Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Modelo Multicritério de Avaliação da Maturidade em Gestão de Riscos

Roberta Brandão do Nascimento

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Orientadora
Prof.ª Dr.ª Ana Carla Bittencourt Reis

Brasília
2018

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Bm

Brandão do Nascimento, Roberta
Modelo Multicritério de Avaliação da Maturidade em Gestão de Riscos / Roberta Brandão do Nascimento; orientador Ana Carla Bittencourt Reis. -- Brasília, 2018.
71 p.

Dissertação (Mestrado - Mestrado Profissional em Computação Aplicada) -- Universidade de Brasília, 2018.

1. Modelo de Maturidade. 2. Gestão de Riscos. 3. Decisão Multicritério. 4. ELECTRE TRI. I. Bittencourt Reis, Ana Carla, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Modelo Multicritério de Avaliação da Maturidade em Gestão de Riscos

Roberta Brandão do Nascimento

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Prof.ª Dr.ª Ana Carla Bittencourt Reis (Orientadora)
EPR/UnB

Prof. Ph.D João Mello da Silva
EPR/UnB

Prof.ª Dr.ª Renata Maciel de Melo
UFPE/CAA

Prof.ª Dr.ª Aletéia Patrícia Favacho de Araújo
Coordenadora do Programa de Pós-graduação em Computação Aplicada

Brasília, 17 de julho de 2018

Dedicatória

À minha família, pelo apoio e amor incondicional.

Agradecimentos

À Deus, pela vida.

Aos meus pais, irmãs e sobrinhos, pelo apoio e paciência.

À professora Ana Carla Bittencourt Reis, pela orientação eficiente e segura.

Ao Programa de Pós-Graduação em Computação Aplicada da Universidade de Brasília, seu corpo docente e discente, direção e administração pela oportunidade.

Aos amigos do trabalho, por me ajudarem a realizar esse sonho.

Ao amigo Glauco Cintra Parreira, pela amizade e por encarar esse desafio comigo.

À amiga Lorena do Prado e Silva, pelo suporte e amizade sincera.

A todos amigos e familiares, pelo incansável apoio e por compreenderem minha ausência ao longo desses anos de trabalho.

Resumo

A gestão de riscos de Tecnologia da Informação (TI) é uma importante ferramenta para a governança de TI, pois permite que os riscos sejam identificados, analisados e adequadamente tratados, minimizando os impactos e fornecendo aos gestores um amplo entendimento sobre a estratégia de gestão de riscos. Para garantir uma gestão de riscos efetiva e devidamente alinhada ao objetivo do negócio, é necessário avaliar continuamente seu nível de maturidade, a fim de conhecer sua situação atual e identificar suas deficiências. Considerando as dificuldades dos gestores em definir e mensurar seus valores e preferências e compreender as consequências de suas decisões no processo de avaliação, a utilização de métodos de apoio multicritério tem sido uma opção capaz de minimizar a subjetividade e fornecer elementos quantitativos ao processo. Este trabalho propõe um modelo de maturidade com base no método ELECTRE TRI para a classificação ordenada dos principais critérios, selecionados através de um estudo aprofundado dos modelos e padrões de ERM tidos como referências mundiais. Ao especificar escalas de julgamento para cada critério, o modelo sintetiza e organiza as informações relacionadas à gestão de riscos e simplifica o processo de decisão do gestor, permitindo que os mesmos tomem suas decisões embasadas em um método cientifico de forma clara e eficiente. O modelo foi validado por um estudo de caso aplicado em uma empresa de distribuição de energia e os resultados apresentados auxiliaram os gestores a diagnosticar a situação atual dos seus processos de TI, identificando seus pontos fortes e fracos e suas oportunidades de melhoria.

Palavras-chave: modelo de maturidade, gestão de riscos, decisão multicritério, ELECTRE TRI

Abstract

Information Technology (IT) risk management is an important tool for IT governance, as it allows risks to be identified, analyzed and adequately addressed, minimizing impacts and providing managers with a broad understanding of risk management strategy. To ensure risk management that is effective and properly aligned with the business objective, it is necessary to continually assess its level of maturity in order to know its current situation and identify its deficiencies. Considering the difficulties of managers in defining and measuring their values and preferences and understanding the consequences of their decisions in the evaluation process, the use of multicriteria support methods has been an option capable of minimizing subjectivity and providing quantitative elements to the process. This work proposes a maturity model based on the ELECTRE TRI method for orderly classification of the main criteria, selected through an in-depth study of the models and patterns of ERM considered as world references. By specifying judgment scales for each criterion, the model synthesizes and organizes information related to risk management and simplifies the decision-making process of the manager, allowing them to make their decisions based on a scientific method in a clear and efficient manner. The model was validated by a case study applied at an energy distribution company and the results presented helped managers to diagnose the current state of their IT processes by identifying their strengths and weaknesses and their opportunities for improvement.

Keywords: maturity model, risk management, multicriteria decision, ELECTRE TRI

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

AHP *Analytic Hierarchy Process.*

ANP *Analytic Network Process.*

ANSI *American National Standards Institute.*

CI-MM *Corporate Informatic Maturity Model.*

CMMI *Capability Maturity Model Integration.*

COBIT *Control Objectives for Information and related Technology.*

CoPS *Complex Product Systems.*

COSO *Committee of Sponsoring Organizations of the Treadway Commission.*

CRO *Chief Risk Officer.*

ELECTRE *Elimination et Choix Traduisant la Réalité.*

ERM *Enterprise Risk Management.*

IBGC Instituto Brasileiro de Governança Corporativa.

ICW *Interval Criterion Weights.*

ISO *International Organization for Standardization.*

ISR3M *Information System Risk Management Maturity Model.*

KPI *Key Performance Indicators.*

MACBETH *Measuring Attractiveness by a Categorical based Evaluation Technique.*

MAUT *Multiattribute Utility Theory.*

MAVT *Multiattribute Value Theory.*

MCDA *Multiple Criteria Decision Aid.*

MM-ERM *Maturity Model for Enterprise Risk Management.*

MMGRSeg *Maturity Model to Risk Management Process in Information Security.*

MOLP *Multi-objective Linear Programming.*

NIS *Negative Ideal Solution.*

OGC *Office of Government Commerce.*

OPM3 *Organizational Project Management Maturity Model.*

P3M3 *Portfolio, Program and Project Management Maturity Model.*

PIS *Positive Ideal Solution.*

PMBOK *Project Management Body of Knowledge.*

PMI *Project Management Institute.*

PMMM *Project Management Maturity Model.*

PMS *Project Management Solutions.*

PRMM *Project Risk Maturity Model.*

PROMETHEE *Preference Ranking Organization Method for Enrichment Evaluations.*

RIMS *Risk and Insurance Management Society.*

RISKSIG *The Risk Management SIG.*

RM-CMM *Risk Management - Capability Maturity Model.*

RMM *Risk Maturity Model.*

RMMM *Risk Management Maturity Model.*

SEI *Software Engineering Institute.*

SMART *Simple Multi Attribute Rating Technique.*

SMARTER *Simple Multi-Attribute Rating Technique using Exploiting Rankings.*

SMARTS *Simple Multi-Attribute Rating Technique using Swings.*

SOX *Lei Sarbanes-Oxley.*

STEM *Step Method.*

TI Tecnologia da Informação.

TODIM Tomada de Decisão Interativa Multicritério.

TOPSIS *Technique for Order Preference by Similarity to the Ideal Solution.*

TRIMAP *Tri-criteria Linear Programming Package.*

Capítulo 1

Introdução

Nos últimos anos, a Tecnologia da Informação (TI) deixou de ser somente uma ferramenta de suporte administrativo e passou a ter um papel estratégico dentro das organizações [1, 2, 3]. Para Laurindo et al [2], a visão da TI como arma estratégica competitiva tem sido cada vez mais discutida e enfatizada, pois não só sustenta as operações de negócio existentes, mas também permite que se viabilizem novas estratégias empresariais. Além disso, Fernandes e Abreu [1] afirmam que o uso eficaz da TI e o alinhamento de seus objetivos aos objetivos do negócio vão além da ideia de ferramenta de produtividade, sendo muitas vezes fator crítico de sucesso.

Com esta mudança de enfoque de TI, o termo governança de TI ganhou destaque entre as organizações, que perceberam a necessidade de estabelecer papéis, controles e direções para atingir os objetivos estratégicos e obter benefícios através da utilização eficiente e inovadora de TI [4]. Segundo a ABNT NBR ISO/IEC 38500 [5], a governança de TI "é o sistema pelo qual o uso atual e futuro da TI são dirigidos e controlados". Lunardi et al [3] definem governança de TI como o sistema responsável pela distribuição de responsabilidades e direitos sobre as decisões de TI, bem como pelo gerenciamento e controle dos recursos tecnológicos da organização, buscando, dessa forma, garantir o alinhamento da TI às estratégias e aos objetivos organizacionais.

Qualquer possibilidade de ocorrência de um evento que afete o cumprimento dos objetivos organizacionais é chamada de risco corporativo e deve ser gerenciada. Ramos [6] afirma que "tomar decisões levando em consideração os componentes dos riscos é a melhor forma de buscar objetivos para as nossas ações e garantir que elas se encontram dentro de patamares razoáveis". Gerenciar os riscos permite aos gestores tratar com eficácia as incertezas, bem como os riscos e as oportunidades a eles associados, fornecendo informações corretas e disponíveis para a tomada de decisões [7].

O Instituto Brasileiro de Governança Corporativa (IBGC) [8] recomenda que as organizações implementem a gestão de riscos como forma preventiva de conhecer os seus

principais riscos, que podem ser operacionais, financeiros, regulatórios, estratégicos, tecnológicos, sistêmicos, sociais e ambientais. A gestão de riscos auxilia na identificação desses riscos, suas probabilidades de ocorrência, seus impactos e medidas de prevenção e mitigação que podem ser adotadas. De acordo com o *Control Objectives for Information and related Technology* (COBIT) [9], a gestão de riscos é um dos elementos chave para uma governança bem-sucedida.

Hopkinson [10] defende que a implementação significativa da gestão de riscos em uma organização é demorada e demanda esforço e tempo. Para garantir o aperfeiçoamento da governança de TI e da gestão de riscos nas organizações é necessário avaliar continuamente seu nível de maturidade, de forma a conhecer sua situação atual, identificar suas deficiências e traçar planos de melhoria.

Existem na literatura vários modelos de maturidade em gestão de riscos de TI [11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22]. Araújo e Oliveira [23] afirmam que os modelos de maturidade são importantes ferramentas para auxiliar os gestores na tomada de decisão. Entretanto, Fernandes e Abreu [1] orientam que, para utilizar esses modelos, cada organização deve ser capaz de elaborar sua própria arquitetura de processos de TI, priorizando o que é importante para o seu negócio e avaliando quais os riscos envolvidos. A simples implantação dos modelos de melhores práticas não é garantia de sucesso.

Em contextos decisórios específicos como é o caso dos modelos de maturidade em gestão de riscos de TI, em que os gestores necessitam definir e mensurar seus valores e preferências e precisam compreender as consequências de suas decisões, o uso de Métodos Multicritérios de Apoio à Decisão ou MCDA tem sido uma boa opção [24, 25]. Os métodos MCDA auxiliam o decisor a compreender as consequências de suas decisões nos aspectos em que julga importante, sem impor os racionalismos da objetividade, e ajudam a identificar oportunidades de aperfeiçoamento ao longo do processo [26, 27, 28, 29].

Diante deste cenário, o presente trabalho propõe um modelo de maturidade que utiliza o método ELECTRE TRI para a classificação ordenada dos principais critérios encontrados na literatura. O modelo é validado por um estudo de caso aplicado em uma empresa de distribuição de energia e os resultados apresentados apoiam os gestores na avaliação da maturidade em gestão de riscos de TI.

1.1 Definição do Problema

Atualmente, a TI é vista como um recurso capaz de suportar a atividade fim da organização, proporcionando agilidade, mobilidade e suporte à tomada de decisão [3]. Com essa dependência em relação à TI, é importante que as organizações protejam suas informações, mantendo-as confiáveis e disponíveis sem interrupções. Nesse sentindo, gerenciar os

riscos ajuda as organizações a identificar os processos que deixam a empresa vulnerável, para então buscar métodos eficazes para controlá-los.

Para uma gestão de riscos eficiente, é comum a adoção de modelos robustos para monitorar as vulnerabilidades e identificar os riscos dos processos de TI [13, 18, 30]. Na prática, cada organização desenvolve sua própria estrutura para gerenciar os riscos baseada nestes modelos existentes, influenciadas pelas diferentes necessidades e pelos contextos político, econômico e social. De acordo com Tomas e Alcântara [31], ao definir suas estratégias de gestão de risco, as empresas geralmente consideram a sua estrutura organizacional, a estratégia de negócios e os processos de trabalho atuais.

Caiado et al [11] afirmam que o gerenciamento de riscos deve ser uma iniciativa liderada pela alta administração e capaz de alinhar a cultura da organização com uma política de gestão de riscos efetiva. É preciso analisar metodicamente todos os riscos envolvidos nas atividades passadas, presente e futuras de uma organização.

O risco é algo inerente a todos os processos de TI de uma empresa e a avaliação da maturidade em gestão de riscos é uma importante ferramenta para reduzir as ameaças e para identificar oportunidades. Para Chapman [12], avaliar a maturidade em gestão de riscos significa determinar quais controles serão gerenciados e como serão medidos. Segundo Coetzee e Lubbe [32], a principal finalidade de um modelo de maturidade de risco é auxiliar os gestores a avaliar o desenvolvimento do seu processo de gestão de riscos e informar às partes interessadas, que por usa vez, utilizam essa informação nas decisões relacionadas ao negócio.

Para Mendonça et al [33], existe uma alta complexidade no processo decisório na área de TI das organizações, confirmada pela dificuldade de obtenção de respostas claras a questionamentos sobre a área, principalmente quando envolve aspectos técnicos, sociais e políticos. Além disso, para a maioria das organizações, é importante que o processo de tomada de decisão seja transparente, a fim de atender as necessidades dos requisitos regulatórios e das partes interessadas.

A empresa de distribuição de energia onde o estudo será aplicado passa pelo processo de integração com os processos da holding para a qual suas ações foram vendidas. A ausência de um mapeamento de processos dificulta a avaliação de sua situação atual, principalmente em relação aos processos de TI e os riscos envolvidos. Considerando as dificuldades dos gestores em avaliar e tomar decisões sobre a gestão de riscos dos processos de TI, este trabalho levanta o seguinte problema: *Como avaliar a maturidade em gestão de riscos de TI de maneira eficiente?*

1.2 Justificativa

Nos últimos anos, a gestão de riscos passou a ser vista como prioridade nas organizações, na medida em que empresas enfrentam ameaças crescentes e cada dia mais complexas. Os riscos são cada vez mais significativos e as empresas precisam gerenciá-los para garantir seu lugar no mercado [20, 24, 34].

Em 2013, a *KPMG International* divulgou uma pesquisa global sobre riscos, conduzida pela *Economist Intelligence Unit*, que expõe a percepção de executivos sobre os riscos a que suas empresas estão sujeitas e como estes riscos estão sendo enfrentados [35]. A pesquisa intitulada *Expectations of Risk Management Outpacing Capabilities - It's Time for Action* (em português, O que esperar do gerenciamento de riscos - É hora de agir) concluiu que a gestão de riscos é vista como prioridade na maior parte das empresas pesquisadas, mas em apenas 66% delas a gestão de riscos é integrada ao processo de planejamento estratégico. Ainda segundo a pesquisa, a maioria das empresas pesquisadas não realiza uma avaliação de riscos consistente. Embora 80% dos entrevistados afirmem que na sua empresa há algum tipo de processo para definição do perfil de risco da organização, quase 50% reconhece dificuldades em compreender o quanto de fato, sua empresa está exposta a estes riscos. Os entrevistados admitem que é necessário motivar mais os gestores a levar em conta os riscos na tomada de decisões, introduzindo medidores de desempenho como parte dos critérios de avaliação [35].

Em 2105, a *Aon Risk Solutions* em parceria com *The Wharton School, University of Pennsylvania*, realizou uma pesquisa chamada *Aon Risk Maturity Index* (em português, Índice de Maturidade de Risco Aon) avaliando a maturidade em gestão de riscos de mais de 900 organizações [36]. De acordo com dados apresentados na pesquisa, aproximadamente 50% das empresas respondentes ainda estão abaixo de um nível de maturidade de gestão de riscos suficiente e consistente e que apenas 0,6% de empresas respondentes possuem a competência bem desenvolvida, como mostra a Figura 1.1. O relatório enfatiza a necessidade de identificar práticas de governança corporativa, tomada de decisões e gestão de riscos para ajudar as organizações a focarem os seus recursos de forma mais estratégica e assim, aumentarem seu valor no mercado.

Ainda de acordo com a pesquisa [36], mais de 50% das organizações classificadas com pontuações acima da média tomam decisões seguras com base em uma análise robusta da exposição ao risco e tolerância para riscos, levando em consideração o impacto no negócio. As demais organizações tomam decisões baseadas principalmente em abordagens históricas e em *benchmarking*, algumas vezes complementados com análise da exposição ao risco para casos específicos. Apesar da utilização cada vez mais frequente de relatórios gerenciais que auxiliem o processo de tomada de decisão, muitas decisões ainda são tomadas de maneira subjetiva, sem suporte científico.

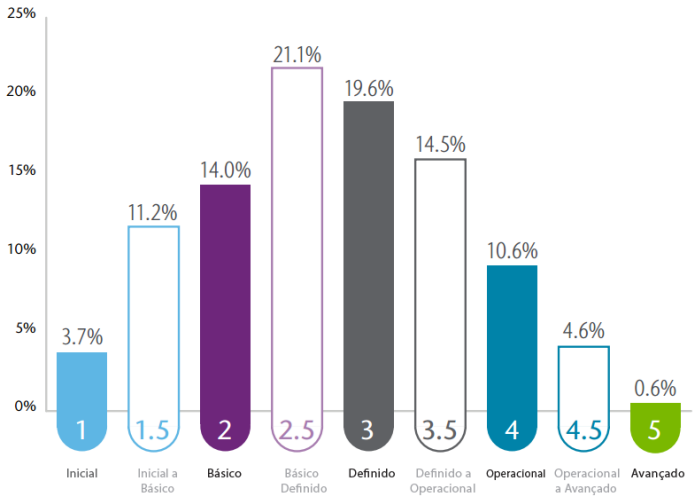

Figura 1.1: Taxa de Distribuição de Maturidade em Riscos - Outubro/2015 (Fonte: [36]).

Em 2017, a *Aon Risk Solutions* publicou um novo relatório sobre as últimas tendências da Gestão de Riscos, revelando os temas de riscos mais comuns compartilhados entre empresas públicas e privadas, de todos os tamanhos e regiões do mundo [37]. Os resultados ressaltam que as empresas estão lidando com novos riscos, mas que não tem um consenso sobre como priorizá-los e tratá-los de maneira assertiva. O relatório *Global Risk Management Survey* (em português, Pesquisa Global de Gerenciamento de Riscos) da Deloitte, publicado no mesmo ano, corrobora este resultado ao afirmar que a análise de riscos continua sendo um desafio para muitos devido à falta de metodologias bem desenvolvidas e comumente aceitas [38].

Assim, os gestores responsáveis por tomar decisões estão inseridos em uma realidade cada vez mais complexa, necessitando de métricas e medidas confiáveis para garantir que a TI agregue impactos positivos à organização. A utilização de métodos científicos na solução de problemas, como métodos de apoio multicritério à decisão, tem sido uma opção capaz de fornecer elementos quantitativos para a tomada de decisão e ajudar os gestores neste processo [26, 28, 29].

Apesar de existir na literatura várias propostas de modelos de avaliação de maturidade em gestão de riscos encontradas nas pesquisas realizadas [11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21], poucos modelos associam utilização de métodos MCDA como ferramenta para tomada de decisão [24, 25]. Utilizando métodos MCDA para a avaliação de maturidade em riscos é possível avaliar as estruturas de risco de forma mais objetiva, prática e viável. Consequentemente, é possível desenvolver um entendimento amplo sobre estratégia de gestão de riscos em ação, bem como elaborar declarações de apetite e tolerância a risco alinhadas ao objetivo do negócio.

Na empresa de distribuição de energia onde o estudo foi aplicado, obteve-se uma avaliação de maturidade em gestão de riscos dos processos de TI fiel à realidade. O resultado auxiliou os gestores a lidarem de forma eficiente com os riscos e vulnerabilidades, buscando um balanceamento ótimo entre desempenho, retorno e riscos associados. Adicionalmente, além do aspecto prático relevante, esta pesquisa também contribuiu com o meio acadêmico ampliando a produção de conteúdos sobre gestão de riscos, modelos de maturidade e métodos MCDA, especialmente o método ELECTRE TRI.

