemplo.

A todos os meus familiares, em especial aos meus avós – Josefa, Aurora, Abel e Laurentino, exemplo de trabalho e força tão presente na minha formação. Também ao meu estimado tio Tarcísio, encorajador e entusiasta de que “conhecimento não ocupa espaço”.

À eterna professora Maria Helena de Moraes, que esteve comigo nos 4 primeiros anos da Educação Básica. Foi ela quem me presenteou os primeiros livros. Isso mudou a minha vida

Aos amigos da Deloitte, do Santander e da Via.

A todos os profissionais a quem consultei – sua disponibilidade e generosidade permitiram a realização deste trabalho.

“Consola-me saber que também o Senhor trabalha com instrumentos limitados.”

(Joseph Ratzinger, ao ser eleito Papa, falando de si próprio)

SANTICIOLI, Leonardo. **Mensuração da Maturidade da Gestão de Riscos em Companhias Abertas dos Segmentos Financeiro e Varejo**. Universidade Municipal de São Caetano do Sul; São Caetano do Sul, SP, 2023.

RESUMO

O cenário atual, caracterizado por profundas interconexões, tem como marca o elevado nível de incertezas, que podem agregar valor ou potencializar prejuízos. Riscos mal identificados e administrados podem impactar a situação financeira, operacional e até mesmo a continuidade das organizações. Assim, a gestão de risco tem sido prática cada vez mais relevante, visando reduzir os impactos indesejados. Este estudo objetiva avaliar o nível de maturidade dos modelos de Gerenciamento de Riscos Corporativos, com base em empresas abertas dos segmentos Financeiro e Varejo. A pesquisa, com metodologia qualitativa e quantitativa, foi realizada com base em revisão da literatura, entrevistas com especialistas e mediante a coleta de avaliação de profissionais dessas empresas, qualificados em gestão de riscos. O principal resultado extraído é que o setor financeiro tem um nível de maturidade superior no geral e em todas as dimensões avaliadas. Ambos os setores têm potencial para a melhoria principalmente nas dimensões de estratégia, utilização de dados e cultura de risco. O instrumento de pesquisa foi baseado no modelo do IBGC, mostrou-se bastante consistente e poderá ter sua aplicação expandida para outros setores com base em amostra. A pesquisa contribui para a reflexão e fomento de melhores práticas de gestão de risco.

Palavras-chave: Riscos Corporativos, Maturidade de Modelos de Risco, Gerenciamento de Riscos, Gestão Organizacional.

SANTICIOLI, Leonardo. **Mensuração da Maturidade da Gestão de Riscos em Companhias Abertas dos Segmentos Financeiro e Varejo**. Universidade Municipal de São Caetano do Sul, São Caetano do Sul, SP, 2023.

ABSTRACT

The current scenario, characterized by deep interconnections, has a high level of uncertainty, which can add value or increase losses. Poorly identified and managed risks can impact the financial, operational and even the continuity of organizations. Thus, risk management has become an increasingly relevant practice, aiming to reduce unwanted impacts. This study aims to evaluate the maturity level of Corporate Risk Management models, based on public companies in the Financial and Retail segments. The research, with qualitative and quantitative methodology, was carried out based on a literature review, interviews with experts and by collecting evaluations from professionals from these companies, qualified in risk management. The main result extracted is that the financial sector has a higher level of maturity overall and in all dimensions assessed. Both sectors have potential for improvement mainly in the dimensions of strategy, use of data and risk culture. The research instrument was based on the IBGC model, proved to be consistent and could be applied to other sectors based on a sample. The research contributes to the reflection and promotion of best risk management practices.

Key-words: Corporate Risks, Risk Model Maturity, Risk Management, Organizational Management

LISTAS DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANPAD	Associação Nacional de Pós-Graduação e Pesquisa em Administração
APFB	Administração Pública Federal Brasileira
B3	Brasil, Bolsa e Balcão ou Bolsa de Valores Brasileira
BIS	<i>Bank of International Settlements</i> ou Banco de Compensações Internacionais
CEO	<i>Chief Executive Officer</i> ou Diretor Geral Executivo
CFO	<i>Chief Finance Officer</i> ou Diretor Geral de Finanças
CMM	<i>Capability Maturity Model</i> ou Modelo de Maturidade em Capacidade
COSO	Committee of Sponsoring Organizations of the Treadway Commission ou Comitê das Organizações Patrocinadoras da Comissão Treadway
CRO	<i>Chief Risk Officer</i> ou Diretor Geral de Riscos
ERM	<i>Enterprise Risk Management</i> ou Gestão Integrada de Risco
FASB	Financial Accounting Standards Board ou Conselho de Normas de Contabilidade Financeira
FERMA	Federation of European Risk Management ou Federação Europeia de Gestão de Riscos
FSB	Financial Stability Board ou Comitê de Estabilidade Financeira
GNDI	Global Network of Director Institutes ou Instituto Global de Colaboração de Dirigentes de Governança
GRC	Gestão de Riscos Corporativos
IBGC	Instituto Brasileiro de Governança Corporativa
IGCLA	Instituto Gobierno Corporativo de Latino América ou Instituto de Governança Corporativa da América Latina
ISO	International Organization for Standardization ou Organização Internacional de Normatização
KPI	Key Performance Indicator ou Indicador Chave de Performance
KRI	Key Risk Indicator ou Indicador Chave de Risco
M_o_R	Management of Risk Methodology ou Metodologia de Gestão de Risco
NBR	Norma Técnica Brasileira

OGC	UK Office of Government Commerce ou Departamento de Comércio do Governo do Reino Unido
PDCA	Plan, Do, Check and Act ou Planejar, Executar, Checar e Atuar
RI	Relação com Investidores
RIMS	Risk and Insurance Management Society ou Sociedade de Gestão de Risco e Seguro
SGI	Sistema de Gestão Integrado
SOX	Lei Sarbanes-Oxley, norma americana sobre relatórios financeiros e controles
USP	Universidade de São Paulo
VaR	Value-at-Risk ou Valor em Risco

LISTA DE FIGURAS

Figura 1: Relacionamentos entre GRC, estrutura e processo	44
Figura 2: Relacionamentos entre as estruturas de GRC	49
Figura 3: PDCA na estrutura de GRC	50
Figura 4: Processo de Gestão de Riscos	54
Figura 5: Apetite ao Risco	59
Figura 6: Linhas de defesa da função de GRC	64
Figura 7: Exemplo de modelo de governança de gestão de riscos	64
Figura 8: Níveis de maturidade do CMM	70
Figura 9: Encadeamento do CMM	71
Figura 10: Riscos Corporativos no Ambiente de Negócios	76
Figura 11: Fatores de capacidade do Modelo Oliva	77
Figura 12: Escala de mensuração da maturidade do IBGC	86
Figura 13: Síntese dos procedimentos metodológicos	91
Figura 14: Frequência absoluta do total de respostas	117
Figura 15: Representação gráfica da avaliação por dimensão	119
Figura 16: Enquadramento no modelo do IBGC	121

LISTA DE QUADROS

Quadro 1: Resumo de artigo sobre estudo de caso de GRC	29
Quadro 2: Resumo de artigo sobre framework	29
Quadro 3: Resumo de artigo sobre GCR na Administração Pública	30
Quadro 4: Resumo de artigo sobre maturidade de GRC	30
Quadro 5: Resumo de artigo sobre maturidade de GRC – Croácia	30
Quadro 6: Resumo de artigo sobre maturidade GRC vs indicadores	31
Quadro 7: Resumo de artigo sobre estudo de caso GRC	31
Quadro 8: Resumo de artigo sobre cultura de risco	32
Quadro 9: Resumo de artigo sobre apetite de risco	32
Quadro 10: Resumo de artigo estudo de caso - setor de alumínio	32
Quadro 11: Resumo de artigo sobre a percepção do CROs	33
Quadro 12: Resumo de artigo sobre GRC setor de telecomunicações	33
Quadro 13: GRC segundo documentos de referência	41
Quadro 14: Matriz exemplificativa da Escala de Probabilidade	56
Quadro 15: Matriz exemplificativa da Escala de Impacto	57
Quadro 16: Matriz exemplificativa de Nível de Risco	58
Quadro 17: Agentes e suas principais funções em GRC	66
Quadro 18: Sumário do Modelo de Maturidade de Hillson	72
Quadro 19: Progressão entre os níveis – Modelo de Hillson	74
Quadro 20: Sumário dos Instrumentos do Modelo de Poltronieri	75
Quadro 21: Níveis de Maturidade do Instrumento de Avaliação dos SGI	75
Quadro 22: Estágios do Modelo de Oliva	78
Quadro 23: Modelo de maturidade de riscos da RIMS	79
Quadro 24: Níveis do modelo da RIMS	80
Quadro 25: Escala de maturidade M_o_R	82
Quadro 26: Reflexões para mensuração da maturidade	84
Quadro 27: Componentes dos Modelos de Mensuração de GRC	88
Quadro 28: Escalas dos Modelos de Mensuração de GRC	89
Quadro 29: Rating das empresas selecionadas	98
Quadro 30: Escala das agências de rating	99
Quadro 31: Principais aspectos mencionados nas entrevistas	108

Quadro 32: Amarração entre entrevista e questionário	109
Quadro 33: Amarração entre questionário e modelo do IBGC	110
Quadro 34: Aspectos contemplados no Instrumento de Coleta	111
Quadro 35: Ordenamento das dimensões do modelo do IBGC	120

LISTA DE TABELAS

Tabela 1: Empresas nacionais do Varejo listadas na B3	94
Tabela 2: Empresas nacionais financeiras listadas na B3	95
Tabela 3: Empresas do Varejo selecionadas para a pesquisa	96
Tabela 4: Empresas Financeiras selecionadas para a pesquisa	97
Tabela 5: Resumo das respostas obtidas na pesquisa	115
Tabela 6: Resumo sobre os respondentes da pesquisa	116
Tabela 7: Frequências absolutas do total das respostas	117
Tabela 8: Frequências relativa em cada dimensão	118
Tabela 9: Avaliação por cada dimensão do modelo do IBGC	119
Tabela 10: Sumário da Dimensão 1: Estratégia	121
Tabela 11: Sumário da Dimensão 2: Governança	122
Tabela 12: Sumário da Dimensão 3: Política	124
Tabela 13: Sumário da Dimensão 4: Processo de GRC	125
Tabela 14: Sumário da Dimensão 5: Linguagem e métodos de avaliação .	126
Tabela 15: Sumário da Dimensão 6: Sistemas, dados e modelos	128
Tabela 16: Sumário da Dimensão 7: Cultura, comunicação e treinamento	129

SUMÁRIO

1 INTRODUÇÃO	19
1.1 Problema de pesquisa	21
1.2 Objetivos da pesquisa	23
1.3 Delimitação do trabalho	23
1.4 Justificativa e relevância do trabalho	24
1.5 Organização do relatório do trabalho	25
1.6 Contribuições da pesquisa	27
2 FUNDAMENTAÇÃO TEÓRICA	28
2.1 Revisão da literatura	28
2.2 Riscos: aspectos gerais	34
2.2.1 Conceitos, categorização e fatos determinantes	34
2.3 Princípios, estruturas e processos de GRC	40
2.4 Governança e maturidade de GRC	62
2.5 Principais agentes do modelo de GRC	65
2.5.1 Avaliação da maturidade em GRC	67
2.5.1.1 Abordagem de Hillson	71
2.5.1.2 Abordagem de Poltronieri <i>et al.</i>	74
2.5.1.3 Abordagem de Oliva	76
2.5.1.4 Abordagem de RIMS	79
2.5.1.5 Abordagem de M_o_R	81
2.5.1.6 Abordagem do IBGC	83
3 PROCEDIMENTOS METODOLÓGICOS	90
3.1 Caracterização e tipo de pesquisa	90
3.2 População e tipo de amostra	92
3.2.1 Justificativa dos setores a serem pesquisados	92
3.2.2 Justificativa das empresas a serem pesquisados	93
3.3 Técnica de coleta de dados	100
4 ANÁLISE DOS DADOS	111

5 CONCLUSÃO	133
REFERÊNCIAS	136
Apêndice 1 – INSTRUMENTO DE COLETA	139

1 INTRODUÇÃO

Organizações de distintos setores econômicos e de diferentes portes deparam-se permanentemente com riscos – fatores internos e externos que geram incertezas ao cumprimento de suas metas estratégicas.

Com o objetivo de melhor compreender e considerar os eventos que podem ameaçar sua reputação, seus resultados, os interesses de seus acionistas e até mesmo a sua própria continuidade, a Gestão de Riscos Corporativos (GRC) ganhou força principalmente após a Lei Americana *Sarbanes-Oxley*, aprovada em 2002. Outras obrigações legais e regulatórias e, também, eventos adversos de grande relevância têm impulsionado a adoção de metodologias e um trabalho evolutivo das práticas de gerenciamento de risco.

Segundo Santos, Bution e Paza (2021), a Gestão de Risco Corporativos é um processo integrado e holístico para o controle e coordenação de diferentes riscos das organizações, tais como os operacionais, financeiros e estratégicos, além de suas correlações. A prática é considerada pelo Instituto Brasileiro de Governança Corporativa – IBGC (2017, p.14) “como um sistema intrínseco ao planejamento estratégico, composto por processos contínuos e estruturados, desenhados para identificar e responder a eventos que possam afetar os objetivos da organização”.

A Gestão de Riscos Corporativos é utilizada para identificar, dimensionar e responder aos diferentes riscos por meio de distintas formas de mitigação e deve gerar uma comunicação fluída que permita à Administração conhecer e monitorar as incertezas intrínsecas.

Segundo o IBGC (2017, p. 15), “a gestão eficaz de riscos é dada pela qualidade da estrutura de governança, das estratégias, da cultura, pela percepção dos riscos trazidos pela qualidade do ambiente de negócios, dos processos, dos controles e da tecnologia empregados”. Assim, a capacidade de reduzir a probabilidade de ocorrência e os impactos desses riscos e a tolerância em relação aos seus efeitos remanescentes devem ser decisões conscientes da Administração e da Governança. Neste sentido, Meirelles (2018) afirma que gerenciar riscos é uma prática associada à garantia da própria perenidade da empresa e que a adoção de uma metodologia permite a uniformidade das ações e um trabalho contínuo e evolutivo na área.

Com a mencionada maior difusão das práticas de GRC, houve uma expansão da literatura e da normatização sobre riscos corporativos, além da ampliação das exigências e acompanhamentos de órgãos de fiscalização dos setores econômicos regulados. Contudo, conforme Meirelles (2018), os estudos a respeito da eficácia do processo de gerenciamento de riscos das empresas brasileiras ainda são incipientes.

De acordo com Bramont (2013) ao estudar o *Capability Maturity Model* (CMM), cada nível é composto de diversos e exclusivos processos-chaves, e atingir gradativamente novos níveis é possível por meio da adoção de atividades interrelacionadas. Assim, ao buscar compreender qual é o seu estágio atual, as Companhias poderão ter indicações sobre o seu grau de maturidade e as principais lacunas para que alcance um patamar mais avançado.

Fraser, Moultrie e Gregory (2002), mencionam que o processo de avaliação da maturidade está atrelado à ideia de amadurecimento, na qual o processo é bem compreendido, documentado, aplicado consistentemente, além de monitorado e melhorado com regularidade. Desta forma, a avaliação da maturidade da gestão de riscos corporativos permite dimensionar o estágio em distintas dimensões, incluindo as contribuições já estabelecidas, aperfeiçoamentos necessários, além de dar indicações sobre o planejamento futuro, conforme indicado por Bramont (2013).

Dado o exposto, esta pesquisa bibliográfica revisará os principais modelos de avaliação de maturidade propostos pela literatura, como as abordagens de Hillson (1997), da *Risk and Insurance Management Society* (2015), de Poltronieri (2014), de Oliva (2016), M_o_R (2007) e a do IBGC (2017), como suporte para a avaliação da maturidade da Gestão de Riscos das empresas pesquisadas.

Para realização dessa avaliação, utilizaremos como referência de pesquisa as companhias abertas, cujas ações são negociadas na Bolsa de Valores Brasileira – B3 de dois segmentos econômicos bastante distintos em relação à sua dinâmica de negócio e regulação: o varejo e o segmento financeiro.

No contexto acadêmico, o estudo contribui para a ampliação da literatura de gestão de riscos corporativos, especialmente em relação à avaliação da maturidade das práticas de gestão existentes. No contexto empresarial, espera-se com essa pesquisa, além de destacar um tema de grande relevância para a Gestão das Organizações no cenário atual, oferecer *insights* para que as empresas possam

reavaliar suas práticas de gestão de risco, a fim de aprimorá-las e alinhá-las às melhores práticas disponíveis no mercado.

1.1 Problema de pesquisa

Certas empresas brasileiras possuem modelos e metodologias de avaliação e mitigação de seus riscos corporativos, mas há expectativa de que empresas com matrizes sediadas nos mercados americano e europeu, que já incorporaram há mais tempo as temáticas de GRC, ou que atuam em setores mais regulados, tenham uma gestão de riscos mais madura.

Contudo, não é possível afirmar que essa mesma prática seja amplamente difundida, aplicada de maneira massiva no mercado brasileiro, especialmente nas empresas de menor porte ou que não se enquadram nas características mencionadas no parágrafo anterior, conforme demonstra a revisão apresentada no capítulo 2.1 desta dissertação. De acordo com a revisão da literatura observou-se, também, que não há um número relevante de publicações e pesquisas que situe as organizações nos diferentes estágios de maturidade dessa prática.

Para auxiliar nessa mensuração, conforme informado acima, existem modelos de avaliação de maturidade propostos e expressos nas abordagens de Hillson (1997), da *Risk and Insurance Management Society* (2015), de Poltronieri (2014), de Oliva (2016), da M_o_R (2007) e a do IBGC (2017). Esses modelos consistem, em linhas gerais, em avaliar por meio de indicadores qual o *status* atual do processo em que uma empresa se encontra e quais são as lacunas para desenvolvimento de melhorias.

Fraser, Moultrie e Gregory (2002) afirmam que o processo de avaliação da maturidade está associado ao amadurecimento, transmitindo a noção da transição de um estágio inicial para outro mais avançado, podendo ser necessário passar por estágios intermédios até que se alcance a maturidade efetiva. Completa mencionando que a maturidade pressupõe que o processo seja bem compreendido, documentado, aplicado de maneira constante e consistente na Organização, além de ser regularmente monitorado e melhorado. Os comportamentos maduros são desenvolvidos ao longo do tempo.

A mesma temática é abordada por Oliva *et al.* (2021, p. 3), que apresentam ideias similares:

Para auxiliar as organizações a avaliarem seus estágios de capacidade e cumprirem processos de negócio, a literatura acadêmica e o ambiente corporativo desenvolveram modelos de maturidade aplicados à gestão, que consistem, em linhas gerais, em avaliar por meio de indicadores, qual o status atual do processo em que uma empresa se encontra e quais as lacunas, permitindo o desenvolvimento de um plano para avanço ou melhoria do processo (...) (OLIVA *et al.*, 2021, p. 3)

Discorrendo sobre o nível de maturidade desses modelos, o IBGC (2017, p. 33) menciona:

Existem distintas alternativas para a construção da governança da Gestão de Riscos Corporativos e para chegar ao nível de maturidade desejado. Cada organização deverá desenhar aquela mais adequada ao seu perfil de negócio, cultura organizacional, modelo de gestão e nível desejado de maturidade em relação às suas práticas. (IBGC, 2017, p. 33)

Em estudo divulgado ao mercado, realizado em 2017, o IBGC apresenta uma lista de aspectos que devem ser considerados na avaliação do estágio de um modelo de Gerenciamento de Riscos Corporativos:

- (...) - As ações adotadas para alcançar suas metas e objetivos em relação ao GRCorp e ao sistema de controles internos;
- O nível de esforço (tempo e investimento) empreendido para alcançar essas metas e objetivos;
- Os resultados obtidos, assim como a eficácia e a eficiência das práticas implementadas;
- O nível de envolvimento dos profissionais em relação a essas práticas;
- O nível de entendimento da maturidade da organização, assim como das oportunidades de melhorias. (IBGC, 2017, p. 33)

Oliva *et al.* (2021) menciona ser notável a dificuldade de gestores em encontrar modelos que possam ser diretamente aplicados à avaliação do nível de maturidade de GRC em suas organizações.

Observa-se, portanto, que é relevante ampliar as discussões sobre a temática.

Dado o exposto, propõe-se o seguinte problema de pesquisa: “Como avaliar os níveis de maturidade do gerenciamento de riscos em Companhias Abertas dos segmentos financeiro e varejo?”

A população de empresas potenciais para esta pesquisa baseia-se na relação de organizações listadas na Bolsa e Balcão – B3, no Brasil, disponíveis no momento da pesquisa. Para estudo, serão incluídas todas as empresas dispostas a contribuir com a pesquisa, respondentes a contato realizado de acordo com as especificações que serão detalhadas na seção sobre a metodologia, na qual também será detalhada e justificada a escolha dos setores

1.2 Objetivos da pesquisa

Com base no problema de pesquisa descrito na seção anterior, o objetivo geral do estudo é “analisar os níveis de maturidade da gestão de riscos corporativos das companhias abertas dos segmentos financeiro e de varejo que atuam no Brasil”.

Os objetivos específicos da pesquisa, por sua vez, são os indicados abaixo:

- 1) Identificar a maturidade da gestão de risco das companhias abertas dos segmentos financeiro e varejo em diferentes dimensões;
- 2) Comparar os estágios de maturidade da gestão de risco dentro e entre os segmentos econômicos pesquisados;
- 3) Identificar os principais fatores limitantes ao maior amadurecimento da gestão de risco nas empresas pesquisadas.

Sobre o segundo objetivo específico, a pesquisa a ser realizada comparará as similaridades e diferenciações quanto à maturidade das práticas de gestão de risco dentro e entre os participantes dos segmentos financeiro e de varejo.

Já, o terceiro objetivo, envolve identificar quais são os principais aspectos que caracterizam o patamar atual de maturidade das práticas de Gestão de Riscos Corporativos e fatores que dificultam a evolução desses modelos nas empresas pesquisadas, ou seja, quais são os aspectos que ainda não estão no patamar mais maduro.

1.3 Delimitação do trabalho

São delimitações deste trabalho:

- a) A opção por estudar as práticas de GRC de empresas com ações negociada na Bolsa de Valores Brasileira no momento desta pesquisa.
- b) A opção por estudar as práticas de GRC de empresas pertencentes a dois segmentos econômicos específicos, cuja justificativa apresentamos no curso da pesquisa.
- c) A seleção de empresas, dentro desse escopo, que permitam certo agrupamento e análise comparativa.

1.4 Justificativa e relevância do trabalho

Os potenciais efeitos adversos causados às empresas sem uma estrutura efetiva de GRC e a consequente redução dos efeitos indesejáveis por meio de modelos estruturados são os grandes motivadores para se estudar os riscos corporativos. Sobre esse assunto, Meirelles (2018, p.19) discorre:

As consequências negativas, sob o ponto de vista das perdas causadas às empresas, à sociedade e ao poder público, decorrentes da ausência de uma visão proativa e preventiva de riscos, e a possibilidade de modificar essa situação, por intermédio de um modelo estruturado, que senão elimine, pelo menos atenuar de forma substancial os efeitos adversos dos riscos, são os grandes fatores motivadores e justificadores para se estudar riscos. Os benefícios provenientes de uma abordagem metodologicamente estruturada através de um modelo de gerenciamento de risco corporativo é o maior agente motivador, justificador e incentivador para tal empreitada. (MEIRELLES, 2018, p. 19)

A Pesquisa de Maturidade do Processo de Gestão de Risco do Brasil, da KPMG (2020, p. 4) diz que “à medida que são exploradas novas abordagens e o cenário atual muda, as empresas que se ‘blindam’, ou seja, conhecem os riscos e os mantêm sob controle, podem ganhar vantagem competitiva”.

A GRC é um dos campos de estudo da Administração Contemporânea. Contudo, conforme Meirelles (2018), o desenvolvimento de pesquisas relacionados à Gestão de Riscos Corporativos e à avaliação de sua maturidade ainda são incipientes no Brasil.

Analisar os níveis de maturidade do gerenciamento de riscos corporativo oferecerá uma contribuição para o campo da gestão organizacional, à medida em que

possibilitará que empresas de distintos segmentos possam focar suas práticas atuais de Gestão de Risco, visando à avaliação e ao aprimoramento, contribuindo, em última instância, para a sua competitividade e crescimento.

A pesquisa revisará, ainda, os principais conceitos relacionados ao estudo da GRC, relacionará os principais modelos de avaliação dessas práticas trazidos pela literatura e pelo ambiente corporativo e apresentará, as realidades das entidades enfocadas no estudo, disponibilizando análises comparativas dos segmentos selecionados no âmbito brasileiro.

A escolha por focar empresas abertas – aquelas com ações negociadas na Bolsa de Valores e cujos requerimentos de governança e de divulgação são superiores aos das empresas de capital fechada –, mais expostas ao escrutínio público e com maior visibilidade perante investidores é relevante para as conclusões deste trabalho. Isso porque possibilitará conhecer a maturidade das práticas de Gestão de Risco naquelas que são, em tese, *benchmarks* em relação às empresas no geral, no que tange à sistemática de identificação, mensuração e mitigação dos principais riscos.

1.5 Organização do relatório do trabalho

O trabalho aqui apresentado está estruturado no seguinte sequencial:

1) Capítulos introdutórios: momento de apresentação do tema da pesquisa, detalhamento dos objetivos geral e específicos, justificativa para a realização da pesquisa e contribuições esperadas.

2 e 2.1) Revisão da literatura: capítulo em que apresentar-se-ão os resultados da revisão da literatura, capturando os principais aspectos mencionados por estudos recentes sobre o tema macro da pesquisa, de forma a permitir a construção de uma rede de pensamentos e conceitos que auxiliarão nos objetivos da pesquisa. Nessa seção, são explorados os principais artigos e autores que abordam os seguintes temas.

2.2) Aspectos gerais: serão apresentados o conceito de risco e outros relevantes no contexto da pesquisa como sua categorização, além de uma breve explanação sobre os marcos históricos do tema, ligados ao estudo e a casos do cenário empresarial.

2.3) Modelo conceitual e princípios: apresentação dos documentos de referência sobre a matéria – principais *frameworks* conhecidos e utilizados ao redor do mundo, sua conexão com a governança corporativa e os princípios da Governança de Riscos Corporativos.

- Estrutura de GRC: detalhamento associado ao estabelecimento de um processo de suporte e estrutura dedicada ao tema, abrangendo sua concepção e implementação quanto à estrutura, política e cultura.

- Processo de GRC: apresentação e detalhamento das principais fases do ciclo do Gerenciamento de Riscos Corporativos, incluindo o contexto, a identificação de riscos, mensuração de sua probabilidade e impacto e mitigações, além dos principais agentes envolvidos no processo e suas funções.

2.4) Governança e maturidade de GRC: apresentação dos conceitos de 1ª, 2ª e 3ª linha de defesa, bem como indicação dos principais agentes das Organizações classicamente envolvidos na atividade de gestão dos riscos corporativos, suas principais atribuições e a relação destas funções.

- Modelos de maturidade de GRC: abrangendo os princípios formais de um modelo de maturidade, os principais marcos históricos desse estudo e detalhamento dos modelos propostos e disponíveis na literatura voltados para as estruturas de gestão de riscos corporativos.

3) Metodologia: explicações detalhadas sobre a natureza e estrutura da pesquisa

- Justificativa em relação às delimitações do estudo: detalhamento das opções relativas aos setores econômicos e empresas selecionadas para a pesquisa, com informações do universo existente, critérios e amostra obtida, bem como dados relevantes caracterizadores das empresas selecionadas, tais como total de ativos, valor de seu patrimônio líquido e rating de crédito.

- Entrevista com especialistas: entrevista com cinco profissionais, membros da administração e governança de empresas de grande porte, reguladores e estudiosos da temática para franquear sua visão e como forma de auxiliar a elaboração do questionário que será aplicado na pesquisa de campo.

- Tratamento e análise dos dados obtidos na pesquisa de campo.

4) Análise dos resultados, com base nos dados coletados, realizando a avaliação de seu nível de maturidade de acordo com o modelo de maturidade do IBGC.

5) Conclusões

Apêndice: Cópia do questionário a ser aplicado.

1.6 Contribuições da pesquisa

A partir da síntese do que foi apresentado nas seções anteriores, vislumbramos contribuições relevantes da pesquisa de natureza econômica.

A revisão dos modelos de avaliação das práticas de Gestão de Risco e avaliação da maturidade de casos concretos dará indicações sobre o estágio atual e as principais lacunas existentes para que sejam aprimoradas. Com estágios mais robustos de sua GRC, as empresas tendem a estar mais preparadas para as incertezas e para os cenários distintos.

Desse modo, minimizam-se os efeitos adversos e passam a atuar com maior assertividade e tempestividade frente aos riscos inerentes às suas atividades, reduzindo potenciais perdas e protegendo valor. Em suma, práticas mais maduras tendem a oferecer maior estabilidade em um cenário de permanente instabilidade.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção, apresentar-se-ão os resultados da revisão da literatura, capturando os principais aspectos mencionados por estudos recentes sobre o tema macro da pesquisa, de forma a permitir a construção de uma rede de pensamentos e conceitos que auxiliarão nos objetivos da pesquisa. Nessa seção, são explorados os principais artigos e autores que abordam os seguintes temas. Além disso, serão abordados o conceito de risco e outros relevantes no contexto da pesquisa, o modelo conceitual e princípios, detalhamento sobre a implementação de GRC, o processo associado a estrutura - incluindo o contexto, a identificação de riscos, mensuração de sua probabilidade e impacto e mitigações, além dos principais agentes envolvidos no processo e suas funções. Sequencialmente, serão abrangidos os princípios formais de um modelo de maturidade e detalhamento dos modelos propostos e disponíveis na literatura voltados para as estruturas de gestão de riscos corporativos.

2.1 Revisão da literatura

No contexto de entendimento do tema, a etapa da revisão bibliográfica compreende a evolução das pesquisas e da literatura nos anos recentes, evidenciando os estudos dos principais autores citados.

Na fase de planejamento do portfólio bibliográfico, consultou-se bases de dados como CAPES, contendo a base Web of Science e Scielo. As bases possuem um acervo relevante e abrangente de publicações nacionais e estrangeiras, que permitem compreender e conhecer a produção científica disponível para a construção de uma rede de pensamento e conceitos na direção dos objetivos da pesquisa.

Nas plataformas de pesquisa consultadas, foram utilizados os seguintes filtros:

- Ano de publicação: desde 2017;
- Textos em qualquer idioma, incluindo publicações nacionais ou estrangeiras;
- Artigos.

Assim, com o intuito de extrair as publicações mais adequadas à pesquisa, buscamos a presença simultânea das seguintes expressões e sua tradução em inglês:

- 1) “Gerenciamento de Riscos Corporativos” e “Maturidade”
- 2) “Gestão de Riscos Corporativos” e “Maturidade”

Finalizada a etapa de planejamento e definidos os critérios e realizada a construção do portfólio bibliográfico, inicia-se a análise com os resultados encontrados nas duas bases, excetuando-se as duplicidades.

No quadro 1 e seguintes foram analisados os títulos e os resumos dos artigos. Eliminou-se aqueles que não abordavam diretamente o gerenciamento de riscos ou os modelos que poderiam ser aplicados na GRC e que não discorriam sobre as áreas de negócios, gestão, economia, finanças e contabilidade.

Nos quadros seguintes incluídos neste capítulo, destaca-se um resumo dos principais artigos identificados com base na pesquisa bibliográfica:

Quadro 1: Resumo de artigo sobre estudo de caso de GRC

Título	Gestão de riscos corporativos: estudo de caso do Itaú Unibanco S.A.
Publicação	Revista de Governança Corporativa
Resumo	O artigo objetiva ilustrar a aplicação de modelo teórico de Gestão de Riscos Corporativos para identificar riscos e avaliar a maturidade da GRC, considerando o ambiente da Entidade. Trata-se de estudo de caso da maturidade em GRC do Itaú Unibanco S.A. O modelo teórico utilizado foi o de Oliva (2016). Os dados foram coletados de documentos públicos do Banco e de organizações setoriais. A partir das práticas identificadas, constatou-se que o Itaú Unibanco está no maior nível de maturidade em GRC. Segundo os autores, o estudo contribui com a literatura de gestão ilustrando aplicação em caso relevante e real a um modelo anteriormente apresentado.

Fonte: Oliva *et al.* (2021); adaptado pelo autor.

Quadro 2: Resumo de artigo sobre *framework*

Título	<i>Framework</i> para Auditoria de Programas e Projetos em Tempo de Execução
Publicação	Revista Inovação, Projetos e Tecnologias
Resumo	O artigo demonstra a aplicabilidade de um <i>framework</i> de auditoria consultiva para a avaliação de programas e projetos em tempo de execução. O objetivo é mensurar o uso das boas práticas em gestão de projetos, de riscos corporativos, a geração de um plano de ação e aumento do nível da maturidade organizacional. Foi realizado um estudo de caso descritivo considerando-se trabalhos de auditoria consultiva realizada em empresa do segmento de varejo. O <i>framework</i> contribuiu para a identificação dos problemas, definições de ações corretivas e pode ser replicado em outras organizações no sentido de colaborar com o aumento do desempenho de projetos e programas.

Fonte: Araújo *et al.* (2019); adaptado pelo autor.

Quadro 3: Resumo de artigo sobre GCR na Administração Pública

Título	Práticas de Governança Pública Adotadas pela Administração Pública Federal Brasileira
Publicação	Administração Pública e Gestão Social
Resumo	O artigo tem como objetivo investigar as práticas de governança pública adotada pelos órgãos da Administração Pública Federal Brasileira (APFB). Para tanto, fez-se uso de uma abordagem quantitativa, do tipo descritiva, viabilizada por meio de aplicação de técnica estatística descritiva sobre o banco de dados resultante da aplicação de questionário, aplicado em 372 órgãos da APFB. Dentre os resultados, o artigo destacou a implementação de um Conselho de Administração em quase todos os órgãos. Contudo, pelas variáveis estudadas, que refletem a efetividade da administração desses conselhos, não houve um nível de maturidade que permita que o órgão realize a gestão de riscos. Portanto, o artigo conclui que os órgãos públicos da APFB estão dando os primeiros passos na adoção de melhores práticas de governança corporativa, mas ainda tem muito a avançar.

Fonte: Oliveira e Vieira (2019); adaptado pelo autor.

Quadro 4: Resumo de artigo sobre maturidade de GRC

Título	<i>Moderating influences on the ERM maturity-performance relationship</i>
Publicação	<i>Research in international business and finance</i>
Resumo	O estudo examina a performance da gestão de riscos corporativos e as implicações dos níveis de maturidade nos resultados das Companhias. O estudo indica que a elevação da maturidade tende a resultar em aumento do retorno sobre os ativos, mediante a redução das volatilidades e ocasionar a queda do risco da empresa na perspectiva dos credores, que passam a exigir uma taxa menor e, também, na perspectiva dos investidores, que têm maior propensão a manter seus investimentos. Como consequência desse incremento da maturidade, o estudo atribuiu a elevação da vantagem competitiva e o valor da Organização.

Fonte: Farrell e Gallagher (2018); adaptado pelo autor.

Quadro 5: Resumo de artigo sobre maturidade de GRC - Croácia

Título	<i>Managers' Support – A Key Driver behind Enterprise Risk Management Maturity</i>
Publicação	Zagreb International Review of Economics & Business
Resumo	As severas consequências das crises econômicas resultaram em uma revisão das abordagens e processos de gerenciamento de riscos das empresas, além da necessidade de uma maior compreensão das premissas dos <i>frameworks</i> de GRC. O estudo aponta que, com isso, houve um aumento das empresas que saíram de modelos de gestão de risco departamental para um modelo mais holístico. O estudo propôs um índice de avaliação da maturidade e realizou aplicação em distintas Companhias abertas da Croácia, concluindo, pelo baixo nível de desenvolvimento de seu sistema de gestão de riscos corporativos: 38%

	das empresas pesquisadas não tinham elementos verificáveis de GRC, das quais 22% não gerenciam nenhum risco corporativo.
--	--

Fonte: Pecina *et al.* (2017); adaptado pelo autor.

Quadro 6: Resumo de artigo maturidade GRC vs indicadores

Título	<i>Enterprise Risk Management Implementation Maturity in Non Bank and Financial Companies</i>
Publicação	Etikonomi (Jakarta, Indonésia)
Resumo	O estudo comenta sobre o baixo volume de estudos que associam a maturidade do risco corporativo nas Companhias com variáveis reais. Nesse sentido, visou à determinação do nível de maturidade de empresas não financeiras listadas na Bolsa de Valores da Indonésia em 2015 e a influência de aspectos como total de ativos, total de funcionários e nível de alavancagem por meio de análises qualitativas e de regressão múltipla. O estudo concluiu que a maioria dessas empresas apresenta baixa maturidade de sua estrutura de GRC e que, dentre as variáveis estudadas, apenas o total de ativos tem influência relevante na maturidade.

Fonte: Tjahjono (2017); adaptado pelo autor.

Quadro 7: Resumo de artigo sobre estudo de caso GRC

Título	<i>Enterprise Risk Management Maturity: A Clinical Study of a U.S. Multinational Nonprofit Firm</i>
Publicação	<i>Journal of accounting, auditing & finance</i>
Resumo	O artigo é baseado em eventos reais, realizando uma análise do processo de implementação e pós-implementação de um sistema de gerenciamento de riscos corporativos de uma empresa multinacional sem fins lucrativas sediada nos Estados Unidos no período de 2015 a 2020, com base no modelo de maturidade da RIMS. A pesquisa revelou que o sistema é classificado como “ad-hoc” e que a gestão de risco é aplicada de forma não consistente; além disso, indicou melhoria na pós implementação em aspectos como governança do Conselho, busca por <i>hedges</i> naturais e por mitigações aos impactos trazidos pelos principais riscos.

Fonte: Jalilvand e Moorthy (2022); adaptado pelo autor.

Conforme vê-se, não existe um número elevado de artigos que apresentam temáticas mais próximas daquelas pretendidas a se abordar neste trabalho, abrangendo simultaneamente a gestão de riscos corporativos e a avaliação de sua maturidade. Por essa razão, optamos por uma extensão da avaliação inicial. Além da pesquisa específica e direta, fizemos uma busca mais geral e ampla, para que fossem selecionados outros artigos com temáticas que pudessem estar indiretamente

vinculadas ao tema deste trabalho, tais como riscos corporativos em geral, apetite a riscos ou cultura corporativa de risco. Com base nessa pesquisa, que permitiu contato com um número maior de artigos, elaboramos as seguintes seleção e revisão de artigos:

Quadro 8: Resumo de artigo sobre cultura de risco

Título	<i>Maturity of risk management culture, entrepreneurship and sustainability issues</i>
Publicação	<i>Enterpreneurship and Sustainability Issues</i>
Resumo	O artigo aponta aspectos relevantes para construção das estruturas de risco nas empresas: (a) cultura de risco, (b) envolvimento dos funcionários e (c) sistema de risco bem desenvolvido. Menciona que não existem publicações em massa sobre o tema e há ênfase em estudos voltados para a comunicação. Aborda a cultura como elemento essencial da gestão de risco e visa encorajar a empresa a tomar risco dentro de certos parâmetros, elevando a probabilidade do atingimento dos objetivos estratégicos. O artigo selecionou várias definições sobre cultura de risco em <i>frameworks</i> e realizou avaliação da maturidade dessa cultura com base em pesquisa de empresas públicas da Polônia.

Fonte: Domanska-Szaruga (2020); adaptado pelo autor.

Quadro 9: Resumo de artigo sobre apetite de risco

Título	Uma estrutura de apetite de risco para suporte à Governança Corporativa
Publicação	IX Encontro de Estudos em Estratégia – ANPAD
Resumo	O artigo aborda o tema de apetite de risco aplicável às instituições financeiras no Brasil. Apresenta indicações que mostram que a adoção de apetite de risco melhora a gestão de risco corporativo. Cita recomendação do <i>Financial Stability Board</i> - FSB para que os bancos alinhem o apetite de risco à sua estratégia e gestão de capital. Em 2011, uma pesquisa mostrava que aproximadamente 60% das empresas não consideravam o apetite de risco como maduro. O artigo apresenta pesquisa com os bancos por meio de <i>survey</i> e mostra as dificuldades na utilização do apetite, destacando-se a fragilidades na integração deste ao processo decisório.

Fonte: Vilela e Neto (2020); adaptado pelo autor.

Quadro 10: Resumo de artigo estudo de caso - setor de alumínio

Título	Transformação do processo de gestão de risco em uma empresa brasileira de alumínio
Publicação	IX Encontro de Estudos em Estratégia – ANPAD

Resumo	O artigo é um estudo de caso e foca na ausência de padrões e aplicação sistêmica no processo de gerenciamento de risco de uma empresa brasileira de alumínio que implementou a área de gestão de riscos. O artigo identificou quatro oportunidades para aprimoramento da gestão dos riscos corporativos da empresa: (a) estabelecer uma cultura focada em gestão de riscos; (b) inserir a gestão de riscos no processo de planejamento estratégico, (c) considerar o impacto dos riscos nas decisões estratégicas e (d) reestruturar a gestão de riscos de modo que ela permita a antecipação dos movimentos do mercado.
--------	--

Fonte: Colantonio, Caldeira e Oliva (2020); adaptado pelo autor.

Quadro 11: Resumo de artigo sobre a percepção do CROs

Título	Gestión de riesgos corporativos: percepción de los Chief risk officers.
Publicação	Revista <i>Facultad de Ciencias Económicas</i>
Resumo	O artigo apresenta uma pesquisa direcionada aos responsáveis pelo Risco Corporativo nas entidades (<i>Chief Risk Officers - CRO</i>), auditores e consultores de risco, incluindo avaliação geral, técnicas e outros. As respostas indicam que se considera relevante a estratégia de aprendizagem para desenvolver competências e habilidades associadas à gestão de risco. O artigo faz menção ainda a mais de 80 <i>frameworks</i> de risco e sintetiza aquilo que é mais comumente mencionado entre eles – o processo de identificação, priorização e quantificação dos riscos. Ainda faz citação sobre a atualização do COSO em 2017, enfatizando a incorporação da estratégia e desempenho corporativos associados aos riscos.

Fonte: Marques, Muller e Silva (2020); adaptado pelo autor.

Quadro 12: Resumo de artigo sobre GRC do setor de telecomunicações

Título	Avaliação de modelo de gerenciamento de riscos corporativos segundo recomendações do IBGC: caso Brasil Telecom
Publicação	Revista Eletrônica de Ciência Administrativa
Resumo	O artigo é um estudo de caso que visa avaliar a aderência da gestão de risco de uma empresa do setor de telefonia com os padrões então vigentes, definidos pelo IBGC, com base em informações públicas dessa empresa e da aplicação de questionários a seus profissionais. Nos capítulos introdutórios, o artigo apresenta descritivos gerais sobre riscos, tipos de riscos e gerenciamento e detalha a orientação de referência emitida pelo IBGC. Os resultados deram uma visão geral sobre a empresa e sobre cada grupo da orientação do IBGC, classificando-os em "atende" ou "atende em partes".

Fonte: Nascimento e Alves (2007); adaptado pelo autor.

A leitura dos artigos contribui para auxiliar na construção de uma rede de pensamentos e conceitos relacionados ao assunto. Da leitura dos textos, destaca-se os seguintes aspectos:

- A maioria dos artigos que apresentam pesquisas aplicadas se referem a estudos de casos. Não identificamos estudos comparativos entre segmentos ou empresas.
- As pesquisas realizadas capturam a implementação de estruturas que indicam priorização das temáticas de GRC recentemente. Contudo, há sinais de que ainda não estão consolidados e existem oportunidades para avançar relacionados especialmente à (i) inclusão dos temas de risco na cultura organizacional, (ii) vínculo com o planejamento e decisões estratégicas e (iii) antecipação de movimentos de mercado.
- A elevação da maturidade da GRC tende a reduzir as volatilidades e reduzir o risco de crédito da empresa na perspectiva dos credores, o que pode contribuir diretamente para ampliar o acesso a linhas de crédito e, por consequência, com sua performance/lucro.

2.2 Riscos: Aspectos Gerais

Nesta seção, apresentar-se-ão o conceito de risco e as suas principais categorizações, além de fatos e marcos, inclusive regulamentares.

2.2.1 Conceitos, categorização e fatos determinantes

O ambiente de negócios é permanentemente marcado pelos desafios decorrentes das mudanças estabelecidas pela competitividade. Disso resulta que as organizações patrocinem um amplo conjunto de conhecimentos, além de capacidade interna e tomada de decisões eficazes e tempestivas. Os modelos de gestão devem ser conduzidos observando as melhores práticas e ao mesmo tempo as realidades internas. Os riscos são parte dessa dinâmica e a tomada de decisão é ocasionada por condições de riscos e incertezas, o que amplifica sua complexidade.

Segundo IBGC (2017, p. 11), a palavra “risco” é proveniente do latim “risicum” ou “riscum”, cuja definição envolve o conceito de ousar. Continua o mesmo estudo ao discorrer sobre os aspectos gerais e conceituais de risco, afirmando que:

Costuma-se entender risco como possibilidade de algo não dar certo. Mas seu conceito atual no mundo corporativo vai além: envolve a quantificação e a qualificação da incerteza, tanto no que diz respeito às perdas quanto aos ganhos por indivíduos ou organizações. Sendo o risco inerente a qualquer atividade – e impossível de eliminar –, a sua administração é um elemento-chave para a sobrevivência das companhias e demais entidades. (IBGC, 2017, p. 11)

Segundo o Código das Melhores Práticas de Governança Corporativa do IBGC (2015), os riscos a que a Organização está sujeita devem ser gerenciados para subsidiar a tomada de decisão.

Cada Organização, influenciada pela sua história, cultura, pelo setor econômico onde atua e pelo seu entorno tem riscos distintos e em graus diferentes de relevância. Portanto, a identificação do contexto, incluindo os objetivos daquela Organização, o ambiente em que ela atua e quem são seus *stakeholders* é fundamental no processo de gerenciamento dos riscos, que abordaremos adiante. De forma equivalente, vê-se que esta é a linha de atuação dos estudos e *frameworks* do tema de riscos, tais como o mencionado acima emitido pelo IBGC e, também, da norma ABNT ISO 31.000 – Gestão de Riscos: Princípios e Diretrizes.

Percorrendo brevemente o histórico do tema, vemos que ele existe há muito tempo no ambiente empresarial. Como comentamos na introdução deste trabalho, o tema ganhou espaço e relevância no século XX, dado o aumento da complexidade das Organizações, além da amplificação da interligação dos mercados por meio da globalização.

Segundo o IBGC (2017), o início da vasta literatura começou na área de seguros e, mais recentemente, tem se desenvolvido com metodologias estruturadas em várias vertentes, entre as quais, finanças, auditoria, estratégia e tecnologia da informação.

Na década de 1980, houve um incentivo relevante dos reguladores da indústria financeira britânicos e americanos – *Bank of England* e *Federal Reserve*, respectivamente, para implementação de estruturas focadas no risco, graças às

preocupações com operações não registradas no balanço e com empréstimos para países dos então denominados “países do terceiro mundo”.

Nessa mesma linha, o *Bank of International Settlements* (BIS) emitiu em 1988 o Acordo de Basileia (Basileia I), com foco na alocação de capital para fazer frente ao risco de crédito das instituições bancárias.

A partir da década de 1990, em resposta aos desafios financeiros, começaram a existir regras para o risco de mercado, tais como a introdução do conceito de VaR – *Value-at-Risk*, que mede a perda potencial máxima do valor de uma carteira com determinado nível de confiança em um intervalo de tempo.

Em junho de 1999, o BIS propôs uma nova estrutura para a adequação do capital das instituições bancárias, denominado Basileia II, substituindo a publicação anterior. O BIS indicou uma estruturada baseada em três pilares: (a) adequação do capital regulatório mínimo com base no risco de mercado, de crédito e operacional; (b) capacidade dos reguladores bancários em avaliar e adaptar o capital a cada instituição regulada e (c) transparência e divulgação de informações como fomento à disciplina de mercado.

Ainda, com a crise financeira de 2007 e 2008, grandes deficiências regulatórias no sistema financeiro global foram identificadas e o BIS efetuou um novo aprimoramento – Basileia III, visando à promoção de um aumento do capital como proteção a eventuais crises e corridas dos bancos.

Seguindo a atuação precursora do regulador bancário, a Comissão Europeia de Supervisão dos Seguros e Previdência elaborou em 2007 as diretrizes para Solvência II, que é, em suma, um regime para as seguradoras melhorarem suas práticas de controle e gestão de riscos envolvendo práticas de governança, com destaque também ao tema de suficiência de capital.

O *Financial Accounting Standards Board* (FASB) publicou guias encorajando a divulgação do que tem sido feito pelas Companhias na mitigação e gerenciamento de riscos. Outros reguladores ao redor do mundo tiveram práticas similares relativas ao gerenciamento de riscos e controles internos.

Além desses primeiros movimentos impulsionados por reguladores, o IBGC (2017, p. 18) menciona os passos seguintes e a disseminação ocorrida:

Paralelamente ao desenvolvimento pelo ramo financeiro, auditores, contadores e legisladores têm devotado atenção crescente aos controles internos. Nas companhias não financeiras, as diretrizes mais utilizadas a respeito de gestão de riscos têm origem nas recomendações do *Committee of Sponsoring Organizations of the Treadway Commission* (COSO). Este Comitê emitiu recomendações e estabeleceu uma metodologia integrada para ajudar as organizações a analisar e a melhorar seus sistemas de controles internos e seus processos de gestão do risco empresarial (ERM – *Enterprise Risk Management*). Essa metodologia, altamente difundida desde então, tem sido incorporada às políticas, regras e regulamentos por várias empresas para melhor controlar suas atividades, de forma a atingir os objetivos estabelecidos. (IBGC, 2017, p. 18)

A década de 2000 foi iniciada como uma série de escândalos corporativos de grande relevância, que demandaram a ampliação da regulação.

- Enron: em 2001, esse caso de fraude e manipulação financeira resultou na falência da empresa de energia, que era a sétima capitalização dos Estados Unidos na época e na falência de seu auditor independente – a Arthur Andersen. Foi a maior falência da história na época, gerando um número sem precedente de inquéritos oficiais, ações judiciais e reações em todo o mundo.

- World.Com: em 2002, descobriu-se que a empresa de telecomunicações havia inflado seus ativos em quase US\$ 11 bilhões, tornando-se, de longe, um dos maiores escândalos de responsabilidade. A empresa tinha reduzido os custos, mantendo-os indevidamente no ativo, ao invés de incorporá-las às suas despesas. O CEO da empresa foi condenado a 25 anos e resultou em 30 mil cortes e mais de US\$ 180 bilhões de perdas por investidores.

- Adelphia: segundo reportagem de 2010 da revista Exame, a família Rigas, fundadora da Adelphia, foi acusada de retirar US\$ 3,1 bilhões como empréstimo da empresa, sem relatar no balanço. Além disso, o grupo superestimou resultados, inflando gastos com investimentos para esconder dívidas. As falcatruas foram descobertas em abril de 2002.

Com isso, em 2002, foi aprovada nos Estados Unidos a Lei Sarbanes-Oxley (SOX), que destacou o papel dos controles internos e transformou as boas práticas de governança em exigência legal. A SOX foi produto de um entendimento entre os dois grandes partidos – Republicanos e Democratas – e alcançou, além das empresas

americanas, todas aquelas estrangeiras com acesso ao mercado de capitais americano (notadamente com ações na Bolsa de Valores de Nova York) e suas subsidiárias, muitas delas brasileiras e estrangeiras com atuação no Brasil.

A Lei passou a exigir que os principais executivos das empresas abertas certificassem de maneira pública e explícita que as demonstrações financeiras têm informações acuradas e livres de fraude, modificou regras de auditoria externa e estabeleceu punições mais rígidas, inclusive criminais. Além dos efeitos diretos, a SOX influenciou a criação de outras regulamentações similares ao redor do mundo, colocando muito foco nas temáticas de riscos e controles.

Após a crise de 2007 e 2008, foi aprovada nos Estados Unidos a Lei Dodd-Frank, que estabeleceu melhores normas e padrões de funcionamento para o mercado financeiro americano, abrangendo temáticas como: (a) regulamentação dos derivativos, ampliando a transparência sobre o tema, (b) limitação das ajudas emergenciais do Governo Federal Americano e (c) robustecimento de reguladores.

O Brasil também avançou na temática. Em 2013, publicou a sua Lei Anticorrupção, que entrou em vigor no ano seguinte. Esta Lei ofereceu uma contribuição indireta à temática de gestão de risco, uma vez que tipicamente a GRC abrange as não conformidades legais. Outros decretos e portarias foram posteriormente emitidos, contribuindo avançar na maturidade do tema. Acerca dos avanços no país, o IBGC (2017, p. 19), comenta:

Especificamente sobre o programa de integridade (compliance), o decreto estabeleceu os mecanismos e procedimentos de integridade, auditoria, aplicação de códigos de ética ou conduta e incentivos de denúncia de irregularidades que devem ser adotados pela empresa e monitorados pelo Ministério da Transparência, Fiscalização e Controle, antiga Controladoria Geral da União. O programa de integridade deve ser estruturado, aplicado e atualizado de acordo com as características de riscos atuais das atividades de cada pessoa jurídica, que, por sua vez, é responsável pelo constante aprimoramento e adaptação do programa. (IBGC, 2017, p. 19)

Estes são alguns dos marcos relevantes relativos ao Gerenciamento de Risco. Outros eventos ocorreram desde o ano 2000, tais como a revisão do COSO e alinhamento com as estratégias e performances da Companhia e aprovação de outros normativos impactantes como o *UK Bribery Act*, no Reino Unido.

Os riscos podem ser internos e externos. No primeiro caso, são restritos à Organização. No segundo, estão associados ao entorno da Organização, produzindo efeitos sobre sua condução, uma vez que dizem respeito ao ambiente no qual ela está inserida. As atuações são mais proativas no caso dos riscos internos, uma vez que conforme Oliva (2021), no caso dos riscos decorrentes de eventos externos, as estratégias a serem adotadas pelas Organizações são mais limitadas, como por exemplo a diversificação de portfólio decorrente de flutuações de indicadores econômicos.

Além disso, os riscos podem ser classificados quanto à sua natureza. Essa categorização ou agrupamento auxilia a tratá-los com ações estruturadas, mais eficientes e mais abrangentes. O IBGC (2017) menciona que alguns riscos podem pertencer a uma ou mais categorias. Existem variações em relação às combinações que descrevemos nos *bullets* abaixo, sem prejuízo das concepções gerais que a classificação agrupa, sendo elas:

- Riscos Estratégicos: relacionados às diretrizes estratégicas com impacto direto à tomada de decisão dos gestores. Abrange aspectos como: (a) cenário político nacional e internacional, (b) panorama econômico nacional e internacional, (c) mudanças tecnológicas e (d) transformações em leis, normas e regulamentações.

- Riscos Operacionais: relacionados à execução e aos aspectos internos e processuais. Abrange aspectos como: (a) fraudes, (b) falhas nos sistemas e (c) falhas humanas.

- Riscos de *Compliance*: relacionados ao cumprimento de legislações, normas e regras aplicadas ao negócio e as de natureza geral, como leis trabalhistas, de saúde, entre outras. Abrange aspectos como: (a) corrupção para vantagem ilícita, (b) fraudes e (c) práticas ilegais.

- Riscos Financeiros: relacionados àquilo que prejudica o fluxo de caixa da Organização, seu capital de giro e/ou seu patrimônio. Abrange aspectos como: (a) endividamento, (b) liquidez e (c) inadimplência.

- Riscos Reputacionais: relacionados à opinião pública sobre ações, produtos, serviços e práticas. Abrange aspectos como: (a) posicionamentos da Organização e (b) ética e integridade da Companhia e de seus representantes.

- Riscos de Tecnologia: relacionados à adequação e à suficiência dos recursos computacionais, sua sustentação e aprimoramento. Abrange aspectos como: (a) identificação e tratamento de incidentes, (b) mudanças em sistemas e (c) obsolescência dos recursos.

- Riscos de Segurança da Informação: relacionados ao acesso e à salvaguarda dos dados custodiados pela Organização. Abrange aspectos como: (a) ataques hackers, (b) fraudes virtuais, (c) acessos ilegais a banco de dados e (d) vazamento de dados.

A categorização de riscos que descrevemos acima deve estar toda abrangida nas práticas de GRC, ou seja, as práticas de riscos corporativos devem ter visão ampla, capturando diferentes tipos de situações que podem dificultar o cumprimento pleno dos objetivos estratégicos das Companhias, não se limitando aos riscos financeiros e/ou que podem gerar perdas financeiras. Essa visão ampliada é ratificada pelo estudo da KPMG que captura os principais fatores de risco divulgados pelas empresas abertas brasileiras. Na 7ª edição, publicada em 2022, apresentam variabilidade ampla, incluindo no topo da lista itens como (a) riscos regulatórios, (b) riscos associados a condições econômicas e de mercado, (c) riscos aos acionistas, (d) riscos operacionais e (e) riscos financeiros.

A necessidade de uma visão ampla e abrangente é um dos aspectos que capturaremos no instrumento de coleta, destinado a compreender as práticas atuais das empresas que serão pesquisadas.

2.3 Princípios, estruturas e processos de GRC

Nesta seção, vamos abordar informações sobre os principais modelos conceituais e princípios das práticas de gerenciamento de riscos corporativos. Sequencialmente, abordaremos sobre a estrutura de GRC nas Organizações e as características mais comumente observadas e por fim os principais processos que estão envolvidos em sua execução.

Segundo Silveira (2021), existem atualmente diversas definições e documentos de referência sobre gestão de risco. No Brasil, há destaque para o “Gerenciamento

de riscos corporativos: evolução em governança e estratégia” do Instituto Brasileiro de Governança Corporativa. No exterior, destacam-se as recomendações do COSO (*The Committee of Sponsoring Organizations of the Treadway Commission*), uma iniciativa de cinco organizações: (a) Instituto Americano de Contadores Públicos Certificados, (b) Instituto dos Auditores Internos, (c) Associação Americana de Contadores, (d) Instituto dos Contadores Gerenciais e (e) Executivos Financeiros Internacionais e da ISO 31.000 da *International Organization for Standardization*.

Conforme o artigo sumariado no Quadro 11, existem mais de 80 *frameworks* de gestão de riscos, entre os quais o Relatório King II, a Norma de Gestão de Riscos da Federação de Gestão de Risco Europeia (FERMA) e a ISO 31000:2009. Segundo Olson e Wu (2008), os frameworks possuem nomes diferentes, são elaborados por órgãos distintos em diversos países, apresentando, contudo, um tema em comum – a identificação, priorização e quantificação dos riscos, visando ajudar as organizações a gerir de forma eficaz a exposição aos seus riscos. Esses frameworks não discorrem sobre mecanismos de mensuração da maturidade da GRC. Olson e Wu (2008) também indicam que o COSO é um dos mais disseminados. Ao discorrer sobre o COSO, os autores mencionam que o objetivo central não é a eliminação dos riscos, mas a administração deles em níveis aceitáveis, considerando os controles necessários para o seu gerenciamento.

As definições do gerenciamento de riscos segundo os documentos indicados estão no quadro 13:

Quadro 13: GRC segundo documentos de referência

Documento de referência	Definição
Gerenciamento de riscos corporativos: evolução em governança e estratégia (IBGC, 2017)	“Sistema intrínseco ao planejamento estratégico de negócios, composto por processos contínuos e estruturados – desenhados para identificar e responder a eventos que possam afetar os objetivos da organização – e por uma estrutura de governança corporativa – responsável por manter esse sistema vivo e em funcionamento. (...) Trata-se, portanto, de um sistema integrado para conduzir o apetite à tomada de riscos no ambiente de negócios, a fim de alcançar os objetivos definidos”.
COSO 2017 <i>Enterprise Risk Management – Integrated Framework</i>	“A cultura, competências e práticas, integradas com a estratégia e sua execução, que a organização se baseia para gerenciar seus riscos e criar valor”.

ISO 31000:2018 <i>Risk management – Guidelines</i>	“Um conjunto de atividades coordenadas e métodos utilizado para dar direção à Organização e para controlar os vários riscos que podem afetar a capacidade de alcançar seus objetivos. Também diz respeito ao programa utilizado pela organização para administrar seus riscos, incluindo seus princípios, estruturas e processos para gestão dos riscos”.
--	---

Fonte: Silveira (2021, p.198)

Ao refletir sobre as definições desses documentos de referência, Silveira (2021, p. 199) indica que a visão moderna da gestão de riscos prevê que GRC esteja plenamente integrado à estratégia e à cultura da Organização, ao afirmar que:

A gestão de risco deve ter um papel-chave na definição dos objetivos estratégicos do negócio e no acompanhamento de sua implementação. O tema deve permear todas as discussões da alta gestão e ser considerado explicitamente em suas deliberações. Ademais, cabe às lideranças assegurar que todos os colaboradores compreendem os riscos que podem afetar o alcance dos objetivos do negócio e os administrem adequadamente.

A gestão de riscos também deve estar integrada à cultura da Organização, uma vez que os fatores humanos e comportamentais impactam diretamente as atividades relacionadas com o tema. Com isso, deve desenvolver-se a chamada “cultura de riscos” desejada pela empresa: isto é, o conjunto de padrões éticos, valores, atitudes, normas e comportamentos praticados na organização que motivam as decisões diárias de executivos e colaboradores em relação à identificação e ao gerenciamento dos riscos do negócio. (SILVEIRA, 2021, p. 199)

O Gerenciamento de Riscos Corporativos é um processo integrado, que deve considerar eventos que possam ameaçar a realização dos objetivos estratégicos das Organizações, incluindo seus resultados, o interesse dos distintos *stakeholders* e sua reputação. Para que isso ocorra, é necessário que exista um conjunto de processos coordenados, além de atividades, procedimentos e práticas de gestão para (a) identificação, (b) análise, (c) avaliação, (d) tratamento e (e) monitoramento dos riscos inerentes àquele negócio, os quais detalharemos nas próximas seções.

A gestão de riscos, segundo Brasiliano (2018), configura-se como uma dessas práticas derivadas da governança corporativa e pode ser aplicada de diferentes maneiras e por diferentes Organizações, independentemente do tamanho ou setor.

Souza e Martins (2020, p. 1) apontam que a implementação do GRC permite à governança ter uma expectativa razoável do que a organização entende e se é capaz de gerenciar riscos associados à sua estratégia e aos objetivos do negócio. Em artigo em que fazem um estudo de caso, os autores mencionam algumas das principais variáveis que impactam a prática do Gerenciamento dos Riscos Corporativos:

(...) é possível compreender a existência de variáveis ambientais que influenciam o modelo de governança corporativa de uma organização e, por conseguinte, que podem interferir na definição das estratégias e das práticas adotadas, como a gestão de riscos (...). Para uma análise comprovada dessas influências (...) [o estudo em questão considerou] o enfoque das variáveis ambientais, cultura organizacional, maturidade estratégica e rede de stakeholders e, conseqüentemente, a prática da gestão de riscos. (SOUZA E MARTINS, 2020, p. 1)

A evolução que comentamos é tal, que alguns autores já estabelecem uma visão mais ampla da prática de GRC. Segundo Souza e Martins (2020, p. 3):

O modelo de gestão de riscos deve ser um instrumento de tomada de decisão da Administração, com a finalidade de melhorar o desempenho da organização pela identificação de oportunidades de ganhos e de redução de probabilidade e, ou, impacto de perdas, indo além do cumprimento de demandas regulatórias (IBGC, 2017). Para a ISO31000 (ABNT, 2018), o sistema de gestão de riscos deve fazer parte integral dos processos organizacionais, participar da tomada de decisão que, explicitamente, envolve incertezas, deve ser sistemático e estar estruturado. (SOUZA E MARTINS, 2020, p. 3)

A norma “ABNT NBR ISO 31000: Gestão de riscos – Princípios e diretrizes” define princípios e diretrizes em gestão de riscos que podem ser adotados por diferentes Organizações nas atividades de GRC, independentemente da natureza dos riscos. A norma sugere que sejam feitos tratamentos de acordo com as especificidades de cada Organização.

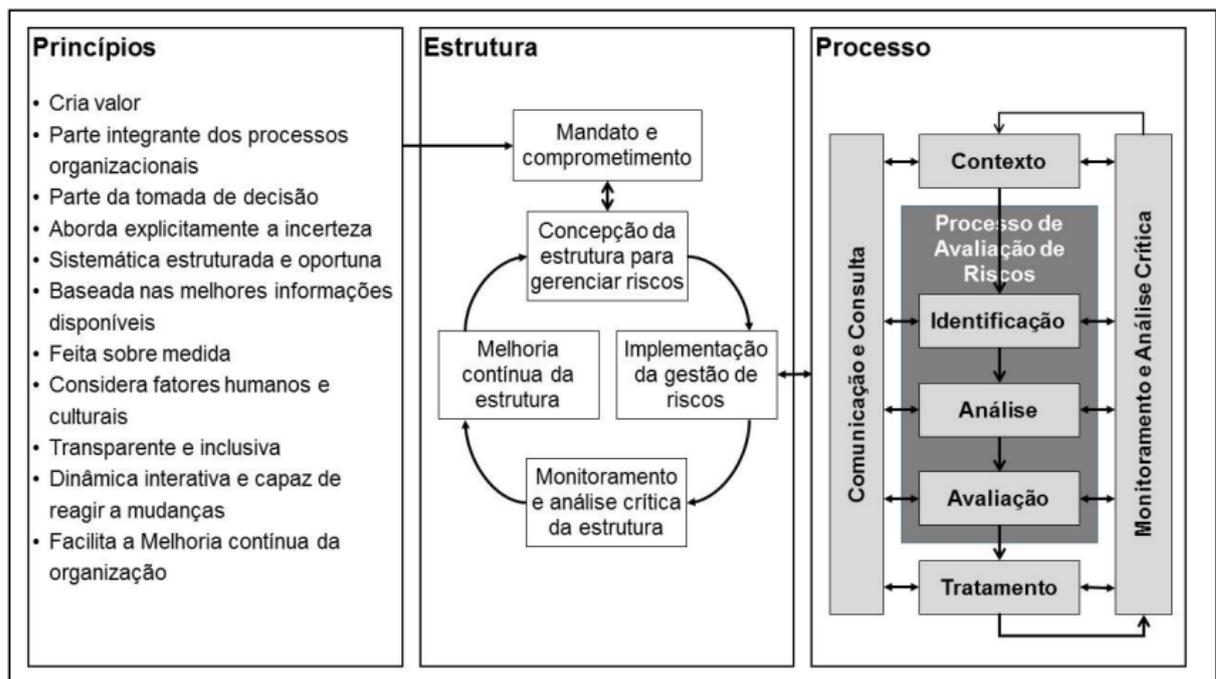
A norma está dividida em três componentes: (a) definição de princípios, (b) estrutura e (c) processo. Segundo a ABNT NBR ISO 31000, partindo de um conjunto de regras e diretrizes contidas nos princípios, é então criada a estrutura para sustentar a implantação do processo de gestão de risco na Organização, visando à sua permanente melhoria. A partir desse conjunto de componentes, o processo da norma objetiva estabelecer o contexto, identificar, analisar, avaliar e tratar o risco, e, ao longo

do processo, comunicar e monitorar, o que detalharemos nas próximas seções. A Figura 1 representa o modelo geral da metodologia.