1.3 Objetivo

1.3.1 Objetivo Geral

O objetivo geral do trabalho é propor um modelo de maturidade em gestão de riscos para auxiliar os gestores na avaliação dos processos de TI por meio de métodos de apoio à decisão.

1.3.2 Objetivos Específicos

1. Identificar e comparar as melhores práticas relacionadas à gestão de riscos, através do estudo de normas de referência, frameworks e modelos de maturidade.
2. Identificar e comparar métodos de apoio multicritério à decisão, através do estudo de conceitos e metodologias voltadas à tomada de decisão.
3. Propor um modelo de maturidade de gestão de riscos que considere os múltiplos critérios necessários para apoiar a decisão dos gestores na avaliação dos processos de TI.
4. Aplicar o modelo proposto a um estudo de caso a fim de diagnosticar a situação atual dos processos de TI da empresa estudada, identificando seus pontos fortes e fracos.

1.4 Metodologia de Desenvolvimento do Trabalho

Segundo Souza et al [39], a metodologia é uma disciplina que estuda, compreende e avalia os vários métodos disponíveis ao se realizar uma pesquisa acadêmica. Ela consiste na aplicação de técnicas e procedimentos para construção do conhecimento, com a finalidade de comprovar sua utilidade nos diversos âmbitos da sociedade.

Quanto à sua natureza, esta pesquisa pode ser classificada como pesquisa aplicada, pois tem como objetivo gerar conhecimento para aplicações práticas à solução de um problema

específico, ou seja, pretende utilizar métodos MCDA para auxiliar os gestores na avaliação da maturidade em gestão de riscos de TI. Quanto aos procedimentos técnicos, classifica-se com uma pesquisa bibliográfica e experimental, pois é elaborada a partir de material já publicado, como artigos, periódicos, livros, etc., mas é determinada pela aplicação prática [40, 41].

Quanto à forma de abordagem ao problema, trata-se de uma pesquisa qualitativa, já que considera que a percepção dos gestores no processo de decisão é subjetiva. Tem o intuito de obter resultados que possam indicar o caminho para a tomada de decisão correta sobre o problema. Além disso, considera que existe uma relação entre os processos de TI a serem avaliados e os ambientes interno e externo, que não pode ser traduzida em números. Quanto aos objetivos, caracteriza-se como pesquisa exploratória, com o intuito de proporcionar maior familiaridade com o problema específico. A pesquisa exploratória é feita através de pesquisas bibliográficas sobre gestão de riscos e os principais modelos de avaliação de maturidade e sobre a tomada de decisão e os principais métodos de apoio multicritério à decisão, além da aplicação prática através de um estudo de caso aplicado em uma empresa de distribuição de energia [39, 40, 41].

A primeira etapa do trabalho, que corresponde aos objetivos específicos 1 e 2, consiste em realizar a revisão da literatura, levantando os principais conceitos e o estado da arte dos temas abordados: modelos de maturidade em gestão de riscos e métodos de apoio multicritério à decisão. Foi realizada uma análise bibliométrica para auxiliar o pesquisador a identificar os principais artigos, teses e livros que devem ser lidos para se embasar a pesquisa. A técnica utilizada para esta etapa foi o enfoque meta analítico.

A segunda etapa, referente aos objetivos específicos 3 e 4, consiste em propor um modelo de maturidade de gestão de riscos e aplicá-lo em um estudo de caso, observando a aderência da utilização de um método MCDA. Para a definição do método multicritério e estruturação do modelo de maturidade, foi utilizada a metodologia proposta por Belton e Stewart [42], representada na Figura 1.2, que abrange a identificação do problema, a estruturação dele, a construção do modelo a ser utilizado, a utilização desse modelo para informar e desafiar o pensamento do tomador de decisão e a definição de um plano de ação.

Após a identificação do problema, iniciou-se a fase de estruturação do problema onde o contexto de decisão foi estabelecido. Nesta fase, foram definidos o escopo (valores, objetivos, limitações, ambiente externo, assuntos chaves, incertezas e alternativas) e identificados os tomadores de decisão e as demais partes interessadas. Dentre os atores centrais do processo, incluem decisores, clientes, patrocinadores, outras partes interessadas, incluindo potenciais sabotadores, e os facilitadores ou analistas.

Além disso, nesta fase foi modelado o sistema social e técnico para condução da MCDA.

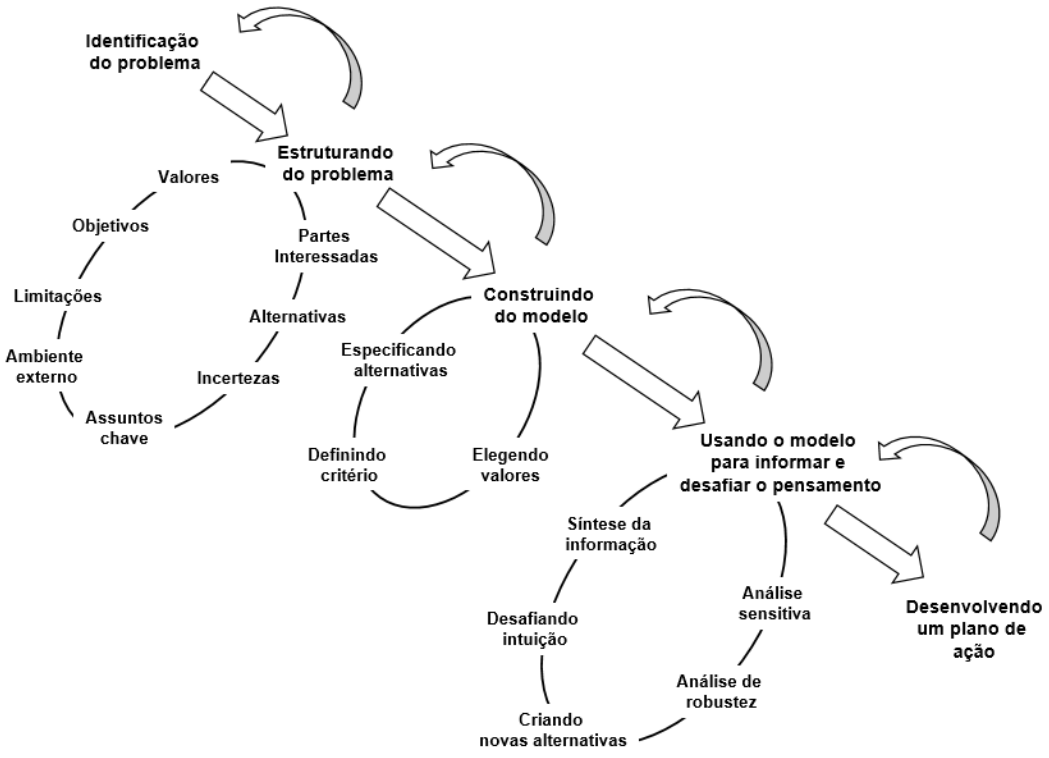

Figura 1.2: Metodologia do processo de MCDA (Fonte: [42]).

O sistema social diz respeito aos papeis e responsabilidades que são designadas às partes interessadas. O aspecto técnico diz respeito à identificação de qual problemática MCDA deve ser utilizada e, por conseguinte, qual método será utilizado. Para este trabalho, a problemática é a classificação, onde as alternativas são ordenadas em grupos homogêneos e pré-definidos. O método escolhido foi o ELECTRE TRI, por tratar do problema de classificação ordenada, apropriado para o caso tratado nesse trabalho.

Na fase de construção do modelo, foram identificadas as alternativas a serem avaliadas. Como a empresa estudada não possui processos mapeados, as alternativas equivalem aos setores que serão avaliados pelo modelo de maturidade. Em seguida, foram levantados os critérios de cada uma das dimensões de maturidade que, de acordo com a revisão da literatura realizada, refletem as principais práticas de gerenciamento de risco em uma organização. Para cada critério, foram atribuídos valores (ou pesos) que definem a importância relativa de cada um deles na solução do problema.

Na fase seguinte, pesos e valoração foram combinados para cada alternativa a fim de obter valor geral. Os resultados foram avaliados e uma análise de sensibilidade foi realizada. Para tanto, foi feita uma avaliação de outras preferências ou pesos que pudessem afetar o ordenamento geral das alternativas, identificando as vantagens e desvantagens

das opções selecionadas. Não foi necessário criar novas alternativas, pois as alternativas identificadas inicialmente foram satisfatórias na construção do modelo.

A última fase desenvolve um plano de ação, que no caso deste trabalho consiste na criação do modelo de avaliação de maturidade proposto. De acordo com Belton e Stewart [42], pode-se esperar uma interação entre as principais fases do processo, cada uma delas sujeita a uma infinidade de influências e pressões internas e externas.

Capítulo 2

Base Conceitual e Revisão da Literatura

2.1 Gestão de Riscos

Quando se realiza um determinado processo, uma atividade ou um projeto, qualquer situação que os desvie do objetivo pode ser considerada um risco e tais desvios podem ser considerados oportunidades ou ameaças. Riscos podem ser definidos como o grau de incerteza sobre os objetivos [43, 44]. Em ambientes organizacionais, o risco é conhecido como risco corporativo e representa a possibilidade de ocorrência de um evento que afete o cumprimento de seus objetivos estratégicos [13].

Coordenar atividades para dirigir e controlar uma organização sobre o que diz respeito a riscos é o principal objetivo da gestão derRiscos [19, 43, 44, 45]. Entre suas principais atividades, destacam definição, análise, avaliação, tratamento, aceitação e comunicação de contexto e monitoramento de riscos.

Para Oliva [20], a gestão de riscos pode melhorar os processos empresariais, pois sua implementação aumenta a eficácia operacional e assim, reduz a perda causada por fraudes e falhas. Elmaallam e Kriouile [14, 15] defendem que a gestão de riscos deve ser gerida pelo conselho de administração e deve estar alinhada aos objetivos estratégicos da organização, pois pode ser capaz de identificar potenciais eventos que afetem a realização de tais objetivos.

Atualmente, muitas organizações enxergam a gestão de riscos como uma ferramenta para cumprir os requisitos impostos pelas novas leis, padrões e regulamentos relativos à segurança da informação [35, 37, 38]. De acordo com Bharathy e McShane [46], muitas empresas estão tentando implementar a gestão de riscos como o novo princípio organizador holístico para lidar com o ambiente de risco dinâmico caracterizado por questões complexas, como mudanças rápidas no ambiente de TI e a explosão da globalização.

O *COBIT 5 for Risk* [18] defende que os riscos devem ser gerenciados, mas não necessariamente devem ser evitados, pois algumas estratégias de negócios incluem assumir riscos para alcançar a proposição de valor e realizar metas. O Guia *Project Management Body of Knowledge* (PMBOK) ou em português, Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos [47], destaca o aumento da probabilidade e do impacto dos eventos positivos e redução da probabilidade e do impacto dos eventos negativos como os principais objetivos de um gerenciamento de riscos.

Entretanto, a gestão de riscos não é um conceito simples, pois difere de uma organização para outra. Para Caiado et al [11], as diferenças são justificadas pela influência de diferentes contextos (político, econômico e social) nas percepções dos gestores sobre os riscos e pelas diferentes necessidades das organizações. Para uma implementação eficaz, é necessário analisar metodicamente todos os riscos envolvidos nas atividades passadas, presentes e futuras da organização e definir uma política efetiva que seja alinhada à cultura organizacional e liderada pela alta administração [18, 48]. Apesar de complexa, a Gestão de Riscos se tornou um elemento central na gestão da estratégia de qualquer organização e por isso, deve ser um processo contínuo e em constante desenvolvimento.

Wieczorek-Kosmala [34] considera duas abordagens para o gerenciamento de riscos: uma tradicional, focada no impacto negativo do risco; e outra estratégica, que considera a gestão do risco como uma maneira de reduzir as ameaças, mas também como um meio para identificar oportunidades que melhorem o desempenho das organizações. Enquanto a abordagem tradicional visa identificar, medir e tratar exposições a possíveis perdas acidentais, gerenciando os riscos separadamente, a abordagem estratégica tem como objetivo promover a conscientização sobre as fontes de riscos e é vista como um processo integrado com todas as outras áreas de tomada de decisão.

Wieczorek-Kosmala [34] destaca ainda dois outros elementos válidos do processo de gerenciamento de riscos: governança corporativa e controle interno. A governança corporativa aborda a necessidade de colocar a responsabilidade do gerenciamento de riscos no conselho de administração para assegurar que as ações adequadas sejam tomadas. O controle interno, que inclui políticas, tarefas, comportamentos e atividades que permitem uma resposta a riscos significativos, ajudam a garantir a qualidade dos relatórios internos e externos e o cumprimento das normas aplicáveis, leis e regulamentos fornecidos por diretrizes e padrões [13, 18, 48].

O gerenciamento de risco estratégico é muitas vezes chamado de gerenciamento de risco "holístico"ou "integrado"ou ainda Gestão de Riscos Corporativos (*Enterprise Risk Management* (ERM)) e corresponde à gestão de riscos em toda a empresa. Uma primeira tentativa de ordenação de gerenciamento de riscos ocorreu em 1994 com a publicação do relatório *Enterprise Risk Management - Integrated Framework* pelo *Committee of Spon-*

soring Organizations of the Treadway Commission (COSO) ou Comitê de Organizações Patrocinadoras da Comissão Treadway [49].

Em 2009, a *International Organization for Standardization* (ISO) publicou a norma ABNT NBR ISO/IEC 31000 com o objetivo de estabelecer princípios e orientações genéricas sobre gestão de riscos para qualquer organização, independentemente do segmento ou tamanho. Além da ABNT NBR ISO/IEC 31000, que contém informações básicas, princípios e diretrizes para a implementação da gestão de riscos [43]; publicou ainda a ABNT NBR ISO/IEC 31010, com técnicas de avaliação e gestão de riscos [45]; e a ABNT ISO Guia 73, que apresenta um vocabulário relacionado à gestão de riscos [44]. Além de estabelecer o contexto de gerenciamento de risco, avaliação de risco, tratamento de risco e monitoramento e revisão do processo, o padrão oferece um modelo conceitual e uma metodologia que agrega comunicação e consulta em cada etapa do processo.

Dois anos depois, foi publicada a norma ABNT NBR ISO/IEC 27005 [50], que trata especificamente o processo de gestão de riscos de TI, auxiliando as organizações a identificar suas necessidades em relação aos requisitos de segurança da informação. É aderente e está em conformidade com a norma ABNT NBR ISO/IEC 31000 e, apesar de ter muitas semelhanças, apresenta um maior nível de detalhamento das atividades a serem executadas, levando em consideração questões como vulnerabilidade, consequências, valoração de ativos, entre outros.

Além do modelo *Enterprise Risk Management - Integrated Framework* publicado pelo COSO e da norma ABNT NBR ISO/IEC 31000, outros exemplos de padrões ERM são conhecidos como referências mundiais, como *FERMA:2002 - A Risk Management Standard* [48], *OCEG "Red Book" 3.0: 2015 - A Governance, Risk and Compliance Capability Model* [51], *Standard and Poor's Risk Management Framework* [52], *The King IV Report on Corporate Governance for South Africa 2016* [53], *The Basel III Framework* [54], entre outros [18, 47, 55]. Para Caiado et al [11], os padrões geralmente são elaborados por instituições que promovem várias iniciativas de gerenciamento de risco ou por consultores especializados e visam unificar a terminologia e o padrão de práticas de gerenciamento de risco, permanecendo alinhados às normas ISO.

A associação profissional dedicada a promover a prática da gestão de risco *Risk and Insurance Management Society* (RIMS) ou Sociedade de Gestão de Riscos e Seguros, sediada em Manhattan, revisou os principais padrões e modelos e concluiu que existem características que são comuns a todos, como possuir etapas de processo estruturado, supervisão e relatório dos riscos identificados, adotar uma abordagem empresarial patrocinada pela alta gestão e com responsabilidades bem definidas, compreender a responsabilidade na definição do apetite ao risco e limites de tolerância aceitáveis, documentar formalmente as avaliações de riscos, estabelecer e comunicar as metas e atividades do processo e monitorar

os planos de tratamento aos riscos [30].

A maneira como os padrões e modelos de gestão de riscos são aplicados e a particularidade de cada contexto organizacional revelam práticas únicas e distintivas que não são descritas em manuais gerais. Entretanto, conhecer as melhores práticas e identificar em que estágio a organização está em relação à Gestão de Riscos Corporativos tem auxiliado as organizações na criação de valor e na evolução contínua de seus processos [13, 18, 30, 43].

Embora a gestão de riscos seja um processo estratégico e ajude as organizações a liderar investimentos para os aspectos mais vulneráveis em seus negócios, uma recente pesquisa realizada pela Deloitte em empresas brasileiras mostrou que 54% dos respondentes não possuem uma estrutura de gestão de riscos operacionais robusta e que, de fato, ajude no gerenciamento dos negócios, e 61% deles nunca realizaram análises de risco de TI [38]. Para Carcary [56], a integração do risco de TI com as práticas de ERM é fundamental, pois promove uma maior compreensão pela TI das prioridades de negócios e proteção de serviços mais críticos. O *COBIT 5 for Risk* [18] afirma que o risco de TI sempre existe, mesmo que não seja detectado ou reconhecido por uma empresa.

A implementação do ERM é um desafio e exige tempo e recursos. Bharathy e McShane [46] afirmam que as empresas que tentam implementar ERM estão lutando para fazer mudanças em sua filosofia. Uma das principais dificuldades encontradas é definição do seu apetite a risco [57], pois não existe um apetite de risco padrão aplicável a todas as organizações. Uma organização deve ser capaz de entender o impacto da determinação de níveis de tolerância de risco maiores e mais baixos para determinados objetivos [14, 20, 58, 59]. Outra dificuldade é encontrar a abordagem correta para comunicar de maneira clara os objetivos, as políticas e os limiares de tolerância de risco, utilizando uma linguagem de risco comum a toda a empresa para garantir um ERM efetivo [11, 19, 56, 59].

A mudança de cultura, incluindo normas e comportamentos que determinam como todos os membros de uma organização devem agir em relação aos riscos corporativos é outro desafio importante na implementação de um sistema ERM [11, 13, 18, 20, 58]. De acordo com o COSO [13], a gestão de riscos é a tarefa de cada pessoa dentro de uma organização. Outra dificuldade está relacionada à definição das novas estruturas organizacionais necessárias para construir e sustentar a gestão de riscos, como a nomeação de um Diretor de Riscos, ou *Chief Risk Officer* (CRO), e a criação de uma função dedicada à ERM para apoiá-lo [18, 58, 59].

Assim, a correta implementação das normas e modelos de gestão de riscos traz vários benefícios para as empresas, como: a identificação precisa dos risco e medição de sucesso no tratamento desse risco; a melhor compreensão do impacto de risco na empresa; oportunidades para integrar o gerenciamento de risco de TI com riscos corporativos e

estruturas de conformidade; promoção da responsabilidade e aceitação de riscos em toda a empresa; entre outros [11, 20, 60]. Entretanto, para se obter tais benefícios, não basta apenas implantar a gestão de riscos. É necessário avaliar e medir a maturidade do risco organizacional continuamente a fim de determinar se os riscos são devidamente gerenciados de acordo com os objetivos do negócio [1, 13, 18, 47, 59]. Modelos de Maturidade em Gestão de Riscos são apresentados na próxima seção.

2.1.1 Modelos de Maturidade

Um modelo de maturidade funciona como um guia para a organização, auxiliando-a a ter conhecimento de onde e como está, para realizar um plano de melhoria na busca da excelência. Considera-se que uma empresa atingiu sua maturidade quando os seus processos são explicitamente definidos, gerenciados, medidos, controlados e eficazes, isto é, quando possuem mecanismos que garantem a repetição sucessiva dos bons resultados, principalmente, em relação à qualidade, custos e prazos [61].

Becker et al [62] definem modelos de maturidade como "modelos conceituais que descrevem os caminhos de evolução antecipados, típicos, lógicos e desejados para a maturidade". Para Öngel [63], a maturidade pode ser melhor descrita combinando a capacidade de agir e decidir com a vontade de se envolver, entendendo o impacto da vontade e da ação.

Segundo Xianbo et al [64], os modelos de maturidade servem para avaliar a capacidade dos processos na realização de seus objetivos, identificar as oportunidades de melhoria de qualidade e produtividade, além de planejar e monitorar as ações de melhoria contínua dos processos empresariais. Entretanto, Junior et al [65] alerta que os modelos de maturidades adquirem um aspecto de diagnóstico, mas que por si só não garantem o sucesso do processo, apenas aumentam sua probabilidade.