Discorrendo sobre os princípios e estrutura da ISO 31.000, Bermejo (2018, p. 56) indica que a norma dá a base para a implementação de um gerenciamento efetivo de riscos corporativos e para o cumprimento das premissas de redução dos impactos indesejados:

Por intermédio desse conjunto de controles estruturados e com o entendimento claro do contexto e dos riscos existentes, são definidas as melhores ferramentas para tratamento dos riscos de acordo com sua natureza. Um plano de implantação para mitigação do risco é desenvolvido, executado, validado e reavaliado. Isso garante que riscos residuais sejam tratados. Assim, existirá qualidade no tratamento dos riscos e maior agregação de valor ao negócio por meio desta gestão. (BERMEJO, 2018, p. 56)

Figura 1: Relacionamentos entre GRC, estrutura e processo



Fonte: NBR ISO 31000:2009 (2009, p. xii)

A normativa NBR ISO 31000: 2009 – um dos documentos de referência no mercado sobre a temática e que comentamos no início desta seção – estabelece 11 princípios relacionados à gestão de riscos corporativos. Nos próximos bullets estão um sumário dos principais tópicos previstos no próprio documento e mais as considerações sobre cada um deles:

a) A gestão de riscos cria e protege valor.

A gestão de riscos contribui para a realização tangível dos objetivos corporativos e para a melhoria do desempenho por meio da redução dos impactos de eventos indesejados, da redução da probabilidade de sua ocorrência ou de ambos. Isso pode ocorrer de várias formas, como nos exemplos dados pela ISO 31.000, incluindo (a) melhoria do desempenho da segurança e saúde das pessoas, (b) melhoria da conformidade legal e regulatória, (iii) ampliação da aceitação pública, (iv) elevação da proteção do meio ambiente, (v) melhoria da qualidade do produto, (vi) aprimoramento do gerenciamento de projetos, (vii) maior eficiência nas operações, (viii) aprimoramento da governança e (ix) melhoria da reputação.

b) A gestão de riscos é parte integrante de todos os processos organizacionais.

A gestão de riscos não é uma atividade distinta ou separada das principais atividades e processos da organização. Ao contrário, faz parte das responsabilidades da Administração da Companhia e é parte integrante de todos os processos organizacionais, incluindo o planejamento estratégico e todos os processos de gestão de projetos e gestão de mudanças, bem como dos processos operacionais dos principais ciclos de negócio e de sustentação/suporte.

c) A gestão de riscos é parte da tomada de decisões.

O risco nos direciona para eventos cuja probabilidade de ocorrência é futura e não estão materializados atualmente. A volatilidade e as incertezas do ambiente são cada vez mais constantes no cenário corporativo. Portanto, a gestão de riscos deve compor o contexto dos tomadores de decisão, auxiliando-os a fazer escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação.

d) A gestão de riscos aborda explicitamente a incerteza.

A gestão de riscos explicitamente leva em consideração a incerteza, a natureza dessa incerteza, os potenciais impactos que podem ser gerados por ela, a

probabilidade de materialização dessa incerteza e como ela pode ser tratada, mitigada ou conscientemente aceita.

e) A gestão de riscos é sistemática, estruturada e oportuna.

Esse é um pressuposto para implementações de uma estrutura de GRC eficiente, que suporta decisões de alocação e uso apropriado dos recursos e otimização de desempenho organizacional. Uma abordagem sistemática, oportuna e estruturada para a gestão de riscos contribui para a eficiência e para os resultados consistentes, comparáveis e confiáveis.

f) A gestão de riscos baseia-se nas melhores informações disponíveis.

Os *inputs* para o processo de gerenciar riscos são baseados em fontes de informação, tais como dados históricos, experiências passadas, retroalimentação das partes interessadas, observações, previsões e opiniões de especialistas. Entretanto, convém que os tomadores de decisão se informem e levem em consideração as particularidades daquela situação, bem como quaisquer limitações dos dados ou modelagem utilizados, ou a possibilidade de divergências entre especialistas.

g) A gestão de riscos é feita sob medida.

A gestão de riscos está alinhada com o contexto interno e externo da organização e com o perfil do risco daquela entidade, bem como dos seus níveis de apetite e tolerância, além das particularidades de cada Organização, incluindo sua estratégia e cultura.

h) A gestão de riscos considera fatores humanos e culturais.

A gestão de riscos reconhece as capacidades, percepções e intenções do pessoal interno e externo que podem facilitar ou dificultar a realização dos objetivos da Organização.

i) A gestão de riscos é transparente e inclusiva.

O envolvimento apropriado e oportuno de partes interessadas, também um pressuposto da implementação da estrutura de GRC e, em particular, dos tomadores de decisão em todos os níveis da Organização assegura que a gestão de riscos permaneça pertinente. O envolvimento também permite que as partes interessadas em toda a dinâmica de gestão de riscos corporativos sejam devidamente representadas e tenham suas opiniões levadas em consideração na determinação dos critérios adotados nas práticas.

j) A gestão de riscos é dinâmica, interativa e capaz de reagir a mudanças.

A gestão de riscos continuamente percebe e reage às mudanças. Na medida em que acontecem eventos externos e internos, o contexto e o conhecimento são modificados. Continuamente, novos riscos surgem, alguns modificam-se e outros desaparecem. Igual processo se dá em relação à relevância desses riscos.

k) A gestão de riscos facilita a melhoria contínua da organização.

Convém que as Organizações desenvolvam e implementem estratégias para melhorar a sua maturidade na gestão de riscos juntamente com todos os demais aspectos da sua organização. Práticas sedimentadas tendem a produzir resultados melhores e mais consistentes.

Franco (2017, p. 20) também discorre sobre os princípios do Gerenciamento de Riscos Corporativos e as principais entregas esperadas, conforme indicam os tópicos abaixo, com clara convergência aos princípios dos *frameworks*:

De forma geral, podemos dizer que a gestão de riscos deve ser:

- Proporcional ao nível de riscos enfrentado pela organização;
- Alinhada às atividades da organização;
- Integrada aos demais processos da organização;
- Compressiva, sistemático e estruturado;
- Dinâmica, interativo e que responda às mudanças.

Os princípios devem ter por base a noção de que riscos são itens que possam ser identificados e controlados. A gestão de riscos deve entregar:

- Conformidade com as leis e regulamento;
- Garantia do gerenciamento dos riscos mais significativos;
- Garantia de que as decisões levem em contas os riscos;

- Efetividade, eficácia e eficiência das estratégias, operações e projetos. (FRANCO, 2017, p. 20)

Após revisarmos os princípios associados ao Gerenciamento de Riscos Corporativos, passamos a abordar a revisão da temática da Estrutura dessa prática. A gestão de riscos como um processo de suporte e uma estrutura dedicada e integrada às demais áreas e processo da organização é muito significativo para cumprimento dos objetivos de redução dos impactos indesejados dos riscos da Organização.

Os documentos de referência ou *frameworks* que mencionamos no capítulo anterior buscam oferecer orientações para implementação do Gerenciamento de Riscos Corporativos.

Segundo a NBR ISO 31000:2019, um desses documentos de referência, o sucesso da gestão de riscos dependerá da eficácia da estrutura de gestão que fornece os fundamentos e os arranjos que irão incorporá-la por meio de toda a Organização, em todos os níveis. A norma também indica que convém que a GRC seja parte integrante da gestão, incorporada na cultura e nas práticas e adaptada aos processos e negócios da Organização.

A existência de uma estrutura própria, típica e dedicada deve auxiliar no gerenciamento de riscos por meio da aplicação de processos de gestão de risco nos diferentes níveis das Organizações e dentro de sua realidade. A estrutura visa a assegurar uma captura adequada e precisa e que as informações sobre os riscos proveniente desse processo sejam correta e tempestivamente reportados e sirvam como base para a tomada de decisões em todos os níveis organizacionais aplicáveis.

Ao revisar os aspectos gerais da NBR ISO 31000:2009 sobre a estrutura de GRC, Franco (2017, p. 21) faz a seguinte síntese:

A NBR ISO 31000 define a estrutura de gestão de riscos como um conjunto de componentes que fornece os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos em toda a organização. Os fundamentos incluem a política, os objetivos, os mandatos e o comprometimento para o gerenciamento de riscos. Os arranjos organizacionais incluem os planos, relacionamentos, responsabilidades, recursos, processos e atividades. (FRANCO, 2017, p. 21)

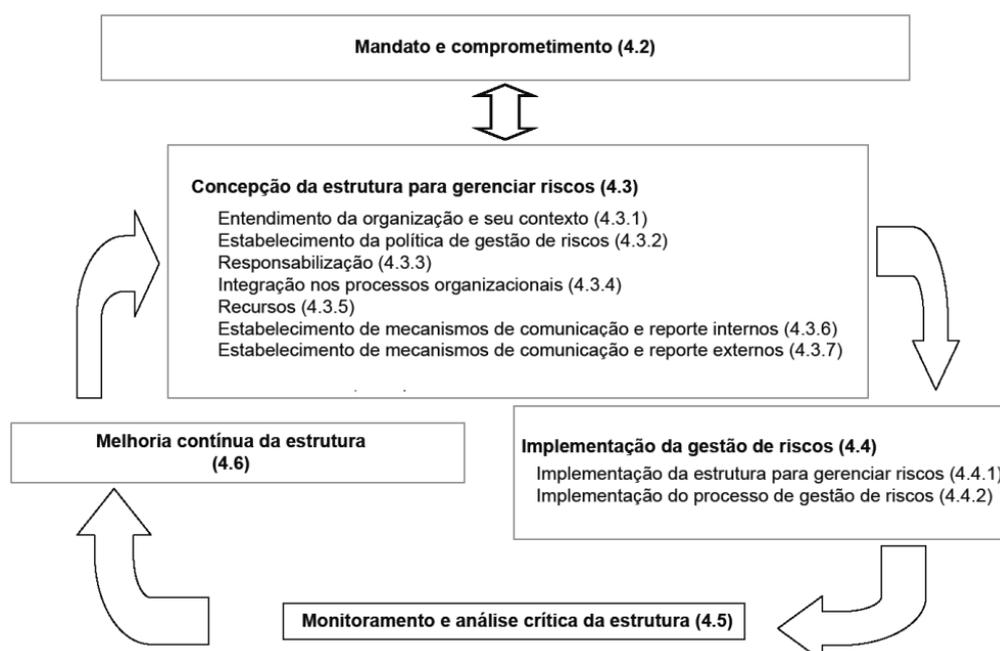
Trivelato, Mendes e Dias (2018, p. 9) também abordam o tema da estrutura ao estudar a relevância do gerenciamento de riscos nas Companhias contemporâneas, mencionando que:

Com base nos princípios do gerenciamento de riscos, a organização deve estabelecer uma estrutura para possibilitar a implantação e garantir a continuidade do processo de gerenciar riscos. De acordo com a norma [NBR ISO 31000:2009], essa estrutura será incorporada nas políticas da organização e consiste em um conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos.

Quando a norma se refere aos fundamentos e aos arranjos organizacionais, estes podem ser compreendidos de uma maneira geral, como: políticas, objetivos, deveres e comprometimento por parte dos colaboradores, planos, relacionamentos, responsabilidades, recursos, processos e atividades. Diante disto, esta estrutura permitirá que as atividades de gerenciamento de riscos possam ser desempenhadas devidamente. (TRIVELATO, MENDES E DIAS, 2018, p. 9)

Ao avançar, a NBR ISO 31000:2009 enumera os componentes da estrutura necessários para o adequado gerenciamento dos riscos corporativos:

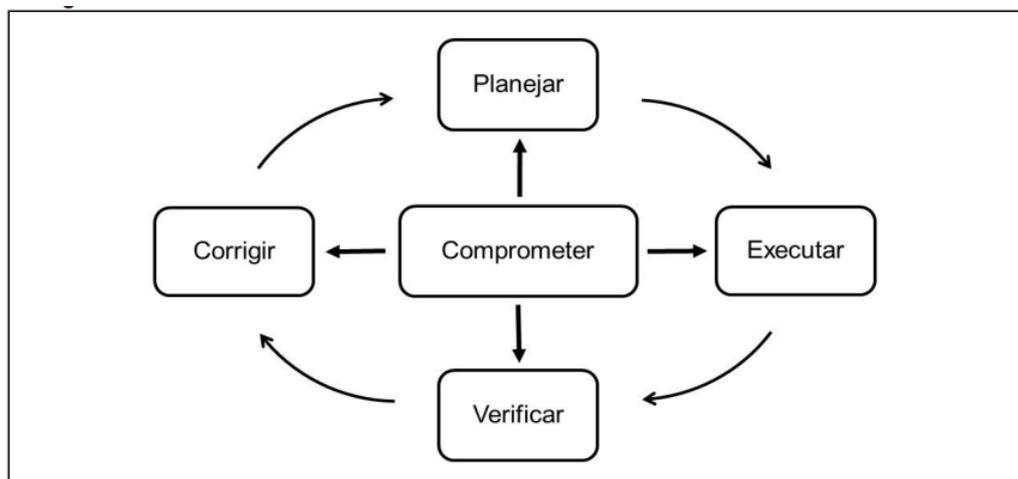
Figura 2: Relacionamentos entre as estruturas de GRC



Fonte: NBR ISO 31000:2009 (2019, p. 9)

Ao comentar sobre os principais componentes da estrutura trazidos pela norma, Franco (2017) aponta que a estrutura segue um modelo PDCA (*plan, do, check e act* – modelo clássico de planejamento, implementação e retroalimentação), com um acréscimo que é o chamado mandato e comprometimento, conforme vê-se na figura 3, que faz alusão ao diagrama da figura anterior:

Figura 3: PDCA na estrutura de GRC



Fonte: Franco (2017, p. 22)

Passamos a enumerar brevemente um resumo sobre os principais componentes sobre as estruturas de GRC, sintetizadas a partir das principais diretrizes trazidas pelos *frameworks* e de acordo com o entendimento manifestado por Franco (2017), apresentados nos itens de “a” a “d”, a seguir.

Convém, novamente, retomar a observação de que essa regra geral, relevante ao entendimento em alto-nível sobre as diretrizes necessárias à estrutura da prática de GRC, demanda ser adaptada às distintas realidades das Companhias, seja decorrente de seu porte, segmento, estrutura, cultura, entre outros.

a) Mandato e comprometimento

Para que o gerenciamento de riscos seja efetivo, é fundamental o comprometimento da Alta Administração da Companhia e um suporte de todos os

níveis gerenciais. A Alta Administração, representada na maioria das vezes pelo Conselho de Administração, Comitês de Assessoramento, *CEO* e Diretoria Executiva, é responsável pelo estabelecimento desse mandato e deve estar comprometida com a estrutura de gestão de riscos, além de ser a patrocinadora da implementação do processo de gestão e da melhoria contínua.

Dentre suas funções, estão: (a) definição e aprovação da política de gestão de riscos, (b) assegurar que os recursos necessários sejam alocados para a gestão de riscos e (c) assegurar que a estrutura para gerenciar riscos seja continuamente apropriada.

b) Estrutura de governança e de gestão de riscos

Para que seja efetiva, a gestão de risco precisa ter uma estrutura de governança e gestão adequadas.

Segundo Franco (2017), a governança de gestão de riscos deve ser parte integrante da estrutura de gestão organizacional, definindo as responsabilidades e o fluxo de informações no que se refere a riscos e ser estabelecida e acompanhada pela Administração Sênior da Organização.

Nesse sentido, a NBR ISO 73:2015 indica que a estrutura da gestão de riscos é um “conjunto de componentes que fornece os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização.

De acordo com Franco (2017), a implantação de uma estrutura formal de gestão de riscos é a forma mais efetiva de garantir que o processo decisório será suportado por um gerenciamento de riscos consistente e efetivo. Esta implementação é um processo evolutivo e que reflete a maturidade na gestão de riscos e a complexidade enfrentadas pela Organização.

A estrutura de gestão de riscos deve ter um desenho funcional e organizacional que atenda os objetivos de cada Organização e que seja capaz de (a) fornecer aos gestores sêniores um conhecimento preciso dos riscos e (b) identificar os responsáveis pelas principais etapas do processo.

Dentro da estrutura de gestão de riscos, as principais normas e modelos incentivam a existência de uma unidade funcional ou departamento responsável pela gestão de riscos, que tenha em seu escopo: (a) coordenação da política estratégica de gestão de risco e sua operacionalização, (b) estabelecimento de um fluxo de informações e sensibilização sobre riscos, (c) elaboração de registros e relatórios e (d) coordenação e acompanhamento dos planos de respostas aos riscos.

A área ou o departamento de gestão de riscos não é o proprietário dos riscos nem dos controles de mitigação.

c) Política de Gestão de Riscos

Outro ponto central na estrutura de GRC é a definição de uma política de gestão de riscos pela Administração Sênior da Companhia. O documento deve definir aspectos relevantes como o apetite e as responsabilidades relativas à gestão de riscos. Além disso, é uma declaração da intenção e direção, devendo definir claramente os objetivos centrais, além de articular a visão de gerenciamento de riscos e descrever os benefícios que proporciona. A política deve definir os indicadores que medem a contribuição da estrutura de gestão de riscos para os objetivos da Organização. Preferencialmente, devem ser utilizados indicadores já existentes.

d) Cultura de Gestão de Riscos

A cultura organizacional é um importante componente da gestão de riscos, que surge de comportamentos repetidos e incorporados à realidade dos membros de uma organização, sendo influenciado e moldado pelos valores, crenças e atitudes dos indivíduos e que está profundamente relacionada à transformação dos valores em ações concretas.

Franco (2017) ressalta que a cultura direciona o desempenho organizacional e engloba as regras de condutas escritas e não escritas e que muitos fatores a influenciam, incluindo as atitudes da alta administração, o código de conduta e as políticas de ética e de recursos humanos.

Cabe ao Conselho da Administração, aos seus Comitês de Assessoramento e à Administração Sênior estabelecerem o modelo e direcionar o comportamento correto da cultura relacionada a riscos.

A cultura de gestão de riscos deve ser o caminho usual para a implementação da gestão de riscos na Organização e está profundamente relacionada a como os profissionais reconhecem e reagem aos riscos.

Entre os objetivos esperados como a criação de uma cultura de gestão de riscos efetiva estão: (a) aplicação da gestão de risco de maneira transversal, desde o planejamento estratégico até as operações do dia a dia, (b) processo de melhoria contínua da habilidade coletiva de gerenciar riscos, (c) utilização de um vocabulário comum que promova conhecimento compartilhado e que favoreça a comunicação sobre riscos e seu gerenciamento.

Para o COSO (2017, p. 6), o gerenciamento de riscos corporativos é:

um processo conduzido em uma organização pelo Conselho de Administração, Diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a Organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatíveis com o apetite a risco da Organização e possibilitar garantia razoável do cumprimento de seus objetivos. (COSO, 2017, p. 6)

O gerenciamento de riscos corporativos deve ser integrado aos processos organizacionais da Companhia, isto é, às suas atividades cotidianas. De maneira geral, os modelos da gestão de risco apresentam uma convergência em sua concepção.

De acordo com Marques, Muller e Silva (2019, p 108), citando outros estudos:

(...) existem mais de oitenta *frameworks* de gestão de riscos, alguns elencados por Daud, Yazid e Hussin (2010), tais como o Relatório King II, a Norma de Gestão de Riscos Europeia (FERMA), a ISSO 31000:2009 e o documento *Enterprise Risk Management: Integrated Framework* do COSO (2004). Os autores salientam que apesar de tais *frameworks* possuírem nomes diferentes, serem elaborados por diferentes órgãos e em diferentes países, todos compartilham um tema em comum – a identificação, priorização e quantificação dos riscos, a fim de

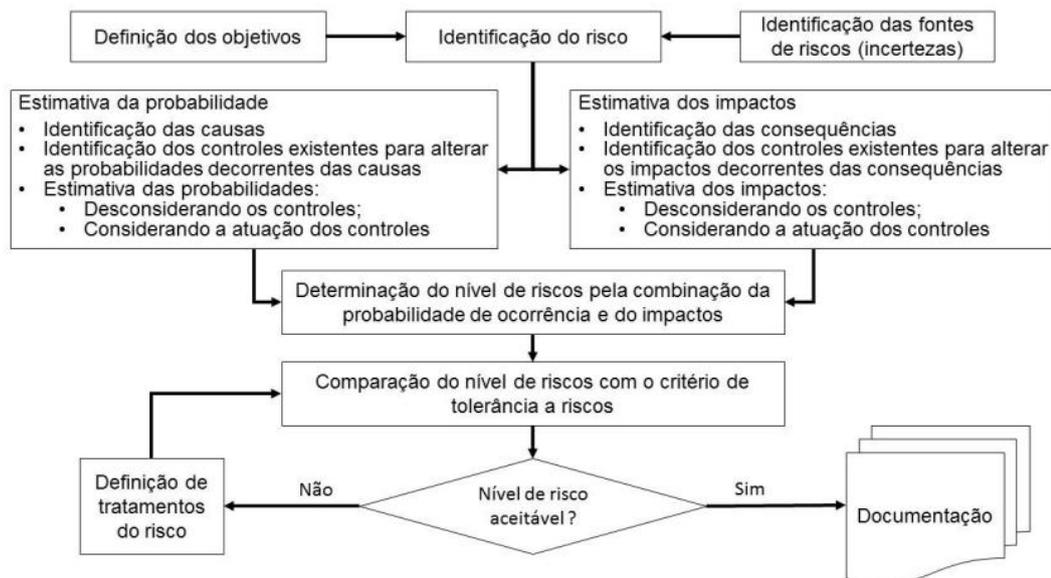
ajudar as organizações a gerir de forma eficaz a sua exposição aos riscos.

(...)

Para tanto, [a Companhia] estabelece uma sequência de eventos, fazendo com que os gestores levem em consideração os riscos aos quais as empresas estão expostas, bem como avaliem quais os controles necessários para o gerenciamento desses riscos. (MARQUES, MULLER E SILVA, 2019, p 108)

Ao definir as principais etapas do processo de Gestão de Risco, Franco (2017) sintetiza a seguinte visão gráfica:

Figura 4: Processo de Gestão de Riscos



Fonte: Franco (2017, p. 39)

Sintetizamos, na sequência, as principais etapas do processo de gestão de risco e as mais relevantes características de cada uma delas de acordo com a visão sequencial proposta por Franco (2017). Esse sequenciamento pode apresentar diferenças de nomenclaturas, agrupamentos em outros estudos ou em outras políticas corporativas adotadas pelas diferentes Organizações, mantendo, contudo, as diretrizes do processo usualmente utilizadas pelas Companhias:

a) Contexto:

Contempla os principais parâmetros internos e externos, que são considerados no processo de GRC como um todo. Abrange o escopo, política, além dos critérios de

análise. Na perspectiva externa, deve considerar os principais *players* com os quais a empresa atua e os principais direcionadores. No contexto interno, considera os objetivos estratégicos, os recursos tangíveis e intangíveis disponíveis à Companhia.

b) Critérios:

Franco (2017) menciona que a gestão de riscos envolve uma lógica e estruturada de pensar e se comunicar e requer uma linguagem estruturada para suportar o processo. Portanto, é fundamental ter-se uma linguagem comum para favorecer a comunicação interna, além de um padrão de mensuração que possa ser utilizado para avaliar e comparar os riscos. Os principais aspectos a serem considerados aí são: (i) a probabilidade e (2) o impacto dos riscos identificados, devendo ser definidas escalas para cada uma dessas dimensões.

c) Tipologias:

Tipologia é um agrupamento de riscos de acordo com sua natureza, visando a facilitar seu gerenciamento. Os diferentes *frameworks* estabelecem sugestões distintas de tipologias. No geral, incluem-se aí grupos como risco estratégico, de imagem e reputação, operacional, legal e conformidade, financeiro. Cada Organização deve estabelecer tipologias que sejam aderentes aos seus principais riscos e que permitam facilitar e racionalizar o gerenciamento.

d) Mensuração de ocorrência:

Visa a estabelecer a probabilidade que um determinado risco se materialize. Existem formas distintas para demonstrar isso como, por exemplo, o número de eventos esperados em determinado período. No geral, os critérios estabelecidos pelas Organizações estabelecem uma escala da ocorrência esperada a uma escala gradual desde um evento improvável até um quase certo. No quadro seguinte, demonstra-se uma escala exemplificativa que associa as respectivas escalas a uma frequência de evento - desde casos raros até mais frequentes, com base em modelos utilizados por empresas de capital aberta que realizam mensuração de seus riscos. Escalas

similares a esta são utilizadas por diferentes Organizações em seus procedimentos de GRC.

Quadro 14: Matriz exemplificativa da Escala de Probabilidade

	Análise de probabilidade e frequência estimada da materialização do risco
Escala	Frequência
5 Quase Certo	Mais de 1 vez por mês
4 Provável	Mais de 1 vez por semestre até 1 vez por mês
3 Possível	1 vez por ano a uma vez por semestre
2 Baixo	Menos de uma vez por ano
1 Raro	Menos de uma vez em 5 anos

Fonte: Elaborado pelo próprio autor (2023)

e) Mensuração de impacto:

O impacto busca capturar a extensão que um risco materializado traz para a Organização, incluindo casos como danos à reputação, descumprimentos legais, despesas indesejáveis, entre outros. Essa mensuração também deve ser definida por meio de réguas específicas, buscando uma aplicação consistente no tempo. No geral, as réguas devem ser abrangentes, contemplando aspectos como impacto financeiro, continuidade das atividades, cumprimento de leis e normas, impactos ambientais, entre outros considerados relevantes para aquela Organização. No quadro seguinte, demonstra-se uma escala exemplificativa que associa as respectivas escalas de relevância a eventos objetivos em sete dimensões específicas – (1) financeira, (2) continuidade e perenidade, (3) conformidade, (4) operação, (5) meio ambiente, (6) imagem e reputação e (7) saúde e segurança com base nas políticas de GRC de uma empresa aberta de grande porte do segmento de varejo. Escalas similares a esta são utilizadas por diferentes Organizações em seus procedimentos de GRC, incluindo estes ou outras dimensões e associando a situações práticas aplicáveis aos seus negócios.

Quadro 15: Matriz exemplificativa da Escala de Impacto

Escala de Impacto	Critérios				
	Financeiro	Continuidade e Perenidade	Conformidade	Operação	Imagem & Reputação
5 - Alto	> 80% do valor do apetite a risco	Continuidade do negócio afetada.	Eventos e/ou processos de larga escala movidos contra a Companhia ou Executivos.	Interrupção das operações acima de 30% das lojas físicas e/ou das operações <i>online</i> a partir de 1 dia.	Exposição negativa nacional e/ou internacional.
4 - Significativo	Entre 61% e 80% do valor do apetite a risco	Continuidade do negócio poderá ser afetada.	Eventos e/ou processos movidos contra a Companhia ou Executivos.	Interrupção das operações em 15% a 29% das lojas físicas e/ou das operações <i>online</i> de 16 a 24 horas.	Exposição negativa estadual.
3 - Moderado	Entre 41% e 60% do valor do apetite a risco	Continuidade de projetos ou ativo(s) afetada.	Notificações e/ou advertências com necessidade de estabelecer provisionamentos.	Interrupção das operações em 5% a 14% das lojas físicas e/ou das operações <i>online</i> de 8 a 16 horas.	Exposição negativa regional.
2 - Baixo	Entre 21% e 40% do valor do apetite a risco	Continuidade de projetos poderá ser afetada.	Notificações e/ou advertências sem necessidade de estabelecer provisionamentos.	Interrupção das operações em até 5% das lojas físicas e/ou operações <i>online</i> de até 8 horas.	Exposição negativa junto a fornecedores e parceiros estratégicos da Via Varejo.
1 - Mínimo	Entre 0% e 20% do valor do apetite a risco	Impacto interno em atividade(s) relacionada(s) a processo(s).	Recomendações dos órgãos competentes (fiscalizadores/regulatórios).	Paralisação pontual do <i>BackOffice</i> .	Exposição negativa exclusiva ao público interno.

Fonte: Elaborado pelo próprio autor (2023)

f) Níveis de risco:

A combinação das escalas de probabilidade e impacto definem os níveis de risco nas visões inerentes (risco *in natura*, característica própria e sem a aplicação de mitigações) e residual (risco após as mitigações existentes e aplicação de controles que reduzem probabilidade, impacto ou ambos). Além disso, em alguns casos utiliza-se a escala de nível desejado, que deverá ser perseguido com base no apetite definido pela Organização, até que se torne o risco em sua visão residual. O quadro seguinte é apresentado com base em uma escala exemplificativa de uma empresa local de grande porte do setor de varejo. Cada empresa estabelece sua visão sobre escalas de relevância do risco com base na combinação entre probabilidade de ocorrência versus impacto esperado.

Quadro 16: Matriz exemplificativa de Nível de Risco

Probabilidade	Extremo	MODERADO	MODERADO	ALTO	EXTREMO	EXTREMO
	Alto	BAIXO	MODERADO	ALTO	ALTO	EXTREMO
	Moderado	BAIXO	BAIXO	MODERADO	ALTO	ALTO
	Baixo	IRRELEVANTE	BAIXO	BAIXO	MODERADO	ALTO
	Mínimo	IRRELEVANTE	IRRELEVANTE	BAIXO	MODERADO	MODERADO
		Raro	Baixo	Moderado	Alto	Extremo
		Impacto				

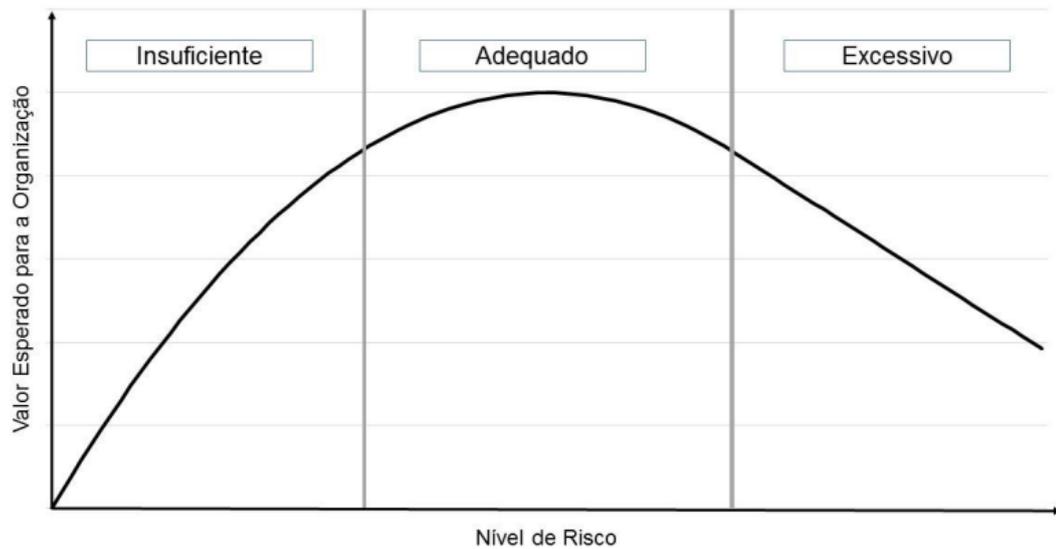
Fonte: Elaborado pelo próprio autor (2023)

g) **Apetite aos riscos:**

Designa, de maneira geral, o nível de risco que uma Organização está disposta a aceitar correr para cumprir seus objetivos estratégicos. A definição do apetite é uma prerrogativa dos altos executivos, devendo esta ser difundida e comunicada a todos aqueles que se envolvem na atividade de gerenciamento dos diferentes riscos.

Franco (2017) explicita que somente com uma avaliação clara dos riscos, em confronto com o apetite, é possível balancear riscos e oportunidades. Com efeito, a resposta ao risco demanda esforço e recursos; daí a necessidade de se equilibrar o valor a ser entregue pela empresa com esses riscos.

Figura 5: Apetite ao Risco
(visão cruzada entre valor esperado pela Organização e Nível de Risco)



Fonte: Franco (2017, p. 44)

h) Atitude Frente aos Riscos

Uma vez identificado o nível de risco, a Organização define se e como quer tratar aquele risco. Com base nisso, estabelece em que condições os riscos devem ser aceitos, quais ações de mitigação são necessárias, com que periodicidade fará o seu acompanhamento e quem são os executivos que deverão gerir e conhecer a evolução efetiva e a comparação com o que era esperado.

i) Avaliação dos Controles

Como mencionamos como tópico “f”, para que tenhamos a avaliação de um risco em sua visão residual é premissa a existência de controles que atuem para reduzir a probabilidade de ocorrência, impactos trazidos pela ocorrência desse risco ou de ambos. Para que um controle ou um conjunto de controles possa atuar para reduzir o nível de risco é fundamental que ultrapasse a pura existência em si, mas que aquele controle ou grupo de controles sejam corretamente desenhados, implementados e adequadamente executados.

j) Identificação do Risco

Compreende a etapa de identificar, descrever e reconhecer as incertezas existentes e que podem reduzir o cumprimento dos objetivos estratégicos daquela Organização. Segundo Franco (2017) a melhor forma de identificar riscos é relacioná-lo a eventos que podem ocorrer e que podem interferir na habilidade da Organização em atingir seus objetivos. Segundo a ABNT NBR ISO 31.000 (2009), a finalidade desta etapa é gerar uma lista abrangente de riscos baseada nestes eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos.

A identificação é um processo contínuo e permanente em relação às atividades da Organização e deve levar em conta novas atividades, erros e desvios identificados, denúncias, apontamentos da auditoria interna e externa e fatores externos que impactam nas rotinas da empresa.

Ao discorrer sobre pontos relevantes a serem considerados na etapa de identificação de riscos, a ABNT NBR ISO 31.000 (2019, p. 17) apresenta uma série de indicações abrangentes a serem observadas:

Convém que a identificação inclua todos os riscos, estando suas fontes sob o controle da organização ou não, mesmo que as fontes ou causas dos riscos possam não ser evidentes. Convém que a identificação de riscos inclua o exame de reações em cadeia provocadas por consequências específicas, incluindo os efeitos cumulativos e em cascata. Convém que também seja considerada uma ampla gama de consequências, ainda que a fonte ou causa do risco não esteja evidente. Além de identificar o que pode acontecer, é necessário considerar possíveis causas e cenários que mostrem quais consequências podem ocorrer. Convém que todas as causas e consequências significativas sejam consideradas. Convém que a Organização aplique ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos e capacidades e aos riscos enfrentados. Informações pertinente e atualizadas são importantes na identificação de riscos. Convém que incluam informações adequadas sobre os fatos por trás dos acontecimentos, sempre que possível. Convém que pessoas com um conhecimento adequado sejam envolvidas na identificação dos riscos. (ABNT NBR ISO 31.000, 2009, p. 17)

k) Análise dos Riscos

A análise permite ampliar o entendimento da natureza e causas do risco, suportando a decisão sobre aqueles que precisarão de eventuais mitigações. Além do

enquadramento nas réguas pré-estabelecidas, que citamos nos tópicos anteriores, entender as causas raízes e ter visão abrangente sobre todas as consequências é fundamental para direcionar as ações mais adequadas de mitigação que devem ser aplicadas e para dimensionar como os recursos e custos em geral, envolvidos no processo de redução das causas, devem ser alocados e como eles impactam as consequências.

Segundo Franco (2017, p. 49):

A efetividade da gestão de riscos é dependente de uma análise correta. Mesmo que a organização tenha um processo de gestão de riscos bem projetado, métodos e ferramentas para gestão de riscos, a análise de riscos é em última análise, a uma atividade dependente de um julgamento subjetivo. (FRANCO, 2017, p. 49)

l) Avaliação e Priorização dos Riscos

A grande atividade desta etapa é determinar os níveis de risco – individualmente e de forma agregada e gerenciar dentro do apetite estabelecido, evitando assumir riscos superiores à capacidade estabelecida. Uma vez identificado, devem ser documentados e comunicados aos responsáveis e à Governança da Organização, a fim de que conheçam o risco, sua relevância e os planos de tratamento que serão estabelecidos. Com isso, espera-se ter os elementos necessários para decidir a priorização com a qual serão tratados, considerando as agregações consideradas mais importantes por aquela Companhia – em algumas há ênfase nas perdas potenciais de natureza financeiras, outras tem menor apetite a riscos de imagem e exposição.

m) Tratamento e Monitoramento dos Riscos

O tratamento dos riscos envolve a definição de medidas de que sejam adequadas e na definição de Franco (2017), no geral envolve as opções de aceitar, reduzir, compartilhar e evitar.

Ao discorrer sobre a etapa do processo de GRC, a ABNT NBR ISO 31.000 (2009, p. 19) sintetiza:

Selecionar a opção mais adequada de tratamento de riscos envolve equilibrar, de um lado, os custos e os esforços de implementação e, de outro, os benefícios decorrentes, relativos a requisitos legais,

regulatórios ou quaisquer outros, tais como o da responsabilidade social e o da proteção do ambiente natural. Convém que as decisões também levem em consideração os riscos que demandam um tratamento economicamente não justificável, como, por exemplo, riscos severos (com grande consequência negativa), porém raros (com probabilidade muito baixa). Várias opções de tratamento podem ser consideradas e aplicadas individualmente ou combinadas. A organização, normalmente, beneficia-se com a adoção de uma combinação de opções de tratamento. (ABNT NBR ISO 31.000, 2009, p. 19)

Os planos de tratamento devem ser documentados e conter aspectos como os responsáveis pela aprovação do plano e por sua implementação, as ações propostas, cronograma, os recursos requeridos, medidas de desempenho, além dos requisitos para o monitoramento.

Monitorar tem como objetivo assegurar que eles alcancem os níveis desejados e são feitos prioritariamente a partir de Indicadores Chaves de Risco (KRI, no acrônimo em inglês). Este acompanhamento permitirá também ampliar o conhecimento e avaliação sobre aquele risco, analisar eventos como mudança e tendências, além de alterações no contexto interno e externo.

2.4 Governança e Maturidade de GRC

Estudiosos, reguladores, órgãos de estudo e intercâmbio possuem definições distintas para o que Governança Corporativa significa e abrange. O IBGC (2017, p. 22), por exemplo, a define como:

O sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. (IBGC, 2017, p. 22)

Bramont (2012, p. 31) ao citar Andrade e Rossetti (2009) identifica seis possíveis dimensões abrangidas pelo conceito de governança corporativa:

(1) sistema que rege valores, (2) sistema que assegura e preserva direitos, (3) sistema que disciplina práticas de relacionamento, (4) sistema de governo, gestão e controle, (5) sistema e estrutura de autoridade, responsabilidade e poder e (6) conjunto de instrumentos,

normas, leis, regulamentos e arranjos contratuais. (BRAMONT, 2012, p. 31)

A gestão de risco está associada ao processo decisório e ao processo que define as estratégias da Organização. Segundo o Caderno de Governança Corporativa do IBGC (2017, p. 22):

O gerenciamento de riscos integra a governança de uma empresa, pois o risco precisa ser identificado, medido, tratado e monitorado – e essas informações alimentam o processo de tomada de decisão por parte de diferentes agentes, sejam os sócios, o conselho de administração, a diretoria, assim como as demais partes interessadas (por exemplo clientes, fornecedores, comunidade, reguladores, o governo, entre outros). Dessa forma, o GRCorp traz vantagens na estrutura de governança das organizações, como o aumento da transparência e da prestação de contas, o fortalecimento dos controles internos e maior comprometimento com a responsabilidade corporativa. (IBGC, 2017, p. 22)

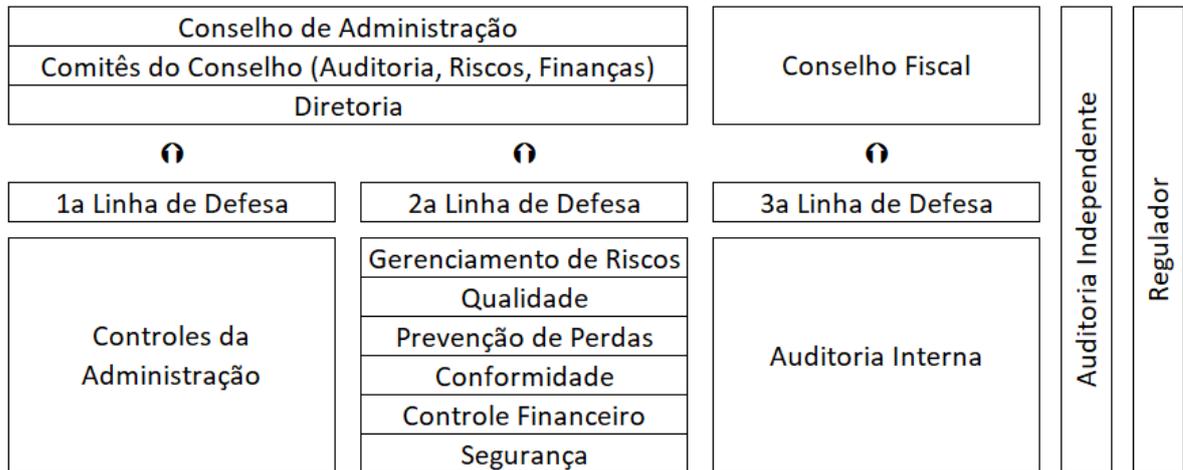
Para que a estrutura de Gerenciamento de Riscos Corporativos funcione adequadamente, é necessário que haja uma estrutura dedicada e com responsabilidades claras de todos os seus agentes. O modelo é representado por funções distribuídas em diferentes níveis da organização, nas diferenças estruturais. Portanto, existem vários agentes com papéis e responsabilidades no processo de GRC, que não podem ser desempenhados apenas por áreas ou profissionais isoladamente.

De acordo com o Caderno de Governança do IBGC (2017, p. 24), os processos e atividades que envolvem a GRC, bem como seu monitoramento devem ser exercidos:

- (I) Pelos diversos agentes dos órgãos de governança, incluindo o Conselho de Administração, o Comitê de Auditoria e demais e comitês de assessoramento (como o comitê de gerenciamento de riscos ou outros que discutam temas técnicos específicos), a diretoria e o conselho fiscal, quando aplicável. (...)
- (II) Pelas três linhas de defesa: 1ª Linha de defesa – realizada pelos gestores das unidades e responsáveis diretos pelos processos: contempla as funções que gerenciam e têm a responsabilidade sobre os riscos; 2ª Linha de defesa – realizada pelos gestores corporativos de GRC, de conformidade ou de outras práticas de controle (...); 3ª Linha de defesa – realizada pela auditoria interna: fornece avaliações independentes por meio do acompanhamento dos controles internos. (IBGC, 2017, p. 24)

A figura seguinte sintetiza a declaração de posicionamento do Instituto dos Auditores Internos em “As três linhas de defesa no gerenciamento eficaz de riscos e controles”.

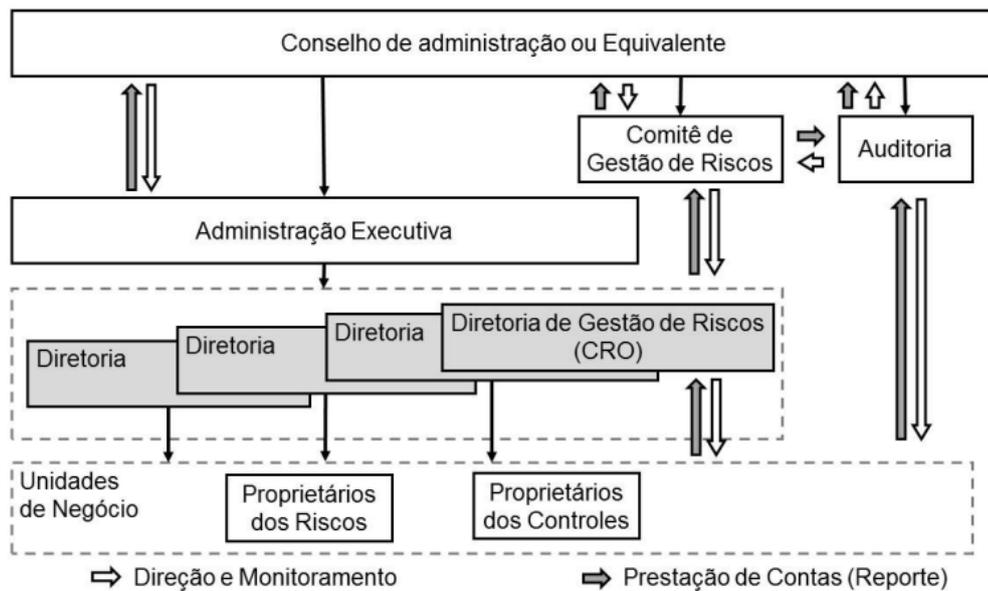
Figura 6: Linhas de defesa da função de GRC



Fonte: Elaborado pelo autor (2023), com base em IBGC (2017, p. 25)

Franco (2017) mostra um exemplo dos principais agentes atuantes e suas relações:

Figura 7: Exemplo de modelo de governança de gestão de riscos



Fonte: Franco (2017, p. 23)

A figura 7 sintetiza alguns aspectos relevantes sobre as funções dos principais agentes que classicamente estão envolvidos na estrutura de GRC das entidades e a interrelação entre eles:

- Conselho de Administração: como órgão supremo da Governança, dá diretrizes gerais sobre as políticas de risco recebe reporte da Administração Executivo, Comitê de Gestão de Riscos e Auditoria.
- Comitê de Gestão de Riscos: órgão da governança interna focado na temática de riscos corporativos, dá diretrizes à 2ª linha de defesa em sua função de provedor de diretrizes, execução de acompanhamento e apoio das áreas de negócio e suporte e recebe deste reporte sobre o andamento dos trabalhos e pontos de atenção.
- Administração Executiva (também denominada como 1ª linha de defesa (IBGC, 2017)): recebe as diretrizes da governança e, na condição de proprietária dos riscos, atua para que sejam mitigados a níveis tolerados pela Companhia, através de controles internos.
- Diretoria de Gestão de Riscos (também denominada como 2ª linha de defesa (IBGC, 2017)): recebe as diretrizes da governança e auxilia as áreas de negócios e de suporte na mitigação de seus riscos, seja pela indicação de diretrizes, suporte técnico, acompanhamento da efetividade e evolução das mitigações:
- Auditoria (também denominado como 3ª. linha de defesa (IBGC, 2017)): atua como agente integralmente independente dentro da Entidade para avaliar a efetividade do sistema de controles internos e implementação das diretrizes estabelecidas pela Governança da Companhia, além de fazer indicações sobre melhorias.

Como reconhecido pelo IBGC (2017), os papéis desses agentes variam em função de cada entidade e da forma como está organizada. Na seção 2.6.1, detalharemos o que é considerado como a função esperada desses agentes.

2.5 Principais agentes do modelo de GRC

No quadro seguinte, apresenta-se uma síntese elaborada pelo autor com base nos principais papéis dos agentes em relação ao sistema de governança de riscos corporativos, conforme recomendado pelo IBGC (2017). Essa visão reflete a atual

legislação societária brasileira e precisa ser contextualizada às realidades das organizações, em seus distintos portes, segmentos e estruturas:

Quadro 17: Agentes e suas principais funções em GRC

Agente	Principais Funções
Conselho de Administração	<ul style="list-style-type: none"> - Determinar o perfil de risco e apetite de risco. - Monitorar o funcionamento do processo de gestão de risco e os planos de ação definidos em resposta aos riscos relevantes. - Monitorar os sistemas internos de controles internos em resposta aos principais riscos. - Avaliar se GRC da empresa é adequado e tem os recursos suficientes. - Assegurar a implementação de controles efetivos para a continuidade de negócios e segurança da informação; - Monitorar os alinhamentos críticos: estratégia, riscos, controles, conformidade, incentivos e pessoas.
Conselho Fiscal	<ul style="list-style-type: none"> - Conhecer os processos, mapa de riscos, indicadores chaves de risco, a estrutura de controles internos, os riscos monitorados, os controles chaves e a adequação de pessoal e orçamento. - Dialogar com os agentes da Organização envolvidos no processo de GRC para formar sua opinião sobre os atos da Administração. - Definir formatos e periodicidade da informação sobre GRC para cumprimento do seu papel de fiscalização.
Comitê de Auditoria	<ul style="list-style-type: none"> - Supervisionar à aderência às normas legais, estatutárias e regulamentares. - Supervisionar a adequação dos processos de GRC e ao sistema de controles internos, em linha com as diretrizes do Conselho de Administração.
Diretoria	<ul style="list-style-type: none"> - <i>Tone of top</i> com direcionamento aos altos executivos. - Conhecer os principais riscos e a forma como são mitigados. - Monitorar que o apetite de riscos seja observado. - Revisar periodicamente os principais direcionadores de GRC, com base nas diretrizes dadas pelo Conselho.
Primeira linha de defesa: gestores das unidades de negócio	<ul style="list-style-type: none"> - Donos dos riscos. - Responsável pela aplicação da adequada e consistente mitigação / controles internos.
Segunda linha de defesa	<ul style="list-style-type: none"> - Fixar as políticas, estruturas e metodologias para identificar, analisar e efetivamente gerenciar seus riscos. - Garantir que as diretrizes dadas pelo Conselho estejam operando adequadamente. - Identificar questões atuais e emergentes que impactem a avaliação dos riscos. - Identificar mudanças no apetite de riscos. - Auxiliar a primeira linha a desenvolver processos e controles para gerenciar riscos. - Prestar contas ao Conselho e Comitês de Assessoramento.

Terceira linha: auditoria interna	<ul style="list-style-type: none"> - Avaliar a confiança das informações e revisar a efetividade e a eficiência das operações da Companhia, que impactam a GRC. - Examinar o sistema de controles internos, provendo à alta Administração avaliação sobre sua efetividade. - Monitorar, examinar, avaliar e recomendar melhorias e adequação no ambiente interno.
--------------------------------------	--

Fonte: Elaborado pelo autor (2023), com base no IBGC (2017).

2.5.1 Avaliação da maturidade em GRC

Segundo Bramont (2013), modelos de maturidade referem-se aos processos de desenvolvimento de uma entidade ou classes de objetos.

Como premissa, os modelos de maturidade pressupõem um caminho estruturado, com estágios sequenciais, que podem ser decompostos e nos quais possam ser observados algumas características específicas e averiguáveis em cada fase. Conseqüentemente, quanto mais elevado o nível de maturidade avaliado, mais bem desenvolvida está aquela Organização no tema.

Segundo Bramont (2013, p. 44), a adoção de um modelo de maturidade permite que seus executivos:

- (1) Visualizem a atual performance da sua Companhia e comparem-na com outras;
- (2) Estipulem metas e planos de melhoria coerentes com a situação atual da empresa;
- (3) Avaliem quão distante está sua empresa das metas desejadas;
- e (4) Estimulem a disseminação de boas práticas e seu aprimoramento contínuo. (BRAMONT, 2013, p. 44)

Poltronieri, Gerolamo e Carpinetti (2015, p. 3) em artigo sobre avaliação da gestão de sistemas integrados vão na mesma direção:

Os modelos de maturidade auxiliam na melhoria do desempenho organizacional, ajudando a identificar os pontos fracos e fortes, contribuindo para o benchmarking (Khoshgoftar & Osman, 2009). A representação da maturidade por meio de número de estágios acumulativos facilita a visualização de onde a empresa está e quanto falta para ela atingir as melhores práticas, sendo que os estágios mais baixos servem de suporte para atingir os requisitos dos estágios mais altos (Maier *et al.*, 2012). (POLTRONIERI; GEROLAMO; CARPINETTI, 2015, p. 3)

A *Risk and Insurance Management Society* (RIMS, p. 4), organização sem fins lucrativos dedicadas ao estudo de temas associados a riscos corporativos, fundada em 1950, sediada em Nova York representando quase 4.000 entidades e quase 10.000 profissionais de risco em distintas geografias explicitou no estudo em que lançou seu Modelo de Maturidade de Risco em 2006 (livre tradução):

O Modelo de Maturidade é um método com comprovada utilização em uma variedade de indústrias. Baseado em extensos estudos de caso dos últimos 25 anos em que um Modelo de Maturidade fora utilizado, as evidências mostram que a cada passo no nível de maturidade, as organizações obtêm resultados concretos. (*RISK AND INSURANCE MANAGEMENT SOCIETY*, 2006, p. 4)

No mesmo documento, a RIMS (2006, p. 4) indica os benefícios de sua utilização. Citamos os principais deles em uma tradução livre:

(1) Cria consenso e estabeleça marcos, (2) benchmarking das melhores práticas, (3) maior clareza na comunicação com os órgãos de Governança, reguladores, agências de rating, executivos gerenciamento, responsáveis pelos processos, áreas de suporte, back office, auditoria interna, TI e compliance, etc., (4) Mede o valor da gestão de riscos corporativos, (5) Criar uma linguagem e uma visão compartilhadas entre os agentes de mercado e (6) construção de um processo escalável para melhor tomada de decisão. (*RISK AND INSURANCE MANAGEMENT SOCIETY*, 2006, p. 4)

Ao discorrer especificamente sobre modelos de maturidade da gestão de riscos corporativos, Meirelles (2018), citando Cuenca, sintetiza a relevância dos modelos de avaliação da maturidade da gestão de riscos corporativos como o de avaliar a maturidade de uma empresa no gerenciamento de risco corporativo, justifica-se por ajudar a entender a situação organizacional e auxiliar a identificar a forma mais adequada de melhorar o sistema.

Oliva *et al.* (2021, p. 3), estudioso brasileiro das temáticas de Riscos Corporativos também discorreu sobre os modelos de avaliação de maturidade na gestão de riscos:

Para auxiliar as organizações a avaliarem seus estágios de capacidade e cumprirem processos de negócio, a literatura acadêmica e o ambiente corporativo desenvolveram modelos de maturidade aplicados à gestão, que consistem, em linhas gerais, em avaliar por meio de indicadores, qual o status atual do processo em que uma empresa se encontra e quais as lacunas, permitindo o desenvolvimento de um plano para avanço ou melhoria do processo. (OLIVA *et al.*, 2021, p. 3)

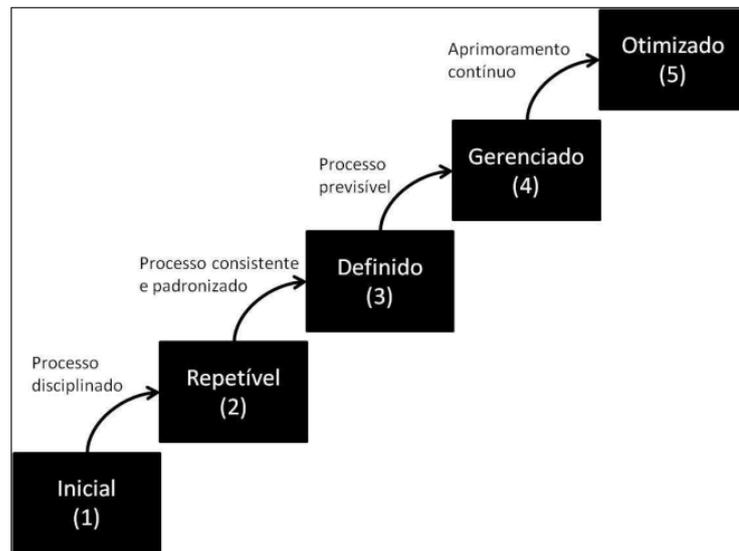
Os modelos são na visão de Röglinger (2011) (a) descritivos – identificam a situação atual, (b) prescritivos – permitem avaliar os *targets* desejados e as recomendações de ações a serem adotadas e (c) comparativo entre unidades de negócio e Companhias.

Alguns estudos foram precursores e ajudaram muito na formatação dos modelos de maturidade, influenciando inclusive àqueles adotados atualmente.

- Modelos de Greiner: na década de 1970, indicou que as empresas em fase de crescimento passavam por fases definidas e sequenciais e que seria possível avançar para a fase posterior se fossem adotadas práticas gerenciais adequadas abrangendo foco gerencial, sistemas de controle e mecanismos de incentivo e recompensa. Dentre as contribuições de Greiner, tem-se as constatações de que (a) as empresas diferentes desenvolvem-se segundo estágios definidos e previsíveis, (b) é relevante saber em que etapa a organização se encontra em seu processo de desenvolvimento e (c) a empresa precisa aprimorar e modificar práticas estruturadas e conscientes.
- Modelo de Crosby: em 1979, o autor estabeleceu estudo sobre desenvolvimento da qualidade, com foco em aspectos internos das Organizações. A partir de 6 critérios / perguntas, ele estabeleceu uma escala de avaliação com 5 estágios. Dentre as contribuições estabelecidas, temos: (a) constatação de que funções ou departamentos dentro de uma empresa podem ter diferentes estágios de maturidade, (b) padronizações podem ser atributos relevantes na maturidade das Organizações, (c) níveis de maturidade servem para a comparação entre Organizações distintas.
- *Capability Maturity Model* (CMM): nasceu de uma demanda da Marinha Americana feita na década de 1980 para o *Software Engineering Institute* – SEI para estabelecimento de um método que permitisse a avaliação da capacidade de prestadores de serviços de softwares. Bramont (2013) exhibe uma ilustração que sintetiza a visão dos estudos de CMM, que representavam patamares progressivos, saindo de um cenário com processos desestruturados, desorganizados e sem previsibilidade para um cenário com processos

gerenciados, gerenciados, institucionalizados e permanentemente aprimorados.

Figura 8: Níveis de maturidade do CMM

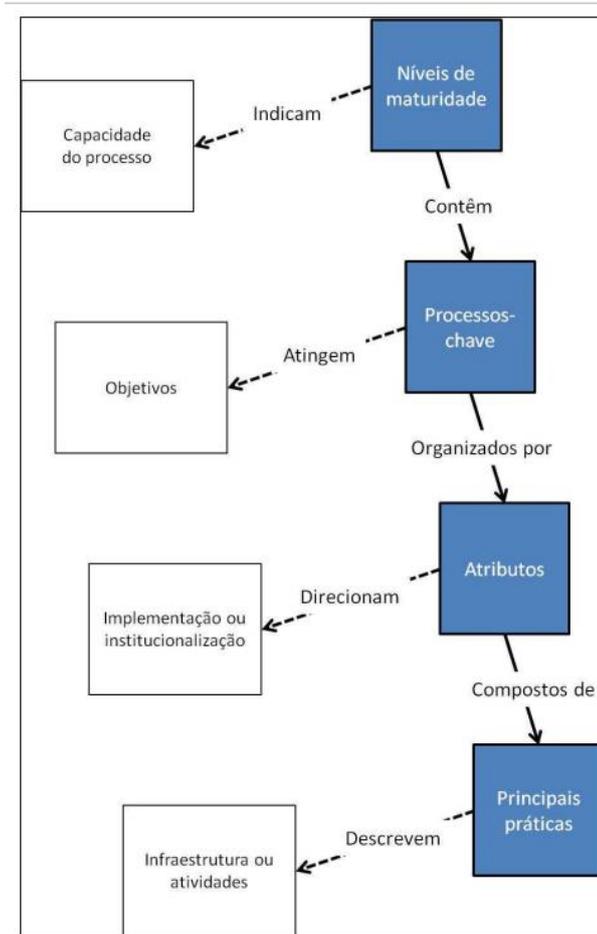


Fonte: Bramont (2013, p. 48)

Ao discorrer sobre como atuava o CMM, Bramont (2013, p. 48) explica:

Cada nível de maturidade é composto de diversos e exclusivos processos-chaves, os quais indicam áreas que devem ser priorizadas (...) e, assim, atingir gradativamente novos níveis. (...) Cada processo-chave, por sua vez, contém uma série de objetivos específicos, alcançáveis mediante a adoção de atividades inter-relacionadas. (BRAMONT, 2013, p. 48)

Figura 9: Encadeamentos do CMM



Fonte: Bramont (2013, p. 49)

As principais contribuições trazidas pelo *Capability Maturity Model* incluem (a) detalhamento dos níveis de maturidade, com metas objetivas, (b) institucionalização de boas práticas como atributo da maturidade organizacional, (c) utilização do modelo para seleção de empresa.

Tendo percorrido os aspectos gerais sobre Modelo de Maturidade, demonstrar-se-á na sequência os Modelos que foram identificadas na revisão da literatura e mais frequentemente citadas, além de um breve sumário sobre suas características e o contexto em que foram propostos, além de outros dados que permitam a compreensão de seus principais aspectos.

2.5.1.1 Abordagem de Hillson

Ao discorrer sobre a Gestão de Risco, Hillson (1997, p. 44) sintetiza:

A implementação da gestão de riscos corporativos não é um item menor e não pode ser estabelecida em um curto período. Também não é um processo de aplicação de técnicas, de treinamento de times ou aquisição de softwares. A habilidade de gerenciar risco é um espectro amplo, através de rotinas formais e incorporado à cultura da Organização. (HILLSON, 1997, p. 44)

Proposto em 1997, o autor capitula os objetivos de seu modelo da seguinte forma (em livre tradução) no artigo publicado:

Organizações que desejam implementar um modelo formal de gestão de riscos ou aprimorar a abordagem existente, precisam de um modelo de referência. Benchmarks das melhores práticas podem ser agrupados em níveis de maturidade, usualmente associados com sofisticação e melhorias desses estágios. O modelo de referência tem quatro níveis, cada um deles associados a atributos. As Organizações podem usar esse modelo para acessar seu estágio atual, identificar targets factíveis de melhoria e elaborar e implementar planos de ações para desenvolver e aprimorar suas habilidades de gestão de risco. (HILLSON, 1997, p. 35)

Ao revisar o modelo de Hillson, Meirelles (2018), sintetiza conforme demonstrado no Quadro 18 as características do modelo proposto:

Quadro 18: Sumário do Modelo de Maturidade de Hillson

	Nível 1 Naive ou Ingênuo	Nível 2 Novice ou Novato	Nível 3 Normalised ou Normalizado	Nível 4 Natural
Definição	Não está ciente da necessidade de gerenciamento de risco. Não possui estrutura para lidar com incertezas. Processo de gerenciamento repetitivo e reativo. Pouco ou nenhum aprendizado com o passado ou preparação para o futuro.	Tentativa de gerenciamento de risco através de um pequeno número de colaboradores. Não possui estrutura formal. Cliente dos benefícios do gerenciamento de risco, mas com implementação ineficiente e com ganhos parciais de benefícios.	Gerenciamento de risco construído sobre processos de negócios de rotina. Gerenciamento de risco implementado nos principais ou em todos os projetos. Estrutura geral de gerenciamento de risco formalizada. Benefícios concedidos em todos os níveis da Organização, ainda que não alcançados plenamente.	Cultura de sensibilização a risco, com gerenciamento de risco em todos os processos de negócios. Uso ativo de informações de risco para incremento dos processos de negócios e ganho de vantagem competitiva. Ênfase em gerenciamento de oportunidade ("positive risk").

Cultura	Sem sensibilização para riscos. Resistente / relutante à mudança. Tendência a continuar com os processos existentes.	Processos de risco são vistos como custos adicionais com benefícios variáveis. Gerenciamento de risco apenas para processos selecionados.	Política de gerenciamento de riscos aceita. Benefícios reconhecidos e esperados. Preparada para comprometer recursos para obter ganhos.	Comprometimento com gerenciamento de risco, tendo a alta direção como exemplo. Gerenciamento de risco proativo, encorajado e remunerado.
Processos	Sem processos formais.	Sem processos formais, embora alguns métodos específicos possam estar em uso. Efetividade do processo depende das habilidades do time interno e de suporte externo.	Processos genéricos aplicados a todos os projetos. Processos formais, incorporados ao sistema de qualidade. Orçamento para gerenciamento de riscos alocado em todos os níveis da organização. Necessidade limitada de suporte externo.	Processos de negócios baseados em risco. Total Risk Management permeando todo o negócio. Revisão e atualização regular dos processos. Métricas de gerenciamento de risco com constante feedback para melhoria de performance.
Experiência	Sem entendimento dos princípios ou linguagem de risco.	Limitado a colaboradores com pouco ou nenhum treinamento em gerenciamento de risco.	Time interno e experts, treinado nas habilidades básicas. Desenvolvimento de processos e ferramentas específicas.	Toda a equipe com atitude de sensibilização a riscos e conhecimento básico da metodologia. Aprendizado com a experiência como parte do processo. Treinamentos externos regulares para aperfeiçoar habilidades.
Aplicação	Sem aplicação estruturada. Sem recursos dedicados. Sem ferramentas de gerenciamento de risco.	Aplicação inconsistente. Disponibilidade variável do time interno. Ferramentas e métodos desenvolvimentos internamente (ad hoc).	Aplicação consistente e rotineira a todos os projetos. Recursos alocados. Conjunto integrado de ferramentas e métodos.	Gerenciamento de risco como uma segunda natureza, aplicado a todas as atividades. Reportes e tomadas de decisões baseadas em riscos. Ferramentas de métodos no estado da arte.

Fonte: Meirelles (2018, p. 104)

No artigo em que publicou o modelo, Hillson chama atenção para que os planos de aprimoramento estabelecidos sejam coerentes e factíveis. Portanto, pressupõe-se que a evolução deve ocorrer nível a nível.

No quadro a seguir, está um sumário da progressão indicada pelo autor para evolução para o estágio seguinte, com as principais características desta progressão.

Quadro 19: Progressão entre os níveis – Modelo de Hillson

Progressão	Principais ações
Nível 1 para Nível 2	Contratação de consultoria especializada, seleção de time interno, estabelecer “patrocinador” de GRC, programa interno de comunicação abrangente, identificação de métricas que serão utilizadas, estabelecimento de métodos e procedimentos.
Nível 2 para Nível 3	Fortalecimento do time interno com autonomia e formação complementar, extensão da gestão de risco para outros departamentos, alocar recursos, inclusive orçamentário, divulgar iniciativas bem-sucedidas, consolidar procedimentos, estabelecer controles transacionais.
Nível 3 para Nível 4	Processo de aprendizagem contínuo, revisão permanente do processo para que seja sempre efetivo, garantir que todos os processos relevantes estejam cobertos pela Gestão de Riscos Corporativo, vincular a tomada de decisão com as práticas de GRC, por meio de uma cultura Total Risk Management. Manter time interno engajado, divulgando métricas e promovendo ajustes e aprimoramentos nas práticas de GRC.
Manutenção do Nível 4	Garantir envolvimento e comprometimento da Alta Administração. Manter padrões de GRC, com revisões periódicas e auditoria. Manejar oportunidades, evidenciando os benefícios da prática.

Fonte: Meirelles (2018, p. 104); adaptado pelo autor.

2.5.1.2 Abordagem de Poltronieri *et al.*

Poltronieri *et al.*, em artigo de 2014, apresentaram uma pesquisa da literatura, elaborando na sequência um modelo de Avaliação de Maturidade Empresarial em Sistemas de Gestão Integrado (SGI), de aplicação bastante ampla e, portanto, possível de utilização em realidades, inclusive na avaliação das práticas de Gerenciamento de Riscos Corporativos.

O modelo propõe a classificação da maturidade em 5 níveis – de 1 a 5, descrevendo para cada um deles aspectos a serem avaliados nas dimensões (a) Política, (b) Planejamento, (c) Implementação e Execução e (d) Verificação e Ação.

Conforme demonstrado no Quadro seguinte, nas 4 áreas/dimensões, os autores identificaram 21 pontos abordados que devem ser estudados para o enquadramento nos níveis que permitirão avaliar o estágio de maturidade (descritos na coluna # Questões).

Quadro 20: Sumário dos Instrumentos do Modelo de Poltronieri

# Itens	Área	Pontos Abordados
4	Política	1) existência de política integrada 2) participação da alta administração 3) atualização e documentos 4) divulgação
6	Planejamento	1) elaboração 2) equipe 3) objetivos e metas 4) manual 5) procedimentos/instruções/registros 6) controle de procedimentos/instruções/registros
7	Implementação / Execução	1) controles operacionais 2) funções/responsabilidades/autoridades 3) equipe 4) recursos 5) treinamentos 6) comunicação 7) monitoramento
4	Verificação / Ação	1) auditoria interna 2) auditoria externa 3) não conformidade / ações corretivas e preventivas 4) análise da Administração

Fonte: Poltronieri *et al.* (2014, p. 8)

Abaixo, uma breve explanação sobre o que é característico a cada nível do modelo de avaliação.