Chapman [12] acredita que os modelos de maturidade podem efetivamente ajudar as organizações a entenderem o nível atual de ERM e melhorar seu desempenho neste processo de gestão. Para Coetzee e Lubbe [32], um modelo de maturidade de risco deve ser utilizado principalmente pelos gestores para que possam tomar suas decisões fundamentadas na gestão de riscos.

De acordo com Wieczorek-Kosmala [34], um modelo de maturidade de risco é estruturado como uma matriz em que os níveis de maturidade são referenciados com os atributos que refletem as principais práticas de gestão de riscos. Cada um dos campos da matriz descreve as competências que indicam as práticas alcançadas ou desejadas, conforme apresentado na Figura 2.1.

Os modelos são concebidos de tal forma que a capacidade nos níveis inferiores provê progressivamente as bases para os estágios superiores. As competências dos níveis inferiores são consideradas bons indicadores das principais etapas que uma organização deve

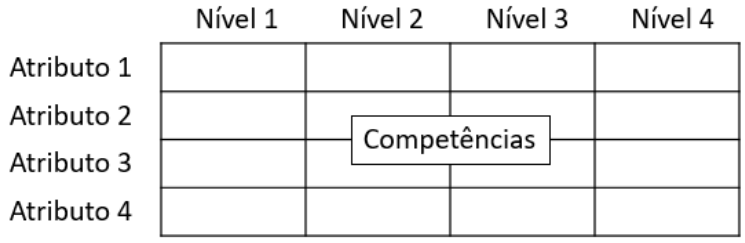

Figura 2.1: Estrutura modelo de maturidade de risco (Fonte: [34]).

empreender ao implementar um processo de gerenciamento de riscos, enquanto os níveis mais altos de maturidade refletem as práticas e competências gerenciais mais avançadas desse processo [34]. Existem na literatura vários modelos de maturidade em gestão de riscos, que variam principalmente em relação aos seus atributos e aos níveis de classificação de maturidade. A Tabela 2.1 apresenta os modelos de maturidade de riscos estudados neste trabalho.

Em todos os modelos de maturidade de riscos estudados, entende-se que no primeiro nível ou Nível 1, uma organização simplesmente não gerencia riscos. Consideram que, mesmo que sejam tomadas medidas gerenciais nesse campo, elas são ingênuas, caóticas, *ad hoc* e individualmente orientadas [12, 14, 16, 17, 19, 20, 21, 30]. Alguns autores consideram ainda um nível predecessor a este, chamado Nível 0 ou inexistente [66].

Os níveis seguintes refletem os avanços que uma organização pode realizar na implementação da gestão de riscos [12]. Em geral, no Nível 2 já existe um procedimento seguido por vários indivíduos, embora ainda seja novato e não documentado. O segundo nível de maturidade é muitas vezes caracterizado pela experimentação do gerenciamento de risco, isto é, a organização adota alguns elementos de níveis mais maduros, mas ainda possui capacidades limitadas para identificar, avaliar, gerenciar e monitorar riscos [16, 17, 19, 30]. O Nível 3, considerado um nível pré-maduro, é caracterizado por capacidades suficientes de gerenciamento de risco, mas ainda não possui uma verdadeira integração com todas as áreas de tomada de decisão. Além disso, não implementa métricas de risco associadas a criação de valor. Normalmente, os procedimentos foram padronizados, documentados e comunicados a todas as partes interessadas [12, 16, 30].

No Nível 4, existe um compromisso evidente do conselho de administração em incorporar o gerenciamento de riscos a cada aspecto da tomada de decisão. O processo de gerenciamento de riscos é monitorado e está em constante melhoria [12, 16, 17, 19, 30]. Quando existe, o Nível 5 caracteriza que o gerenciamento de riscos atingiu o nível de excelência [14, 19, 21, 30, 49]. Apesar da maioria dos modelos estudados apresentarem

entre quatro e cinco níveis de maturidade, não existem limites para um modelo. Aksu [67], por exemplo, prevê dez níveis de maturidade em seu modelo de maturidade para organizações de TI: ausente, consciente, trabalhando, principal, geral, em desenvolvimento, desenvolvido, científico, expert e líder.

Em relação aos atributos ou dimensões de maturidade, eles refletem as principais práticas de gerenciamento de risco em uma organização. Entre os modelos estudados, foram identificados quatro atributos mais utilizados: cultura, processo, experiência e aplicação [11, 16, 47]. Em geral, as dimensões possuem sub-dimensões ou critérios, que fornecem a base para a definição dos objetivos de controle ou dos fatores de riscos nas diferentes categorias de níveis de maturidade de risco [24, 68].

O atributo cultura representa os valores, normas e comportamentos compartilhados por todos os membros de uma organização e como eles atuam em relação aos riscos corporativos [58]. Para Wieczorek-Kosmala [34], a dimensão cultura está associada ao gerenciamento proativo de risco encorajado e recompensado e ao envolvimento da alta gestão no processo. Segundo Ren et al [22], a cultura de risco pode ser medida usando o nível de consistência entre as decisões sobre riscos e as políticas existentes e o perfil de risco desejado. De acordo com a literatura estudada, os principais critérios que caracterizam o atributo cultura são:

1. **Política de gestão de riscos**: Declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos. Fornecem orientações detalhadas sobre como colocar os princípios em prática e como os mesmos influenciarão a tomada de decisões [11, 12, 13, 14, 18, 19, 20, 22, 24, 30, 34, 35, 37, 38, 43, 46, 47, 48, 51, 53, 56, 58].

2. **Comunicação do risco**: Processos contínuos e iterativos conduzidos pela organização para obter, fornecer e compartilhar informações relacionadas ao gerenciamento de riscos de forma clara e objetiva a todas as partes interessadas [11, 13, 14, 18, 19, 20, 24, 25, 30, 34, 35, 37, 38, 43, 47, 48, 50, 51, 52, 53, 58, 59].

3. **Comprometimento da alta gestão**: A alta administração da organização define direção e demonstra suporte visível e genuíno às práticas de gerenciamento de riscos [11, 12, 13, 18, 24, 30, 35, 37, 38, 43, 47, 48, 53, 59].

4. **Governança corporativa**: Conjunto de processos que garante que as necessidades, condições e opções das partes interessadas sejam avaliadas de forma a determinar objetivos corporativos, definir a direção estratégica através de priorizações e tomadas de decisão e monitorar o desempenho e a conformidade das atividades em relação aos objetivos estabelecidos [5, 11, 12, 13, 18, 24, 30, 43, 48, 51, 53, 59].

5. **Responsabilidade e autoridade**: A alta administração deve assegurar que as responsabilidades e autoridades para gerenciar riscos sejam atribuídas, comunicadas e entendidas na organização [11, 12, 13, 18, 19, 24, 25, 30, 43, 48, 51, 58, 59, 60].

6. **Integridade e ética**: Conjunto de medidas com o objetivo de prevenir, detectar e remediar a ocorrência de fraude, corrupção ou qualquer ato que vá contra os valores das empresas, pensadas e implementadas de forma sistêmica, com aprovação da alta administração e sob coordenação de uma área ou pessoa responsável [13, 18, 19, 20, 24, 30, 47, 51, 56, 59].

7. **Competência**: Definição dos níveis de educação e qualificação, habilidades técnicas, níveis de experiência, conhecimento e habilidades comportamentais necessários para executar atividades no gerenciamento de riscos [13, 18, 24, 30, 47, 51].

8. **Apetite ao risco**: A quantidade de risco, em um nível amplo, que uma entidade está disposta a aceitar em busca de sua missão. É o reflexo da gestão de riscos e tem forte influência sobre a cultura dentro da organização [12, 13, 14, 16, 18, 19, 20, 30, 34, 35, 37, 38, 43, 46, 47, 48, 51, 53, 58, 59].

A dimensão processo explica como o gerenciamento de riscos é institucionalizado dentro da organização. Compreende também a eficácia do processo, suas métricas e a sua integração com outras funções organizacionais. Os principais critérios que caracterizam essa dimensão incluem os processos de gerenciamento de riscos definidos pela ABNT NBR ISO/IEC 31000 [43]. São eles:

1. **Identificação do risco**: Processo de busca, reconhecimento e descrição do risco. Inclui a identificação das causas e fontes de risco, eventos, situações ou circunstâncias que podem impactar os objetivos e a natureza desse impacto [12, 13, 14, 17, 18, 19, 20, 22, 24, 25, 30, 35, 37, 38, 43, 47, 48, 51, 53, 56, 58, 69].

2. **Análise de risco**: Processo de compreender a natureza do risco e determinar as consequências e suas probabilidades para eventos identificados de risco, levando em consideração a presença (ou não) e a eficácia de quaisquer controles existentes. Envolve a consideração das causas e fontes de risco, suas consequências e a probabilidade de que essas consequências possam ocorrer [12, 13, 14, 17, 18, 19, 20, 22, 24, 25, 30, 35, 37, 38, 43, 47, 48, 51, 53, 56, 58, 69].

3. **Avaliação de risco**: Processo de comparar os resultados da análise de risco com os critérios de risco para determinar se o risco e sua magnitude é aceitável ou tolerável. Utiliza a compreensão do risco para tomar decisões sobre as ações futuras [12, 13, 14, 17, 18, 19, 20, 22, 24, 25, 30, 35, 37, 38, 43, 47, 48, 51, 53, 56, 58, 69].

4. **Tratamento do risco**: Processo para selecionar uma ou mais opções para modificar os riscos e a implementação dessas opções. Uma vez implementado fornece novos controles ou modifica os existentes. As principais formas de tratamento de risco são: evitar o risco, eliminar o risco, mitigar ou atenuar o risco, aceitar o risco, compartilhar ou transferir o risco e aumentar o risco [12, 13, 14, 17, 18, 19, 20, 22, 24, 25, 30, 35, 37, 38, 43, 47, 48, 51, 53, 56, 58, 69].

5. **Monitoramento e controle**: Processos para acompanhar, analisar e controlar o progresso e desempenho do gerenciamento de riscos. Inclui monitorar os riscos residuais, identificar novos riscos e executar planos de respostas a riscos de forma contínua, em busca de riscos novos, modificados e desatualizados [12, 13, 14, 17, 18, 19, 20, 22, 24, 25, 30, 35, 37, 38, 43, 47, 48, 51, 53, 56, 58, 69].

6. **Atualização da base de risco**: Processo de manter atualizado o conjunto de informações relevantes para gerenciamento do risco, incluindo eventos e perdas, ganhos operacionais, custos de oportunidade e receitas perdidas decorrentes de situações que poderiam ter resultado em eventos de risco. Estão incluídas na base de risco informações referentes aos dados internos, dados externos, análise de cenário e fatores de controles internos e ambiente de negócios [13, 18, 24, 30, 43, 47, 51, 69].

7. **Gerenciamento da informação do risco**: Processo formal de compartilhamento de conhecimento e de informações relacionadas ao gerenciamento de riscos [13, 18, 24, 30, 43, 47, 51, 69].

8. **Auditoria**: Função organizacional responsável por avaliar a existência, o cumprimento, a eficácia e a otimização dos controlos internos e processos de governança relacionados ao gerenciamento de riscos, fornecendo relatórios sobre o risco associado às falhas identificadas [12, 13, 18, 19, 24, 25, 30, 37, 38, 43, 47, 51, 56, 58, 60, 69].

A experiência é o terceiro atributo estudado. Este atributo avalia os fatores relacionados aos recursos humanos, considerando as lições aprendidas ao longo do processo de gerenciamento de riscos. Esta dimensão também destaca a capacidade das organizações em programas de desenvolvimento e capacitação para melhorar as habilidades de recursos humanos dedicados à gestão de riscos. Os principais critérios que caracterizam a dimensão experiência são:

1. **Orçamento**: Processo de agregação dos custos estimados relacionados às pessoas, habilidades e competências necessárias para fornecer e executar com sucesso as atividades do processo de gerenciamento de riscos. Inclui mão de obra direta, materiais, equipamentos, treinamentos, certificações, entre outros [18, 19, 20, 24, 30, 34, 47, 58, 59].

2. **Equipe de apoio dedicada**: Equipe dedicada a fornecer orientação sobre o gerenciamento de riscos, avaliando os níveis adequados de conhecimentos e práticas de risco de todos os papéis da empresa e definindo ações necessárias para assegurar a sua correta implementação [18, 19, 20, 24, 30, 34, 35, 37, 38, 46, 47, 51, 58, 59].

3. **Treinamento**: Programas de treinamento e capacitação para garantir que os indivíduos sejam efetivos em suas funções no gerenciamento de riscos. Devem ser direcionados aos diferentes níveis de consciência de risco da organização [18, 24, 30, 47, 58, 59].

4. **Pesquisa e desenvolvimento**: Atividades de longo prazo orientadas ao futuro, relacionadas à aplicação da ciência e tecnologia no processo de gerenciamento de riscos, a partir da originalidade e a inovação [13, 18, 24, 30, 47].

5. **Capacidade de aprendizado**: Processo de aquisição e compartilhamento de conhecimentos, habilidades, valores e atitudes, possibilitado através do estudo, do ensino ou da experiência [11, 18, 19, 20, 24, 30, 47, 56, 58, 59].

6. **Capacidade de gerenciamento de mudanças**: Processo de gerenciar todas as mudanças de forma controlada a fim de minimizar riscos e impactos para as partes interessadas. Qualquer acréscimo, modificação ou remoção de qualquer aspecto que afete os serviços da organização deve ser considerado uma mudança [13, 18, 24, 30, 47].

A quarta dimensão, chamada de aplicação, se refere ao conjunto de ferramentas, métodos e aplicações utilizados no gerenciamento de riscos. Provê informações relacionadas à riscos e auxiliam os gestores na tomada de decisão, pois evidenciam como a organização pode deixar de atingir seus objetivos se não gerenciar os riscos de forma eficiente. Os critérios de destaque para esta dimensão são:

1. **Planejamento**: Definição ponta a ponta de como as atividades de gerenciamento dos riscos serão estruturadas e executadas. Deve-se especificar as abordagens, metodologias, ferramentas e fontes de dados específicas que serão usadas [13, 18, 19, 20, 25, 30, 35, 37, 38, 43, 47, 51, 56, 58, 59, 60, 69].

2. **Escopo**: Definição do escopo e das restrições do processo de gerenciamento de riscos para garantir que todos os ativos relevantes sejam levados em consideração durante a análise e avaliação de risco. Deve-se justificar quaisquer exclusões no escopo [13, 18, 19, 20, 24, 30, 35, 37, 38, 43, 47, 51, 60, 62, 69].

3. **Integração com outras tarefas de gerenciamento**: Incorporação de práticas de gerenciamento de riscos em todas as práticas e processos da organização, de forma

pertinente, eficaz e eficiente [11, 13, 14, 18, 20, 22, 24, 30, 35, 37, 38, 43, 47, 51, 58, 60, 62].

4. **Relacionamento partes interessadas**: Processo de comunicar e trabalhar com as partes interessadas para atender suas necessidades e expectativas e promover a sua participação de forma adequada [12, 13, 14, 17, 18, 19, 20, 22, 24, 25, 30, 35, 37, 38, 43, 47, 48, 51, 53, 56, 58, 69].

5. **Função dedicada**: Criação de uma unidade responsável por integrar e orientar as atividades pelo gerenciamento de riscos, que pode ser um departamento, núcleo, área ou unidade funcional composta por representantes de diversas áreas (comitê) [14, 18, 19, 20, 24, 25, 30, 34, 35, 37, 38, 46, 47, 48, 51, 53, 58, 59, 69].

6. **Medição de desempenho na gestão de riscos**: Definição de Indicadores Chaves de Desempenho (*Key Performance Indicators* (KPI)) para prover as informações certas para a tomada de decisão, diminuindo ou eliminando o impacto dos riscos na organização [11, 12, 13, 14, 18, 19, 24, 30, 35, 37, 38, 43, 47, 53, 56, 58, 59, 69].

7. **Tomada de decisão baseada na gestão de riscos**: Fornecimento de informações chaves sobre o impacto dos riscos no negócio com o objetivo de apoiar os gestores na tomada de decisão. Considera os cenários mais pessimistas e mais prováveis, os eventos futuros não controláveis e os Indicadores Chaves de Desempenho resultantes do processo de gerenciamento de riscos [12, 13, 14, 17, 18, 19, 20, 22, 24, 25, 30, 35, 37, 38, 43, 45, 47, 48, 51, 53, 56, 58, 69].

8. **Processo de negócio baseado na gestão de riscos**: Compreensão de como o gerenciamento eficaz de riscos de TI otimiza o valor da organização, com eficácia e eficiência do processo comercial, qualidade melhorada e redução de resíduos e custos [12, 13, 14, 17, 18, 19, 20, 22, 24, 25, 30, 35, 37, 38, 43, 45, 47, 48, 51, 53, 56, 58, 69].

Dos modelos de maturidade em gestão de riscos estudados, apresentados na Tabela 2.1, o modelo de Hillson [16], publicado em 1997, é baseado no processo de gerenciamento de projetos e considerado um modelo pioneiro, que serviu de referência para outros modelos criados nos anos subsequentes [11, 12, 17]. Em 2000, Hopkinson [17] desenvolveu um modelo chamado de *Project Risk Maturity Model* (PRMM), baseado nos níveis apresentados por Hillson, mas definiu seis atributos de maturidade, que chamou de perspectivas.

Dois anos mais tarde, o *Software Engineering Institute* (SEI) ou Instituto de Engenharia de Software, desenvolveu o *Capability Maturity Model Integration* (CMMI) ou Modelo Integrado de Maturidade em Capacitação, com o objetivo de combinar os vários modelos existentes para análise de maturidade em engenharia de software. O CMMI, coordenado

pelo *CMMI Institute*, tornou-se uma referência mundial de melhores práticas para desenvolver e entregar sistemas de informação e acabou servindo de inspiração para a criação de novos modelos de maturidade, entre eles, os voltados à avaliação de maturidade em gestão de riscos [14, 19, 23, 69]. No mesmo ano,*Project Management Solutions* (PMS) desenvolveu o *Project Management Maturity Model* (PMMM), um modelo para ajudar as organizações a melhorarem seus processos de gerenciamento de projetos, fornecendo uma estrutura conceitual e se tornando um padrão da indústria na medição da maturidade em gerenciamento de projetos [11, 70, 71]. Seus níveis de maturidade foram influenciados pelos níveis de maturidades definidos pelo CMMI.

Ainda em 2002, a partir da iniciativa do Programa de Pesquisa e Desenvolvimento de Gerenciamento de Riscos patrocinado pelo *The Risk Management SIG* (RISKSIG), ou Grupo Mundial de Interesses Específicos de Riscos do *Project Management Institute* (PMI), foi lançado o modelo *Risk Management Maturity Model* (RMMM), voltado especificamente para o gerenciamento de riscos, apresentando uma metodologia menos formal que a apresentada pelo CMMI [72]. É um modelo genérico de maturidade, aplicado a todos os tipos de projetos e organizações de qualquer setor, focado em ajudar na implementação de processos formais de risco ou na melhoria de sua abordagem atual. Seus níveis de maturidade se apresentam como uma versão simplificada dos níveis de maturidades definidos pelo CMMI e seus atributos são os mesmos definidos por Hillson [11, 23, 70].

O *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) ou Comitê de Organizações Patrocinadoras da Comissão Treadway publicou em 2004 a obra *Enterprise Risk Management – Integrated Framework (COSO ERM ou COSO II)* com a finalidade de ajudar as entidades a proteger e aperfeiçoar o valor das partes interessadas [49]. Projetado para criar uma "consciência sobre riscos e controles" por toda a empresa e tornar-se um modelo comum para a discussão e avaliação de riscos organizacionais, o COSO ERM tornou-se uma das principais referências em gerenciamento de riscos corporativos, capaz de integrar conceitos de controle interno, a *Lei Sarbanes-Oxley* (SOX) e planejamento estratégico. O modelo define cinco níveis de maturidade que evoluem de muito fraco até ótimo, e possui oito principais atributos, chamados de componentes [13, 49]. A versão atual, publicada em 2017, aborda diferentes pontos de vista da estrutura organizacional e contemplam meios de alinhamento da gestão de riscos com a estratégia e tomada de decisões.

Ainda em 2004, Ren e Yeo publicaram uma estrutura multinível para *Risk Management - Capability Maturity Model* (RM-CMM) ou Modelo de Maturidade da Capacidade de Gerenciamento de Risco, especificamente para projetos *Complex Product Systems* (CoPS) ou Sistemas Complexos de Produtos [21, 22]. O CoPS é uma classe especial de projetos, que são produtos ou sistemas de alto valor, intensivos em tecnologia e engenharia, que são

normalmente usados para produzir bens de consumo e serviços. Seus níveis de maturidade são inspirados nos níveis de maturidade do CMMI. O entendimento da complexidade inerente aos projetos CoPS inclui a tecnologia como uma nova dimensão. O modelo proposto também é construído sobre uma estrutura de gerenciamento de mudanças associada aos processos de gerenciamento de riscos [22].