Quadro 21: Níveis de Maturidade do Instrumento de Avaliação dos SGI

Nível 1	A Organização não consegue trabalhar suas normas de modo integrado. Quando ocorre alguma iniciativa de integração, nota-se que não é sólida e, ao menor grau de dificuldade, a integração pode ser desfeita. Os benefícios não são aparentes.
Nível 2	É possível notar uma efetiva integração em alguns pontos das normas e mesmo as partes não integradas estão alinhadas entre elas, evitando que uma norma contradiga a outra.
Nível 3	A integração já é uma realidade. Praticamente 100% dos requisitos se encontram integrados. O problema é que a integração não trouxe os benefícios esperados, talvez em parte por não ter sido feita de forma adequada ou por falta de conseguir levantar corretamente os benefícios reais, ficando a sensação de que não foi tão benéfico quanto deveria.

Nível 4	A integração é total e se encontra fortemente ligada ao planejamento estratégico, sendo que no desdobramento do plano estratégico estão indicadores quantitativos diretamente relacionados com os objetivos do SGI.
Nível 5	Há uma revisão contínua dos indicadores quantitativos definidos no nível 4.

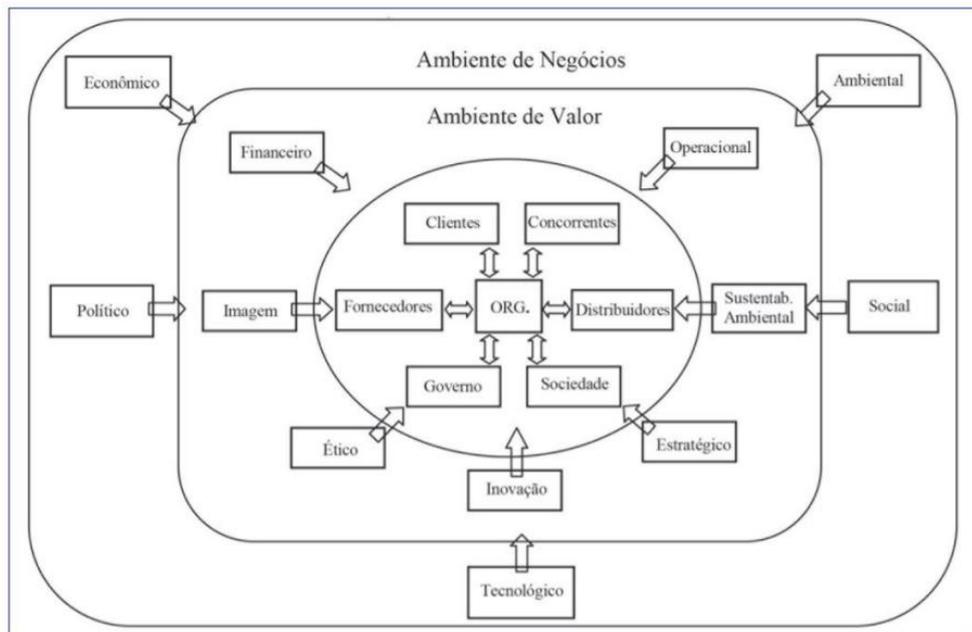
Fonte: Poltronieri *et al.* (2014, p. 7)

2.5.1.3 Abordagem de Oliva

Conforme estamos observando na revisão e relato dos modelos de avaliação da maturidade da Gestão de Riscos, grande parte deles incluem etapas equivalentes e foco nos aspectos internos da Companhia.

Reconhecendo a relevância dos aspectos externos às Organizações, Oliva propôs no artigo “*A maturity model for enterprise risk management*” de 2016, um modelo de análise de risco no ambiente de negócios da empresa.

Figura 10: Riscos Corporativos no Ambiente de Negócios



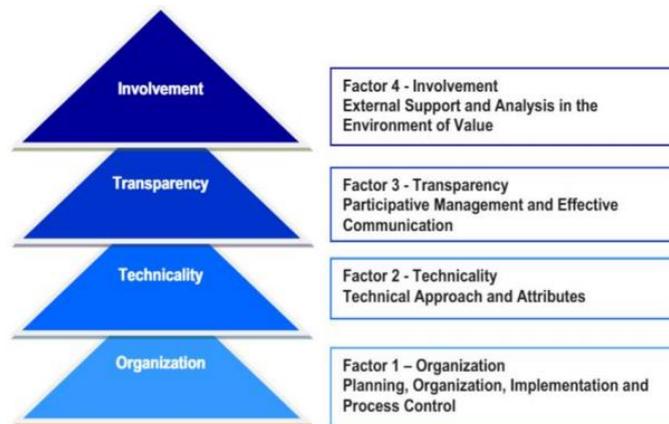
Fonte: Oliva (2016, p. 5)

No mesmo estudo, ao explicar esse modelo, Oliva (2016, p. 3):

Este ambiente é dividido em macroambiente e microambiente. De acordo com o autor, o macroambiente é composto pelas forças ambientais que podem afetar os objetivos da organização que, por sua vez, não possui controle sobre seus acontecimentos. As principais forças do macroambiente são: econômicas, sociais, políticas, tecnológicas e ambientais. Já o microambiente é composto pelos principais agentes, sendo eles os clientes, concorrentes, fornecedores, distribuidores, governo e sociedade, e pelas forças que se manifestam por meio do poder de barganha, oportunismo, inovação e estratégia destes agentes. As relações estabelecidas entre a empresa e os demais agentes podem gerar riscos e, portanto, devem ser consideradas no processo de GRC. (OLIVA, 2016, p. 3)

No estudo em questão, em que propôs um modelo de mensuração, o autor optou por não definir no início os aspectos para determinação da maturidade de risco. Para esta definição, realizou pesquisa com 243 empresas, dentre as 1.000 maiores Companhias brasileiras e, com base nos resultados da pesquisa, indicou quatro fatores de avaliação, conforme figura extraída do referido artigo.

Figura 11: Fatores de capacidade Modelo Oliva



Fonte: Oliva (2016, p. 9)

Os fatores identificados refletem uma ordenação em que a adequada tecnicidade pressupõe um nível adequado e suficiente de organização, a adequada transparência pressupõe um nível adequado e suficiente de tecnicidade e, assim por diante. Segundo Oliva (2016, p. 4):

(1) Organização: Esforço dedicado pela empresa para estruturar sua gestão de riscos, tais como planejar, organizar, implementar e controlar a forma como os riscos serão geridos;

(2) **Tecnicidade:** É o desenvolvimento de atributos técnicos para suportar a gestão de riscos;

(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;

(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. (OLIVA, 2016, p. 4)

Com base nisso, o autor estabeleceu um Modelo em que as empresas são enquadradas em cinco níveis, conforme sumário apresentado no quadro seguinte:

Quadro 22: Estágios do Modelo de Oliva

Nível	Principais características
Nível 1 Insuficiente	Baixa consciência dos riscos e atuação não estruturada na gestão de riscos, não disseminando práticas e procedimentos organizados que resultem na avaliação contínua e tempestiva dos riscos.
Nível 2 Contingência	Consciência dos riscos aos quais estão sujeitos, aplicação de técnicas e ferramentas para auxílio da GRC, sem engajamento dos colaboradores na cultura de riscos.
Nível 3 Estruturado	Maior grau de controle e estruturação dos temas de riscos, com adoção de ferramentas, técnicas e métodos que auxiliam na tomada de decisão e mitigação dos riscos. Capilaridade do assunto por meio dos empregados.
Nível 4 Participativo	Profundidade na frente de riscos corporativos – tem comunicação e conscientização como aliados no controle de seus processos de GRC, que ocorre descentralizadamente. Elevado engajamento dos empregados.
Nível 5 Sistêmico	Forte transparência no tratamento de riscos e cultura que empodera os empregados e dissemina conhecimento. Utilização de conhecimentos externos e aprimoramento permanente das práticas de GRC. Visão ampliada dos riscos, incluindo aspectos externos.

Fonte: Meirelles (2018, p. 43); adaptado pelo autor

2.5.1.4 Abordagem de RIMS

A *Risk and Insurance Management Society* (RIMS) também desenvolveu e tornou público um modelo de mensuração da maturidade do Risco Corporativo.

Segundo Farrell e Gallagher (2015):

Desenvolvido em 2006, o modelo de Maturidade de Riscos da RIMS foi conceituado com base no Capability Maturity Model Integration, um modelo desenvolvido pelo Software Engineering Institute. Ele abrange vários estudos referenciais de riscos como ISO 31.000, BS31100, FERMA (2002) e COSO (2004). Este modelo de maturidade de riscos é utilizado em inúmeras indústrias para avaliação e benchmark, permitindo às Organizações mensurar sua performance no caminho da maturidade desejada. (FARRELL E GALLAGHER, 2015)

O Modelo da RIMS é baseado em 7 atributos, conforme sumário apresentado no quadro seguinte construído pelo autor, com base no detalhamento apresentado pela própria entidade:

Quadro 23: Modelo de maturidade de riscos da RIMS

Atributo	Foco	Mensuração da maturidade
Abordagem geral de GRC	Extensão e nível de suporte da Administração para GRC	Comunicação em decisões cotidianas e habilidades em gestão de risco como requisito para posições de liderança
Processo de gestão de riscos corporativos	Como a GRC está integrada às práticas cotidianas. Extensão e consistência de como o processo de gestão de riscos está incorporado às várias unidades de negócio através da gestão quantitativa e qualitativa dos riscos, reportes adequados e tempestivos, além de funções claras associadas ao GRC.	Comunicações fluídas e em toda a empresa sobre as iniciativas de risco e efetivo empoderamento dos funcionários nas práticas de gestão de riscos
Apetite de Risco	Nível de compreensão adequado sobre os trade-offs envolvendo a gestão de risco e exposição aos riscos que permita a maximização das oportunidades.	Aprimoramento da compreensão interna sobre risco-retorno na gestão de riscos.
Foco em causa raiz	Habilidade em identificar proativamente a causa raiz, visando	Entendimento dos eventos passados como parte da avaliação da frequência e impacto dos riscos

	evitar ou minimizar os impactos indesejados. Aprimorar a disciplina e foco no entendimento das causas raízes.	
Identificação de riscos	Habilidade permanente em mensurar os riscos e gerar comunicações precisas e tempestivas. Qualidade e cobertura do processo de identificação e documentação dos riscos que permita auxiliar às mitigações posteriores.	Abrangência das distintas fontes utilizadas na identificação como conhecimento dos funcionários, bases de dados e outras que permitam correlações. Indicadores relevantes de riscos utilizados pelas várias áreas.
Gerenciando incertezas	Nível de habilidade da empresa em conciliar seus objetivos estratégicos em conjunto com a gestão de seus riscos.	Comunicação sobre os objetivos estratégicos. Identificação, mensuração e reporte de desvios que impactam os objetivos estratégicos.
Resiliência e sustentabilidade do negócio com o gerenciamento de eventos indesejados de grande impacto	Habilidades em identificar tempestivamente eventos indesejados.	Balanceamento entre os entregáveis de curto e longo prazo. Inclusão de testes de stress e análise de cenários visando compreender e evitando o que pode dar errado, contribuindo para o crescimento e continuidade do negócio.

Fonte: RIMS (2016, p. 9), adaptado pelo autor

Com base nesses atributos, o modelo proposto pela RIMS prevê a segregação das Organizações em um dos 5 estágios descritos no quadro seguinte, com base na maturidade da Gestão de Riscos Corporativos efetuada:

Quadro 24: Níveis do modelo da RIMS

Nível	Característica
1. Ad Hoc	Níveis básicos de GRC, com dependência das ações de certos indivíduos, com baixa consistência, compreensão e disseminação dos processos.
2. Inicial	Gestão de riscos em silos, com baixa integração. Baixa disciplina e rigor na aplicação dos processos.
3. Escalável	Framework Organizacional define as diretrizes da atuação de GRC, com aplicável estável e consistente de práticas.

4. Gerenciado	Processos da jornada de GRC como identificar, mensurar, monitorar e reportar são integrados e mitigados pela aplicação consistente de controles. Os procedimentos associados ao GRC são comunicados e compreendidos em toda a Organização, além de integrados à gestão estratégica.
5. Líder	Discussões estratégicas de longo prazo envolvendo alocação de capital, planejamento e processo de decisão consideram a gestão de risco. Apetite de risco é claramente compreendido e considerado pela Alta Administração em suas decisões.

Fonte: RIMS (2016, p. 9), adaptado pelo autor

Na apresentação de seu modelo, trazendo contexto e motivações que se assemelham ao enunciado aqui nos capítulos anteriores, a RIMS (2006, p. 10) conclui (livre tradução):

Nenhuma empresa pode manifestar com confiança que estabeleceu um programa de Gestão de Riscos se não puder medi-lo. E um conjunto de diretrizes empíricas sólidas para medir a competência da GRC é fundamental. Estas orientações, elaboradas para entregar valor, também permitem avaliar o progresso da jornada. (*RISK AND INSURANCE MANAGEMENT SOCIETY*, 2006, p. 10)

2.5.1.5 Abordagem de M_o_R

O *Management of Risk Methodology* (M_o_R) é um modelo britânico, focado no Gerenciamento de Riscos Estratégicos, de Programas, de Projetos e Operacionais.

Também contém princípios, processos, técnicas, boas práticas, documentos e guia de verificação do Gerenciamento de Riscos eficaz.

O Método foi criado pelo Governo Britânico – pelo *UK Office of Government Commerce* (OGC) - para uso do próprio Governo. Contudo, fornece orientações gerais para que organizações de diferentes origens e segmentos possam colocar em prática um *framework* no segmento da Gestão de Riscos.

O M_o_R ainda fornece uma escala de maturidade para apoiar os gestores e a Alta Administração definirem os objetivos quanto à evolução da gestão de riscos e a sua maturidade na organização, segregada em 5 níveis (desde o inicial, mais incipiente até o otimizado, mais maduro), demonstrado nas colunas da Figura seguinte

e com base em 8 pilares que permitem avaliar a estrutura de GRC na Entidade, incluindo (1) alinhamento com os objetivos, (2) adequação ao contexto da Organização, (3) envolvimento dos stakeholders, (4) definição de um processo, (5) alinhamento ao processo de tomada de decisão, (6) melhoria contínua do próprio modelo em si, (7) cultura organizacional colaborativa e disseminada e (8) habilidade de implementar e mensurar ações. A figura a seguir denota a escala elaborada, conforme tradução e adaptações de Bermejo (2018):

Quadro 25: Escala de maturidade M_o_R

	Nível 1 Inicial	Nível 2 Repetitivo	Nível 3 Definido	Nível 4 Gerenciado	Nível 5 Otimizado
Alinhado aos objetivos	Os objetivos não estão definidos.	Riscos associados a objetivos definidos.	Objetivos definidos e atualizados durante a gestão de riscos.	Objetivos alterados conforme resposta aos riscos.	Objetivos definidos conforme a gestão de riscos.
Adequado ao contexto	Contexto não refletido na identificação.	O contexto é examinado ao longo do processo de risco.	O contexto é rigoroso.	Os gerentes informaram com antecedência sobre o contexto.	O contexto é usado para definir ações da gestão.
Envolve stakeholders	Nem todos os stakeholders são consultados.	Os stakeholders são identificados e minimamente engajados.	Os objetivos dos stakeholders são identificados, registrados, alinhados e atribuídos.	Os stakeholders são ativamente envolvidos.	Os stakeholders são incentivados e envolvidos no ciclo de investimento.
Processo definido	Política e processos não documentados e vagos.	A política e os processos estão definidos.	Processos uniformes são adotados em toda a Organização.	A gestão de riscos está totalmente integrada às atividades dos gerentes.	Melhores práticas são identificadas e compartilhadas na organização.
Tomada de decisão	Não há definição de limites operacionais, revisões ou relatórios.	Relatórios de gestão são emitidos consistentemente e em prazos definidos.	Gerentes seniores reportam em um formato consistente.	Existem análises quantitativas de qualidade.	Técnicas de planejamento de cenários são naturalmente utilizadas.
Melhoria contínua	Ausência de treinamentos e de conhecimento sobre gestão de riscos.	As pessoas são treinadas ao longo da implantação da gestão de riscos.	Diferentes níveis de treinamento estão definidos.	Pessoal experiente analisando resultados quantitativos.	Conhecimentos e habilidades atualizados constantemente.

Cultura colaborativa	A equipe age por conta própria em grupos independentes.	Os donos dos riscos, os gerentes e os agentes estão identificados.	Times integrados na organização com papéis e responsabilidades	Atitudes de gestão de riscos são reconhecidas e condecoradas.	Riscos estão apenas na organização, presentes nas descrições dos cargos.
Valores mensuráveis	Sem mensurações.	Mensurações dos processos, mas não de desempenho.	Medidas de desempenho implantadas.	Medidas de desempenho demonstram o alcance de valor.	Alcance de valor mensurável para stakeholders internos e externos.

Fonte: Bermejo (2018, p. 65)

2.5.1.6 Abordagem do IBGC

O Instituto Brasileiro de Governança Corporativa (IBGC) é uma organização sem fins lucrativos e um dos principais fóruns nacionais em governança corporativa e temas correlacionados. O Instituto participa de redes internacionais que congregam institutos relacionados à governança e Conselho de Administração ao redor do mundo como o *Instituto Gobierno Corporativo de Latino América (IGCLA)* e o *Global Network of Director Institutes (GNDI)*.

Segundo a seção institucional de sua página na Internet, o IBGC complementa sua apresentação:

O instituto contribui para o desempenho sustentável das organizações por meio da geração e disseminação de conhecimento das melhores práticas em governança corporativa, influenciando e representando os mais diversos agentes, visando uma sociedade melhor. (...) Fundado em 27 de novembro de 1995, em São Paulo, o IBGC desenvolve programas de capacitação e certificação profissionais, eventos e, também, atua regionalmente por meio de oito capítulos regionais (...). (Website IBGC, acessado em 2023)

Desde 1999, com o lançamento da primeira edição do Código das Melhores Práticas de Governança Corporativa, o Instituto passou a publicar uma série de documentos específicos no âmbito das boas práticas de governança corporativa.

Em 2017, publicou-se o “Gerenciamento de Riscos Corporativos: Evolução em Governança e Estratégia, apresentando os papéis dos principais agentes de governança e algumas das principais práticas recomendadas, auxiliando na

implementação de estruturas efetivas de gerenciamento de riscos que se conecte com a estratégia de longo prazo das Organizações.

O estudo também trata dos níveis de maturidade da prática de GRC. Segundo IBGC (2017, p. 33):

Existem distintas alternativas para a construção da governança de GRC e para chegar ao nível de maturidade desejado. Cada organização deverá desenhar aquela mais adequada ao seu perfil de negócio, cultura organizacional, modelo de gestão e nível desejado de maturidade em relação às suas práticas de GRC. (IBGC, 2017, p. 33)

Ainda, o estudo indica que o nível de maturidade é deveras influenciado pelos seguintes aspectos:

(1) As ações adotadas para alcançar suas metas e objetivos em relação ao GRC e ao sistema de controles internos; (2) O nível de esforço (tempo e investimento) empreendido para alcançar essas metas e objetivos; (3) Os resultados obtidos, assim como a eficácia e a eficiência das práticas implementadas; (4) O nível de envolvimento dos profissionais em relação a essas práticas e (5) O nível de entendimento da maturidade da organização, assim como das oportunidades de melhorias. (IBGC, 2017, p. 33)

Para formatar seu modelo de maturidade, o IBGC apresentou no estudo uma visão geral dos componentes de GRC integrados ao processo de governança corporativa da Organização, bem como algumas reflexões de referência, que entende auxiliarem para que a avaliação sobre o estágio atual possa ser realizada.

Quadro 26: Reflexões para mensuração da maturidade

#	Dimensão	Aspecto
1	Estratégia	a) Existem estratégias, objetivos e metas de GRC estabelecidos?
2	Governança	a) Existe estrutura organizacional com papéis e responsabilidades claramente definidos nas práticas de GRC? B) A estrutura considera papel do CA e da diretoria e de todas as três linhas de defesa detalhadas no modelo de governança de GRC?
3	Política	a) As questões acima mencionadas estão regimentadas, aprovadas e divulgadas por meio de uma política de GRC?

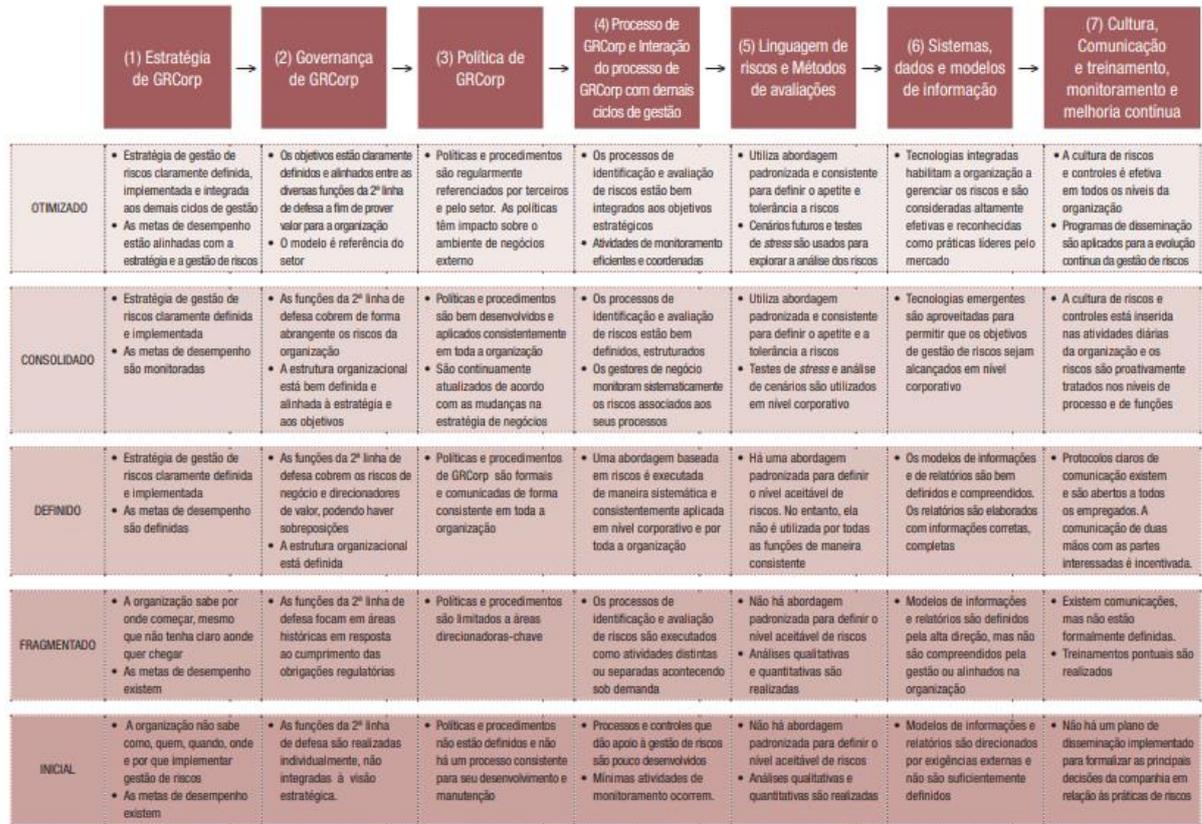
4	Processo de GRC e interação com demais ciclos de negócio	<p>a) Existe processo de GRC definido e implementado com atividades de identificação e avaliação de riscos, avaliação das atividades de controle, resposta, monitoramento e comunicação?</p> <p>b) Existe norma de gestão de risco (ou documento equivalente), de divulgação interna, que estabelece procedimentos, responsabilidades - inclusive de relato - segregação de funções, fronteiras de atuação e o sistema geral de governança da gestão de riscos?</p> <p>c) As práticas de GRC estão alinhadas às demais práticas de controle?</p> <p>d) Existe um modelo definido para a incorporação do GRC nos processos decisórios e nos ciclos de gestão?</p>
5	Linguagem e método de avaliação	a) A Organização utiliza-se de técnicas de mensuração?
6	Sistemas, dados e modelos de informação	a) As informações sobre a exposição de riscos da organização são compartilhadas com os diferentes níveis da organização e capturadas de forma consistente?
7	Cultura, comunicação, treinamento e melhoria contínua	<p>a) O GRC está incorporado na cultura da Organização?</p> <p>b) A Organização avalia o entendimento dos empregados em relação à cultura, às práticas de GRC e ao sistema de controles internos?</p> <p>c) As ações de comunicação e treinamentos de GRC são realizadas com os diferentes públicos da Organização?</p> <p>d) Os órgãos de governança e as três linhas de defesa monitoram permanentemente as práticas de GRC?</p>

Fonte: Elaborado pelo autor (2023), com base em IBGC (2017, p. 35)

Para que a mensuração ocorra, as Organizações devem avaliar a atual capacidade em relação às suas práticas e compreender por que e como serão aprimoradas.

Com base nessa interseção entre os principais componentes da Gestão de Riscos Corporativos e as autoavaliações correspondentes a cada uma delas, o IBGC propôs uma matriz de maturidade, segregada em 5 estágios: (1) inicial, (2) fragmentado, (3) definido, (4) consolidado e (5) otimizado.

Figura 12: Escala de mensuração da maturidade do IBGC



Fonte: IBGC (2017, p. 36)

Ainda, ao discorrer sobre o processo de mensuração, indica o IBGC (2017, p. 37):

Considerando que cada organização está inserida em um contexto externo e interno determinado pelo seu setor, nível de atuação e regulamentação, além de suas partes interessadas e modelo de negócio, para que possa se posicionar e obter o resultado da mensuração de sua maturidade é recomendado que avalie seu estágio em cada dimensão e, então, realize a autoclassificação nos níveis de maturidades propostos. Vale destacar que, em geral, as organizações apresentam maturidades distintas para cada dimensão analisada. Este fato é parte do processo. Cabe à própria entidade avaliar seu nível de maturidade em cada dimensão/estágio à luz de sua realidade e expectativas futuras em relação às práticas de GRCorp. (IBGC, 2017, p. 37)

Revisados os modelos disponíveis na literatura, que tratamos nessas seções, vê-se que existe convergência dos aspectos avaliados e da forma como as escalas são formadas.

Conforme o sumário do quadro 27, existem similaridades de alguns dos aspectos que são considerados na avaliação entre parte dos modelos, em que pese algumas delas serem expressas por nomenclaturas similares ou sinônimas. Os modelos de Hillson, Poltronieri e RIMS apresentam, de maneira geral, os grandes marcos associados com o processo de Gerenciamento de Riscos – similar a um ciclo PDCA (Plan, Do, Check, Act). Os demais modelos apresentam visão mais ampla, abrangendo outros aspectos além daqueles típicos do processo de identificação-mensuração-mitigação de riscos, incluindo o contexto ou análise do ambiente, o envolvimento da Gestão e cultura. No modelo de Oliva, o fator (a) Organização engloba o planejamento, implementação e o controle do processo, o fator (b) Tecnicidade engloba o suporte técnico necessário à implementação do gerenciamento dos riscos corporativos, o fator (c) Transparência engloba o gerenciamento participativo, com envolvimento da Alta Gestão e a comunicação das etapas do processo e o fator (d) Envolvimento inclui o suporte externo necessário ao processo e à análise do ambiente de Valor. O modelo do IBGC é o mais amplo entre os identificados na literatura em relação à abrangência dos aspectos que são considerados. Além daqueles que citamos acima e que estão presente nos demais modelos, o IBGC também abrange aspectos como comunicação interna, treinamento, modelos de captura e tratamento de informações, linguagem adotada no processo, aderência a frameworks, independência de área para tratar deste assunto, posicionamento funcional, entre outros.

Quadro 27 – Componentes dos Modelos de Mensuração de GRC

Componentes de avaliação					
Hillson	Poltronieri	Oliva	RIMS	M_o_R	IBGC
Definição	Política	Organização	Abordagem geral de GRC	Objetivos	Estratégia de GRC
Cultura	Planejamento	Tecnicidade	Processo de GRC	Contexto	Governança de GRC
Processos	Implementação	Transparência	Apetite de Risco	Envolvimento de stakeholders	Política de GRC
Experiência	Verificação	Envolvimento	Foco em causa raiz	Processo definido	Processo de GRC
Aplicação			Identificação de risco	Tomada de decisão	Linguagem de riscos e modelos de avaliação
			Gerenciando incertezas	Melhoria contínua	Sistemas, dados e modelos de informação
			Sustentabilidade do negócio	Cultura colaborativa	Cultura de GRC, comunicação e treinamento
				Valores mensuráveis	

Fonte: Síntese elaborada pelo autor com base nos modelos pesquisados (2023)

Também em relação à sua escala, os modelos são similares, apresentando classificações sinônimas e escalas que vão desde os modelos mais elementares até aqueles considerados maduros. Hillson apresenta 4 escalas, enquanto os demais apresentam 5 escalas.

Quadro 28 – Escalas dos Modelos de Mensuração de GRC

Grau de Maturidade da Gestão de Risco					
Hillson	Poltronieri	Oliva	RIMS	M_o_R	IBGC
1 Ingênuo	1 Imaturo	N1 Insuficiente	1 Ad-Hoc	N1 Inicial	Inicial
2 Novato	2	N2 Contingencial	2 Inicial	N2 Repetitivo	Fragmentado
	3	N3 Estruturado	3 Escalável	Nível 3 Definido	Definido
3 Normatizado	4	N4 Participativo	4 Gerenciado	Nível 4 Gerenciado	Consolidado
	5 Maduro	N5 Sistêmico	5 Líder	Nível 5 Otimizado	Otimizado

Fonte: Síntese elaborada pelo autor com base nos modelos pesquisados (2023)

A pesquisa de campo que se pretende nessa pesquisa visará aprofundar as reflexões sobre as práticas das organizações dos segmentos selecionados, para que se faça um enquadramento com base na coleta de dados diretamente com as empresas participantes da pesquisa.

Para tanto, optou-se pela utilização do modelo do IBGC. A escolha, em suma, considera os seguintes fatos: (a) decorre do fato de ser este um reconhecido difusor de conhecimento na temática da governança corporativa, incluindo a gestão de riscos corporativos, além de provedor de boas práticas nessa área para o mercado de capitais brasileiros; (b) o Instituto é atualmente um centro de formação de agentes que atuam nos Conselhos e Comitês de Governança das empresas abertas brasileiras (foco desta pesquisa); (c) o IBGC é um notório agente produtor de conhecimento e provedor de discussões sobre temáticas que incluem a gestão de riscos corporativos; (d) inexistência de pesquisas acadêmicas que utilizam essa escala; (e) ser este um modelo elaborado localmente, considerando as realidades do mercado brasileiro e (f) ser o mais atual e mais amplo entre os modelos identificados na revisão da literatura

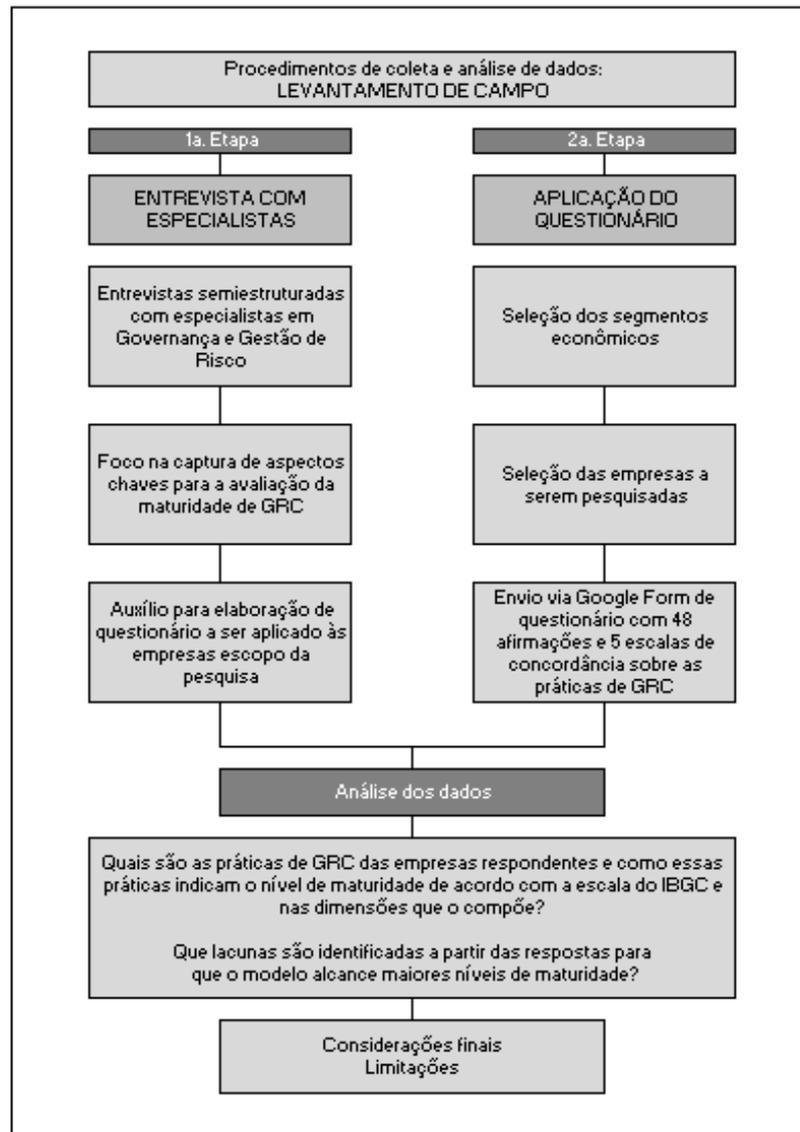
3 PROCEDIMENTOS METODOLÓGICOS

3.1 Caracterização e tipo de pesquisa

A pesquisa é de natureza mista (qualitativa e quantitativa). A pesquisa tem como objetivos a descrição e compreensão do seu objeto de estudo, e se relaciona a conceitos mensuráveis, que podem ser testados dentro de um contexto observável e que possam ser ampliados. A natureza da pesquisa é exploratória e aplicada, buscando por meio de sua metodologia e critérios aproximar-se da realidade do objeto estudado e cujo principal objetivo é a geração de conhecimento que permita aplicação prática, envolvendo questões organizacionais e de gestão das Organizações Empresariais.

Abaixo, temos uma síntese das etapas dos procedimentos de coleta e análise de dados.