O *Risk Maturity Model* (RMM) publicado em 2006 pelo *Risk and Insurance Management Society* (RIMS) é uma ferramenta usada para gerenciamento de riscos para desenvolver programas de gestão de riscos de negócios sustentáveis [30]. O modelo permite que os profissionais de risco classifiquem seus programas de gerenciamento de riscos e estabeleçam um roteiro para melhoria. Definem cinco níveis de maturidade que variam de inexistente a liderada e fornecem um conjunto de oito atributos baseados em gestão de negócio que impulsionam o valor comercial, projetados para serem compatíveis com várias estruturas especializadas, como o COSO ERM [13, 49], COBIT 5 [18], Standard & Poor's ERM [52], entre outros.

Chapman [12] realizou um estudo do gerenciamento de riscos e criou um modelo simplificado de avaliação de maturidade, contendo quatro níveis de maturidade e cinco atributos. Em 2008, o COBIT apresentou um modelo de maturidade voltado para de governança e gestão de TI, que embora não seja dedicado exclusivamente à gestão de riscos, faz referência ao tema como um dos processos fundamentais para criação de valor para as empresas [66]. Assim como o CMMI, o COBIT é um dos principais modelos de referência em avaliação de maturidade.

O *Organizational Project Management Maturity Model* (OPM3), ou Modelo de Maturidade de Gerenciamento de Projetos Organizacional, é um padrão de melhores práticas reconhecidas mundialmente que auxilia as organizações a entenderem seus processos e práticas de Gerenciamento de Projetos Organizacionais. Define quatro níveis de maturidade e três atributos para ajudar as organizações a desenvolverem um roteiro para melhorar seu desempenho. Em 2008 foi reconhecida pelo *American National Standards Institute* (ANSI) como um padrão nacional americano (ANSI/PMI 08-004-2008) [47].

Em seu modelo, chamado *Maturity Model to Risk Management Process in Information Security* (MMGRSeg), Mayer e Fagundes [19] avaliam o nível de maturidade das empresas em relação ao processo de gerenciamento de riscos em segurança da informação. Com cinco níveis de maturidade e seis atributos inspirados nos processos definidos pela ABNT NBR ISO/IEC 31000 [43], o modelo visa fornecer informações valiosas que para auxiliar as organizações a planejar, executar e monitorar suas iniciativas de melhoria e gerenciamento de seus processos de negócios e orientar os processos de tomada de decisão.

O *Portfolio, Program and Project Management Maturity Model* (P3M3), ou Modelo de Maturidade de Gerenciamento de Portfólio, Programa e Projeto, desenvolvido pela *Office*

of Government Commerce (OGC) em 2010, é um modelo de maturidade de gerenciamento que avalia como a organização como um todo entrega seus projetos, programas e portfólios. Seu diferencial consiste em avaliar todo o sistema e não apenas os processos [73].

Elmaallam e Kriouile [14, 15] propuseram um modelo de maturidade em gestão de riscos para o desenvolvimento da governança em sistemas de informação, mais especificamente, do gerenciamento de risco, também utilizando os processos ABNT NBR ISO/IEC 31000 [43] para definição dos seus objetivos de controle. O modelo conhecido por *Information System Risk Management Maturity Model* (ISR3M), envolve a avaliação dos objetivos de controle em cada elemento de controle para cada um dos nove atributos definidos.

Na literatura estudada, o modelo que mais se diferencia dos demais é o proposto por Asku [67], baseado na estrutura de processos de TI, e define dez níveis de maturidade, de ausente a líder. Em seu modelo, denominado *Corporate Informatic Maturity Model* (CI-MM), cada nível é avaliado em dez atributos ou dimensões. Oliva [20] também se destaca por criar um modelo de maturidade específico para ERM, chamado *Maturity Model for Enterprise Risk Management* (MM-ERM), mantendo cinco níveis de maturidade semelhante a maioria dos modelos. Em seu modelo, Oliva [20] classifica os atributos em quatro fatores: organização, que representa o quanto a empresa dedica esforços para produzir uma gerenciamento de risco estruturado; tecnicidade, que retrata a frequência com que a empresa faz uso de técnicas qualitativas ou quantitativas para suportar o processo de gerenciamento de riscos na corporação; transparência, que revela a frequência com que a empresa aborda o assunto abertamente com seus colaboradores; e envolvimento, que mostra o quanto a empresa é capaz de envolver outros agentes do seu ambiente de valor para tornar sua administração de riscos mais eficiente e efetiva.

A Tabela 2.1 apresenta um resumo dos principais modelos de maturidade em gestão de riscos estudados.

Tabela 2.1 : Resumo dos principais modelos de maturidade em gestão de riscos estudados

Modelo	Autor	Ano	Níveis de Maturidade	Atributos	Referências
RMM	Hillson [16]	1997	1. Ingênuo 2. Novato 3. Normalizado 4. Natural	1. Cultura 2. Processo 3. Experiência 4. Aplicação	[11, 14, 17, 34]
PRMM	Hopkinson [17]	2000	1. Ingênuo 2. Novato 3. Normalizado 4. Natural	1. Gestão 2. Identificação do Risco 3. Análise do Risco 4. Resposta ao Risco 5. Gerenciamento de Projeto 6. Gestão de Risco Cultural	[11, 34]
CMMI	SEI [74]	2000	1. Inicial 2. Gerenciado 3. Definido 4. Quantitativamente Gerenciado 5. Otimizado	1. Pessoas 2. Ferramentas 3. Procedimento	[14, 19, 23, 69]
PMMM	PMS [71]	2002	1. Processo Inicial 2. Processo Estruturado e Padronizado 3. Padrões Organizacionais e Processos institucionalizados 4. Processo Gerenciado 5. Processo Otimizado	1. Identificação do risco 2. Quantificação do risco 3. Desenvolvimento de resposta ao risco 4. Controle do risco 5. Documentação do risco	[11, 70]

Tabela 2.1 : Resumo dos principais modelos de maturidade em gestão de riscos estudados

Modelo	Autor	Ano	Níveis de Maturidade	Atributos	Referências
RMMM	PMI–EUA [72]	2002	1. Ad Hoc 2. Inicial 3. Repetitiva 4. Gerenciada	1. Cultura 2. Processo 3. Experiência 4. Aplicação	[11, 23, 70]
ERM	COSO[49]	2004	1. Muito Fraco 2. Pobre 3. Médio 4. Bom 5. Bom	1. Ambiente Interno 2. Definição de Objetivos 3. Identificação de Evento 4. Avaliação de Risco 5. Respostas aos Riscos 6. Atividades de Controle 7. Informação e Comunicação 8. Monitoramento	[11, 13, 23]
RM-CMM CoPS	Ren e Yeo [21]	2002	1. Ad Hoc 2. Inicial 3. Definida 4. Gerenciada 5. Otimizada	1. Cultura 2. Processo 3. Tecnologia	[22, 68]
RMM for ERM	RIMS [30]	2006	1. Ad Hoc 2. Inicial 3. Repetitiva 4. Gerenciada 5. Liderada	1. Gestão baseada em ERM 2. Gestão de processos de ERM 3. Gestão de apetite de risco 4. Disciplina de causa raiz 5. Descoberta de riscos 6. Gestão de desempenho	[11]

Tabela 2.1 : Resumo dos principais modelos de maturidade em gestão de riscos estudados

Modelo	Autor	Ano	Níveis de Maturidade	Atributos	Referências
				7. Resiliência 8. Sustentabilidade dos negócios	
RMM	Chapman[12]	2006	1. Inicial 2. Básico 3. Padrão 4. Avançado	1. Cultura 2. Sistema 3. Experiência 4. Treinamento 5. Gestão	[34]
COBIT	ISACA [9, 66]	2008	0. Não existente 1. Inicial / Ad Hoc 2. Repetitivo, mas Intuitivo 3. Processo Definido 4. Gerenciado e Mensurável 5. Otimizado	1. Conscientização e Comunicação 2. Políticas, Planos e Procedimentos 3. Ferramentas e Automação 4. Habilidades e Expertise 5. Responsabilidades 6. Definição de Metas e Medição	[19, 23]
OPM3	PMI [47]	2008	1. Padronizado 2. Medido 3. Controlado 4. Melhoria Contínua	1. Conhecimento 2. Avaliação 3. Melhoria	[14, 19]
MMGRSeg	Mayer e Fagundes [19]	2009	1. Inicial 2. Conhecido 3. Padronizado 4. Gerenciado 5. Otimizado	1. Definições do Contexto 2. Análise/Avaliação de Risco 3. Tratamento de Risco 4. Aceitação de Risco 5. Comunicação de Risco 6. Monitoramento e Análise Crítica	[11, 14]

Tabela 2.1 : Resumo dos principais modelos de maturidade em gestão de riscos estudados

Modelo	Autor	Ano	Níveis de Maturidade	Atributos	Referências
P3M3	OCG [51]	2010	1. Processo inicial 2. Processo repetitivo 3. Processo definido 4. Processo gerenciado 5. Processo otimizado	1. Contexto organizacional 2. Objetivos organizacionais 3. Envolvimento das partes interessadas 4. Estrutura de suporte 5. Cultura de suporte 6. Funções e responsabilidades 7. Indicadores de alerta precoce 8. Abordagem de Gestão de Riscos 9. Superando barreiras de Gestão de Riscos 10. Relatórios 11. Ciclo de revisão 12. Melhoria contínua	[11]
ISR3M	Elmaallam e Kriouile [14]	2011	1. Inicial 2. Definido 3. Normalizado 4. Gerenciado 5. Otimizado	1. Infraestrutura 2. Ambiente 3. Estratégias 4. Participantes 5. Informação 6. Tecnologias 7. Processos de negócio 8. Produtos e serviços 9. Clientes	[15, 22]

Tabela 2.1 : Resumo dos principais modelos de maturidade em gestão de riscos estudados

Modelo	Autor	Ano	Níveis de Maturidade	Atributos	Referências
CI-MM	Aksu [67]	2013	1. Ausente 2. Consciente 3. Trabalhando 4. Principal 5. Geral 6. Em desenvolvimento 7. Desenvolvido 8. Científico 9. Expert 10. Líder	1. Significado 2. Descrição 3. Cobertura 4. Papéis 5. Processos 6. Governança 7. Medição 8. Automação 9. Comunicação 10. Modelo de maturidade	[69]
MM-ERM	Oliva [20]	2016	1. ERM Insuficiente 2. ERM Contingente 3. ERM Estruturado 4. ERM Participativo 5. ERM Sistêmico	1. Organização 2. Tecnicidade 3. Transparência 4. Envolvimento	

Analisando os diversos modelos de maturidade em gestão de riscos resumidos na Tabela 2.1, é possível perceber um crescente interesse pelo assunto desde o modelo proposto por Hillson, em 1997 [16]. Ao longo dos anos, houveram diversas iniciativas para concepção de novos modelos, principalmente em setores específicos, como engenharia de software, gestão de projetos e gestão de negócios. Tais modelos, mesmo não sendo dedicados exclusivamente à gestão de riscos, referenciam o tema em algum grau e permitem a melhoria da maturidade de gestão de riscos de acordo com os tipos de riscos frequentemente observados [11, 12, 14, 17, 19, 22, 30, 49, 51, 66]. Nos modelos mais recentes, nota-se uma preocupação com a integração dos processos de gestão de riscos com os demais processos das organizações [20, 67].

A maioria dos modelos de maturidade tem influência dos modelos já existentes, seja na definição dos seus níveis de maturidade ou dos seus atributos [11, 12, 16, 17]. Quanto à quantidade de níveis de maturidade, a maioria dos modelos estudados apresentam entre 4 e 5 níveis, que vão de inicial a otimizado, ou outro termo semelhante que indique a clara progressão entre os níveis. Alguns modelos consideram o nível 0 como inexistente. O modelo proposto por Aksu [67] difere dos demais pois propõe 10 níveis de maturidade, de ausente a líder. Todos os modelos estudados apresentam os níveis em ordem crescente de maturidade.

Em relação aos atributos ou dimensões, os mais utilizados são cultura, processo, experiência e aplicação [11, 16, 47]. Embora alguns modelos utilizem outros atributos, a maioria utiliza pelo menos um destes quatro [12, 14, 21]. Alguns modelos preferem definir seus atributos baseados nos processos da ABNT NBR ISO/IEC 31000 [17, 19, 49] e outros criam seus próprios atributos, de acordo com suas necessidades [20, 30, 69, 70, 73].

Na prática, com tantos modelos de maturidade em gestão de riscos, é comum que as organizações desenvolvam sua própria estrutura para avaliação da maturidade dos seus processos baseada nos modelos existentes, influenciadas pelas suas próprias necessidades [11, 20, 31, 64]. Em muitos casos, não se preocupam com a qualidade da avaliação e apresentam resultados imprevisíveis e inconsistentes [61]. Isso porque para os gestores, tomar decisões e avaliar a maturidade dos processos de gestão de riscos é uma tarefa complexa, principalmente quando envolve aspectos técnicos, sociais e políticos [33].

A utilização de métodos científicos na tomada de decisão pode dar ao gestor um maior entendimento sobre seu nível de maturidade e sobre a melhor estratégia de implementação da gestão de riscos. É uma maneira de fornecer elementos quantitativos para a tomada de decisão e ajudar os gestores a realizarem uma avaliação de maturidade em riscos mais objetiva e prática.

É o caso de Wibowo e Taufic [24], que usam o método Delphi para selecionar e validar os atributos mais relevante e o método *Analytic Hierarchy Process* (AHP) para deter-

minar os pesos dos atributos selecionados. Os níveis de maturidade são classificas em quatro níveis: ingênuo (0-24), novato (25-49), normalizado (50-74) e gerenciado (57-100). Yudatama e Sarno [25] também utilizam métodos de apoio multicritério para desenhar seu modelo de maturidade em gestão de riscos: utilizam o método AHP para determinar o peso de cada critério especificado e o método *Technique for Order Preference by Similarity to the Ideal Solution* (TOPSIS) para selecionar a melhor alternativa. Na revisão da literatura não foram encontrados modelos de avaliação de maturidade em gestão de riscos que utilizassem o método ELECTRE-TRI, em problemas de classificação.

2.2 Métodos de Apoio Multicritério à Decisão

A tomada de decisão está presente em todas as atividades desenvolvidas pelo homem. Diariamente, as pessoas passam por situações que envolvem preferências sobre um conjunto de alternativas e devem optar por aquela que melhor satisfaça os objetivos em questão [29]. O ato de decidir é um processo que pode se apresentar complexo, envolve colher informações, atribuir importância a elas, buscar possíveis alternativas de solução, fazer as escolhas entre as inúmeras alternativas encontradas, dar solução, deliberar e tomar decisão, monitorando o processo como um todo [27].

Certo [75] afirma que a decisão é a escolha feita entre duas ou mais alternativas disponíveis e tomada de decisão é o processo de escolha da melhor alternativa para a organização. Robbins et al [76] sugerem que a tomada de decisão ocorre em reação a um problema, quando o estado atual diverge do seu estado desejável. Para Gomes et al [27], existem seis elementos essenciais e comuns a toda decisão: decisor, objetivo, preferências, estratégia, situação e resultado.

Para Souza [77], uma boa decisão é uma consequência lógica daquilo que se quer, daquilo que se sabe e daquilo que se pode fazer. O que se quer se refere às consequências das decisões, que podem ser incertas ou distribuídas ao longo do tempo. O que se sabe é o conhecimento em relação às grandezas envolvidas no processo e das relações entre elas, bem como as informações ao longo do processo e a percepção das circunstâncias e das leis que a afetam. O que se pode fazer são as alternativas disponíveis e possíveis de ação.

No contexto organizacional, cada empresa é um sistema de decisões em que cada pessoa participa de forma consciente, escolhendo entre alternativas mais ou menos racionais que são apresentadas de acordo com sua personalidade, motivações e atitudes. Embora algumas decisões sejam rotineiras e bem definidas, os problemas geralmente surgem de forma singular e desestruturada, deixando os decisores inseguros quanto à melhor forma de agir [76, 78].

Em geral, nos problemas de decisão existe um tipo de padrão, ou critério, pelo qual uma escolha ou um curso de ação particular poderia ser considerado mais desejável do que outro. A consideração de diferentes escolhas ou cursos de ação torna-se um problema de tomada de decisão de múltiplos critérios quando existem vários desses padrões que conflitam substancialmente [42].

Apesar de haver algumas semelhanças, o processo decisório não é único e deve ser adaptado para cada caso. Para uma decisão inteligente, o gestor deve estar ciente das etapas do processo decisório e buscar subsídios para que a decisão seja pautada em critérios consistentes. Devem se apoiar nos procedimentos e métodos de análise da teoria de decisão para assegurar a coerência, a eficácia e a eficiência das decisões tomadas em função das informações disponíveis, antevendo cenários possíveis [79].

Segundo Belton e Stewart [42], o termo MCDA (*Multiple Criteria Decision Aid*) é abrangente e descreve uma coleção de abordagens formais que consideram vários critérios para ajudar indivíduos ou grupos a explorar decisões que importam. As decisões importam quando o nível de conflito entre critérios ou entre a relevância dos critérios para as partes interessadas assume tais proporções que a tomada de decisão intuitiva não é mais satisfatória. Para Bana e Costa e Vansnick [80], a aplicação de um método MCDA ocorre quando, diante da definição de um problema, se compara as várias alternativas de decisão utilizando múltiplos critérios.

De acordo com Gomes e Gomes [81], o que diferencia os métodos MCDA das metodologias tradicionais de avaliação é a possibilidade de incorporar percepções do decisor nos modelos de avaliação, aceitando a subjetividade presente nos processos de decisão causada pelos diferentes entendimentos dos atores da decisão. Ensslin el al [82] defendem que enquanto as abordagens tradicionais tentam dar uma solução ao problema, os métodos MCDA priorizam a construção do problema, ou seja, se dedicam a modelar o contexto do problema, através da consideração e valores das pessoas envolvidas no processo decisório. Esta modelagem permite a construção de um modelo de avaliação adequado para o contexto em questão.

Belton e Stewart [42] defendem que o principal objetivo dos métodos MCDA é ajudar os decisores a sintetizar e organizar as informações de maneira a se sentirem confortáveis e confiantes em tomar decisões, minimizando o arrependimento após a decisão e satisfazendo todos os critérios ou fatores considerados. Os métodos MCDA não darão a resposta "certa" nem fornecerão uma análise "objetiva" que irá poupar os decisores da responsabilidade de fazer julgamentos difíceis. Eles não eliminam a subjetividade inerente às tomadas de decisão, apenas tornam explícita a necessidade de julgamentos subjetivos. Gomes et al [27] adicionam que não é objetivo dos métodos MCDA dar ao decisor uma solução única para o problema. Como seu nome sugere, os métodos pretendem apoiar o

processo de decisão recomendando uma solução que se encaixe sob todos os pontos de vista restritivos do contexto analisado, da maneira mais prática e satisfatória possível. Dessa forma, auxiliam os tomadores de decisão a incluir suas preferências junto às alternativas selecionadas.

Os métodos MCDA surgiram em meados de 1970, trazendo um caráter científico e ao mesmo tempo subjetivo aos problemas de tomada de decisões. Estes métodos permitiram agregar características consideradas importantes, inclusive as qualitativas, possibilitando a sistematização do processo relacionado aos problemas de decisão [83]. Dentre as vantagens em se utilizar os métodos MCDA, destacam-se a facilidade de utilização por não especialistas, principalmente quando se utiliza algum sistema que dispõe de recursos gráficos e a incorporação de questões do comportamento humano nos processos de decisão [26, 28].

Gomes e Gomes [81] destacam que é preciso ter cuidado para não criar um modelo que não reflita a realidade, pois dessa forma, a solução não teria nenhum resultado prático. Para um bom resultado, é preciso avaliar precisamente a consequência das alternativas. Geralmente, a busca da solução de um problema ocorre em ambiente onde os critérios são conflitantes e onde o ganho de um critério acarretará na perda em outro [84].

Segundo Guarnieri [28], antes da escolha do método a ser utilizado, deve-se escolher a abordagem do método. A maioria dos autores dividem os métodos MCDA em três abordagens [26, 42, 81, 83, 85]:

1. **Escola Americana ou Escola da Teoria da Utilidade Multiatributo**: se baseia na comparação par a par entre as alternativas. Caracteriza pela não criação de uma função única que agregue os valores das alternativas, segundo cada critério. A importância relativa de cada critério sucede o conceito de taxa de substituição ou trade-off. Esta teoria assume que todos os estados são comparáveis; que existe transitividade na relação de preferências; e que existe transitividade nas relações de indiferença [86, 87]. Alguns métodos desta abordagem são: MAUT, SMART, AHP, ANP e TOPSIS.