Figura 13 – Síntese dos procedimentos metodológicos



Fonte: Elaborado pelo autor (2023)

-Exploração inicial: entrevistas com especialistas

Foram realizadas cinco entrevistas com especialistas das áreas executiva e de governança de grandes empresas, visando capturar destes quais são os aspectos considerados relevantes na avaliação da maturidade das estruturas de Gestão de Riscos Corporativos. Considerou-se, portanto, que as respostas apontadas pelos especialistas apresentaram congruência, havendo repetição em mais da metade dos aspectos destacados. Com base nas respostas colhidas, foram identificados 20

apontamentos, dos quais 11 deles foram citados por mais de um especialista. Esta etapa considera implicitamente as interpretações, experiências e vivências dos indivíduos consultados. Portanto, os dados colhidos refletem a participação desses participantes e as limitações daí decorrentes. Com base nas respostas colhidas e na revisão dos modelos de maturidade das práticas de GRC, efetuada na Fundamentação Teórica, especialmente do modelo do IBGC, selecionado como referência, foram elaboradas 48 questões a serem aplicadas à amostra selecionada íntegra do questionário no Apêndice à pesquisa).

- Levantamento de campo

Foram realizadas as seleções dos segmentos econômicos e das empresas a serem pesquisadas, conforme detalhamento do capítulo 3.2.1. Após essa seleção, foram identificados os profissionais que atuam na 2ª linha de defesa ou nos órgãos de Governança das empresas e remetidos via Google *Forms* os questionários elaborados. Para as empresas respondentes, foram acessadas documentações em seu website de Relações com Investidores para complementar as informações dos sujeitos de pesquisas sobre as práticas de Gestão de Riscos.

3.2 População e tipo de amostra

Nas seções seguintes, estão descritas as justificativas para escolha dos segmentos econômicos e empresas a serem pesquisadas.

3.2.1 Justificativa dos setores a serem pesquisados

Para a realização desta pesquisa, foram selecionados dois segmentos econômicos: (a) o varejo e o (b) setor financeiro. Selecionaremos empresas pertencentes a ambos os segmentos que estejam listadas na Bolsa de Valores B3, com base nos critérios detalhados na sequência. A pesquisa visa avaliar a maturidade da Gestão de Riscos Corporativos das empresas dos dois segmentos, possibilitando

a comparação entre as empresas pesquisadas e a identificação de quais são os aspectos que podem auxiliar o aprimoramento desta prática nas empresas.

A escolha dos dois segmentos traz a possibilidade de que sejam comparadas empresas de setores influenciadas por realidades, culturas organizacionais, ambientes e estratégias de negócio bastante distintos. A opção pelo varejo e segmento financeiro está relacionada substancialmente aos dois aspectos a seguir:

- a) Relevância dos segmentos na economia. Ambos são setores centrais e que movimentam bilhões na economia brasileira, empregam quantidade extensiva de mão de obra, além de terem uma atuação pervasiva, dada as conexões que mantêm com os demais setores da cadeia onde estão inseridos.
- b) Regulamentação aplicada. Ambos os setores têm níveis distintos em relação à regulamentação. Enquanto o setor financeiro é amplamente regulado no Brasil, o varejo é bastante desregulamentado. De acordo com Filardi e Macedo (2022), pressão regulatória é um dos motivadores chaves para a percepção de valor na trajetória de amadurecimento do GRC nas organizações. Assim, é relevante capturar a forma como essa estrutura está constituída em setores com e sem esse motivador. Também poder-se-á constatar ou descartar que o nível de regulamentação também pode impactar a disposição das Companhias em melhor estabelecer e formalizar suas estruturas, políticas e procedimentos.

3.2.2 Justificativa das empresas a serem pesquisadas

Justificados os segmentos escolhidos para a pesquisa, são definidos os seguir os critérios amostrais para escolha das empresas

O primeiro critério considerado foi o de abranger as empresas listadas na Bolsa de Valores Brasileiras – B3, ou seja, aquelas cujas ações estão disponíveis para os investidores com atuação local. A B3 é a única bolsa de valores em operação no Brasil e é a quinta maior do mundo. Em 2021, segundo informações de seu próprio site, estavam listadas mais de 400 companhias brasileiras, além de outras aproximadamente 100 empresas estrangeiras, dos distintos segmentos econômicos.

Como exigência, todas as empresas listadas na B3 devem atender a vários aspectos de governança tais como (a) ter autorização da Comissão de Valores Mobiliários - CVM, autarquia ligada ao Ministério da Fazenda, que regula o mercado de capitais, (b) cumprimento de todos os requerimentos e divulgações exigidos pela CVM, tais como o Formulário de Referência, material extensivo que apresenta de maneira detalhada dados associados às atividades da Companhia, índices financeiros e patrimoniais, estrutura acionária, política de dividendos, riscos, entre outros, (c) publicação de demonstrações financeiras trimestrais, com avaliação de auditor independente. As práticas requeridas às empresas de capital aberto permitem-nos classificá-las em um grupo de especial transparência e escrutínio do mercado, superior ao oferecido pela imensa maioria das empresas de capital fechado, ou seja, que não negociam suas ações na Bolsa de Valores.

A B3 dispõe de vários índices, que agrupam portfólios distintos de empresas. O mais conhecido deles é o Ibovespa, que agrupa as empresas com maior volume de negociação nos últimos meses. Além disso, existem outros índices que agrupam empresas em função de suas práticas de Governança. De qualquer maneira, todas as empresas listadas na B3 se submetem a “um conjunto básico de requerimentos” incluindo àqueles exemplificativos que trouxemos há pouco.

Além disso, existe uma separação das empresas listadas em distintos índices, considerando critérios como seu setor de atuação. Ao agrupar as empresas setorialmente, a B3 utiliza-se de critérios próprios, que não são inicialmente foco dessa avaliação. As tabelas 1 e 2 descrevem os segmentos dos dois setores escolhidos e o número de empresas de capital aberto em cada segmento vigentes em dezembro de 2022.

Tabela 1: Empresas nacionais do varejo listadas na B3

Varejo		Quantidade
<u>Consumo não cíclico</u>		
Agropecuária	Agricultura	10
Alimentos processados	Açúcar e Álcool	3
	Carnes e Derivados	6
	Alimentos Diversos	5
Bebidas	Cervejas e Refrigerantes	1
Produtos de Uso Pessoal e de Limpeza	Produtos de Uso Pessoal	1

	Produtos de Limpeza	1
Comércio e Distribuição	Alimentos	4
<u>Consumo cíclico</u>		
Comércio	Tecidos, Vestuário e Calçados	8
	Eletrodomésticos	3
	Produtos Diversos	7
TOTAL		49

Fonte: Site da B3: a Bolsa do Brasil; adaptado pelo autor (2023)

Tabela 2: Empresas nacionais financeiras listadas na B3

Financeiro		Quantidade
Intermediários Financeiros	Bancos	26
	Soc. Crédito e Financiamento	3
	Soc. Arrendamento Mercantil	2
Securitizadoras de Recebíveis	Securitizadoras de Recebíveis	14
Serviços Financeiros Diversos	Gestão de Recursos e Investimentos	5
	Serviços Financeiros Diversos	8
Previdência e Seguros	Seguradoras	6
	Resseguradoras	1
	Corretoras de Seguros e Resseguros	2
TOTAL		67

Fonte: Site da B3: a Bolsa do Brasil; adaptado pelo autor (2023)

Entende-se que é relevante subsegmentar o grupo acima, para permitir que as empresas selecionadas guardem maior homogeneidade em relação às suas atividades, porte ou estruturas, de tal forma que possa ser mais fácil comparar as práticas de Gestão de Riscos Corporativos executada entre elas. Dentro do universo destes dois segmentos, aplicou-se os seguintes critérios para formar a subpopulação que será o público de interesse da pesquisa:

- Setor de varejo: considerou-se quais dentre as empresas abertas estavam incluídas entre as 10 primeiras em cada um dos rankings das empresas com maior faturamento em todas as divisões de subsegmentos divulgadas pelo IBEVAR em 2022, com base nos dados de 2021: (i) eletroeletrônicos e móveis, (ii) moda e esporte, (iii) drogaria e perfumaria, (iv) material de construção, (v) fastfood e restaurantes, (vi) especializados e outros, (vii) lojas de departamento e (viii) super e hipermercado. Segundo seu site institucional, o IBEVAR é uma entidade sem fins lucrativos que tem o propósito de

fomentar o desenvolvimento do setor varejista e o intercâmbio de seus agentes. O setor de varejo tem várias divisões pela atividade e neste sentido optou-se por agrupar e selecionar para a pesquisa aquelas que são de maior porte, que tendem a ter desafios mais similares e uma necessidade das respostas das estruturas da Gestão de Risco mais semelhantes. Nesta compilação, optou-se pela exclusão Lojas Americanas, dado os eventos divulgados pela própria empresa em janeiro de 2023, que deram conta de uma distorção contábil bilionária (assim definida pela própria Companhia). O professor de contabilidade Eliseu Martins, em seu artigo na Revista Capital Aberto em 7 de maio de 2023, indicou que não há como deixar de nominar como fraude o ocorrido, com absoluta falha de sua estrutura interna de riscos e governança.

Assim, o público da pesquisa será composto pelas seguintes 15 empresas.

Tabela 3: Empresas do varejo selecionadas para a pesquisa

Nome da empresa	Valor dos ativos - R\$ MM	Valor do Patrimônio Líquido - R\$ MM
AREZZO CO	2.665	1.591
ASSAI	22.854	2.766
CARREFOUR BR	58.924	18.396
CEA MODAS	8.655	2.995
GRUPO MATEUS	6.407	6.404
GRUPO NATURA	28.831	28.545
GRUPO SBF	2.927	2.224
GUARARAPES	14.478	5.266
LE BISCUIT	1.232	161
LOJAS MARISA	3.423	1.447
LOJAS RENNER	17.895	9.806
MAGAZ LUIZA	38.384	11.261
P. ACUCAR-CBD	33.646	13.649
QUERO-QUERO	2.017	542
VIA	35.340	5.637

Fonte: Site da B3: a Bolsa do Brasil; adaptado pelo autor (2023)

- Setor financeiro: consideramos focar especificamente no sub-segmento “Bancos”. As atividades bancárias são bastante distintas daquelas executadas pelas empresas dos outros grupos e representam individualmente uma amostra quantitativa relevante (26 empresas equivalente a 39% da quantidade de empresas do segmento

Financeiro). No mais, os Bancos tendem a ter um portfólio mais amplo de serviços e de clientes, resultando em natural complexidade, situação em que a Gestão de Riscos ganha maior relevância. Assim, o público de pesquisas será composto pelas seguintes deste grupo, excetuando-se 3 empresas dos grupos Alfa, Itaú e Mercantil, que possuem seus Bancos e empresas Holding listadas e computadas dentre este grupo de 26 Companhias. Por essa razão, totalizaremos 23 empresas:

Tabela 4: Empresas Financeiras selecionadas para a pesquisa
Dados de ativos e patrimônios líquidos relativos a 31/12/2021

Nome da empresa	Valor dos ativos - R\$ MM	Valor do Patrimônio Líquido - R\$ MM
ABC BRASIL	48.298	4.669
ALFA	22.257	2.642
AMAZONIA	25.952	2.945
BANCO BMG	34.399	3.863
BANCO INTER	36.496	8.489
BANCO PAN	47.904	5.799
BANESE	7.320	561
BANESTES	33.931	1.890
BANPARA	12.519	1.639
BANRISUL	104.116	9.047
BR PARTNERS	2.930	634
BRADESCO	1.424.533	150.662
BRASIL	1.919.469	134.854
BRB BANCO	30.541	2.602
BTGP BANCO	374.163	39.035
ITAUUNIBANCO	1.989.883	155.397
MERC BRASIL	12.581	1.171
MODALMAIS	7.847	1.316
NORD BRASIL	60.302	7.479
NU-NUBANK	53.151	4.092
PARANA	8.813	1.295
PINE	15.367	779
SANTANDER BR	994.939	81.189

Fonte: Site de Relação de Investidores das empresas pesquisadas; adaptado pelo Autor (2023)

Os dados financeiros – de ativo e do patrimônio líquido – das Companhias expresso nas duas tabelas anteriores foram extraídos do próprio site de RI das respectivas empresas ou no site do Banco Central do Brasil, no caso dos Bancos. Os

dados se referem a 31/12/2021, última posição financeira auditada e divulgada na data da coleta.

Além disso, obteve-se dos sites das principais agências de avaliação de rating a nota atual de avaliação de crédito das empresas escopo de nosso trabalho, decorrente do trabalho de avaliação feita por essas agências e vigentes ao final do mês de maio de 2023. Segundo o site Modal Mais, as classificadoras que utilizamos nesta pesquisa – Moody’s, Fitch e Standard & Poor’s (S&P) são as mais representativas e possuem 95% do mercado global de classificação do risco de crédito/

Em suma, uma agência de classificação de risco, emite uma nota, cujo objetivo é ter uma avaliação sobre a qualidade do risco de crédito, ou seja, o quanto aquela empresa tem capacidade de honrar com os pagamentos de investidores que detenham seus títulos (dívidas).

Quadro 29 – Rating das empresas selecionadas

	Rating	Agência	Data
ASSAI	AAA	Ficth	out/22
CARREFOUR BR	AAA	S&P	abr/21
CEA MODAS	AA-	Ficth	mar/23
GRUPO MATEUS	AA+	Ficth	set/22
GRUPO NATURA	BB	Ficth	abr/23
GRUPO SBF	AA-	Ficth	jan/23
GUARARAPES	A	Ficth	mar/23
LE BISCUIT	BB	Ficth	fev/22
LOJAS RENNEN	AA+	S&P	jul/22
MAGAZ LUIZA	AA+	S&P	dez/22
P.ACUCAR-CBD	AA	Ficth	mar/23
QUERO-QUERO	AAA	S&P	dez/22
VIA	AA-	S&P	jun/23
ABC BRASIL	AA+	Moody	abr/23
ALFA	AA+	Moody	dez/23
AMAZONIA	BB-	Ficth	mai/23
BANCO BMG	A-	Moody	mai/22
BANCO INTER	A	Ficth	nov/22
BANCO PAN	AAA	Moody	abr/23
BANESE	A+	Moody	jul/22
BANESTES	BB-	Ficth	jun/22
BANPARA	AA	Moody	abr/23
BANRISUL	A+	Moody	jul/22
BR PARTNERS	AA-	Moody	jul/22
BRADESCO	AAA	Moody	abr/23
BRASIL	AAA	Moody	set/22
BRB BANCO	A	Moody	abr/23
BTGP BANCO	AAA	Moody	abr/23

ITAUUNIBANCO	AAA	Moody	out/22
MERC BRASIL	A-	Ficth	out/22
MODALMAIS	A	Moody	mar/23
NORD BRASIL	BB-	Ficth	mai/23
NU-NUBANK	AA	S&P	abr/22
PARANA	AA-	Ficth	out/22
PINE	BBB	Moody	jun/22
SANTANDER BR	AAA	Moody	set/22

Fonte: Elaborado pelo autor (2023), com base no site das classificadoras de risco Moody's, Fitch e Standard & Poor's

No momento da pesquisa, Arezzo&Co e Lojas Marisa não tinham avaliação de risco realizada pelas classificadoras.

Para fins de identificação do significado das notas atribuídas, realizou-se no quadro seguinte uma classificação comparativa das notas dessas agências. Com base nelas, vemos que das 36 empresas selecionadas na pesquisa e com rating disponível, 31 estão classificadas nos quatro grupos de maior nota – mais alta qualidade, qualidade muito alta, qualidade alta ou boa qualidade. As demais 5 empresas estão nos grupos especulativo e altamente especulativo. Nenhuma delas está no grupo de risco substancial, muito alto, excepcionalmente alto ou inadimplente.

Quadro 30 – Escala das agências de rating

	Moody's	S&P	Ficth
Mais alta qualidade	Aaa	AAA	AAA
Qualidade muito alta	Aa1, Aa2 e Aa3	AA	AA
Qualidade alta	A1, A2 e A3	A	A
Boa qualidade	Baa1, Baa2 e Baa3	BBB	BBB
Especulativo	Ba1, Ba2	BB	BB
Altamente especulativo	B1, B2 e B3	B	B
Risco substancial	Caa1, Caa2 e Caa3	CCC	CCC
Risco muito alto	Ca	CC	CC
Risco excepcionalmente alto	C	C	C
Inadimplente		D	

Fonte: Elaborado pelo autor (2023), com base no site das classificadoras de risco Moody's, Fitch e Standard & Poor's

A coleta de dados será feita por meio do envio de um questionário elaborado no formato Google *Forms* a um profissional de cada empresa, representante das áreas de 2ª linha (responsáveis pela estrutura de Gerenciamento de Riscos Corporativos) ou de sua Governança.

3.3 Técnica de coleta de dados

Para coleta de dados primários, elaborou-se o questionário apresentado no apêndice 1, que foi encaminhado aos responsáveis pelas áreas de gestão de risco e/ou da governança das empresas selecionadas, visando capturar informações sobre suas práticas de gestão de risco, que permitirão enquadrar sua maturidade de acordo com o modelo estabelecido pelo IBGC.

Para elaboração deste questionário, aplicado às empresas selecionadas para a pesquisa, duas etapas foram planejadas:

- 1) Entrevistas semiestruturadas com profissionais especialistas
- 2) Pré-testes, com a aplicação prévia e assistida
- 3) Entrevistas semiestruturadas com profissionais especialistas

Para a etapa 1, foram ouvidos os especialistas caracterizados na sequência, cujas entrevistas estão sumariadas e cujos inputs em relação ao questionário estão apresentados ao final do relato. As entrevistas visam capturar a visão de profissionais com experiência em temáticas de Risco Corporativo em relação aos pontos relevantes que devem ser levados em conta para avaliação das práticas estabelecidas e implementadas pelas Organizações e o seu grau de maturidade. Os relatos a seguir sumarizam os pontos principais identificados nas entrevistas, sendo que a transcrição dos relatos nesta pesquisa foi autorizada pelos profissionais consultados.

Profissional 1:

Breve síntese da formação acadêmica: Contador pela PUC-Campinas, tem MBA em Administração, Conhecimento, Tecnologia e Inovação pela Universidade de São Paulo, tem curso de extensão executiva com foco em gestão e estratégia pela INSEAD e curso de formação de Conselheiros de Administração pelo IBGC.

Breve síntese da experiência profissional: é sócio de Governança, Riscos e Compliance da PwC, onde atua há 30 anos. Além disso, é membro da Comissão de Comunicação e de Mercados de Capitais e Professor de Governança Corporativa do IBGC. Participou das publicações Novo COSO – Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance, em 2017 e do Guia das Melhores Práticas de Governança em Cooperativas, estudo do IBGC de 2015.

A entrevista foi realizada em 14 de dezembro de 2022, on-line, através do Microsoft Teams.

Principais tópicos indicados pela especialista:

- Para o entrevistado, a atividade de Gestão de Riscos Corporativos é típica de Governança e deve ser capitaneada primariamente pelo Comitê Executivo da Companhia e pelo seu Conselho de Administração e seus Comitês de Assessoramento. A gestão deve ser feita com base nos indicadores chaves de riscos (KRIs, no acrônimo em inglês) que representam as medidas chaves utilizadas na gestão, para indicar os riscos envolvidos, fornecendo um sinal precoce do aumento da exposição destes riscos nas várias áreas da empresa. Os KRIs estão no geral associados aos objetivos de negócio, expressos pelos indicadores chaves de performance (KPI, no acrônimo em inglês). A gestão dos riscos corporativos não é prerrogativa de uma área e seus gestores não devem tomar decisões sozinhos; é necessário que haja visibilidade e transparência para toda empresa sobre aquilo que envolve os principais riscos. Nesta dinâmica, a segunda linha de defesa deve sempre estar envolvida, dando creditação, homologando a visão sobre os riscos em si, probabilidade de ocorrência e impacto associados, mitigações existentes e necessárias e atuando sobre eventuais conflitos de interesse existente. Nesse sentido, acredita que o primeiro aspecto a ser considerado na avaliação de uma estrutura de GRC é o respeito a essa lógica, isto é, riscos pervasivos devem ser conhecidos e acompanhados pela Alta Administração, na preservação e na realização de valor e não mantidos em áreas específicas e tratados somente pela média gestão.
- O entrevistado ratificou o entendimento de que a gestão de riscos corporativos precisa fazer parte do planejamento estratégico da Companhia, mantendo-se sustentável e sendo um “input” para a definição de prioridades e investimentos.

- O entrevistado entende que a identificação dos riscos é um exercício “top down” ou seja, a abordagem parte da visão dos principais executivos da empresa e tocam, portanto, os objetivos estratégicos. Sem descartar os riscos operacionais (ou poderia citar riscos no nível dos processos de negócio), o foco primordial é abranger aqueles que possam impossibilitar a plena realização dos objetivos de negócio.
- Outro ponto relevante apresentado foi a relevância de se identificar se a estrutura de GRC está situada em posição organizacional que lhe possibilite acesso e reporte efetivo ao Comitê Executivo da Companhia, bem como a alocação de tempo do Risk Officer. Com isso, é possível se avaliar a maturidade das práticas seja pelo acesso da estrutura de GRC à Alta Administração, seja pelo quanto está dedicado a esta temática.

Profissional 2:

Breve síntese da formação acadêmica: Doutor e Mestre em Administração pela FEA - USP, com MBA Economia e Setor Financeiro pela Fipe - USP.

Breve síntese da experiência profissional: Membro da Comissão de Gerenciamento de Riscos do Instituto Brasileiro de Governança Corporativa (IBGC), membro da *Global Association of Risk Professionals* (GARP) e da *Professional Risk Managers International Association* (PRMIA). Desde 2002, é funcionário de carreira do Banco Central do Brasil (BCB), com atuação na Supervisão de Bancos e na Supervisão de Infraestruturas do Mercado Financeiro, avaliando a governança corporativa, governança de riscos, gestão de riscos, controles internos e compliance dessas Instituições. Sua experiência profissional anterior ao BCB inclui trabalhos na Accenture, Telefônica e Lojas Americanas. Professor em cursos de MBA, pós-graduação, graduação e educação executiva. Coordenador do MBA Gestão de Riscos e Compliance da FECAP. Docência em disciplinas ligadas à Governança Corporativa, Gestão de Riscos Corporativos, Gestão de Riscos Operacionais, Controles Internos, Compliance, Ética Corporativa e Gestão Estratégica. Palestrante e escritor.

Principais tópicos indicados pelo especialista relativos à maturidade da Gestão de Riscos Corporativos:

- Enfatizou a visão de que são muitos os fatores que influenciam a maturidade da Gestão de Riscos Corporativos nas empresas e que todos devem ser vistos como interdependentes.

- Entre esses principais fatores, citou:

(a) a cultura da Organização, incluindo seu apetite a risco.

(b) o setor de atuação, incluindo as regulações as quais estão submetidas – que podem eventualmente impulsionar as estruturas e práticas de GRC.

(c) o porte da Organização, que tende a possibilitar uma estrutura mais robusta para empresas maiores.

(d) a existência de uma visão ampla de risco, que não foque apenas em aspectos financeiros e que não enfatize em demasia alguns tópicos em detrimento de uma visão abrangente.

(e) alocação de GRC na estrutura funcional, de tal sorte que esteja investida de autonomia e da influência necessária para execução e reporte de seu trabalho. Neste caso, comenta sua preocupação com estruturas de GRC que estejam dentro da estrutura Jurídica ou CFO, podendo ter uma ênfase limitada a determinadas temáticas.

(f) modelo de organização das atividades, de tal sorte que as operações centrais à atividade da 2ª linha de defesa não estejam distribuídas nas áreas operacionais – 1ª linha. Neste tópico, comenta já ter identificado em sua experiência profissional estruturas que tinham como referências modelos descentralizados, que podem ser influenciados por *drivers* que não são escopo das atividades típicas de GRC.

(g) existência de segregação entre as atividades de Governança de Riscos Corporativos e Auditoria Interna.

(h) garantia de que os Comitês Executivos e da Governança que tem em seu escopo as atividades de acompanhamento e supervisão de Riscos tenham tempo e dedicação adequada para execução desta atividade complexa.

O entrevistado citou os estudos do IBGC como referência na temática de maturidade de GRC e fez referência ao Caderno 19 do *Think Tank*, que aborda em sua página 36 os principais pilares e escalas de um modelo de avaliação.

Insights colhidos aplicáveis ao questionário

Consideramos que os principais destaques trazidos pelo especialista foram considerados e estão presentes nas questões elaboradas e ainda que estão bastante alinhados aos principais drivers trazidos pelo modelo do IBGC que citamos há pouco.

Profissional 3:

Breve síntese da formação acadêmica: Bacharel em Economia pela PUC-RJ, com MBA em Gestão do Luxo pela FAAP, participante do Senior Management Program pela IE Business School, diversos cursos de formação na área de Governança, Riscos e Compliance pela KPMG e IBGC.

Breve síntese da experiência profissional: Atualmente é (a) membro independente do Comitê de Auditoria do Banco Santander Brasil, (b) conselheiro fiscal da B3, (c) membro independente do Comitê de Auditoria da BR Properties S/A, (d) membro independente do Comitê de Auditoria do Hospital Albert Einstein e (e) conselheiro fiscal da Camil Alimentos. Além disso, teve passagens nos órgãos de governança das Lojas Americanas, CCR e HSBC e foi executivo do Banco Santander Global, da KPMG, do HSBC, do Banco Bilbao Vizcaya Argentina e da Artur Andersen.

Entrevista realizada em 4 de novembro de 2022, on-line, através do Microsoft Teams.

Principais tópicos indicados pela especialista:

- É uma preocupação permanente da Governança de que as empresas sejam dotadas de área dedicada e com profissionais preparados para lidar com os temas de Gestão de Risco, com conhecimentos profundos sobre os negócios da Companhia.
- Para supervisionar a efetividade desses trabalhos, a Governança deve ter a Gestão de Risco como um tema permanente em sua agenda, com atividades como conversas com executivos e profissionais chaves, leitura e estudo de materiais internos, observação das práticas e comparação com o mercado.
- A governança deve avaliar se diversos indicadores como apetite, avaliação de risco, atribuição de responsabilidade, planos de mitigação bem definido, existem e são atualizados.
- A especialista considera que, dentre todos os modelos existentes e possíveis, as Companhias deveriam priorizar o envolvimento da primeira linha de defesa, como

forma de envolver as áreas de negócio nas temáticas de risco e garantir um engajamento e responsabilização.

- Nas diversas empresas que a especialista teve contato, seja como membro da governança ou executiva, existe um contraste de maturidade nas práticas de GRC. No geral, acredita que aquelas que possuem um regulador forte ou um acompanhamento extensivo da Matriz tendem a ter estruturas mais bem estabelecidas. Acredita que o porte da Companhia, por si só, não define as práticas e a maturidade.

- Atribui diversos fatores como relevantes para avaliação da adequação das estruturas de Gerenciamento de Risco, dentre as quais a qualidade e independência dos profissionais, um reporte permanente às estruturas de governança, acompanhamento dos movimentos e tendências de mercado, além da aderência aos temas regulatórios.

Insights colhidos aplicáveis ao questionário

Questões chaves apontadas pela especialista estão contempladas no questionário, como existência de estrutura própria dedicada ao tema, independência do time de GRC, existência de reportes permanentes, inputs relacionados ao mercado, relevância dos aspectos regulatórios na estrutura de GRC. Acreditamos que o preparo dos times de GRC seja um aspecto de bastante subjetividade e optamos por priorizar elementos estruturais que indicam as práticas atuais e sua consolidação.

Profissional 4:

Breve síntese da formação acadêmica: Bacharel em Análise de Sistemas pela UNIP, com MBA em Administração pela FGV e formação complementar sobre Inovação e Gestão pela Stanford University.

Breve síntese da experiência profissional: Atualmente é Líder Global sobre Riscos Operacionais e de TI do Nubank. Anteriormente, foi sócio da prática de Riscos da Deloitte e executivo da MS Senior Management e da Artur Andersen.

Entrevista realizada em 3 de novembro de 2022, on-line, através do Microsoft Teams.

Principais tópicos indicados pelo especialista:

- Como executivo da prática de GRC, considera fundamental que as empresas tenham construída uma política de risco, para nortear suas ações mais estratégicas da prática e um mapa de risco, com a indicação dos principais riscos existentes e acompanhados.
- O entrevistado confirma que a área de Risco tem extensivo contato com outras áreas de negócio e permanente contato e reporte com a Governança da Companhia, incluindo Comitê de Auditoria e Conselho de Administração. Menciona que nestes reportes, deve ajudar à Governança a ter uma visão clara dos riscos existentes e das ações de mitigação existentes e a ser implementadas.
- O especialista entende que a avaliação da efetividade uma estrutura de GRC deve englobar três pontos, que chamou de Antes, Durante e Depois. “Antes” tem relação com o quanto a área é envolvida antes do lançamento de um novo produto ou antes da modificação de um processo relevante; isto é, o quanto ela conhece e opina nas implicações que isso traz aos principais riscos e os cuidados que devem ser observados. O “durante” é o que se chama de “Business as Usual”, ou seja, o cumprimento das tarefas habituais da área. O “depois” está relacionada à avaliação de eventos adversos materializados, isto é, o quanto a área de GRC capturou a possibilidade de existência deste evento e quanto avaliou adequadamente a probabilidade de realização e o seu impacto. Segundo Francesco, essa é uma oportunidade de autoavaliação e calibragem e correções das metodologias empregadas.
- O entrevistado considera que é absolutamente desejável que as temáticas de risco estejam muito presentes nas áreas de negócio e de suporte – 1ª. linha, afinal, elas é quem tomam as decisões e devem considerar o impacto dos riscos nessa dinâmica. Além disso, o especialista considera que é fundamental que as áreas conheçam seus riscos, a visão de probabilidade e impacto inerente e após a aplicação das mitigações, bem como conheçam e avaliem a necessidade de ajustes e novas mitigações.
- O profissional acredita que existe um movimento natural em se avançar nas avaliações quantitativas, a medida em que a estrutura de GRC vai adquirindo maturidade e que esta esteja cada vez mais diluída à gestão. Além disso, considera que a Alta Administração e a Governança estejam cientes e comprometidas com a relevância estratégica da área, para que esta opere com a força esperada.

- Por fim, menciona que um dos aspectos que deve ser sempre avaliado na GRC é o cumprimento das regulações aplicáveis. O cumprimento pleno deve ser sempre visto como um ponto positivo da maturidade.

Insights colhidos aplicáveis ao questionário

Consideramos que os principais destaques trazidos pelo especialista foram considerados e estão presentes nas questões elaboradas: existência de política de risco, avaliação da prática de identificação da probabilidade e do impacto dos riscos mapeados, interação e envolvimento da Alta Administração, avaliação das regulamentações como parte do escopo de GRC e avaliação permanente e atualização periódica das avaliações. Esses critérios podem ser correlacionados à matriz de maturidade proposta pelo IBGC, selecionada na pesquisa.

Profissional 5:

Breve síntese da formação acadêmica: Bacharel em Administração com MBA em Finanças pela Anhembi Morumbi e MBA em Finanças Bancárias pela Fundação Instituto de Administração. É certificado como profissional especializado em investimentos pela Ambima – CPA 20.

Breve síntese da experiência profissional: Atualmente é Superintendente Contábil do Banco Santander Brasil, responsável pela elaboração das informações contábeis e reporte ao mercado. Além disso, é membro do Conselho Fiscal da Banesprev – Instituição de Previdência Patrocinada pelo Banco Santander, designado pelo patrocinador. Anteriormente, foi líder de Planejamento Tributário na mesma Instituição Bancária.

Principais tópicos indicados pelo especialista:

- O entrevistado mencionou que os temas decorrentes da estrutura de Gestão de Riscos Corporativos são partilhados e fazem parte das temáticas prioritárias da Governança. Indica que como representante da Governança tem sempre um olhar atento à evolução; como o processo se altera no tempo e que aprimoramentos são realizados.

- O especialista citou a relevância da independência dos representantes da área e do conhecimento que devem demonstrar a respeito do negócio da Companhia, bem como da amplitude de sua avaliação, isto é, necessidade que percorram os principais ciclos.
- Enfatizou sobre a necessidade de avaliação externa. Indica que, como membro da Governança tem especial conforto ao receber uma avaliação independente sobre as práticas de GRC e sobre os resultados alcançados.
- Além disso, o especialista apontou preocupação sobre os principais riscos terem sempre planos de mitigação apontados, com responsabilidade clara e prazos de execução, para que a Companhia tenha disciplina ao tratá-los.
- O entrevistado indicou que um aspecto fundamental na avaliação sobre a maturidade dos processos e práticas de GRC é a difusão entre todos os colaboradores. Julga que este é um processo permanente e que deve sempre estar na agenda de prioridades dos executivos e acompanhados pela governança.

Insights colhidos aplicáveis ao questionário

As principais temáticas abordadas pelos especialistas foram consideradas e estão contempladas no questionário elaborado, apresentado integralmente no apêndice.

A segunda etapa, referente ao pré-teste, foi realizada antes do envio aos profissionais respondentes.

O quadro seguinte sintetiza os principais *insights* trazidos pelos especialistas ouvidos e que auxiliaram no processo de elaboração do instrumento de coleta. Observa-se o sumário de 20 tópicos abrangidos, dos quais 11 foram citados por pelo menos 2 dos 5 especialistas ouvidos.

Quadro 31: Principais aspectos mencionados nas entrevistas

	1	2	3	4	5	Citações
Envolvimento da governança nos temas de GRC	x	x	x	x	X	5
Atividade capitaneada pela Alta Administração	x	x		x		3
Segunda linha de defesa atuante e independente	x	x			x	3

Cultura organizacional que favoreça a implementação e foco em GRC		x	x		x	3
Necessidade de gestão com base em indicadores – KRI	x		x			2
Visão abrangente de riscos	x	x				2
Posição funcional da segunda linha que permita acesso a Alta Administração	x	x				2
Tempo e foco dedicado às estruturas de GRC	x		x			2
Relevância de foco nas leis e regulamentos dentro da GRC, em função do segmento		x		x		2
2a linha como detentora de profundo conhecimento do negócio			x		x	2
PDCA do processo de GRC (autoavaliação, calibragem e correções)				x	x	2
Associação de GRC com os objetivos e estratégias de negócio	x					1
Estrutura de GRC compatível com o porte e complexidade da Organização		x				1
Atividade de 2a linha centralizadas em área específica e não distribuídas na 1a linha		x				1
Segregação entre atividades da 2a linha e Auditoria Interna		x				1
Acompanhamento dos movimentos e tendências do mercado			x			1
Existência de política formal de GRC				x		1
Existência de mapa de risco com os principais temas acompanhados				x		1
GRC by design (avaliando novos projetos, produtos e investimentos)				x		1
Foco em avaliações quantitativas e qualitativas do risco				x		1

Fonte: Elaborado pelo próprio autor (2023)

O quadro a seguir apresenta a associação entre cada um dos aspectos do quadro acima, citados pelos especialistas e as respectivas perguntas do instrumento de coleta, cuja íntegra apresenta-se no apêndice.