2. **Escola Francesa ou Escola Européia ou Métodos de Subordinação e Síntese**: admite um modelo mais flexível do problema, pois não implica necessariamente na comparação entre as alternativas. Além disso, não impõe ao decisor uma estruturação hierárquica dos critérios existentes. Tais métodos consideram a atratividade ou a falta de atratividade (ou indiferença) entre os critérios ao invés da intensidade da preferência, criando um ranking de classes dos componentes da decisão [42, 84, 85]. Os métodos mais conhecidos são: ELECTRE e PROMETHEE.

3. **Métodos Interativos ou de Programação Matemática Multiobjetivo**: desenvolvidos em ambiente computacional utilizando *Multi-objective Linear Programming* (MOLP) ou Programação Linear Multiobjetivo, estes métodos permitem encontrar a dominância de uma alternativa diante dos objetivos estabelecidos, através de cálculos matemáticos e de sucessivas e interativas avaliações. Os resultados podem inclusive reconfigurar a estrutura de preferências ao considerar novas informações [88]. Métodos como o STEM, ICW e TRIMAP pertencem a essa abordagem, mas não serão estudados neste trabalho.

Alguns autores [26, 81] propõem acrescentar uma quarta abordagem, que incluiria os **Métodos Híbridos**, aqueles que utilizam tanto os conceitos da Escola Americana como os da Escola Francesa, simultaneamente. É o caso dos métodos MACBETH e TODIM.

Na literatura, diversos autores comparam os métodos MCDA e analisam os possíveis resultados. Como é o caso de Herva e Roca [89], que analisaram as principais metodologias utilizadas para avaliação ambiental e os métodos multicritério com maior relevância no campo ambiental: MAUT/MAVT (AHP/ANP, MACBETH); métodos de superação (ELECTRE, PROMETHEE/GAIA) e Lógica Fuzzy. Concluíram que os métodos MCDA mostraram-se úteis quando um grande número de critérios estava sendo considerado. De acordo com a pesquisa, os métodos de superação, principalmente o PROMETHEE e o ELECTRE, são os mais utilizados em problemas ambientais quando várias alternativas discretas estão disponíveis. AHP e ANP também são muito populares, especialmente na estruturação do problema e são frequentemente utilizados como um passo preliminar para a aplicação de métodos de superação e para a determinação de pesos. Perceberam que a Lógica Fuzzy passou a ser mais utilizada em aplicações recentes, revelando a necessidade de incorporar tais características em um problema caracterizado por imprecisão e subjetividade. Herva e Roca [89] lembram que os métodos MCDA devem ser acompanhados de análises de sensibilidade, pois as mesmas aumentam a robustez e a confiabilidade dos resultados.

Para Almeida [26], a escolha do método MCDA depende de vários fatores, entre eles as características do problema analisado, do contexto considerado, da estrutura de preferências do decisor e da problemática em si. Segundo Gomes et al [27], as soluções dos problemas de decisão variam em função do resultado pretendido. Após definir qual o problema a ser estudado, deve-se definir a problemática a ser abordada. Roy [90] distinguiu quatro problemáticas básicas, apresentadas na Tabela 2.2.

A escolha do método MCDA geralmente é feita considerando aspectos ligados às preferências do decisor [26]. Guarnieri [28] lembra que em determinadas circunstâncias, a simplicidade e a facilidade são fatores determinantes para a solução do problema. Al-

Tabela 2.2: Problemática em função do tipo de problema (Fonte: [90]).

Tipo do Problema	**Problemática abordada**
Tipo α (Pα)	Escolher a(s) melhor(es) alternativa(s).
Tipo β (Pβ)	Classificar as alternativas.
Tipo γ (Pγ)	Ordenar as alternativas.
Tipo δ (Pδ)	Descrever as alternativas.

gumas vezes, o conhecimento limitado do decisor sobre outras metodologias implica na escolha de um determinado método, que nem sempre é o mais apropriado para a situação.

2.2.1 Elimination et Choix Traduisant la Réalité (ELECTRE)

O método *Elimination et Choix Traduisant la Réalité* (ELECTRE) ou Eliminação e Escolha como Expressão da Realidade foi proposto por Bernard Roy na década de 1960 [91]. Basicamente, este método da escola francesa produz índices de concordância e de discordância para determinar relações de dominância entre as alternativas e categorizá-las [42, 92, 93].

É um método de superação, pois resolve o problema de decisão pelas informações inter e intracritérios utilizadas e pela quantidade de relações de superação construídas e pesquisadas [92, 93]. Diz-se que uma alternativa a supera outra alternativa b se, ao considerar todas as informações disponíveis sobre o problema e as preferências dos decisores, há um argumento forte o suficiente para sustentar a conclusão de que a é pelo menos tão bom quanto b e nenhum argumento forte que prove o contrário [42].

De acordo com Belton e Stewart [42], os métodos ELECTRE baseiam-se na avaliação de dois índices: o índice de concordância e o índice de discordância, definidos para cada par de opções a e b. O índice de concordância $C(a, b)$ mede a força de apoio na informação dada, para a hipótese de que a é pelo menos tão bom quanto b. Consiste na proporção de pesos de critérios alocados àqueles critérios para os quais a é preferível ou indiferente a b. O índice assume valores entre 0 e 1, de tal forma que valores mais altos indicam evidências mais fortes em apoio à afirmação de que a é preferível a b.

O índice de discordância $D(a, b)$ mede a força da evidência contra a hipótese de que a é pelo menos tão bom quanto b. É o valor ponderado máximo pelo qual b é melhor que a, expresso como uma proporção da diferença ponderada máxima entre quaisquer duas alternativas em qualquer critério. Também assume valores entre 0 e 1, com um valor alto indicando que em pelo menos um critério b supera a, fornecendo assim uma contra evidência para a afirmação de que a é preferível a b.

Entretanto, a utilização destes índices só é apropriada se todas as avaliações são feitas em uma escala cardinal e se os pesos atribuídos aos critérios possuem escalas comparáveis,

o que são suposições bastante restritivas. Uma abordagem alternativa consiste em definir um limiar de veto para cada critério, tal que a não pode superar b se a pontuação para b em qualquer critério exceder a pontuação para a nesse critério por um valor igual ou maior que seu limite de veto.

Para construir uma relação de superação, é preciso definir os limiares de concordância e discordância, respectivamente, C^* e D^*. A alternativa a é definida como a variável de superação b se o coeficiente de concordância $C(a, b)$ for maior ou igual ao limiar C^* e o coeficiente de discordância $D(a, b)$ for menor ou igual a D^*. Os valores de C^* e D^* são especificados para uma relação de superação específica e podem ser variados para fornecer relações de superação mais ou menos severas: quanto maior o valor de C^* e quanto menor o valor de D^*, mais difícil é para uma alternativa superar outra. Se a relação de superação é muito severa, quase todos os pares de alternativas serão considerados "incomparáveis"; enquanto que, se a relação de superação não for suficientemente severa, muitas alternativas superarão muitas outras. Como nenhum desses resultados é útil, é importante encontrar um C^* grande o suficiente (mas não muito grande) e um D^* pequeno o suficiente (mas não pequeno demais) para definir uma relação consistente. A Figura 2.2 representa as possíveis relações de superação.

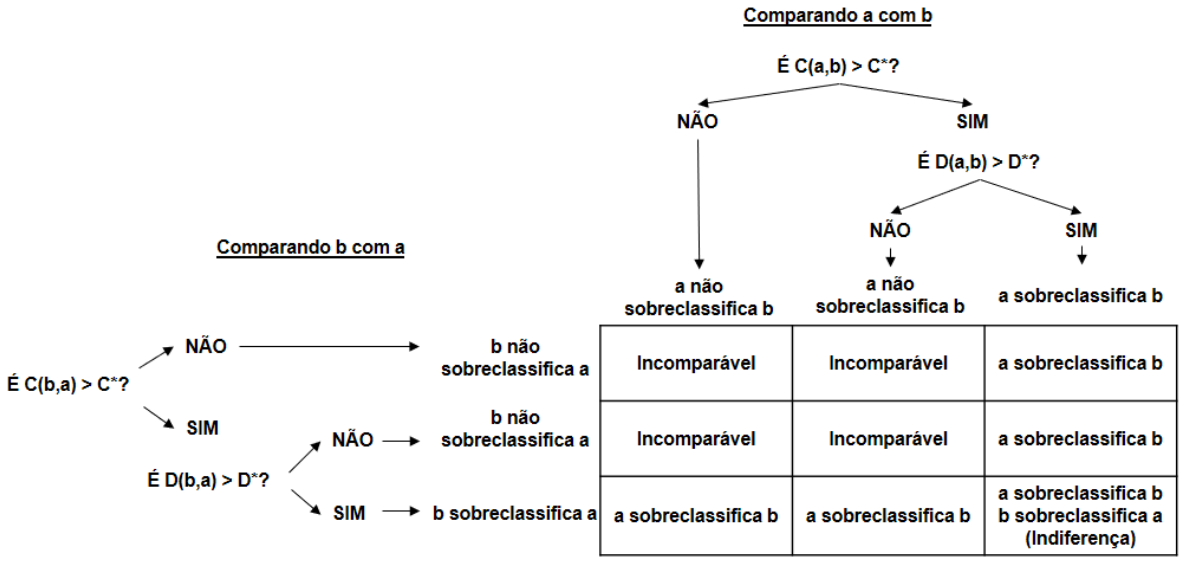

Figura 2.2: Relação de Superação (Fonte: [42]).

Para Belton e Stewart [42], a relação de superação pode ser representada por um grafo direcionado, chamado kernel, que seleciona as alternativas não sobreclassificadas por nenhuma outra e as alternativas que não são sobreclassificadas por quem já pertence

ao kernel. Se o grafo não contém circuitos, o kernel existe e é único. Se há circuitos, o kernel não é unico e pode não existir.

É importante analisar o impacto das mudanças nos valores C^* e D^* usados para definir a relação de superação realizando uma análise de sensibilidade e robustez [27, 42, 81]. Belton e Stewart [42] lembram que esta análise não deve ser feita de forma automatizada ou interativa, pois pode tornar uma investigação *ad hoc* sobre o efeito da mudança de valores. O decisor deve realizar a análise de sensibilidade respondendo a perguntas do tipo "WHAT-IF", ou seja, "O QUE aconteceria com a decisão escolhida, SE o panorama ou condições fossem outros". Já a análise de robustez tem por objetivo verificar até que ponto, após análise de sensibilidade, o resultado encontrado não se altera [27].

Existem várias versões do método ELECTRE, baseadas no mesmo princípio, mas diferenciando-se quanto a natureza do problema e quanto ao grau de complexidade das informações requeridas. Todas as versões se iniciam com a definição do objeto de decisão para as diversas alternativas em relação aos critérios, seguida da construção das relações de superação e finalizando com a exploração destas relações. A meta depende da problemática abordada e consiste em selecionar um conjunto de alternativas dominantes, classificar, ordenar ou descrever o conjunto de alternativas segundo a sua dominância [94].

A versão ELECTRE I, proposta por Roy em 1968 [91], tenta resolver a problemática de preferência Pα, ou seja, escolher a melhor alternativa. A relação de superação é definida pelos valores dos índices de concordância e discordância que, indiretamente, incorporam um risco a ser aceito ao estabelecer a superação de uma alternativa por outra. Esse risco pode significar uma não compreensão das reais preferências do decisor. A versão ELECTRE II foi proposta por Roy e Bertier em meados de 1970 [83]. É considerada um aprimoramento da versão ELECTRE I, pois visa produzir um ranking das alternativas (problemática Pγ) e não apenas indicar a melhor delas. Define duas relações de superação: uma forte e outra fraca, para então construir dois grafos, um para cada relação considerada.

A versão ELECTRE III, proposta por Roy em 1978 [92], classifica as diversas alternativas para a solução de um problema no caso de um único decisor, enquadrando-se na problemática decisória Pγ. Introduz a noção de limiares de preferência (pi) e indiferença (qi), que são utilizados para construir um índice de concordância *Ci(a,b)* para cada critério. Com o índice de concordância parcial de cada critério, calcula-se o índice geral de concordância *C(a,b)*. O índice de discordância parcial é calculado de maneira semelhante pela introdução de um limiar de veto para cada critério.

O índice geral de concordância e os índices de discordância são então combinados para fornecer uma relação de superação e calcular o índice de credibilidade *S(a, b)*. Para Belton e Stewart [42], se não há critério discordante, ou seja, se o critério onde o índice de

discordância é maior que o índice de concordância, então o índice de credibilidade *S(a,b)* é igual ao índice geral de concordância *C(a,b)*. O índice de credibilidade *S(a,b)* deve ser compreendido como um indicador da "ordem de magnitude" que suporta a afirmação de que *a* sobreclassifica *b*.

Assim como a versão ELECTRE II, o ELECTRE III resulta em uma ordenação descendente (otimista) e ascendente (pessimista) das alternativas. Para isso, é calculado o nível de corte λ, que é o menor valor de um índice de credibilidade em que se pode afirmar que *a* sobreclassifica *b*. As duas ordenações são então combinadas, resultando na ordenação final das alternativas.

O ELECTRE III permite uma modelagem mais sofisticada de preferências em critérios individuais, mas exige mais trabalho por parte do decisor, que precisa determinar como cada critério deve ser modelado. Além disso, Belton e Stewart [42] afirmam que os limiares de indiferença, preferência e veto são conceitos intuitivos e dependem do conhecimento do decisor.

O ELECTRE IV foi desenvolvido por Roy e Hugonnard em 1981 [92] e é mais simples que a estrutura dos demais métodos, pois utiliza critérios associados a um limite de preferência estrita e a um limite de indiferença. Esse método é útil quando não é possível especificar pesos de critérios e funciona como uma sequência de relações de superação agrupadas. Busca a problemática decisória de preferência Pδ. Já a versão ELECTRE IS, proposto por Roy e Skalka em 1985 [93], utiliza o conceito de pseudocritério, que considera a possibilidade de hesitação ou incerteza de um decisor ao afirmar que uma alternativa é, de fato, pelo menos tão boa quanto uma outra. Como o ELECTRE I, tenta resolver a problemática de preferência Pα.

A versão ELECTRE TRI é baseada no ELECTRE III mas considera a problemática Pβ, ou seja, classifica as diversas alternativas para a solução de um problema comparando cada alternativa potencial com uma referência estável. O procedimento original, proposto por Yu Wei em 1992 [95], foi projetado para classificar alternativas em três categorias: aceitável, inaceitável ou indeterminado. As categorias são ordenadas e definidas por um conjunto de ações de referência, ou perfis limitantes, determinados pelos decisores. Posteriormente, foi estendido para uso em problemas nos quais existem mais de três categorias diferentes e passou a ser chamado ELECTRE TRI-B (ETRI-B) [96].

O método ELECTRE TRI-C (ETRI-C), proposto por Almeida Dias em 2010 [97] e derivado do ETRI-B, foi desenvolvido para ser utilizado em problemas onde é difícil a definição das fronteiras. É um método de classificação indicado para problemas nos quais as alternativas podem ser alocadas em categorias pré-definidas, através de avaliação de múltiplos critérios. Diferente do ETRI-B que utiliza duas fronteiras ou bordas para determinar uma categoria, o ETRI-C utiliza uma ação de referência de uma única característica

para classificar as alternativas.

Bouysssou e Marchant [98] analisaram vários aspectos do ELECTRE TRI, mostrando as relações entre o ETRI-B e ETRI-C. Perceberam que alguns problemas podem ser classificados utilizando o ETRI-B e não podem ser classificados utilizando o ETRI-C, e vice-versa, e concluíram que existe uma grande diferença entre definir limiares superiores e inferiores e definir valores intermediários.

Costa e Freitas [99] utilizam o ELECTRE TRI para avaliar e classificar a qualidade de serviços através da mensuração do grau de satisfação do cliente com o desempenho do serviço, à luz de um conjunto de critérios considerados relevantes. Para Guarnieri [28], o grande número de parâmetros presentes nos métodos ELECTRE pode dificultar a sua aplicabilidade. Apesar disso, a possibilidade de utilizar dados quantitativos e qualitativos é uma vantagem deste método.

2.2.2 Outros Métodos MCDA

Outro método conhecido da escola francesa, por causa da sua facilidade de manuseio e pelas suas capacidades matemáticas é o *Preference Ranking Organization Method for Enrichment Evaluations* (PROMETHEE) ou Método de Organização de Ranking de Preferência de Avaliação de Enriquecimento. Foi proposto no início da década de 1980 por Jean Pierre Brans, Bertrand Mareschal e Philippe Vincke [85] e pretende solucionar problemas do tipo Pγ, usando comparações binárias entre as alternativas, comparando os seus desempenhos critério a critério.

Em se tratando da escola americana, destaca-se o método *Multiattribute Utility Theory* (MAUT) ou Teoria da Utilidade Multiatributo, introduzido por Keeney e Raiffa [87], que consiste em uma extensão natural da Teoria da Utilidade [100], onde cada alternativa é descrita por uma lista de atributos. Tem Pα como problemática decisória e baseia-se nos conceitos de modelagem de preferência tradicional, admitindo apenas duas situações: preferência estrita (P) e indiferença (I), ambas transitivas.

Já o método *Simple Multi Attribute Rating Technique* (SMART) ou Simples Técnica de Classificação de Multiplos Atributos é uma simplificação do método MAUT, proposto por Ward Edwards [86]. Este método julga a avaliação das alternativas considerando o pior e melhor estímulo, fazendo uso da estratégia da aproximação heroica para justificar aproximações lineares das funções utilidade multidimensional. Também é um método da escola americana que possui Pγ como problemática decisória. Possui duas derivações: *Simple Multi-Attribute Rating Technique using Swings* (SMARTS) e Simple *Simple Multi-Attribute Rating Technique using Exploiting Rankings* (SMARTER) [101].

Outro método muito conhecido da escola americana é o *Analytic Hierarchy Process* (AHP) ou Análise Hierárquica de Processos, criado por Thomas L. Saaty [102]. Este

método apresenta como problemática de decisão Pα e Pγ e é muito utilizado por causa da simplicidade no processo de modelagem da decisão [27]. O método *Analytic Network Process* (ANP) ou Método de Análise em Redes foi desenvolvido por Thomas L. Saaty e é considerado uma generalização do método AHP. No método ANP, os níveis hierárquicos dão lugar a uma estrutura em rede que dispensa a especificação de níveis [103]. O método ANP, assim como o método AHP é um método da escola americana e apresenta como problemática de decisão Pα e Pγ.

O último método da escola americana estudado é o *Technique for Order Preference by Similarity to the Ideal Solution* (TOPSIS) ou Técnica para Avaliar o Desempenho das Alternativas através de Similaridade com a Solução Ideal. Foi desenvolvido inicialmente por Hwang e Yoon em 1981 [104] com novos desenvolvimentos por Yoon em 1987 [105] e Hwang, Lai e Liu em 1993 [106]. Este método procura solucionar problemas do tipo Pα e baseia-se no conceito de que a alternativa escolhida deve ter a menor distância geométrica da solução ideal positiva (*Positive Ideal Solution*) e a distância geométrica mais longa da solução ideal negativa (*Negative Ideal Solution*).

Dos métodos híbridos estudados destaca-se o método *Measuring Attractiveness by a Categorical based Evaluation Technique* (MACBETH) ou em português, Medir a Atratividade por uma Técnica de Avaliação Baseada em Categorias. Desenvolvido por Carlos A. Bana e Costa e J. C. Vansnisck, na década de 90 [80], é um método que tem Pα e Pγ como problemáticas decisórias, agregando conceitos tanto da escola americana como da escola europeia, embora haja uma sutil predominância da primeira sobre a segunda. Esta abordagem requer apenas julgamentos qualitativos sobre as diferenças de atratividade em múltiplos critérios para ajudar o decisor a quantificar a atratividade relativa das opções. O foco principal do MACBETH é a interação entre os agentes e o decisor.

Outro método que tem como base a escola francesa e a escola americana, combinando aspectos provenientes dos métodos MAUT, AHP e ELECTRE é o Tomada de Decisão Interativa Multicritério (TODIM), desenvolvido por Gomes e Lima [107], que busca resolver problemas do tipo Pγ. Incorpora em sua formulação padrões de preferência dos decisores em presença de risco, baseado na Teoria dos Prospectos.

A Tabela 2.3 apresenta os principais métodos MCDA estudados, suas variações, abordagens e problemáticas.

Tabela 2.3: Principais métodos de MCDA estudados.