Quadro 32: Amarração entre entrevista e questionário

	Perguntas
Envolvimento da governança nos temas de GRC	7, 10, 11, 12, 14, 29, 34 e 36
Atividade capitaneada pela Alta Administração	6,7, 13, 15 e 45
Segunda linha de defesa atuante e independente	8 e 9

Cultura organizacional que favoreça a implementação e foco em GRC	44, 45, 46, 47 e 48
Necessidade de gestão com base em indicadores – KRI	6 e 28
Visão abrangente de riscos	3, 4, 17, 24, 25 e 26
Posição funcional da segunda linha que permita acesso a Alta Administração	7 e 15
Tempo e foco dedicado às estruturas de GRC	10, 11, 12, 14, 29, 34 e 36
Relevância de foco nas leis e regulamentos dentro da GRC, em função do segmento	11, 13 e 27
2a linha como detentora de profundo conhecimento do negócio	2, 3, 4, 28 e 39
PDCA do processo de GRC (autoavaliação, calibragem e correções)	16, 22, 23 e 30
Associação de GRC com os objetivos e estratégias de negócio	1, 6, 20 e 26
Estrutura de GRC compatível com o porte e complexidade da Organização	3
Atividade de 2a linha centralizadas em área específica e não distribuídas na 1a linha	8
Segregação entre atividades da 2a linha e Auditoria Interna	9
Acompanhamento dos movimentos e tendências do mercado	21
Existência de política formal de GRC	18, 19, 32 e 34
Existência de mapa de risco com os principais temas acompanhados	31, 32, 33, 34
GRC <i>by design</i> (avaliando novos projetos, produtos e investimentos)	5 e 47
Foco em avaliações quantitativas e qualitativas do risco	35

Fonte: Elaborado pelo próprio autor (2023)

Quadro 33: Amarração entre questionário e modelo do IBGC

Dimensões do Modelo de Mensuração do IBGC	Perguntas
Estratégia	1 a 6
Governança	7 a 16
Política	17 a 23
Processo de GRC e Interação com demais ciclos de negócio	24 a 30
Linguagem e métodos de avaliação	31 a 37
Sistemas, dados e modelos de informação	38 a 43
Cultura, comunicação, treinamento e melhoria contínua	44 a 48

Fonte: Elaborado pelo próprio autor (2023)

4 ANÁLISE DOS DADOS

O Instrumento de Coleta desta pesquisa foi elaborado com base na revisão da literatura, no modelo proposto pelo IBGC e nas entrevistas feita com cinco especialistas. Os 20 aspectos mencionados pelos especialistas, dos quais 11 mencionados por mais de um especialista estão contemplados no instrumento aplicado, cuja cópia consta no Apêndice 1 e cuja amarração entre os tópicos citados pelos especialistas e as respectivas questões constam no Apêndice. O instrumento de coleta foi elaborado para permitir avaliar o estágio de maturidade das 7 dimensões previstas no modelo de avaliação do IBGC e contemplou e, portanto, aspectos relativos às temáticas constantes nesse modelo de avaliação, conforme evidenciamos no quadro abaixo. A relação entre as 48 questões do instrumento de coleta e cada uma dessas dimensões está evidenciada no Apêndice 1.

Quadro 34: Aspectos contemplados no Instrumento de Coleta

Dimensão	Aspecto contemplado
Estratégia	<ul style="list-style-type: none"> - Integração de GRC com a gestão - Compatibilidade de GRC com porte e complexidade - Alinhamento dos objetivos da gestão com a GRC - Avaliação e mensuração de riscos disseminada - Priorizações de investimento consideram GRC - Metas de desempenho das áreas contemplam a GRC
Governança	<ul style="list-style-type: none"> - GRC com acesso e reporte à alta gestão e governança - Estrutura específica e independente - Acompanhamento permanente dos riscos e mitigações, deficiências, não cumprimentos legais e desvios éticos - GRC é pauta permanente na governança, com tempo e profundidade adequados - Avaliação de GRC por agente externo
Política	<ul style="list-style-type: none"> - Temas críticos do negócio são normatizados - Políticas e diretrizes de GRC são normatizados e divulgados de maneira consistente - Diretrizes permanentemente atualizadas - Acompanhamento interno e externo sobre aplicação das diretrizes de GRC
Processo de GRC e integração com demais ciclos de negócio	<ul style="list-style-type: none"> - Capacidade de capturar os principais riscos e de mensurar adequadamente seus efeitos - Capacidade de propor mitigações efetivas que reduzem probabilidade e/ou impacto - Identifica corretamente descumprimentos legais

	<ul style="list-style-type: none"> - Gera indicadores úteis na gestão - Monitora e reporta planos de mitigação críticos - Governança monitora e aprimora processo de GRC
Linguagem e métodos de avaliação	<ul style="list-style-type: none"> - Procedimentos implementado para identificação, mensuração e mitigação de riscos e baseado em framework reconhecido - Definição de apetite de risco quantitativo e qualitativo - Teste de stress utilizado no cálculo de apetite - Assunção de riscos críticos destinada à Governança
Sistemas, dados e modelos de informação	<ul style="list-style-type: none"> - Geração de reportes decorrentes de GRC e utilização para fins externos (regulamentação) e interno (gestão) - Liderança conhece, entendem e usam reportes de GRC - Uso extensivo de dados no processo de GRC - Ciclos de negócio e TI utilizados no processo de GRC - Integração com dados e acompanhamentos on-line
Cultura, comunicação, treinamento e melhoria contínua	<ul style="list-style-type: none"> - Cultura de risco disseminada em toda a Companhia - Times compreendem os benefícios da gestão de risco - Liderança ativa na identificação e mitigação de riscos - Novos processos e projetos têm visão de riscos - Treinamentos regulares sobre a temática

Fonte: Elaborado pelo próprio autor (2023)

Esses principais tópicos serão avaliados, posteriormente, em função das respostas coletadas.

Como parte do processo de elaboração, realizamos uma primeira versão do formulário que foi submetida à avaliação prévia com dois profissionais da área de riscos, para capturar percepções distintas e com o objetivo de verificar (a) a compreensão de um potencial respondente às afirmações que foram propostas, (b) eventuais dúvidas que poderiam surgir ao se responder o formulário, (c) razoabilidade do tempo de preenchimento e (d) aderência dos questionamentos à típica experiência dos profissionais que seriam selecionados para realização da pesquisa.

Para maior conveniência e controle dos envios e respostas, o formulário foi inserido mediante a ferramenta “Google Forms”. A ferramenta permite a criação de link e mantém Traceabilidade de data e horário de acesso, além de guarda e extração das opções selecionadas que são indicadas pelos respondentes.

Com base nos comentários recebidos, ajustes foram realizados para que as afirmações ficassem mais claras, para que fossem eliminadas redundâncias e para que houvesse uma melhor amarração entre os aspectos mencionados pelos

especialistas e as respectivas indagações. Com base nos comentários, não se identificou a necessidade de novas validações.

Cada questão deve ser respondida mediante a seleção de uma entre as 5 respostas abaixo, de acordo com a Escala de Likert, a partir das quais os respondentes indicam seu grau de concordância:

- Discordo totalmente
- Discordo em partes
- Nem discordo nem concordo
- Concordo em partes
- Concordo totalmente

A inclusão dos cinco graus de maturidade em cada resposta às afirmações também permitiu uma associação com os cinco graus da escala do Modelo de Avaliação de Maturidade do IBGC:

- Inicial
- Fragmentado
- Definido
- Consolidado
- Otimizado

Para obter as respostas das empresas componentes da população da pesquisa, considerou-se o envio a profissionais que atendessem aos critérios definidos abaixo, que seriam os sujeitos de pesquisa mais qualificados para responder:

- a) Profissionais que estão atuando na empresa pesquisa, com vínculo ativo ou que tenham se desligado em período inferior a 1 ano;
- b) Profissionais que tem pelo menos 1 ano de experiência na empresa pesquisada;

- c) Profissionais participantes da governança da Companhia (membro do Conselho de Administração, Comitê de Auditoria e Riscos e Conselho Fiscal, ou outro equiparado, responsável pelo acompanhamento dos temas de Gerenciamento dos Riscos Corporativos) ou membros de sua administração com cargo de Gestão e que tenham função vinculada à segunda linha de defesa – áreas típicas de GRC como controles internos, compliance, riscos, canal de denúncias ou de áreas correlatas com envolvimento extensivo nas temáticas de riscos, como auditoria interna ou finanças.

Em que pese ter-se buscado elencar indagações objetivas sobre as práticas de Gestão de Riscos Corporativos das empresas, o seu enquadramento envolve a avaliação e perspectiva pessoal de cada respondente. Com isso, uma das limitações desta pesquisa é o teor subjetivo que pode ser trazido às respostas devido aos profissionais que foram contatados e que responderam às indagações. Caso outros profissionais da mesma empresa tivessem sido selecionados, respostas distintas poderiam ser dadas.

O envio do pedido de preenchimento aos potenciais participantes ocorreu primariamente pelo LinkedIn – rede social com ênfase em relacionamentos profissionais, por meio de buscas que permitissem identificar profissionais que atendessem aos critérios acima. Todos os envios foram feitos com a respectiva contextualização sobre a pesquisa e com a ratificação de que os dados não seriam utilizados para outro propósito, além da confirmação de que as respostas não seriam divulgadas de maneira individualizada na pesquisa. Após este envio e período de aguardo das devolutivas, foi feito um segundo contato com as empresas para as quais ainda não se havia resposta. Este segundo envio do pedido de participação ocorreu por meio das caixas corporativas disponibilizadas ao público externo, nas áreas de Relações com Investidores.

As respostas foram obtidas em período de 1 mês – entre 21 de junho até 20 de julho de 2023. Durante o final de julho e agosto de 2023, foram feitos novos contatos com os profissionais e reforço por meio do site de Relações com o Investidores, conforme descrito acima. Em 1º de setembro de 2023, optou-se por um corte, para que a consolidação considerasse as respostas recebidas até então.

O instrumento de pesquisa foi enviado para as 38 empresas selecionadas em nosso escopo constantes nas Tabelas 3 e 4, ou população da pesquisa, e obteve-se a devolutiva de 15 empresas, conforme a tabela 5, abaixo. As respostas representam 39% da população selecionada e as empresas respondentes representam 44% dos valores de ativos e patrimônio líquido das empresas escopo.

Tabela 5: Resumo das respostas obtidas na pesquisa

	Total	Varejo	Financeiro
Escopo pesquisa (população)	38	15	23
Envio questionário	38	15	23
Respostas recebidas (amostra)	15	6	9
% Respostas recebidas	39%	40%	39%
% Ativo correspondente	44%	66%	43%
% Patrimônio líquido correspondente	44%	50%	43%

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

As amostras retornadas representam um número pequeno para se fazer inferências estatísticas, mas o desvio em relação à média é pequeno, o que permite sua utilização para as análises seguintes.

Os respondentes selecionados e que participaram das respostas são profissionais sêniores, atuando na governança e gestão das respectivas Companhias há pelo menos 2 anos, o que os habilita a discorrer sobre as práticas de Gestão de Riscos Corporativos de suas empresas. Dos respondentes, 1/3 são membros da Governança, enquanto os demais são membros da Gestão de suas Companhias. Deste total, 60% têm envolvimento diretamente como participantes da segunda linha de defesa. O tempo médio de atuação dos profissionais respondentes é superior a 7 anos na Companhia, sendo que o profissional que está a mais tempo, atua há 20 anos.

Abaixo, um sumário sobre as informações sobre os respondentes:

Tabela 6: Resumo sobre os respondentes da pesquisa

	Total	Varejo	Financeiro
Respondentes	15	6	9
Tempo de casa			
Médio	7,3 anos	9,2 anos	6 anos
Menor	2 anos	3 anos	2 anos
Maior	20 anos	18 anos	20 anos

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Com base na resposta ao formulário das 15 empresas, realizou-se a extração das respostas via a própria Ferramenta “Google Forms” para o Excel, permitindo organizar os dados e gerar as visões sumariadas que consolidam as principais questões. Percorreu-se as respostas recebidas, que estavam integralmente respondidas e sem sinalizações únicas, isto é, mesma resposta dada em todas as questões por cada um dos respondentes. Os sumários elaborados são aqueles que nos permitirão percorrer as respostas recebidas e realizar a análise em relação ao processo de maturidade dos dois segmentos e das dimensões constantes no Modelo de Avaliação do IBGC.

Enumerou-se na sequência visões consolidadas referentes às respostas dadas nos 15 formulários coletados em relação à frequência para cada uma das 5 opções possíveis, em uma visão única e separada para cada um dos 2 segmentos.

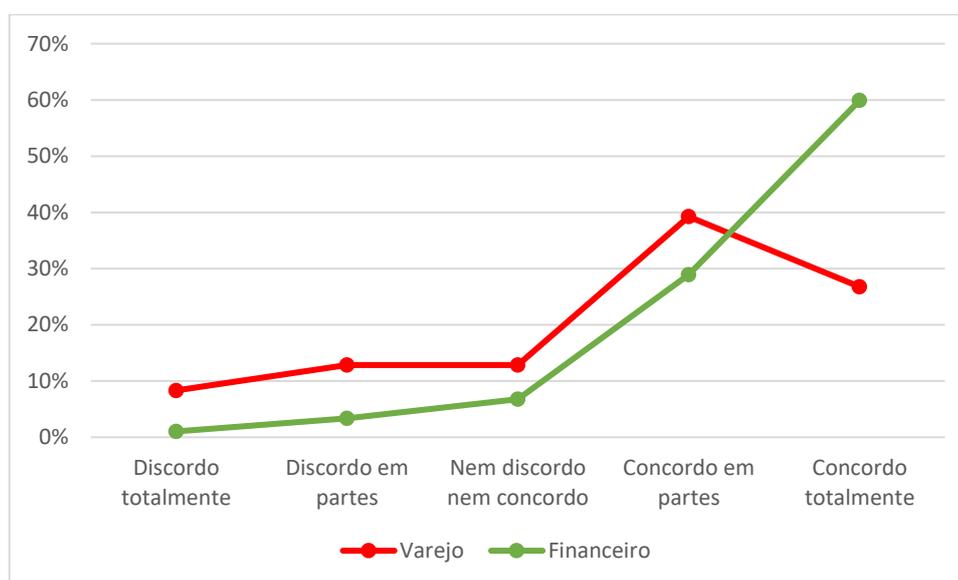
Em suma, essa visão indica que, dentre as 720 respostas coletadas, quase a metade tem concordância total em relação às afirmativas realizadas; a concordância total ou em partes excede 80% das respostas, enquanto a discordância total ou em partes chega a 11%. Já é possível notar no primeiro extrato dos dados que existe uma diferença entre a visão de maturidade das práticas de GRC dos dois segmentos: (a) a concordância total é mais que o dobro no setor financeiro em relação ao segmento de varejo, (b) a discordância total ou em partes é 8% para as respostas do setor financeiro; no de varejo chega a 21%. Nas tabelas 7 e 8 as frequências absolutas e relativas das respostas coletadas.

Tabela 7: Frequências absolutas do total das respostas

	Ambos os Setores		Setor Varejo		Setor Financeiro	
	Absoluta	Relativa	Absoluta	Relativa	Absoluta	Relativa
Nota 1	29	4%	24	8%	4	1%
Nota 2	50	7%	37	13%	13	3%
Nota 3	63	9%	37	13%	26	7%
Nota 4	234	33%	113	39%	111	29%
Nota 5	344	48%	77	27%	230	60%
TOTAL	720	100%	288	100%	384	100%

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Figura 14: Frequências absolutas do total de respostas



Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Agregou-se as respostas para cada uma das 7 dimensões previstas no modelo de avaliação de maturidade do IBGC e apresentamos a frequência relativa de cada uma das cinco respostas possíveis. As próximas tabelas apresentam essa visão de forma agregada, no conjunto dos dois segmentos e posteriormente, para cada um desses dois segmentos separadamente. Os dados além de também demonstrarem a diferença entre os dois segmentos pesquisados, indicam que existe uma diferença na concordância relativa às afirmações que se referem a cada uma das sete dimensões. Apenas a título exemplificativo, enquanto “governança” tem concordância total ou em partes de 88%, a dimensão “sistemas, dados e modelos de informação” tem concordância total ou em partes de 64%. Essas ponderações serão consideradas ao final desta seção, quando avaliaremos os principais insights trazidos pelas respostas.

“A” representa a visão agregada – dos dois segmentos, “V” representa os dados dos respondentes do setor de varejo e “F” do setor financeiro.

Tabela 8: Frequências relativa em cada dimensão

	Discordo totalmente			Discordo em partes			Nem discordo nem concordo			Concordo em partes			Concordo totalmente		
	A	V	F	A	V	F	A	V	F	A	V	F	A	V	F
Estratégia	8%	17%	2%	16%	25%	9%	7%	8%	6%	33%	33%	33%	36%	17%	50%
Governança	3%	4%	1%	1%	2%	0%	8%	12%	6%	20%	22%	19%	68%	60%	74%
Política	3%	7%	0%	3%	7%	0%	10%	14%	8%	40%	46%	36%	44%	26%	56%
Processo de GRC e interação com demais ciclos de negócio	2%	5%	0%	2%	5%	2%	10%	17%	5%	43%	56%	33%	43%	17%	60%
Linguagem e método de avaliação	1%	1%	0%	5%	10%	2%	5%	10%	3%	30%	48%	17%	59%	31%	78%
Sistemas, dados e modelos de informação	8%	11%	7%	14%	25%	7%	14%	25%	7%	32%	31%	31%	32%	8%	48%
Cultura, comunicação, treinamento e melhoria contínua	7%	17%	0%	14%	30%	4%	7%	3%	9%	37%	47%	31%	35%	3%	56%

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Como forma de facilitar a compreensão e análise dos dados trazidos pelas respostas, fizemos uma correlação das respostas recebidas com escala numéricas (de 1 a 5):

- Discordo totalmente: 1
- Discordo em partes: 2
- Nem discordo nem concordo: 3
- Concordo em partes: 4
- Concordo totalmente: 5

A partir daí, consolidou-se as visões de maneira agregada e em cada um dos dois segmentos, bem como a diferença percentual entre as notas. Além das considerações que fizemos ao analisar as tabelas anteriores – sobre evidente diferença entre as avaliações dadas em cada uma das sete dimensões e a diferença entre os dois segmentos econômicos estudados, a visão da Tabela 9 e da Figura 15 nos indica um insight adicional de que a diferença de visão entre os dois segmentos não é linear quando comparamos em cada dimensão. Enquanto no aspecto “Governança”, existe uma diferença inferior a 10%, na dimensão “Cultura,

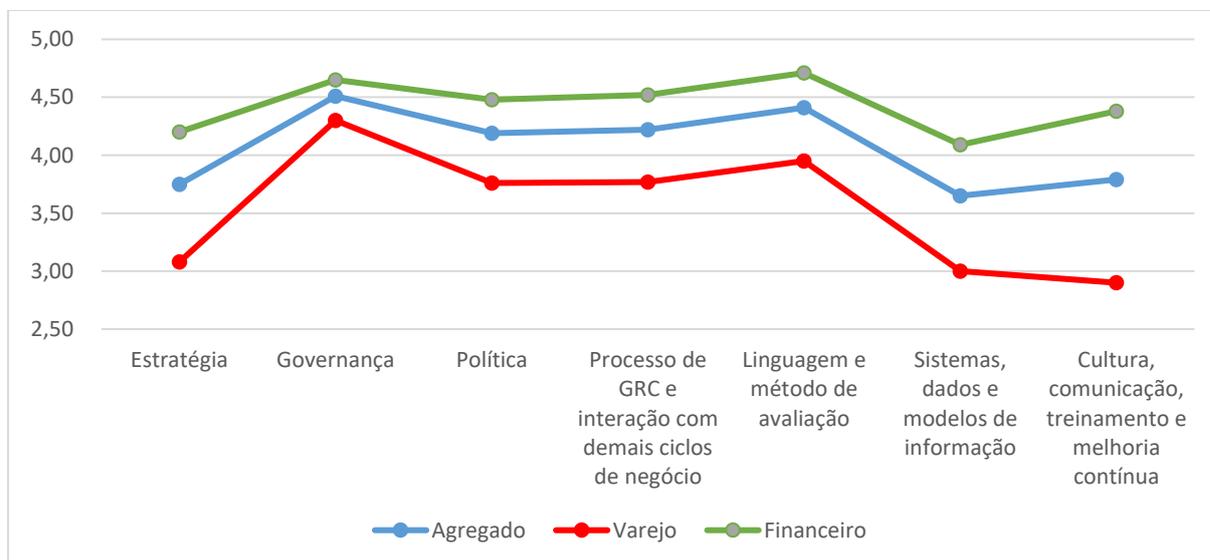
comunicação, treinamento e melhoria contínua” a visão entre os respondentes gera uma diferença de quase 50%.

Tabela 9: Avaliação para cada dimensão do modelo do IBGC

	Agregado	Segmento Varejo	Segmento Financeiro	% Dif
Média Total	4,13	3,63	4,46	123%
Estratégia	3,75	3,08	4,20	136%
Governança	4,51	4,30	4,65	108%
Política	4,19	3,76	4,48	119%
Processo de GRC e interação com demais ciclos de negócio	4,22	3,77	4,52	120%
Linguagem e método de avaliação	4,41	3,95	4,71	119%
Sistemas, dados e modelos de informação	3,65	3,00	4,09	136%
Cultura, comunicação, treinamento e melhoria contínua	3,79	2,90	4,38	151%

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Figura 15: Representação gráfica da avaliação por dimensão



Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Com base na associação entre a escala de concordância utilizada no Instrumento de Coleta e as escalas do modelo de avaliação da maturidade do IBGC, realizamos um enquadramento geral e de cada dimensão.

Na visão agregada, as respostas indicam a alocação como “Otimizado” para a maturidade das práticas de GRC nas empresas pesquisadas. Ao observar as dimensões separadamente, vemos que “Governança”, “Linguagem e método de avaliação”, “Processos de GRC e interação com os demais ciclos de negócio” e “Política” são vistos como otimizado, enquanto as dimensões “Cultura, comunicação, treinamento e melhoria contínua”, “Estratégia” e “Sistemas, dados e modelos de informação” foram classificados como “Consolidado”.

As classificações variam entre os segmentos varejo e financeiro, alinhado com o que falamos anteriormente. Para o segmento “Varejo”, vemos que as respostas dadas às assertivas indicam uma classificação geral de maturidade como “Consolidado”, sendo que na visão entre as dimensões, vemos que 4 delas estão alocadas neste grupo, 1 está alocada como “Otimizado” e 2 dimensões foram alocadas como “Definido”. Para o setor Financeiro, todas as dimensões e o resultado geral ficaram no grupo “Otimizado”, em que pese terem notas distintas, conforme ordenamento constante no Quadro seguinte. A Figura 16, apresentada na sequência, demonstra visualmente o enquadramento nas classificações de maturidade. Com base nas respostas, vê-se que nenhuma dimensão em nenhum dos dois segmentos econômicos foi alocado nos grupos Inicial ou Fragmentado.

Quadro 35: Ordenamento das dimensões do modelo do IBGC

	Agregado	Varejo	Financeiro
Governança	1º	1º	2º
Linguagem e método de avaliação	2º	2º	1º
Processo de GRC e interação com demais ciclos de negócio	3º	3º	3º
Política	4º	4º	4º
Cultura, comunicação, treinamento e melhoria contínua	5º	7º	5º
Estratégia	6º	5º	6º
Sistemas, dados e modelos de informação	7º	6º	7º

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Figura 16: Enquadramento no modelo do IBGC

	Estratégia	Governança	Política	Processo de GRC e interação com demais ciclos de negócio	Linguagem e método de avaliação	Sistemas, dados e modelos de informação	Cultura, comunicação, treinamento e melhoria contínua
Otimizado							
Consolidado	 	 	 	 	 	 	 
Definido							
Fragmentado							
Inicial							

 Agregado  Varejo  Financeiro

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Consideramos as respostas recebidas, identificamos a seguir, as principais avaliações feitas para cada dimensão e para os aspectos gerais, retomando os principais temas abrangidos pelos especialistas e os pontos principais de cada dimensão, conforme modelo de maturidade do IBGC, sumariado abaixo:

Tabela 10: Sumário da Dimensão 1 - Estratégia

Aspecto contemplado	Agregado	Varejo	Financeiro
- Priorizações de investimento consideram GRC	3,07	2,33	3,56
- Metas de desempenho das áreas contemplam a GRC	3,33	2,33	4,00
- Alinhamento dos objetivos da gestão com a GRC	3,67	3,00	4,11
- Integração de GRC com a gestão	3,93	3,17	4,44
- Compatibilidade de GRC com porte e complexidade	4,07	3,17	4,67
- Avaliação e mensuração de riscos disseminada	4,47	4,50	4,44

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

De acordo com as respostas, a dimensão foi classificada no agregado como na faixa “Consolidado”. Para o setor financeiro, foi classificado como “Otimizado” e para o setor varejo como “Consolidado”. Setor Financeiro tem uma nota 36% superior ao Varejo.

A classificação “Consolidado” prevista no modelo de avaliação de maturidade do IBGC tem como principais características a existência de uma estratégia de riscos claramente definida e implementada, com metas monitoradas. Para o estágio seguinte

– o “Otimizado”, as principais diferenças são a integração desta estratégia com os demais ciclos de gestão da Companhia e a existência de metas de negócio que são formadas e influenciadas pela gestão de riscos.

A maior nota obtida no setor Financeiro foi a compatibilidade com o porte e a complexidade da Instituição. Este aspecto é muito inferior no Varejo, o que indica a inexistência de estruturas que tenham a cobertura adequada na avaliação dos respondentes.

Ao avaliar o quanto o monitoramento dos riscos e a probabilidade de impacto e ocorrência são disseminados entre os executivos, a nota foi praticamente a mesma entre os segmentos, ambas elevadas. Isso demonstra que os principais riscos são de conhecimento da Administração em ambos os segmentos, em que pese o apontamento de estruturas mais enxutas no varejo.

As menores notas do segmento Varejo são relativas aos quesitos (a) escolha e priorização de projetos e investimentos com base nas avaliações de GRC e (b) que as metas de desempenho de negócios contemplam *inputs* de gestão de riscos corporativos. Os dois aspectos também representam a maior distância com o segmento financeiro. Aqui, temos uma indicação de que as práticas de GRC ainda não permeiam decisões estratégicas mais pervasivas nem influenciam os direcionamentos estratégicos e metas do negócio no varejo, como já ocorre no segmento financeiro, de acordo com os respondentes.

Tabela 11: Sumário da Dimensão 2 - Governança

Aspecto contemplado	Agregado	Varejo	Financeiro
- Avaliação de GRC por agente externo	3,87	3,33	4,22
- Reporte de GRC ao CEO ou governança	3,93	3,17	4,44
- GRC é pauta permanente na governança, com tempo e profundidade adequados	4,40	4,00	4,67
- Acompanhamento permanente dos riscos e mitigações, deficiências, não cumprimentos legais e desvios éticos	4,63	4,67	4,61
- GRC com acesso e reporte à alta gestão e governança	4,80	4,50	5,00
- Estrutura específica e independente	4,80	4,67	4,89

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Governança é a dimensão em que os segmentos Varejo e Financeiro mais se aproximam. Em parte das assertivas do instrumento de coleta, as notas são similares.

Na visão agregada e em ambos os segmentos individualmente, a classificação obtida com as respostas foi “Otimizado”. De acordo com o IBGC, este estágio é caracterizado pela existência de uma segunda linha de defesa independente, com funções claramente definidas e objetivos que ofereçam valor para a Companhia. Ainda, caracteriza-se por uma estrutura funcional bem estabelecida, sem sobreposições e alinhada às estratégias da Companhia.

O principal GAPs é no quesito que avalia se o principal profissional e GRC se reporta diretamente ao CEO e ao Conselho. O posicionamento funcional da área e de seu principal executivo dá peso a esta agenda e possibilita uma comunicação direta e fluída com a Alta Administração. Enquanto no setor Financeiro, este quesito foi avaliado com concordância em 4,44 (de escala entre 1 até 5), ela é 40% menor para os respondentes do segmento do Varejo, indicando que a existência de camadas intermediárias pode

A indicação sobre acesso da área de GRC à Alta Administração é elevada em ambos os segmentos. Sua independência em relação às áreas de negócios também é apontada pela maioria dos respondentes, alcançando concordância máxima para os respondentes do setor financeiro – nota 5,00 e 4,50 para o setor de varejo. Apenas 1 resposta não indicou concordância com o fato das atividades de GRC serem realizadas em estrutura distinta à Auditoria Interna. Nas demais 14 respostas, a concordância foi plena.

As respostas indicam concordância elevada de que a alta administração e governança conheçam os principais riscos, planos de mitigação, não conformidades em relação a leis e políticas internas, deficiências de controle e desvios éticos.

A maioria das respostas indicam que a Governança destina foco, tempo e profundidade adequados. Esse tema tem concordância na escala de 4,40 dos respondentes, elevada em ambos os segmentos.

A avaliação de GRC por agente externo foi o aspecto com menor concordância nesta dimensão. Teve avaliação em escala de 3,87, na visão conjunta dos dois segmentos. Aqui, resulta um insight importante a oportunidade um olhar externo e independente – seja da auditoria (3ª linha de defesa da própria instituição), de consultoria ou órgão de classe sobre as práticas de gestão de risco que existem na Companhia.

Tabela 12: Sumário da Dimensão 3 - Política

Aspecto contemplado	Agregado	Varejo	Financeiro
- Acompanhamento externo sobre aplicação das diretrizes de GRC	3,80	3,33	4,11
- Diretrizes de risco permanentemente atualizadas em função de tendências do mercado	3,87	3,50	4,11
- Temas críticos do negócio e de riscos são normatizados	4,07	3,50	4,44
- Diretrizes de risco permanentemente atualizadas em função de estratégia e aspectos gerais do negócio	4,27	4,00	4,44
- Acompanhamento interno sobre aplicação das diretrizes de GRC	4,40	4,00	4,67
- Políticas e diretrizes de GRC são normatizados e divulgados de maneira consistente	4,47	4,00	4,78

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Política foi categorizado como “Otimizado” para o setor Financeiro e “Consolidado” no setor Varejo, com um GAP de quase 20% entre as escalas de respostas entre os dois segmentos.

Segundo o IBGC, na classificação “Consolidado”, a prática de GRC é caracterizada por políticas e procedimentos desenvolvidos e aplicados em todo o negócio, sendo permanente atualizados. Para a categoria seguinte – “Otimizado”, inclui-se que esses procedimentos são regularmente avaliados e referendados por terceiros.

Temas críticos do negócio são normatizados, de acordo com a maioria das respostas recebidas. Tivemos apenas 1 discordância neste aspecto e 2 respostas neutras. A concordância no setor Financeiro foi 27% superior que a do Varejo. Quando abordamos a normatização de temas ligados às práticas de risco, a concordância se eleva em ambos os segmentos e o GAP entre os segmentos cai para 6%. Esta análise conjunta pode resultar em um insight de que existe oportunidade de avançar em se normatizar e formalizar mais amplamente as políticas e diretrizes das áreas de negócio, especialmente no Varejo.

Quando consolidamos as respostas em relação à divulgação das diretrizes e políticas de GRC, vemos que alta concordância em ambos os segmentos (4 ou mais), em que pese seja 20% inferior no Varejo.

A maioria dos respondentes concorda que as políticas e diretrizes de GRC são atualizadas e observam o dinamismo do negócio. A concordância agregada dos

respondentes foi de 4,27. Quando falamos de atualizações decorrentes de tendências do mercado essa nota alcança 3,87, caindo nos dois segmentos, um pouco mais acentuadamente no Varejo. Enxerga-se decorrente destas respostas, uma oportunidade de ampliar o olhar externo e capturar mais fortemente tendências de mercado ao revisar as diretrizes de GRC.

A maioria dos respondentes concorda que há acompanhamento sobre aplicação das diretrizes de GRC. Contudo, em escalas diferentes quando considerado o acompanhamento “interno” e “externo”. A concordância alcança 4,40 em relação ao acompanhamento interno e 3,80 quando se pensa em acompanhamento externo, com GAPs similares entre os dois segmentos pesquisados.

Tabela 13: Sumário da Dimensão 4
Processos de GRC e integração com demais ciclos de negócio

Aspecto contemplado	Agregado	Varejo	Financeiro
- Gera indicadores úteis na gestão	3,73	2,50	4,56
- Capacidade de propor mitigações efetivas que reduzem probabilidade e/ou impacto	4,13	3,67	4,44
- Governança monitora e aprimora processo de GRC	4,20	3,83	4,44
- Capacidade de capturar os principais riscos e de mensurar adequadamente seus efeitos	4,40	4,00	4,67
- Identifica corretamente descumprimentos legais	4,47	4,33	4,56
- Monitora e reporta planos de mitigação críticos	4,47	4,33	4,56

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Esta dimensão foi categorizada como “Otimizado” para o setor Financeiro e “Consolidado” no setor Varejo, com um GAP de 20% entre as escalas de respostas entre os dois segmentos.

De acordo com o modelo do IBGC, a classificação “Consolidado” para esta dimensão indica que os processos de identificação e avaliação de riscos são bem definidos e estruturadas e que os gestores monitoram permanentemente seus riscos. Na visão “Otimizado”, inclui-se que esses processos estão interligados aos objetivos estratégicos da Companhia e que as atividades de monitoramento de riscos são coordenadas e eficientes.