Modelo	**Autor**	**Ano**	**Abordagem**	**Problemática**
Elimination et Choix Traduisant la Réalité (ELECTRE)				
ELECTRE I	Roy	1968		Pα - Escolha
ELECTRE II	Roy e Bertier	1973		Pγ - Ordenação
ELECTRE III	Roy	1978		Pγ - Ordenação
ELECTRE IV	Roy e Hugonnard	1982	Escola Francesa	Pδ - Descrição
ELECTRE IS	Roy e Skaika	1985		Pα - Escolha
ELECTRE TRI	Yu Wei	1992		Pβ - Classificação
ELECTRE TRI-B	Roy e Bouyssou	1993		Pβ - Classificação
ELECTRE TRI-C	Almeida Dias	2010		Pβ - Classificação
Preference Ranking Organization Method for Enrichment Evaluations (PROMETHEE)	Jean Pierre Brans, Bertrand Mareschal e Philippe Vincke	1980	Escola Francesa	Pγ - Ordenação
Multiattribute Utility Theory (MAUT)	Keeney e Raiffa	1976	Escola Americana	Pα - Escolha
Simple Multi Attribute Rating Technique (SMART)	Ward Edwards	1977	Escola Americana	Pγ - Ordenação
Analytic Hierarchy Process (AHP)	Thomas L. Saaty	1980	Escola Americana	Pα - Escolha e Pγ - Ordenação
Analytic Network Process (ANP)	Thomas L. Saaty	1996	Escola Americana	Pα - Escolha e Pγ - Ordenação
Technique for Order Preference by Similarity to the Ideal Solution (TOPSIS)	Hwang e Yoon	1981	Escola Americana	Pα - Escolha
Measuring Attractiveness by a Categorical based Evaluation Technique (MACBETH)	Carlos A. Bana e Costa e J. C. Vansnisck	1990	Escola Francesa e Escola Americana	Pα - Escolha e Pγ - Ordenação
Tomada de Decisão Interativa Multicritério (TODIM)	Gomes e Lima	1992	Escola Francesa e Escola Americana	Pγ - Ordenação

Capítulo 3

Modelo para Avaliação da Maturidade em Gestão de Riscos

Após identificar e comparar as melhores práticas relacionadas à gestão de riscos e os principais métodos de apoio multicritério à decisão, através da revisão bibliográfica realizada, este trabalho apresenta um modelo de maturidade que utiliza o método ELECTRE TRI para auxiliar os gestores a definir e mensurar seus valores e preferências. O modelo é validado por um estudo de caso aplicado na área de TI de uma empresa de distribuição de energia, levando-se em consideração o problema, as justificativas e o objetivo apresentados nas Seções 1.1, 1.2 e 1.3, respectivamente.

A empresa de distribuição de energia onde o estudo será aplicado passa por uma integração com os processos da holding para a qual suas ações foram vendidas. Parte do processo de integração requer um relatório de avaliação de maturidade em gestão de riscos de todas as áreas da empresa, incluindo o departamento de TI, onde o estudo de caso será aplicado.

O departamento de TI é composto por seis setores: Infraestrutura, Suporte a Usuários, Telecomunicação e Redes, Sistemas de Apoio e Serviços, Sistemas de Mercado, Sistemas de Rede. Cada um dos setores possui um gerente que toma suas decisões baseados na experiência, sem qualquer método ou ferramenta que o auxilie em suas escolhas. Atualmente, enfrenta uma grande dificuldade em avaliar a situação atual de seus processos, pois os mesmos não foram mapeados.

A solução proposta visa classificar os departamentos de TI de acordo com níveis de maturidade pré-definidos, baseados em múltiplos critérios selecionados a partir da revisão da literatura. Esses critérios representam os principais aspectos que devem ser observados em um gerenciamento de riscos, de acordo com as melhores práticas. Os métodos de apoio multicritério auxiliam os decisores a organizar as informações e assim, tomar decisões mais assertivas.

3.1 Estruturação do Problema

Considerando as dificuldades dos gestores em avaliar e tomar decisões sobre a gestão de riscos dos processos de TI, este trabalho identificou o seguinte problema: Como avaliar a maturidade em gestão de riscos de TI de maneira eficiente? De acordo com a metodologia proposta por Belton e Stewart [42], apresentada na Figura 1.2, após a identificação do problema, deve-se estabelecer o contexto de decisão do problema.

Para isso, é necessário determinar a abrangência do problema e identificar quais os papéis e responsabilidades das partes interessadas. Para este estudo de caso, foram levantados os seguintes aspectos:

- Valores: Responsabilidade, inovação, confiança e proatividade.
- Objetivos: Avaliar a maturidade em gestão de riscos de TI.
- Limitações: O estudo de caso se limita ao departamento de TI da empresa. Como a mesma não possui um mapeamento dos processos definido, optou-se em avaliar o nível de maturidade dos seis setores que compõem o departamento de TI.
- Ambiente externo: Costumes e tradições locais, políticas corporativas, legislação nacional, variação do dólar, problemas políticos internacionais.
- Assuntos chaves: gestão de riscos de TI, maturidade, critérios
- Incertezas: Possíveis alterações no organograma de TI, aumentando ou diminuindo a quantidade de alternativas
- Alternativas: Setor de Infraestrutura, Suporte a Usuários, Telecomunicação e Redes, Apoio e Serviços, Sistemas de Mercado e Sistemas de Rede.
- Partes Interessadas: diretores, gestores e especialistas de TI, colaboradores terceiros, usuários de TI, fornecedores e parceiros comerciais.

Para o estudo de caso, foram selecionados 18 decisores, responsáveis por fornecer as informações necessárias para alimentar o modelo. Cada departamento da organização estudada foi representado por 3 decisores (um gerente e dois especialistas), todos graduados em Computação, com mais de 8 anos de experiência no cargo. Estes decisores, atores centrais do processo, atuam de forma direta com os processos de TI de seus departamentos e avaliaram os critérios através de questionários elaborados pela autora do modelo. As demais partes interessadas são os patrocinadores, representados pelos diretores da empresa, para quem os resultados serão apresentados e os facilitadores ou analistas, que são apenas informados dos resultados.

Em relação ao aspecto técnico, a escolha do método deve ser resultado de uma avaliação dos parâmetros escolhidos, do tipo e da precisão dos dados, da forma de pensar do decisor, e do seu conhecimento do problema [98]. Para este trabalho, optou-se por utilizar o método ELECTRE TRI por se tratar de um problema de classificação ordenada (Pβ). Este método separa o conjunto de alternativas potenciais, que no estudo de caso equivalem aos setores que compõe o departamento de TI, em classes ou categorias definidas previamente, que equivalem aos níveis de maturidade do modelo.

A escolha do método está relacionada ao fato do trabalho apresentar um problema de avaliação de alternativas à luz de múltiplos critérios e que envolve julgamentos subjetivos dos diversos tomadores de decisão. Neste tipo de ambiente, imprecisões e incertezas são amplificadas e podem originar em escolhas inadequadas. Outro ponto observado na escolha do método está relacionado à necessidade de envolver vários decisores, isto é, realizar uma decisão em grupo. A dinâmica desse processo, apesar de envolver conflitos e negociações na inserção dos dados no modelo, permitiu o aumento da confiança no resultado obtido.

De acordo com Santos [27], algumas características que devem ser observadas quando se implementa um método da escola francesa:

- Devem existir critérios qualitativos, que permitem adicionar ao modelo características não quantificáveis, cujas diferenças de performances intercritérios não tenham significado comparativo no que diz respeito a uma gradação de preferência;
- A natureza dos critérios deve ser fortemente heterogênea, possibilitando uma avaliação das performances das alternativas nas mais diferentes escalas e unidades;
- A compensação de uma perda segundo um critério, representado por um ganho segundo outro critério, pode ocorrer de forma complexa e em ligação com sistemas de valores não necessariamente considerados na modelagem do problema;
- A necessidade de utilização de pseudocritérios para obtenção das preferências globais.

Dada a complexidade dos critérios selecionados na literatura para o desenvolvimento do modelo proposto, todas as características acima estão contempladas neste trabalho.

3.2 Construção do Modelo

Esta seção apresenta o detalhamento do processo de construção do modelo de avaliação de maturidade em gestão de riscos de TI. As fases de estruturação do modelo, sugeridas

Tabela 3.1: Alternativas para o modelo de decisão.

Alternativa	**Setor**	**Descrição das Atividades**
A1	Infraestrutura	Suporte a infraestrutura.
A2	Suporte a Usuários	Suporte ao usuário final de TI.
A3	Telecomunicação e Redes	Suporte a toda a rede de comunicação e dados.
A4	Sistemas de Apoio e Serviços	Suporte aos sistemas de apoio e serviços.
A5	Sistemas de Mercado	Suporte aos sistemas de mercado.
A6	Sistemas de Rede	Suporte aos sistemas de rede elétrica.

por Costa e Freitas [99] para a utilização do método ELECTRE TRI são descritas na sequência.

3.2.1 Identificação das Alternativas

Segundo Gomes, Gomes e Almeida [27], uma alternativa ou ação constitui nas possibilidades de escolha do agente de decisão. Cada alternativa introduzida em um modelo deve ter algum sentido, alguma contribuição para o modelo. O conjunto das alternativas potenciais é normalmente representado por $''a''$ [93].

Como a empresa onde o estudo de caso foi aplicado não possuía mapeamento de processos, optou-se por classificar os seis setores que compõe o departamento de TI, tendo como resultado a avaliação de maturidade geral da TI. A Tabela 3.1 apresenta os setores e uma breve descrição de suas atividades.

3.2.2 Especificação dos Critérios

Nesta fase, são definidos os critérios a serem considerados no modelo. Para Wibowo e Taufik [24], a percepção destes critérios depende do contexto ambiental e pessoal, e está em constante evolução, dada a dinâmica do ambiente e da própria percepção pessoal de quem define os critérios.

Gomes et al. [108] alertam para a necessidade de respeitar alguns axiomas para que se considere que os critérios estejam desempenhando seu papel no processo de decisão: o axioma de exaustividade, o axioma da coesão e o axioma da não redundância. O conjunto dos critérios potenciais é normalmente representado por $''g''$ [93].

A seleção dos critérios utilizados no modelo para avaliação da maturidade em gestão de riscos de TI foi feita através da revisão da literatura, onde foram levantadas as dimensões mais utilizadas pelos autores e os 30 critérios mais citados entre eles. Em seguida, reduziu-se a quantidade de critérios para 12, distribuídos em 4 dimensões, por causa de uma limitação do software utilizado para os cálculos do método ELECTRE TRI, o Decision Deck - divz [108]. Os critérios selecionados são apresentados na Tabela 3.2.

Tabela 3.2: Dimensões e critérios para o modelo de decisão.

Dimensão	**Critério**
D1. Cultura	G1. Política de gestão de riscos G2. Comunicação do risco G3. Governança corporativa G4. Apetite ao risco
D2. Processo	G5. Identificação do risco G6. Análise de risco G7. Avaliação de risco G8. Tratamento do risco
D3. Experiência	G9. Orçamento G10. Treinamento
D4. Aplicação	G11. Função dedicada G12. Tomada de decisão baseada na gestão de riscos

Tabela 3.3: Escala de Julgamento dos Pesos dos Critérios.

Escala Verbal	**Valor Numérico**
Muito Alta	5
Alta	4
Média	3
Baixa	2
Desprezível	1

3.2.3 Escala de Julgamento dos Pesos dos Critérios

A próxima etapa consiste em definir uma escala de julgamento para o peso dos critérios. O peso indica a importância ou influência do critério no grau da classificação final do problema pelos decisores. Para tanto, adotou-se a escala verbal da Tabela 3.3 definida pela autora, com base na revisão da literatura [109].

3.2.4 Pesos para os Critérios

Nesta etapa, foram estabelecidos os pesos para cada critério, utilizando a escala de julgamento definida no item 3.2.3. Para a definição dos pesos, foram realizadas reuniões e entrevistas com os decisores, que avaliaram os critérios selecionados e os potenciais riscos a eles associados, chegando a uma decisão por consenso [110]. O resultado é apresentado na Tabela 3.4.

3.2.5 Escala de Julgamento das Alternativas para cada Critério

Após estabelecer o peso dos critérios, é necessário especificar a escala de julgamentos das alternativas para cada critério. As alternativas são avaliadas separadamente em cada cri-

Tabela 3.4: Pesos atribuídos aos critérios.

Dimensão	**Critério**	**Pesos**
D1. Cultura	G1. Política de gestão de riscos	4
	G2. Comunicação do Risco	4
	G3. Governança corporativa	3
	G4. Apetite ao Risco	5
D2. Processo	G5. Identificação do risco	5
	G6. Análise de risco	4
	G7. Avaliação de risco	4
	G8. Tratamento do risco	4
D3. Experiência	G9. Orçamento	5
	G10. Treinamento	3
D4. Aplicação	G11. Função dedicada	4
	G12. Tomada de decisão baseada na gestão de riscos	5

tério. Como os critérios são qualitativos e heterogêneos, foi adotada uma escala específica para cada um deles. São elas:

1. Política de gestão de riscos: Declaração das intenções e diretrizes gerais de uma organização relacionadas a gestão de riscos. Fornecem orientações detalhadas sobre como colocar os princípios em prática e como os mesmos influenciarão a tomada de decisões. Este atributo poderá ser avaliado segundo a seguinte escala:

   (1) Não adota nem tem conhecimento da política de gestão de riscos.

   (2) Tem conhecimento, mas não adota a política de gestão de riscoss.

   (3) Iniciou plano para adotar a política de gestão de riscos.

   (4) Adota parcialmente a política de gestão de riscos.

   (5) Adota integralmente a política de gestão de riscos.

2. Comunicação do risco: Processos contínuos e iterativos conduzidos pela organização para obter, fornecer e compartilhar informações relacionadas ao gerenciamento de riscos de forma clara e objetiva a todas as partes interessadas. Este atributo poderá ser avaliado segundo a seguinte escala:

   (1) Não tem conhecimento de nenhum processo de comunicação de riscos.

   (2) Tem conhecimento, mas não adota nenhum processo de comunicação de riscos.

   (3) Iniciou plano para adotar processo de comunicação de riscos.

   (4) Adota parcialmente o processo de comunicação de riscos.

   (5) Adota integralmente o nenhum processo de comunicação de riscos.

3. Governança corporativa: Conjunto de processos que garante que as necessidades, condições e opções das partes interessadas sejam avaliadas de forma a determinar objetivos corporativos, definir a direção estratégica através de priorizações e tomadas de decisão e monitorar o desempenho e a conformidade das atividades em relação aos objetivos estabelecidos. Este atributo poderá ser avaliado segundo a seguinte escala:

   (1) Não tem conhecimento de nenhum processo de governança corporativa.

   (2) Tem conhecimento, mas não adota nenhum processo de governança corporativa.

   (3) Iniciou plano para adotar os processos de governança corporativa.

   (4) Adota parcialmente os processos de governança corporativa

   (5) Adota integralmente os processos de governança corporativa

4. Apetite ao risco: A quantidade de risco, em um nível amplo, que uma entidade está disposta a aceitar em busca de sua missão. É o reflexo da gestão de riscos e tem forte influência sobre a cultura dentro da organização. Este atributo poderá ser avaliado segundo a seguinte escala:

   (1) Não tem conhecimento do apetite ao risco adotado pela empresa.

   (2) Tem conhecimento do apetite ao risco adotado pela empresa, mas raramente o consulta para o planejamento de seus projetos.

   (3) Tem conhecimento do apetite ao risco adotado pela empresa e o consulta esporadicamente para o planejamento de seus projetos.

   (4) Tem conhecimento do apetite ao risco adotado pela empresa e sempre o consulta para o planejamento de seus projetos.

   (5) Foi consultado para definição do apetite ao risco adotado pela empresa.

5. Identificação do risco: Processo de busca, reconhecimento e descrição do risco. Inclui a identificação das causas e fontes de risco, eventos, situações ou circunstâncias que podem impactar os objetivos e a natureza desse impacto. Este atributo poderá ser avaliado segundo a seguinte escala:

   (1) Não adota nem tem conhecimento do processo de identificação do risco.

   (2) Tem conhecimento mas não adota o processo de identificação do risco.

   (3) Iniciou plano para adotar o processo de identificação do risco.

   (4) Adota parcialmente o processo de identificação do risco.

   (5) Adota integralmente o processo de identificação do risco.

6. Análise de risco: Processo de compreender a natureza do risco e determinar as consequências e suas probabilidades para eventos identificados de risco, levando em consideração a presença (ou não) e a eficácia de quaisquer controles existentes. Envolve a consideração das causas e fontes de risco, suas consequências e a probabilidade de que essas consequências possam ocorrer. Este atributo poderá ser avaliado segundo a seguinte escala:

   (1) Não adota nem tem conhecimento do processo de análise de risco.

   (2) Tem conhecimento mas não adota o processo de análise de risco.

   (3) Iniciou plano para adotar o processo de análise de risco.

   (4) Adota parcialmente o processo de análise de risco.

   (5) Adota integralmente o processo de análise de risco.

7. Avaliação de risco: Processo de comparar os resultados da análise de risco com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável. Utiliza a compreensão do risco para tomar decisões sobre as ações futuras. Este atributo poderá ser avaliado segundo a seguinte escala:

   (1) Não adota nem tem conhecimento do processo de avaliação de risco.

   (2) Tem conhecimento mas não adota o processo de avaliação de risco.

   (3) Iniciou plano para adotar o processo de avaliação de risco.

   (4) Adota parcialmente o processo de avaliação de risco.

   (5) Adota integralmente o processo de avaliação de risco.

8. Tratamento do risco: Processo para selecionar uma ou mais opções para modificar os riscos e a implementação dessas opções. Uma vez implementado fornece novos controles ou modifica os existentes. As principais formas de tratamento de risco são: evitar o risco, eliminar o risco, mitigar ou atenuar o risco, aceitar o risco, compartilhar ou transferir o risco e aumentar o risco. Este atributo poderá ser avaliado segundo a seguinte escala:

   (1) Não adota nem tem conhecimento do processo de tratamento do risco.

   (2) Tem conhecimento mas não adota o processo de tratamento do risco.

   (3) Iniciou plano para adotar o processo de tratamento do risco.

   (4) Adota parcialmente o processo de tratamento do risco.

   (5) Adota integralmente o processo de tratamento do risco.

9. Orçamento: Processo de agregação dos custos estimados relacionados às pessoas, habilidades e competências necessárias para fornecer e executar com sucesso as atividades do processo de gerenciamento de riscos. Inclui mão de obra direta, materiais, equipamentos, treinamentos, certificações, entre outros. Este atributo poderá ser avaliado segundo a seguinte escala:

   (1) Impacto desprezível no orçamento geral de TI.

   (2) Impacto baixo no orçamento geral de TI.

   (3) Impacto médio no orçamento geral de TI.

   (4) Impacto alto no orçamento geral de TI.

   (5) Impacto muito alto no orçamento geral de TI.

10. Treinamento: Programas de treinamento e capacitação para garantir que os indivíduos sejam efetivos em suas funções no gerenciamento de riscos. Devem ser direcionados aos diferentes níveis de consciência de risco da organização. Este atributo poderá ser avaliado segundo a seguinte escala:

    (1) Não realizou nenhum treinamento em gestão de riscos no último ano.

    (2) Realizou pelo menos 1 treinamento em gestão de riscos no último ano.

    (3) Realizou pelo entre 2 e 4 treinamentos em gestão de riscos no último ano.

    (4) Realizou pelo mais de 4 treinamentos em gestão de riscos no último ano.

    (5) Ministrou pelo menos 1 treinamento em gestão de riscos no último ano.

11. Função dedicada: Criação de uma unidade responsável por integrar e orientar as atividades pelo gerenciamento de riscos, que pode ser um departamento, núcleo, área ou unidade funcional composta por representantes de diversas áreas (comitê). Este atributo poderá ser avaliado segundo a seguinte escala:

    (1) Não existe uma função dedicada para gestão de riscos na empresa.

    (2) Existe um plano para criação de uma função dedicada para gestão de riscos na empresa.

    (3) Existe uma função parcialmente dedicada para gestão de riscos na empresa.

    (4) Existe uma função dedicada exclusivamente à gestão de riscos na empresa.

    (5) Faço parte da função dedicada para gestão de riscos na empresa.

12. Tomada de decisão baseada na gestão de riscos: Fornecimento de informações chaves sobre o impacto dos riscos no negócio com o objetivo de apoiar os gestores na tomada de decisão. Considera os cenários mais pessimistas e mais prováveis, os eventos

Tabela 3.5: Classes de equivalência.

Classe	Descrição	Limite Inferior	Limite Superior
C1	Nível Inicial	0	1
C2	Nível Estruturado	1	2
C3	Nível Definido	2	3
C4	Nível Gerenciado	3	4
C5	Nível Otimizado	4	5

futuros não controláveis e os indicadores de desempenho resultantes do processo de gerenciamento de riscos. Este atributo poderá ser avaliado segundo a seguinte escala:

(1) Nunca tomo decisões baseadas na gestão de riscos.

(2) Raramente nunca tomo decisões baseadas na gestão de riscos.

(3) As vezes tomo decisões baseadas na gestão de riscos.

(4) Muitas vezes tomo decisões baseadas na gestão de riscos.

(5) Sempre tomo decisões baseadas na gestão de riscos.

3.2.6 Identificação das Classes de Equivalência

Nesta etapa, deve-se identificar as classes de equivalência, bem como seus respectivos limites inferiores e superiores, que servirão de padrão para a classificação das alternativas sob análise. O conjunto das classes de equivalência é normalmente representado por $''c''$ [93].

Para o estudo de caso, são estabelecidas as classes que servirão de padrão para classificar os setores sob análise. No modelo de avaliação de maturidade em gestão de riscos de TI, estas classes equivalem aos níveis de maturidade, que foram definidos com base na revisão da literatura e possuem limites interiores e superiores definido pela autora. As classes de equivalência são apresentadas na Tabela 3.5.

3.2.7 Limites de Preferência, Indiferença e Veto para cada Critério

Após estabelecer as classes de equivalência, deve-se definir os limites de preferência (p) e de indiferença (q). Tais limites permitem considerar as imprecisões resultantes das avaliações realizadas. Pode-se definir ainda um limite de veto (v) associado a cada critério. Segundo Costa e Freitas [99], este limite lida com o conceito de rejeição quanto à afirmação de que uma alternativa subordina um limite de classe (e vice-versa).

Tabela 3.6: Resultado do julgamento de valor de cada alternativa à luz de cada critério.

	G1	**G2**	**G3**	**G4**	**G5**	**G6**	**G7**	**G8**	**G9**	**G10**	**G11**	**G12**
A1	4	4	4	3	3	3	3	4	4	2	2	4
A2	2	2	4	1	2	2	2	2	4	2	1	3
A3	3	3	3	2	2	2	2	2	4	2	2	3
A4	3	2	4	3	3	3	3	3	3	3	1	4
A5	3	2	4	3	3	3	3	3	3	2	2	4
A6	2	2	4	1	2	2	2	2	3	2	1	3

Para este trabalho, os valores dos limites de preferência (p), indiferença (q) e de veto (v) foram considerados iguais a zero, pois não são aplicáveis ao tipo de escala utilizada. Isso equivale a usar critérios verdade ao invés de pseudocritérios, como é considerado no ELECTRE TRI.

3.2.8 Julgamento de Valor de cada Alterativa a luz de cada Critério

Nesta fase, emitem-se julgamentos de valor de cada alternativa à luz de cada critério. Para o estudo de caso, os decisores responderam um questionário avaliando seu departamento (alternativa) em relação a cada um dos critérios, de acordo com a escala de julgamento definida na Seção 3.2.5. Como cada departamento possui 3 decisores, utilizou-se a média dos valores encontrados para chegar ao valor resultante da alternativa, apresentado na Tabela 3.6.

3.2.9 Algoritmo de Classificação do ELECTRE TRI

A próxima etapa consiste em executar o algoritmo de classificação do ELECTRE TRI. De acordo Belton e Stewart [42], dado um conjunto finito de alternativas a, valoradas sobre um conjunto de critérios g, são construídas relações de subordinação entre as alternativas, a partir das valorações estabelecidas pelo decisor. A construção destas relações de baseia em uma lógica não compensatória.

A relação de subordinação é construída de forma a tornar possível a comparação de uma alternativa a com um limite padrão b_h. A afirmação de que aSb_h significa que "a não tem um desempenho pior do que o limite b_h". Diz-se que uma alternativa a supera outra alternativa b_h se, ao considerar todas as informações disponíveis sobre o problema e as preferências dos decisores, há um argumento forte o suficiente para sustentar a conclusão de que a é pelo menos tão bom quanto b_h e nenhum argumento forte que prove o contrário [42, 95, 96].

Para cada critério g, as preferências são definidas através de pseudocritérios detalhados na representação de preferências de limites superiores e inferiores. Os limites de indiferença $q_j(b_h)$ e de preferência $p_j(b_h)$ constituem a informação preferencial sobre o critério. Eles analisam a natureza imprecisa das avaliações $g_j(a)$. Enquanto, $q_j(b_h)$ especifica a maior diferença g_j(a) - $g_j(b_h)$ que preserva a indiferença entre a e b_h no critério g_j; $p_j(b_h)$ representa a menor diferença $g_j(a)$ - $g_j(b_h)$ compatível com a preferência a favor de a no critério g_j.

Segundo Roy e Bouyssou [96] e Yu [95], os seguintes passos são seguidos na obtenção da relação de subordinação:

1. Calcular o índice de concordância parcial c_j(a,b_h) e c_j(b_h,a)

   Quando g_j tem uma preferência ascendente, c_j(a,b_h) é calculado da seguinte forma:

$$\begin{cases} \text{Se } g_j(\text{a}) \leq g_j(b_h) \text{ - } p_j(b_h), \text{ então } c_j(\text{a},b_h) = 0 \\ \text{Se } g_j(b_h) \text{ - } p_j(b_h) < g_j(\text{a}) \leq g_j(b_h) \text{ - } q_j(b_h), \text{ então } c_j(\text{a},b_h) = \frac{[g_j(a)-g_j(b_h)+p_j(b_h)]}{[p_j(b_h)-q_j(b_h)]} \\ \text{Se } g_j(b_h) \text{ - } q_j(b_h) < g_j(\text{a}), \text{ então } c_j(\text{a},b_h) = 1 \end{cases}$$

   Quando g_j tem uma preferência descendente, c_j(a,b_h) é calculado da seguinte forma:

$$\begin{cases} \text{Se } g_j(\text{a}) \geq g_j(b_h) + p_j(b_h), \text{ então } c_j(\text{a},b_h) = 0 \\ \text{Se } g_j(b_h) + q_j(b_h) \leq g_j(\text{a}) \leq g_j(b_h) + p_j(b_h), \text{ então } c_j(\text{a},b_h) = \frac{[g_j(b_h)-g_j(a)+p_j(b_h)]}{[p_j(b_h)-q_j(b_h)]} \\ \text{Se } g_j(b_h) + q_j(b_h) > g_j(\text{a}), \text{ então } c_j(\text{a},b_h) = 1 \end{cases}$$

2. Calcular o índice de concordância global c(a,b_h)

   O índice de concordância global c(b_h,a) expressa até que ponto as avaliações de a e b_h em todos os critérios estão de acordo com a afirmação de que "a subordina b_h": c(a,b_h) = $\frac{\sum_{j\in F} k_j c_j(a,b_h)}{\sum_{j\in F} k_j}$

3. Calcular o índice de discordância parcial d_j(a,b_h) e d_j(b_h,a)

   Quando g_j tem uma preferência ascendente, d_j(a,b_h) é calculado da seguinte forma:

$$\begin{cases} \text{Se } g_j(\text{a}) > g_j(b_h) \text{ - } p_j(b_h), \text{ então } d_j(\text{a},b_h) = 0 \\ \text{Se } g_j(b_h) \text{ - } v_j(b_h) < g_j(\text{a}) \leq g_j(b_h) \text{ - } p_j(b_h), \text{ então } d_j(\text{a},b_h) = \frac{[g_j(b_h)-g_j(a)+p_j(b_h)]}{[v_j(b_h)-p_j(b_h)]} \\ \text{Se } g_j(b_h) \text{ - } v_j(b_h) \geq q_j(\text{a}), \text{ então } d_j(\text{a},b_h) = 1 \end{cases}$$

Quando g_j tem uma preferência descendente, d_j(a,b_h) é calculado da seguinte forma:

$$\begin{cases} \text{Se } g_j(\text{a}) \leq g_j(b_h) + p_j(b_h), \text{ então } d_j(\text{a},b_h) = 0 \\ \text{Se } g_j(b_h) + p_j(b_h) < g_j(\text{a}) \leq g_j(b_h) + v_j(b_h), \text{ então } d_j(\text{a},b_h) = \frac{[g_j(a) - g_j(b_h) - p_j(b_h)]}{[v_j(b_h) - p_j(b_h)]} \\ \text{Se } g_j(b_h) + v_j(b_h) < g_j(\text{a}), \text{ então } d_j(b_h,\text{a}) = 1 \end{cases}$$

4. Calcular o índice de credibilidade σ(a,b_h)

   O grau de credibilidade da relação de subordinação σ(a,b_h) expressa até que ponto "a subordina b_h" de acordo com o índice de concordância global c_j(a,b_h) e com o índice de discordância d_j(a,b_h), ∀j∈ F. Calcula-se o índice de credibilidade σ(a,b_h) e σ(b_h,a) somando-se os valores estabelecidos na relação de subordinação.

5. Calcular o nível de corte (λ)

   O nível de corte (λ) equivale ao menor valor de um índice de credibilidade σ(a,b_h) em que se pode afirmar que a S b_h.

   Se σ(a,b_h) $\geq \lambda$ => a S b_h.

Após os cálculos, verifica-se que o índice de credibilidade σ(a,b_h) corresponde ao índice de concordância fraca por um eventual efeito de veto. Quando não há discordância em nenhum critério, o índice de credibilidade σ(a,b_h) é igual ao índice de concordância global c(a,b_h). Logo, quando não é considerado o veto, tem-se σ(a,b_h) = c(a,b_h).

Finalmente, a regra de procedimento de exploração é realizada para analisar o modo em que uma alternativa *a* é comparada aos limites padrões determinados para a classe na qual *a* deve ser enquadrada. Os procedimentos de classificação descendente (otimista) e ascendente (pessimista) são aplicados nesse contexto.

Para este trabalho, os cálculos do método ELECTRE TRI foram realizados utilizando o software Decision Deck - divz [111], que apesar de apresentar uma interface pouco intuitiva, permite uma análise de sensibilidade, através da alteração de parâmetros chaves. O algoritmo *method.ELECTRE-TRI* utilizado por este software permite duas classificações: uma otimista, que tende a associar as alternativas às classes de melhor desempenho e o pessimista, que busca associar as ações às classes com pior desempenho. Para execução do algoritmo foi necessário criar os seguintes arquivos no formato .xml:

- *categories_profiles*: contém as classes de equivalência definidas na Seção 3.2.6
- *weights*: contém os pesos atribuídos aos critérios definidos na Seção 3.2.4
- *performances_alternatives*: contém o resultado do julgamento de valor de cada alternativa à luz de cada critério definidos na Seção 3.2.8

- *performances_profiles*: contém os limites das classes de equivalência definidas na Seção 3.2.6
- *criteria*: contém os critérios utilizados no modelo, definidos na Seção 3.2.2
- *alternatives*: contém as alternativas utilizadas no modelo, definidas na Seção 3.2.1

Estes arquivos são fornecidos como entrada para a função *ElectreTriExploitation-1*, que realiza os cálculos do ELECTRE TRI, e para outras três funções – *plotStarGraphPerformanceTable-1*, *plotCriteriaCalues-1* e *plotAlternativesAssignments-1*, que apresentam gráficos da análise da performance das alternativas, dos critérios e o resultado da classificação, respectivamente. A Figura 3.1 mostra o diagrama de execução do algoritmo *method.ELECTRE-TRI* utilizando o software Decision Deck - divz [111].

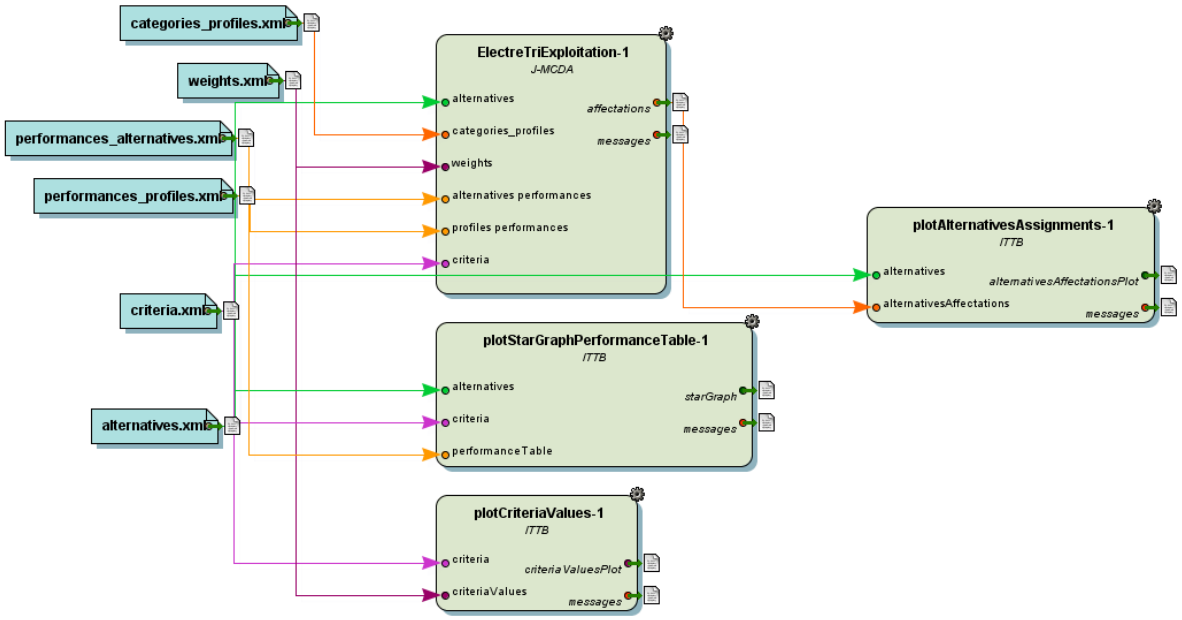

Figura 3.1: Diagrama de execução do algoritmo method.ELECTRE-TRI utilizando o software Decision Deck - divz (Fonte: [111]).

O resultado da primeira execução do algoritmo, utilizando a classificação otimista, é apresentado na Figura 3.2.

O resultado da classificação otimista utilizando o software Decision Deck-divz [111] indica que as alternativas A2 e A6 estão classificadas no Nível Inicial e as alternativas A1, A3, A4 e A5 estão classificadas no Nível Estruturado. O resultado da segunda execução do algoritmo, utilizando a classificação pessimista, é apresentado na Figura 3.3.

O resultado da classificação pessimista utilizando o software Decision Deck-divz [111] indica que as alternativas A2, A4 e A6 estão classificadas no Nível Inicial e as alternativas

Figura 3.2: Resultado da classificação otimista utilizando o software Decision Deck - divz (Fonte: [111]).

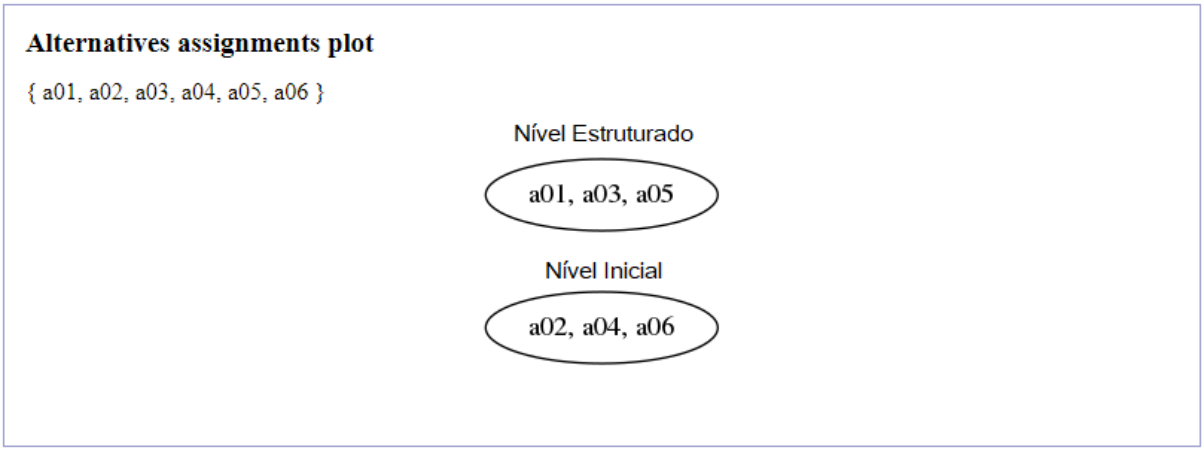

Figura 3.3: Resultado da classificação pessimista utilizando o software Decision Deck - divz (Fonte: [111]).

A1, A3 e A5 estão classificadas no Nível Estruturado. O resultado encontrado na classificação pessimista difere do resultado encontrado na classificação otimista, indicando uma incomparabilidade quanto a classificação da alternativa A4. Para Costa et al. [112], uma divergência entre classificações pode indicar uma incapacidade em comparar a alternativa com pelo menos um dos perfis das classes de equivalência utilizadas. Esta incapacidade pode ser causada pelo avaliador, pelo modelo de classificação (incluindo o conjunto de critérios) ou pelo sistema de coleta de dados (incluindo as escalas utilizadas). A identificação de incomparabilidades constitui-se em um sinal adicional sobre inconsistências na construção do modelo não detectadas pelos métodos convencionais.

Além dos resultados da classificação otimista e pessimista, o software Decision Deck -

divz [111] apresenta um gráfico da análise de performance do julgamento de valor de cada alternativa à luz de cada critério definidos na Seção 3.2.8. Esse gráfico é apresentado na Figura 3.4.

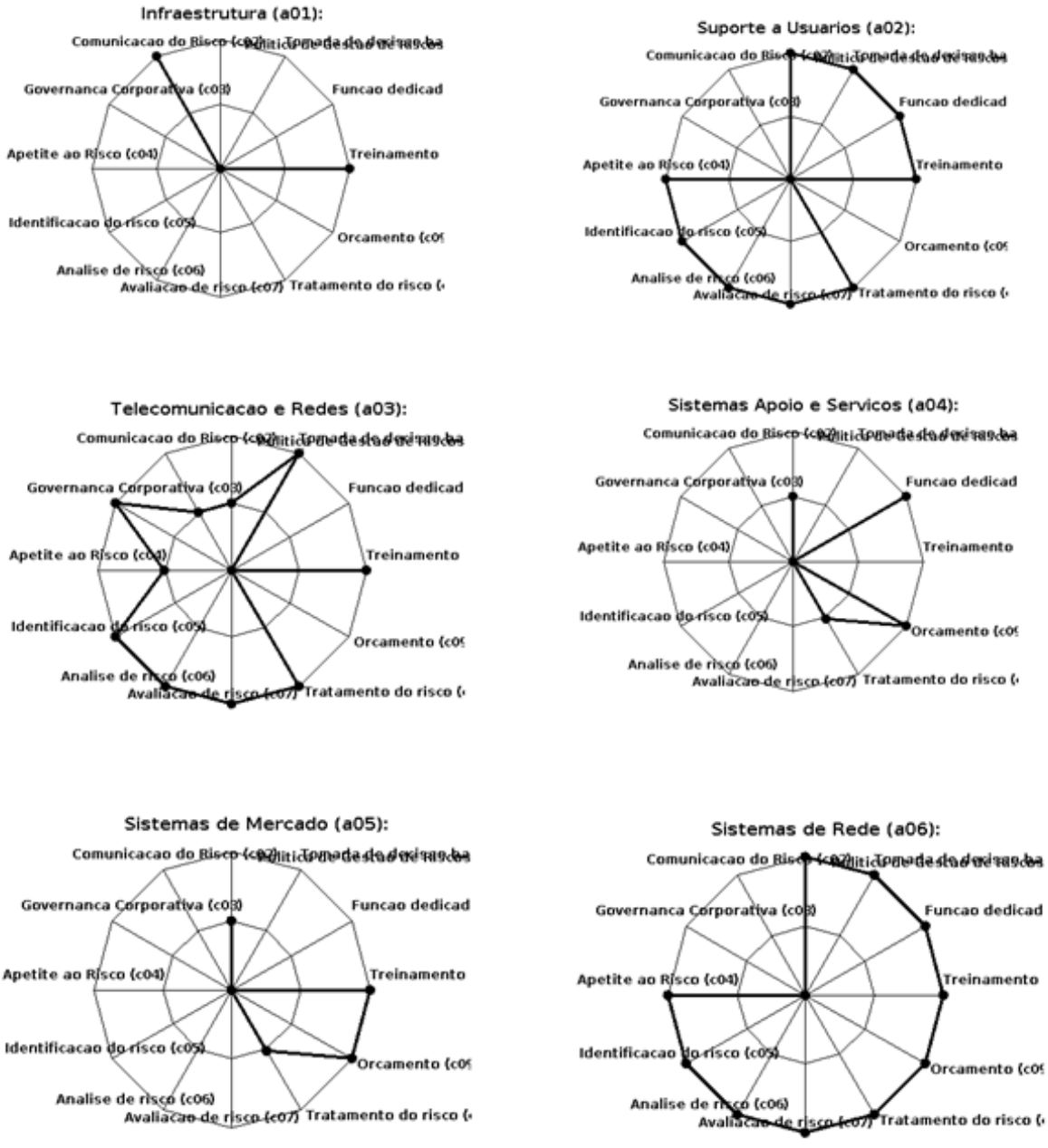

Figura 3.4: Análise de performance do julgamento de valor de cada alternativa à luz de cada critério utilizando o software Decision Deck - divz (Fonte: [111]).