As respostas indicam alto grau de concordância em relação à capacidade da Companhia em capturar os principais riscos e de diferentes naturezas e de mensurar

adequadamente seus efeitos. Na escala de 1 a 5, essa resposta teve concordância de 4,4 na visão agregada e com notas elevadas em ambos os setores econômicos.

A confirmação de que a prática de GRC da Companhia resulta em redução consistente da probabilidade e/ou impacto dos riscos tem nível de concordância elevado e mantém o GAP médio da dimensão entre os dois segmentos. Idem em relação à visão de que os riscos e preocupações sinalizadas por GRC indicam aspectos que podem afetar os objetivos estratégicos da Companhia.

A concordância de que as práticas de GRC permitem identificar eventuais não cumprimentos legais e normativos junto com a concordância de que os planos de ação em relação às mitigações críticas são conhecidos e acompanhados pela Governança são os aspectos com maior nota nesta categoria e com menor gap entre os dois segmentos – na casa de 5% em cada tópico.

A geração de indicadores úteis e utilizados na gestão é o ponto de menor concordância na categoria. Alcança escala geral de 3,73 no agregado e tem um GAP com varejo 82% pior do que o setor financeiro, chegando a uma concordância de 2,50, entre as mais baixas de toda a pesquisa. Excluído o respondente com maior nota entre os varejistas que apontou elevada concordância para este tópico, a média dos demais chega a 2. Este é um aspecto muito relevante e que nos indica que GRC nas Companhias pesquisadas ainda carece de se conectar às necessidades das áreas de negócio e possa, a partir disso, produzir indicadores que possam auxiliar a gestão, dando indicativos úteis relativos à antecipação de riscos ou redução de seu impacto pelas áreas de Negócios.

Tabela 14: Sumário da Dimensão 5 – Linguagem e métodos de avaliação

Aspecto contemplado	Agregado	Varejo	Financeiro
- Teste de stress utilizado no cálculo de apetite	3,80	2,83	4,44
- Assunção de riscos críticos destinada à Governança	4,47	4,00	4,78
- Procedimentos implementado e aplicado de maneira consistente para identificação, mensuração e mitigação de riscos e baseado em framework reconhecido	4,51	4,11	4,78
- Definição de apetite de risco quantitativo e qualitativo	4,53	4,25	4,72

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Esta dimensão foi categorizada como “Otimizado” para o setor Financeiro e “Consolidado” no setor Varejo, com um GAP de quase 20% entre as escalas de respostas entre os dois segmentos.

No modelo de avaliação de maturidade do IBGC, a classificação “Consolidado” indica que as abordagens empregadas pela Companhia são padronizadas e consistentes para definir o apetite de riscos e para as atividades de identificação, mensuração e mitigação de riscos. No estágio seguinte, inclui-se que essas definições consideram cenários de “Stress” com variáveis adicionais àquelas de um cenário de normalidade.

A maioria dos critérios avaliados nesta dimensão tiveram respostas próximas à banda média. Igualmente, o GAP entre os dois setores pesquisados também foi consistente. Exceção em relação à afirmação sobre se o apetite de risco da Companhia considera situações de stress. Nesse aspecto a nota agregada ficou abaixo da média geral, especialmente nas respostas de empresas do varejo, que ficaram 56% abaixo da nota do segmento financeiro. Podemos entender como uma oportunidade que as Companhias incorporem em seus modelos certas variáveis que representem cenário de stress para a definição de seus níveis de aceitação de risco, uma vez que hoje ele é feito substancialmente com base em cenários de normalidade ou já vivenciados.

Tivemos elevada concordância (14 das 15 respostas) de que os procedimentos de GRC das empresas estão baseados em frameworks reconhecidos.

Mesmo nível de concordância foi obtida em relação à existência de um apetite formal de risco, aprovado pela Administração e de que esse apetite considera aspectos qualitativos e quantitativos. Idem para à afirmação de que todos os riscos com impacto superior ao apetite são reportados à Administração e acompanhado por ela.

Tabela 15: Sumário da Dimensão 6 – Sistemas, dados e modelos de informação

Aspecto contemplado	Agregado	Varejo	Financeiro
- Geração de reportes decorrentes de GRC com viés substancialmente regulatório	2,87	2,50	3,11
- Liderança conhece, entendem e usam reportes de GRC	3,63	2,83	4,17
- Uso extensivo de dados no processo de GRC	3,80	2,83	4,44
- Integração com dados e acompanhamentos on-line	3,93	3,50	4,22
- Ciclos de negócio e TI utilizados no processo de GRC	4,07	3,50	4,44

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Esta dimensão foi categorizada como “Otimizado” para o setor Financeiro e “Definido” no setor Varejo, sendo que o primeiro tem nota de concordância 36% superior ao segundo. Trata-se da dimensão com pior nota na visão agregada e para o setor Financeiro e a segunda pior para o Varejo.

Como principais características indicadas pelo modelo do IBGC, o estágio “Definido” indica que os modelos de informação e reportes são definidos e compreendidos, com informações corretas e completas. Já na visão mais madura, chamada “Otimizado”, caracteriza-se pelo aproveitamento de tecnologias e integração com os sistemas da Companhia.

As respostas indicam que parte relevante dos reportes que são produzidos por GRC são destinados aos reguladores ou tem um viés de prevalência regulatória. As atividades de GRC foram historicamente impulsionadas pelas ações dos reguladores e de acordo com as respostas, vê-se que o produto das práticas de GRC ainda tem muito esse viés. Existem, portanto, desafios para que sejam mais voltadas às atividades de negócio e às realidades de cada empresa, alimentando à liderança com informações úteis e que tenham aplicabilidade.

Existe um GAP relevante entre os dois segmentos em relação à utilização dos reportes e relatórios gerados pelo Gerenciamento de Riscos Corporativos. Enquanto a concordância para as empresas do setor Financeiro chega a 4,17, ela é de 2,83 para as empresas do Varejo. Quanto à afirmação sobre a plena compreensão daqueles que recebem esses reportes, vemos que o GAP é ainda maior, com notas de 4,22 e 2,83, respectivamente. Isso indica uma clara lacuna no Varejo: as avaliações feitas a partir de suas práticas ainda não é disseminada e não existe compreensão plena da

liderança que o recebe, impactando no valor que a prática pode oferecer à gestão e à Companhia.

O uso extensivo de dados é apontado como uma lacuna no Varejo. 2,83 é o nível de concordância de que as empresas fazem uso extensivo em suas atividades de identificação, mensuração e mitigação de riscos. No setor Financeiro, as respostas indicam um nível 56% superior.

Ao propor a concordância sobre se a Companhia se aproveita dos sistemas de negócios e tecnologias disponíveis no negócio, existe concordância na escala de 4,44 no setor Financeiro. Na maioria das respostas do Varejo, a indicação foi “Não discordo nem concordo”, o que pode indicar falta de conhecimento de que a prática da gestão de risco se utiliza do ferramental disponível ou de que essa utilização não é perceptível.

Tabela 16: Sumário da Dimensão 7 – Cultura, comunicação, treinamento e melhoria contínua

Aspecto contemplado	Agregado	Varejo	Financeiro
- Cultura de risco disseminada em toda a Companhia	3,40	2,33	4,11
- Novos processos e projetos têm visão de riscos	3,53	2,50	4,22
- Times compreendem os benefícios da gestão de risco	3,67	2,67	4,33
- Treinamentos regulares sobre a temática	4,13	3,50	4,56
- Liderança ativa na identificação e mitigação de riscos	4,20	3,50	4,67

Fonte: Elaborado pelo próprio autor (2023) com base na pesquisa realizada

Esta dimensão foi categorizada como “Otimizado” para o setor Financeiro e “Definido” no setor Varejo, sendo que o primeiro tem nota de concordância 51% superior ao segundo. Trata-se da dimensão com pior nota na visão do Varejo e com maior diferença entre os níveis de concordância respondido entre os segmentos.

Uma cultura de riscos bem disseminada é um aspecto de baixa concordância e representa uma oportunidade de avanço nessa agenda: ampliar o conhecimento dos times sobre a necessidade e valor de se reduzir os principais aspectos que podem dificultar o cumprimento dos objetivos estratégicos é fundamental para que ela alcance os resultados esperados e produza o valor.

Alta Administração e funcionários compreendem a necessidade e benefícios de uma gestão de risco efetiva também representa uma lacuna no segmento de Varejo, cuja ação está associada ao ponto acima, em que pese os elevados níveis de concordância sobre a Companhia oferecer treinamentos regulares sobre o tema. Este segundo tópico também tem níveis elevados de concordância no segmento Financeiro.

De todos os aspectos avaliados nessa dimensão, o com maior concordância é em relação ao envolvimento da liderança no processo de identificação e mitigação dos riscos sob sua responsabilidade. Ele atinge 3,50 no Varejo e 4,67 no setor Financeiro.

Novos processos e projetos considerarem a avaliação de seus principais riscos ainda não é uma prática reconhecida pelos profissionais de Varejo nas práticas atuais de suas Companhias e deve compor a lista de tópicos prioritários para que seja possível alcançar um patamar mais elevado de maturidade.

Com base nas respostas recebidas, vemos que existem uma elevada concordância – total ou parcial - com relação a maioria dos aspectos considerados no Instrumento de Coleta, que expressam os tópicos relevantes sinalizados pelos especialistas e os itens constantes no modelo de avaliação da maturidade proposto pelo IBGC.

Em que pese, vemos diferenças visíveis na maior parte dos aspectos entre os segmentos Financeiro e de Varejo.

O setor Financeiro apresenta uma maturidade mais elevada. No agregado e nas sete dimensões, as respostas indicam estar no patamar mais elevado do modelo de referência que utilizamos, ainda que existam algumas oportunidades, especialmente relacionadas à (a) vinculação de metas de negócios das diferentes áreas com as práticas de GRC, (b) priorizações de investimento que devem considerar os temas de risco, (c) avanços na utilização de dados e (d) uma cultura de risco, disseminada e que permita o pleno reconhecimento da relevância dessa prática.

O Varejo, por sua vez, tem patamar similar ao setor Financeiro na dimensão “Governança”, que inclui aspectos como a existência de estrutura própria e

independente e acesso a alta gestão. Nos demais aspectos avaliados, a maturidade é intermediária – gravitando entre “Definido” e “Consolidado”. Na visão média das dimensões não foi considerada nos menores patamares, em que pese alguns aspectos específicos com notas inferiores, conforme comentou-se na análise acima. Além das mesmas lacunas do setor Financeiro, destaca-se lacunas próprias como compatibilidade das estruturas de GRC com o porte e complexidade das Companhias, utilização extensiva de dados em suas práticas e existência de uma cultura de riscos e comunicação efetivas sobre o tema, além da geração de indicadores que sejam úteis aos executivos da empresa. Vê-se, no conjunto, que as empresas desta área ainda carecem de melhor estruturar suas práticas, ampliar os esforços para que existam avanços nessas lacunas, de tal sorte que ela possa se consolidar internamente e ser mais pervasiva.

Abaixo um resumo com os principais aspectos das análises apresentadas neste capítulo.

- a) Mais de 80% das respostas indicaram concordância parcial ou total em relação às afirmativas sobre práticas de gerenciamento de risco esperadas.
- b) A concordância total é o dobro no setor financeiro do que no setor de varejo.
- c) Em uma associação das respostas com uma escala numérica de 1 a 5, tem-se uma nota de 4,13 do conjunto de empresas; sendo 3,63 do setor de varejo e 4,46 do segmento financeiro – uma diferença relativa de 23%.
- d) Com base nessas notas, o setor financeiro é classificado como “Otimizado” – que é o maior nível da escala do IBGC e o setor de Varejo fica situado na faixa de Consolidado que é a 4^o camada, sendo que 2 das 7 dimensões avaliadas ficam situada em uma faixa abaixo, intermediária da escala.
- e) A maioria das empresas nos dois segmentos aponta a existência de um processo estabelecido para avaliação e mensuração de seus principais riscos. No varejo, há indicação de incompatibilidade entre a estrutura que tem essa missão e o porte e complexidade das empresas, além de se apontar uma integração com a gestão ainda intermediária. Além disso, esse processo de avaliação dos riscos não se conecta de maneira satisfatória com a priorização de investimentos e metas de desempenho dos times.

- f) Elevados patamares de empresas com estruturas próprias e dedicadas a este tema e que reportam à alta gestão, com baixo acesso ao principal executivo e com baixos níveis de avaliação externa quanto à sua efetividade.
- g) A maioria das empresas pesquisadas possuem diretrizes formais sobre o processo de gestão de risco, acompanhamento estruturado sobre aplicação dessas diretrizes e atualizações desses marcos em função de mudanças nos negócios.
- h) Efetividade do monitoramento dos principais riscos e de sua mensuração e, também, do reporte de planos de ação de aprimoramento das mitigações desses riscos. No varejo, a principal deficiência está na geração de indicadores que sejam úteis à gestão das áreas de negócios.
- i) Baixo uso de aspectos fora da normalidade na definição de apetites de risco e outras métricas qualitativas, o que indica que as empresas ainda pensam pouco em situações de atipicidade severa.
- j) A dimensão Sistemas, Dados e Modelos foi a nota baixa na visão agregada e no segmento financeiro. Apresenta também um GAP relevante com o segmento varejo (média é de 23% e neste caso temos 36%). Uso extensivo de dados destaque-se em patamar mais baixo que a média das respostas. Também vemos que a produção de outputs do processo de GRC ainda tem um caráter muito regulatório.
- k) O tópico de Cultura e melhoria contínua é o de avaliação mais baixa do segmento de varejo. Neste segmento, ainda existem lacunas importantes para disseminação de uma cultura de risco, compreensão dos benefícios desse sistema e incorporação desta avaliação de risco em novos projetos e iniciativas. No segmento financeiro, todos estes aspectos estão na faixa mais madura de avaliação.

5 CONCLUSÃO

Ao longo da pesquisa, evidenciou-se a relevância do tema gestão de risco para as organizações no cenário contemporâneo, e sua presença extensiva nos estudos recentes sobre Gestão Empresarial. O momento do mercado e o contexto econômico atual, caracterizados por profundas interconexões, têm como uma de suas maiores marcas o elevado nível de incertezas, que podem impactar os objetivos organizacionais.

Em qualquer cenário, incertezas podem potencializar os efeitos indesejáveis e, portanto, riscos mal identificados, dimensionados e administrados podem impactar de maneira relevante a situação financeira, o posicionamento de mercado e até mesmo a continuidade das organizações. Para reduzir a probabilidade e o impacto potencial de eventos indesejados, as práticas de gerenciamento de riscos têm sido cada vez mais relevantes e presentes nas empresas.

Para que as práticas de Gerenciamento dos Riscos Corporativos cumpram plenamente o propósito de preservar os objetivos estratégicos, é fundamental garantir que as suas diretrizes e ações tenham elevada maturidade. O processo de atingimento dessa maturidade pressupõe a transitoriedade de um estágio inicial para outro mais saliente, em que as diretrizes e ações são documentadas, aplicadas consistentemente, além de serem permanentemente monitoradas e aprimoradas.

Avaliar a maturidade permite conhecer com maior profundidade a situação atual dessas práticas em cada empresa e ter a indicação sobre quais são as principais lacunas e caminhos para sua evolução. Durante a pesquisa, identificou-se na literatura distintos, porém congruentes, modelos de avaliação da maturidade de GRC, desenvolvidos localmente e no exterior em duas décadas entre os anos de 1997 e 2017.

Para compreender o fenômeno de maturidade das práticas de Gerenciamento de Risco, a pesquisa apresentou justificativas para a delimitação dos setores econômicos e empresas que foram estudadas. A consulta a especialistas de mercado, com vasta e justificada experiência em adição aos aspectos contemplados no modelo de avaliação do Instituto Brasileiro de Governança Corporativa – IBGC, selecionado de forma justificada como referência para a pesquisa, permitiu a formulação de instrumento de coleta. O instrumento visou identificar informações sobre a maturidade em empresas de grande porte e negociadas na Bolsa Brasileira no âmbito geral e nas

dimensões previstas no modelo, que representam, em última instância os pilares esperados para que GRC funcione e seja efetivo.

Com base nas respostas coletadas, abrangendo profissionais com senioridade e experiência nas organizações pesquisadas, foi possível identificar o nível de maturidade da gestão de riscos nos segmentos pesquisados: as práticas de GRC no setor Financeiro foram classificadas como “Otimizadas” – nível mais alto - e as do setor de Varejo como “Consolidadas” – quarta das cinco escalas.

O trabalho contém uma análise detalhada das respostas recebidas, principais congruências entre os segmentos, principais particularidades de cada segmento e de cada dimensão, além das lacunas mais evidentes para que as empresas ampliem a maturidade de suas práticas de Gestão de Riscos, destacando-se:

- a) Maior congruência entre os setores no aspecto Governança, que indica existência de estrutura própria de GRC - independente e com acesso à Alta Administração.
- b) Maiores oportunidades nos dois segmentos relacionadas: (i) à vinculação de metas de negócio com GRC, (ii) às prioridades de investimento que considerem às avaliações de risco, (iii) ao avanço na utilização de dados no processo de identificação, mensuração e mitigação dos principais riscos e (iv) a maior disseminação de uma cultura corporativa que valorize e incorpore a gestão de riscos.
- c) O setor de Varejo apresenta oportunidades adicionais relacionadas: (i) à compatibilidade da estrutura de GRC com complexidade e porte da Companhia, (ii) à ampliação da comunicação interna sobre o tema e (iii) à geração de indicadores úteis às áreas de negócios.

Para aplicações futuras, é possível sugerir o aumento da amostra nos segmentos econômicos contemplados na pesquisa ou mesmo a ampliação da pesquisa em segmentos econômicos distintos. Para aprofundamento das respostas, podem ser incluídas entrevistas pessoais com os respondentes, de modo a se obter detalhes mais amplos sobre as respostas, a partir da interação pessoal.

Como considerações finais, permanece a expectativa de que o estudo ajude a fortalecer a relevância da Gestão de Riscos na agenda prioritária das empresas e estimule a avaliação sobre a efetividade no objetivo de contribuir para a realização das estratégias estabelecidas. Além disso, espera-se que o estudo forneça *insights*

úteis sobre os principais pontos que merecem atenção dos gestores no propósito de aprimorá-la e qual é o estágio atual de GRC em outros agentes de mercado.

REFERÊNCIAS

Associação Brasileira de Normas Técnicas. ISO:31.000. **Gestão de Riscos – Princípios e Diretrizes** (p. 1-32). Rio de Janeiro: Editora ABNT, 2009.

AON – **Pesquisa Global de Gerenciamento de Risco**. São Paulo, 2019. Disponível em <www.aon.com>. Acesso em: 22 mai.2022

ARAÚJO, M.; OLIVEIRA, P. S. C.; MAZIERI, M. R.; GARCEZ, M. P. Framework para Auditoria de Programas e Projetos em Tempo de Execução. **IPTEC – Revista Inovação, Projetos e Tecnologias**. São Paulo, v.7, n.1, p. 1-15, jan-jun. 2019

ARRUDA, C.L.; MENCHINI, F.; RUSSO, P.T. Percepção sobre os fatores de gerenciamento de riscos corporativos que influenciam o planejamento estratégico. **Future Studies Research Journal** – FIA Business School, São Paulo: v.11, n. 2, P. 241-254, mai-ago 2019

BANCO CENTRAL DO BRASIL. **Dados Selecionados das Instituições Financeiras**. Disponível em <<https://www3.bcb.gov.br/ifdata/index.html#>>. Acesso em: 22.jan.2023.

BERMEJO, P.H.S. **ForRisco: gerenciamento de riscos em instituições públicas na prática**. Brasília/DF: Evobiz, 2018.

BRAMONT, P. **Maturidade em governança corporativa: diretrizes para um modelo preliminar**. 2012. 131f. Dissertação (Mestrado em Gestão do Conhecimento e da Tecnologia da Informação) – Universidade Católica de Brasília, Brasília – DF, 2012.

COLANTONIO, B.; CALDEIRA, A.; OLIVA, F. L. Transformação do processo de gestão de risco em uma empresa brasileira de alumínio. **IX Encontro de Estudos em Estratégia – 3Es 2020**, setembro de 2020.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **Enterprise Risk Management - Integrating with Strategy and Performance**. 2017. Disponível em <www.coso.org>. Acesso em: 27 mar. 2022.

Committee of Sponsoring Organizations of The Treadway Commission. **Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance**. 2017. Disponível em <<http://iiabrazil.org.br>>. Acesso em: 26 dez. 2022.

FARRELL, M. e GALLAGHER, R. Moderating influences on the ERM maturity-performance relationship. **Research in International Business and Finance**. The University of Edinburgh, 2018.

FERRO, D. S. **Gestão de riscos corporativos: um estudo multicaso sobre seus métodos e técnicas**, 2015, 118f. Dissertação (Mestrado em Administração) – Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, SP, 2015.

FILARDI, F.; MACEDO, F. Análise dos resultados da implantação dos processos integrados de governança, riscos e compliance em empresas de capital aberto. **XLVI Encontro da Anpad**, setembro de 2022.

FRANCO, F. L. **Governança e Gestão de Riscos em Organizações Públicas**.

Disponível em

<brasil.mackenzie.br/apps/files/fpmb_governanca_e_gestao_de_riscos_em_organizacao_publicas_apostila.pdf>. Acesso em: 22.jul.2022

FRASER, P.; MOULTRIE, J.; GREGORY, M. The use of maturity models / grids as a tool in assessing product development capability: a review. **IEEE International Engineering Management Conference**. Cambridge UK, 2002.

HILLSON, D.A. Towards a Risk Maturity Model. **The International Journal of Project & Business Risk Management**. v. 1, n. 1, p. 35-45, 1997.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**. 5. ed. São Paulo: 2015. 103 p.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Gerenciamento de riscos corporativos: evolução, governança e estratégia**. São Paulo: 2017. 64 p.

INSTITUTO BRASILEIRO DO VAREJO. Ranking 2022 IBEVAR. Disponível em <<https://www.ibevar.org.br/ranking-ibevar-2022>>. Acesso em: 22.jan.2023

KPMG. **Gerenciamento de Riscos: os principais fatores de risco divulgados pelas empresas abertas brasileiras**. 7ª. edição. São Paulo, 2022.

KPMG. **Pesquisa da Maturidade do Processo de Gestão de Riscos no Brasil**. 2ª edição. São Paulo, 2020.

MARQUES, L.; MULLER, S.H.; SILVA, M. Z. Gestión de riesgos corporativos: percepción de los Chief risk officers. **Revista de Facultad de Ciencias Económicas**, vol. 27, n. 2, 2019.

MEIRELLES, R. **Gerenciamento de risco corporativo e avaliação da maturidade empresarial em gerenciamento de risco corporativo: um estudo de caso na Azkonobel**. Dissertação (Mestrado Profissional em Empreendedorismo) - Faculdade de Economia, Administração e Contabilidade – FEA da Universidade de São Paulo, São Paulo, SP, 2018.

NASCIMENTO V.P.; ALVES, C.A. de M. Avaliação de modelo de gerenciamento de riscos corporativos segundo recomendação do IBGC. **Revista Eletrônica de Ciência Administrativa**, v.6, n.2, nov.2007.

OLESKOVICZ, M.; OLIVA, F.L.; PEDROSO, M. C. Gestão de Riscos, governança corporativa e alinhamento estratégico: um estudo de caso. **Revista Ibero-Americana de estratégia**, 2018-04-01, v.17 (2), p.18.

OLIVA, F. L. A maturity model for enterprise risk management. **Int. J. Production Economics** 173 (2016) – p. 66-69.

OLIVA, F. L.; SILVA, M. C.; CARDOSO, C. C.; PAZA, A. C. T.; BUTION, J. L. Gestão de riscos corporativos: estudo de caso do Itaú Unibanco S.A. In: SEMINÁRIOS EM ADMINISTRAÇÃO, 24, 2021, São Paulo. **Anais...** São Paulo: USP, 2021, p. 1-16. Disponível em <<https://login.semead.com.br/24semead/anais/arquivos/561.pdf?>> Acesso em: 22.fev.2023.

POLTRONIERI, C.F.; GEROLAMO, M. C.; CARPINETTI, L.C.R. Um instrumento para a avaliação de sistemas de gestão integrados. **Gestão & Produção**, 2015, v. 24, n. 4.

RAMPINI, G.H.S. **Estudo do impacto dos fatores críticos de sucesso e do gerenciamento de riscos nos resultados das organizações**. Dissertação (Mestrado em Engenharia de Produção) - Escola Politécnica da Universidade de São Paulo. São Paulo, SP, 2020.

RIMS, Risk and Insurance Management Society. **RIMS Risk Maturity Model (RMM) for Enterprise Risk Management**, 2006. Disponível em <www.rims.org>. Acesso em: 15 mai. 2022.

SANTOS, M. P.; BUTION, J. L. e PAZA, A. C. T. Fatores determinantes da maturidade em gestão de riscos corporativos: o caso da Embraer. **XLV Encontro da Anpad – EnANPAD 2021**, On-line – 4 a 8 de out. de 2021.

SILVEIRA, A. D. M. **Governança corporativa no Brasil e no mundo: teoria e prática**. 3. ed, Vinhedo, SP: Virtuos Company, 2021.

SOUZA, S. R. F.; MARTINS, H. C. A influência da governança e seus fatores ambientais na prática de gestão de risco: um estudo na Fundação Renova. **IX Encontro de Estudos em Estratégia – 3Es 2020**, set. de 2020.

SZARUGA, B. D. Maturity of risk management culture, entrepreneurship and sustainability issues. **Siedlce** - Poland, v.7, mar. de 2020.

TEBERGA, P. M. F.; FORTES, R. C.; CORRÊA, H. L.; CALDEIRA, A.; PAZA, A. C. T.; BUTION, J. L. Análise de riscos e desempenhos em Startups Early Stage. **IX Encontro de Estudos em Estratégia – 3Es 2020**, set. de 2020.

TJAHJONO, SUBAGIO. Enterprise Risk Management Implementation Maturity in Non Bank and Financial Companies. **Etikonomi**. Vol. 16(2), out. 2017 p.173-186

TRIVELATO, B. F., MENDES, D. P. e DIAS, M.A. A importância do gerenciamento de riscos nas organizações contemporâneas. **Revista Fatec Zona Sul**, v.4, n.2, fevereiro de 2018.

VILELA, C. H. S.; NETO, J. S. Uma estrutura de apetite de risco para suporte à Governança Corporativa. **IX Encontro de Estudos em Estratégia – 3Es 2020**, set. de 2020.

APÊNDICE 1

INSTRUMENTO DE COLETA

Na sequência, apresenta-se a íntegra do questionário elaborado para capturar as informações sobre a maturidade da Gestão de Riscos Corporativos, que será enviado aos profissionais das empresas selecionadas:

Pesquisa sobre maturidade da gestão de riscos corporativos

Muito obrigado pela disposição em responder essa pesquisa.

Os dados coletados serão utilizados exclusivamente para fins acadêmicos na dissertação "Mensuração da Maturidade da Gestão de Risco em Companhias Abertas dos Segmentos Financeiro e Varejo" de autoria de Leonardo Santicioli, mestrando da Universidade Municipal de São Caetano do Sul (leonardo.santicioli@uscsonline.com.br).

Empresa
 Profissional
 Cargo
 Tempo de casa

Afirmações	Grau de Concordância				
	Discordo totalmente	Discordo em partes	Não discordo nem concordo	Concordo em partes	Concordo totalmente
1) A estratégia da gestão dos riscos corporativos da empresa, incluindo sua integração com a gestão e disseminação na cultura organizacional, está bem consolidada.					
2) A gestão de riscos corporativos da empresa é compatível com seu porte e complexidade de seus negócios.					

Afirmações	Grau de Concordância				
	Discordo totalmente	Discordo em partes	Não discordo nem concordo	Concordo em partes	Concordo totalmente
3) Todas as áreas de negócio e suporte recebem <i>inputs</i> da Gestão de Risco Corporativos para definição de seus objetivos anuais.					
4) As avaliações sobre os principais riscos e as respectivas probabilidades de ocorrência e impacto são compartilhadas com os principais executivos da Companhia.					
5) As escolhas e prioridades de projetos e investimentos realizados pela empresa consideram as avaliações.					
6) As metas de desempenho estabelecidas contemplam <i>inputs</i> decorrentes da avaliação dos riscos corporativos.					
7) A estrutura de GRC tem acesso e reporte direto a Alta Administração e à Governança da Companhia.					
8) As atividades de GRC são desenvolvidas por uma estrutura específica, independente da área de negócios.					
9) As atividades de GRC são desenvolvidas por uma estrutura específica, diferente da Auditoria Interna.					
10) Os riscos identificados, bem como sua probabilidade de ocorrência, impacto, mitigadores existentes e a serem implementados são reportados e acompanhados pelos órgãos de Governança da empresa.					
11) As não conformidades identificadas em relação ao cumprimento de leis e políticas internas, bem como desvios éticos identificados são reportados e acompanhados pelos órgãos de Governança da empresa.					

Afirmações	Grau de Concordância				
	Discordo totalmente	Discordo em partes	Não discordo nem concordo	Concordo em partes	Concordo totalmente
12) As deficiências de controle e necessidade de aprimoramento nos processos internos são reportadas e acompanhadas pelos órgãos de Governança da empresa.					
14) As temáticas de gestão de riscos corporativos são pautas permanentes da Governança e tratadas com tempo e profundidade.					
15) O principal profissional da área de GRC reporta ao CEO da Companhia ou diretamente ao Conselho de Administração ou colegiado delegado por este.					
16) O processo de GRC é avaliado por algum agente externo (empresa de consultoria, auditoria ou órgão representativo de classe) periodicamente.					
17) Os temas críticos de negócio e de suporte são estabelecidos em políticas e procedimentos internos nas diferentes áreas da Companhia.					
18) As políticas e procedimentos relativas ao gerenciamento de riscos corporativos são formalizadas.					
19) As políticas e procedimentos relativos ao gerenciamento de riscos corporativos são divulgadas de maneira consistente a toda a Companhia.					
20) As políticas e procedimentos relativos ao gerenciamento de riscos corporativos são frequentemente atualizadas em decorrência de novas estratégias do negócio.					

Afirmações	Grau de Concordância				
	Discordo totalmente	Discordo em partes	Não discordo nem concordo	Concordo em partes	Concordo totalmente
21) As políticas e procedimentos relativos ao gerenciamento de riscos corporativos são frequentemente atualizadas em decorrência de novas tendências do mercado.					
22) Existe acompanhamento interno sobre a aplicação consistente das diretrizes das políticas relativas ao gerenciamento de riscos corporativos.					
23) Existe acompanhamento externo sobre a aplicação consistente das diretrizes das políticas relativas ao gerenciamento de riscos corporativos.					
24) A gestão de riscos corporativos da empresa identifica adequadamente os principais riscos aplicáveis à Companhia, decorrentes de diferentes naturezas.					
25) A gestão de riscos corporativos da empresa reduz de maneira consistente a probabilidade de ocorrência e/ou impacto dos riscos de distintas naturezas.					
26) A gestão de riscos corporativos da empresa mensura os riscos e aponta aqueles que podem afetar de maneira mais relevante os objetivos estratégicos.					

Afirmações	Grau de Concordância				
	Discordo totalmente	Discordo em partes	Não discordo nem concordo	Concordo em partes	Concordo totalmente
27) A gestão de riscos corporativos da empresa identifica se a empresa está cumprindo adequadamente as leis e normas regulamentares aplicáveis.					
28) A gestão de riscos corporativos da empresa gera indicadores disseminados e utilizados na condução dos negócios.					
29) A gestão de riscos corporativos da empresa monitora todos os planos de ação esperados e reporta à Governança desconformidade e atrasos em sua execução.					
30) A Governança indica de maneira consistente aprimoramentos e mudanças no sistema de GRC da Companhia.					
31) A Companhia dispõe de procedimentos específicos para identificação, mensuração e mitigação dos riscos.					
32) A Companhia se utiliza de framework de riscos como referência em suas políticas.					
33) A Companhia aplica de maneira consistente critérios objetivos na identificação, mensuração e mitigação dos riscos.					

Afirmações	Grau de Concordância				
	Discordo totalmente	Discordo em partes	Não discordo nem concordo	Concordo em partes	Concordo totalmente
34) A Companhia tem um apetite de risco definido e aprovado pela Governança.					
35) O apetite de risco da Companhia é calculado com base em aspectos qualitativos e quantitativos.					
36) Riscos com impacto ou probabilidade superior ao apetite são reportados à Governança.					
37) A Companhia trabalha com testes de stress para definir seu apetite a risco ou outra métrica de referência da gestão de riscos corporativos.					
38) Os dados e reportes gerados a partir da gestão de riscos corporativos são destinados apenas a consumo externo, decorrente de exigências e regulamentações.					
39) Os reportes e relatórios gerados pela GRC da empresa são utilizados por toda a liderança.					
40) Os reportes e relatórios gerados pela GRC da empresa são compreendidos por todos aqueles que o utilizam.					
41) A empresa faz uso extensivo de dados na Gestão de seus riscos corporativos.					

Afirmações	Grau de Concordância				
	Discordo totalmente	Discordo em partes	Não discordo nem concordo	Concordo em partes	Concordo totalmente
42) A empresa aproveita os sistemas de negócios e tecnologias existentes em suas atividades de identificação, mensuração e mitigação de riscos.					
43) A empresa utiliza de maneira extensiva sistemas e fontes de dados integradas que permitem acompanhamentos online em suas práticas de GRC.					
44) A empresa possui uma cultura de risco bem disseminada entre seus colaboradores e não apenas à liderança.					
45) A Alta Administração e os funcionários de maneira geral compreendem a necessidade e benefícios de uma gestão de riscos corporativos efetiva.					
46) A liderança da empresa participa de maneira ativa na identificação e mitigação de seus principais riscos corporativos.					
47) Os novos produtos e projetos estabelecidos pela empresa consideram sempre a avaliação de seus principais riscos.					
48) A empresa oferece treinamentos regulares que disseminam as temáticas de risco e ajudam a incluí-la na agenda prioritária das lideranças.					