Outro resultado gráfico apresentado pelo software Decision Deck - divz [111] é a análise da performance dos critérios, de acordo com os valores definidos na Seção 3.2.8. A análise da performance dos critérios é apresentada na Figura 3.5.

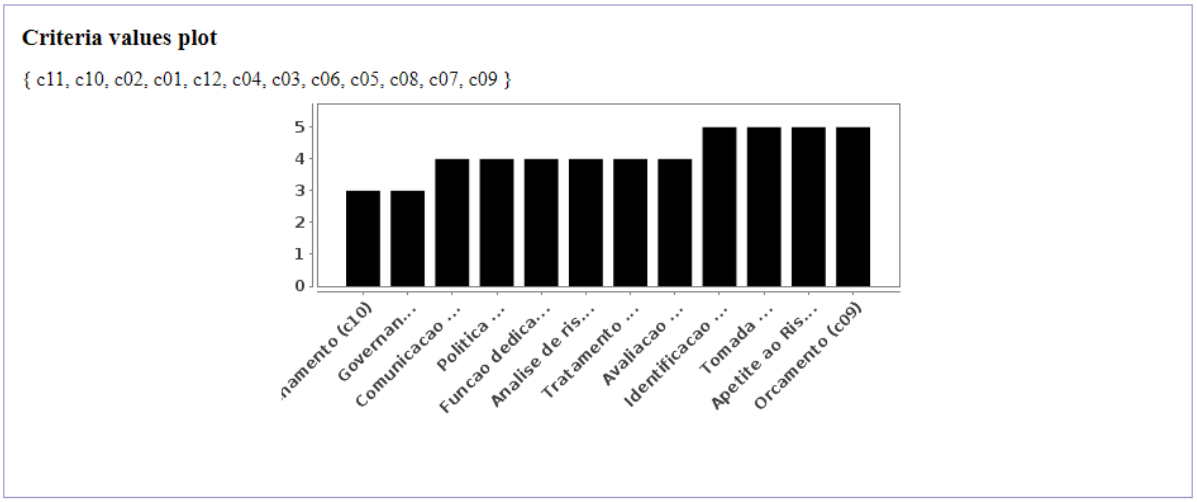

Figura 3.5: Análise de performance dos critérios utilizando o software Decision Deck - divz (Fonte: [111]).

3.2.10 Análise dos Resultados Obtidos

A última etapa sugeridas por Costa e Freitas [99] para a utilização do método ELECTRE TRI consiste em analisar os resultados obtidos na Seção 3.2.9. Nesta etapa, deve-se avaliar a classificação final encontrada, analisando inclusive, o grau de credibilidade destes resultados. O grau de credibilidade é uma medida da intensidade com que se pode "acreditar"na classificação obtida, sendo definido a partir de uma integração entre o conceito de concordância (o quanto o decisor "concorda"com a classificação) e o conceito de discordância (o quanto o decisor rejeita a classificação).

Houve uma incomparabilidade encontrada quanto à classificação da alternativa A4, que na classificação otimista foi classificada como Nível Estruturado e na classificação pessimista foi classificada como Nível Inicial. Considerando apenas os julgamentos para os quais não ocorreu incomparabilidade, observou-se que nenhum dos setores avaliados foi classificado nos Níveis Definido, Gerenciado e Otimizado, o que significa que o nível de maturidade geral para a TI da empresa avaliada ainda é muito baixo, embora na análise otimista, houve uma preponderância da classificação dos setores para o Nível Estruturado. Isso significa que, mesmo que seja novato e não documentado, existe um procedimento de gestão de riscos seguido por vários setores.

Com esse resultado, é possível afirmar que, em alguns critérios, os setores experimentam níveis mais maduros, que podem ser claramente reconhecidos na Figura 3.4. Apesar de haver uma consciência sobre os riscos, ainda existem dificuldades em identificar, avaliar, gerenciar e monitorar esses riscos. Embora existam diferenças entre as avaliações de maturidade dos setores, em geral, não há uma forte discrepância entre eles.

Foi feita uma análise de sensibilidade através de três simulações para verificar a robustez do modelo e analisar seu comportamento quanto às variações impostas. Na primeira simulação, foi variado o nível de corte de 0,5 para 0,6. Como resultado, a classificação otimista se manteve e a pessimista passou a classificar as alternativas A2, A4 e A6 no Nível Inicial e as alternativas A1, A3 e A5 no Nível Estruturado, eliminando as incomparabilidades. Ao variar o nível de corte para 0,5, todas as alternativas passaram a ser classificadas como Nível Estruturado, alterando assim o grau de credibilidade do resultado.

Na segunda simulação, os limites estabelecidos para as classes foram variados em torno de 5% acima de seus valores iniciais. Para estes valores o resultado permaneceu o mesmo. Na terceira e última simulação, o peso dos critérios foi variado, a fim de verificar a influência dos critérios na avaliação. Para isso, os critérios de maior peso (Apetite ao risco, Identificação do Risco, Orçamento e Tomada de Decisão) foram variados em 20% cada um. Aumentando o peso de cada um desses critérios de maior peso em 20%, o resultado se manteve o mesmo, exceto para o critério Orçamento, que apresentou como resultado as alternativas A1, A2 e A3 classificadas no Nível Gerenciado e as alternativas A1, A3 e A5 classificadas no Nível Definido, alterado substancialmente o grau de credibilidade do resultado. Em suma, a análise de sensibilidade realizada corrobora os valores estabelecidos para os limites das classes e os pesos dos atributos. Para eliminar a incomparabilidade encontrada, o valor do nível de corte foi mantido em 0,6.

3.3 Modelo para Avaliação da Maturidade em Gestão de Riscos de TI

De acordo com Belton e Stewart [42], a última fase desenvolve um plano de ação, que no caso deste trabalho consiste na criação do modelo de avaliação de maturidade. Segundo Gomes et al [108], os métodos MCDA visam apoiar o processo de decisão com a recomendação de ações que estejam em sintonia com as preferências e julgamentos de valores expressas pelos decisores. Por esse motivo, não se espera com este trabalho definir um resultado que constitua uma solução única para o problema de avaliação da maturidade em gestão de riscos de qualquer empresa.

Nesse sentido, o modelo proposto funciona como um guia para as empresas, auxiliando os gestores a avaliarem de forma objetiva e clara seus processos de gestão de riscos. Permite diagnosticar qual o status atual dos processos de gestão de riscos de TI e realizar um plano de melhoria, identificando pontos fortes e fracos baseados nos critérios. Foram utilizados critérios e classes selecionados com base na revisão da literatura e pressupõe com isso que eles abordem os principais aspectos que devem ser considerados em uma

avaliação de maturidade. Nada impede que se utilizem diferentes critérios e pesos, nem diferentes classes.

É importante ressaltar que qualquer plano de ação para melhoria da gestão de riscos em uma organização deve ser uma iniciativa liderada pela alta administração. Deve-se também alinhar a cultura da organização com uma política de gestão de riscos efetiva.

Capítulo 4

Conclusões Finais

4.1 Resultados Obtidos

O uso de Métodos Multicritérios de Apoio à Decisão ou MCDA tem auxiliado os gestores no processo de tomada de decisão, pois se afasta dos procedimentos intuitivo-empíricos usuais e conferem transparência ao processo de tomada de decisão, principalmente em contextos decisórios específicos, como é o caso dos modelos de maturidade em Gestão de Riscos de TI. Os métodos MCDA tem auxiliado os decisores a compreender melhor as consequências de suas decisões, identificando oportunidades de aperfeiçoamento ao longo do processo.

Os métodos MCDA da escola francesa propõem modelos mais flexíveis que não pressupõem, necessariamente, a comparação entre as alternativas e não impõem ao decisor uma estruturação hierárquica dos critérios. Além disso, possui uma estrutura axiomática lógica e transparente que permite ao decisor a obtenção de um valor único proveniente da síntese de seus julgamentos para cada alternativa, diferente dos outros métodos.

A utilização do método ELECTRE TRI representou um diferencial no processo de avaliação de maturidade em Gestão de Riscos de TI proposto neste trabalho, pois a sua utilização permitiu que os gestores pudessem tomar suas decisões embasadas em um método cientifico de forma clara e eficiente, em resposta ao problema levantado. Apesar de não ser um método muito difundido no meio organizacional, sua utilização surpreendeu positivamente os gestores da empresa onde o estudo de caso foi aplicado, despertando interesse em desenvolver novos projetos utilizando o ELECTRE TRI.

Existem vários modelos de maturidade em Gestão de Riscos na literatura, mas o modelo proposto difere-se dos demais por indicar os principais critérios relacionados à Gestão de Riscos, selecionados através de um estudo aprofundado dos modelos e padrões de ERM tidos como referências mundiais, como COSO, ABNT NBR ISO/IEC 31000, COBIT, FERMA, OCEG, The King IV Report, The Basel III Framework, entre outros.

Estes critérios estão presentes na maioria dos modelos estudados e refletem os aspectos fundamentais que devem ser considerados ao se avaliar como os riscos relacionados à TI estão sendo gerenciados nas organizações.

Além disso, ao especificar a escala de julgamento das alternativas para cada critério, o modelo sintetiza e organiza as informações relacionadas à Gestão de Riscos e simplifica o processo de decisão do gestor, permitindo que os mesmos se sintam confortáveis e seguros ao avaliarem cada um dos critérios. Dessa forma, são capazes de incluir suas preferências junto as alternativas selecionadas de modo a garantir um resultado satisfatório e que reflete a realidade da organização.

No estudo de caso realizado, os julgamentos dependeram da avaliação de diversas variáveis simultaneamente e de interpretações pessoais múltiplas, que variaram de acordo com a preferência do decisor para a classificação das alternativas que representava cada um dos departamentos de TI da empresa. Essa subjetividade ficou bem evidente no sistema de notas adotado e para montar a tabelas das alternativas versus critérios, para posteriormente efetuar os cálculos.

Dessa forma, pode-se concluir que o modelo construído utilizando o método de classificação ELECTRE TRI agregou características consideradas importantes, inclusive as qualitativas, na sistematização do processo de avaliação de Gestão de Riscos de TI. Permitiu diagnosticar o status atual da Gestão de Riscos do departamento de TI da empresa avaliada e identificar os pontos fortes e fracos de cada departamento baseados nos critérios.

Como contribuição do trabalho, destaca-se, no nível teórico, o estudo de modelos de maturidade de Gestão de Riscos realizado e a utilização de Métodos Multicritérios de Apoio à Decisão, especificamente o método ELECTRE TRI. O detalhamento da construção do modelo viabiliza o entendimento de aspectos específicos da implementação da metodologia. No nível prático, destaca-se a capacidade do modelo proposto de gerar entendimento aos decisores, que participam ativamente do processo, além de trazer a solução para o problema enfrentado.

Entretanto, é importante ressaltar que o modelo criado avalia a maturidade em gestão de riscos de TI e não a maturidade de TI como um todo. Além da gestão de riscos, existem diversos outros processos que devem ser observados ao se avaliar a maturidade de TI, como gestão de mudanças, gestão de programas e projetos, gestão de qualidade, entre outros.

4.2 Trabalhos Futuros

Os conhecimentos teóricos e práticos obtidos no desenvolvimento deste trabalho podem ser consideravelmente ampliados através de futuros trabalhos que possam utilizar o modelo

proposto como um modelo genérico de avaliação de maturidade em Gestão de Riscos, estendendo sua aplicação a outras áreas, além da TI. Para isso, deve-se observar a escala de julgamento das alternativas para cada critério e adequá-las à aplicação desejada.

Outra sugestão está relacionada ao estudo aprofundado do método ELECTRE TRI e suas variações, possibilitando a definição de novas escalas de julgamento de valor a fim de determinar valores dos limites de preferência (p), indiferença (q) e de veto (v) diferentes de zero.

Em relação à empresa onde o estudo de caso foi aplicado, sugere-se o mapeamento dos processos de Gestão de Riscos. Com esses processos, é possível executar novamente o modelo utilizando-os como alternativas e permitindo a comparação dos resultados encontrados. Sugere-se ainda a utilização do modelo em todo o grupo, permitindo uma avaliação geral da maturidade em Gestão de Riscos de TI da empresa.

Referências

[1] Fernandes, Aguinaldo Aragon e Vladimir Ferraz de Abreu: *Implantando a Governança de TI - 4ª Ed.: Da estratégia à Gestão de Processos e Serviços*. Brasport, abril 2014, ISBN 978-85-7452-658-4. 1, 2, 14

[2] Laurindo, Fernando José Barbin, Tamio Shimizu, Marly Monteiro de Carvalho e Roque Rabechini Jr: *O papel da tecnologia da informação (TI) na estratégia das organizações*. Gestão and Produção, 8(2):160–179, agosto 2001, ISSN 0104-530X. 1

[3] Lunardi, Guilherme Lerch, João Luiz Becker e Antonio Carlos Gastaud Maçada: *Impacto da adoção de mecanismos de governança de Tecnologia de Informação (TI) no desempenho da gestão da TI: uma análise baseada na percepção dos executivos.* Revista de Ciências da Administração, 12(28):11–39, dezembro 2010, ISSN 2175-8077. 1, 2

[4] Mansur, Ricardo: *Governança de TI: Metodologias, Frameworks e Melhores Práticas*. Brasport, 2007, ISBN 978-85-7452-322-4. 1

[5] Normas Técnicas, Associação Brasileira de: *ABNT NBR ISO/IEC 38500 - Governança Corporativa de Tecnologiada Informação*, 2009. 1, 16

[6] Ramos, Anderson: *Security Officer 1 - Guia Oficial para Formação: de Gestores em Segurança da Informação*, volume 1. Zouk, Porto Alegre, 2ª edição, 2008, ISBN 978-85-88840-82-9. 1

[7] Hopkin, Paul: *Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management*. Kogan Page Publishers, 4ª edição, janeiro 2017, ISBN 978-0-7494-7962-6. 1

[8] Governança Corporativa, Instituto Brasileiro de: *Código das melhores práticas de governança corporativa*. 5ª edição, 2015. 1

[9] Association, Information Systems Audit and Control: *COBIT 5: Modelo Corporativo para Governança e Gestão de TI da Organização*, 2012. `http://www.isaca.org`, acesso em 2016-02-05. 2, 26

[10] Hopkinson, Mr Martin: *The Project Risk Maturity Model: Measuring and Improving Risk Management Capability*. Gower Publishing, Ltd., setembro 2012, ISBN 978-1-4094-5895-1. 2

[11] Caiado, Rodrigo Goyannes Gusmão, Gilson Brito Alves Lima, Daniel Luiz de Mattos Nascimento, Julio Vieira Neto e Rodolpho Augusto Maultasch Oliveira: *Guidelines to Risk Management Maturity in Construction Projects*. Brazilian Journal of Operations and Production Management, páginas 372–385, 2016. 2, 3, 5, 11, 12, 13, 14, 16, 17, 19, 20, 21, 24, 25, 26, 27, 29

[12] Chapman, Robert J.: *Simple Tools and Techniques for Enterprise Risk Management*. John Wiley & Sons, dezembro 2011, ISBN 978-1-119-98997-4. 2, 3, 5, 14, 15, 16, 17, 18, 20, 22, 26, 29

[13] Treadway Commission, Committee of Sponsoring Organizations of the: *Internal Control: Integrated Framework 2013.*, 2013. `https://www.coso.org`, acesso em 2018-06-11TZ. 2, 3, 5, 10, 11, 13, 14, 16, 17, 18, 19, 20, 21, 22, 25

[14] Elmaallam, Mina e Abdelaziz Kriouile: *Towards A Model Of Maturity For Is Risk Management*. International Journal of Computer Science and Information Technology, 3, agosto 2011. 2, 5, 10, 13, 15, 16, 17, 18, 20, 21, 23, 24, 26, 27, 29

[15] Elmaallam, Mina e Abdelaziz Kriouile: *Model ISR3m for assessing maturity of IS risk management process: Case study*. Em *2012 Colloquium in Information Science and Technology*, páginas 16–21, outubro 2012. 2, 5, 10, 23, 27

[16] Hillson, D. A.: *Towards a risk maturity model*. The International Journal of Project and Business Risk Management, 1(1):35–45, 1997. 2, 5, 15, 16, 17, 20, 24, 29

[17] Hopkinson, Martin: *Risk Maturity Models in Practice*. Risk Management Bulletin, 5(4), 2000. 2, 5, 15, 17, 18, 20, 24, 29

[18] Association, Information Systems Audit and Control: *COBIT 5 for Risk*, 2013. `http://www.isaca.org`, acesso em 2017-06-05. 2, 3, 5, 11, 12, 13, 14, 16, 17, 18, 19, 20, 22

[19] Mayer, J. e L. Lemes Fagundes: *A model to assess the maturity level of the Risk Management process in information security*. Em *2009 IFIP/IEEE International Symposium on Integrated Network Management-Workshops*, páginas 61–70, junho 2009. 2, 5, 10, 13, 15, 16, 17, 18, 19, 20, 21, 22, 24, 26, 29

[20] Oliva, Fábio Lotti: *A maturity model for enterprise risk management*. International Journal of Production Economics, 173:66–79, março 2016, ISSN 0925-5273. 2, 4, 5, 10, 13, 14, 15, 16, 17, 18, 19, 20, 23, 28, 29

[21] Ren, Y. T. e K. T. Yeo: *Risk management capability maturity model for complex product systems (CoPS) projects*. Em *2004 IEEE International Engineering Management Conference (IEEE Cat. No.04CH37574)*, volume 2, páginas 807–811 Vol.2, outubro 2004. 2, 5, 15, 21, 25, 29

[22] Ren, Y., K. T. Yeo e Y. Ren: *Risk Management Capability Maturity and Performance of Complex Product and System (CoPS) Projects with an Asian Perspective*. Journal of Engineering, Project, and Production Management, 4(2):81–98, julho 2014, ISSN 2221-6529, 2223-8379. 2, 16, 17, 18, 20, 21, 22, 25, 27, 29

[23] Araújo, Misael Sousa e Edgard Costa Oliveira: *Estudo Comparativo de Modelos de Maturidade Aplicados à Gestãod e Riscos - Uma Abordagem sob a Perspectiva da Tecnologia da Informação*. X Congresso Nacional de Excelência em Gestão, agosto 2014. 2, 21, 24, 25, 26

[24] Wibowo, Andreas e Januar Taufik: *Developing a Self-assessment Model of Risk Management Maturity for Client Organizations of Public Construction Projects: Indonesian Context*. Procedia Engineering, 171:274–281, 2017, ISSN 18777058. 2, 4, 5, 16, 17, 18, 19, 20, 29, 44

[25] Yudatama, Uky e Riyanarto Sarno: *Evaluation maturity index and risk management for it governance using Fuzzy AHP and Fuzzy TOPSIS (case Study Bank XYZ)*. páginas 323–328. IEEE, maio 2015, ISBN 978-1-4799-7710-9 978-1-4799-7711-6. 2, 5, 16, 17, 18, 19, 20, 30

[26] Almeida, A.T.: *O conhecimento e o uso de métodos multicritério de apoio a decisão*. Editora Universitária da UFPE, Recife, 2011. 2, 5, 32, 33

[27] Gomes, Luiz Flavio Autran Monteiro, Marcela Cecilia Araya González e Claudia Carignano: *Tomada de decisões em cenários complexos: introdução aos métodos discretos do apoio multicritério à decisão*. Thomson, 2004, ISBN 978-85-221-0354-6. 2, 30, 31, 33, 36, 39, 43, 44

[28] Guarnieri, Patricia: *Synthesis of Main Criteria, Methods and Issues of Multicriteria Supplier Selection*. Revista de Administração Contemporânea, 19(1):1–25, fevereiro 2015, ISSN 1415-6555. 2, 5, 32, 33, 38

[29] Herrera, F., S. Alonso, F. Chiclana e E. Herrera-Viedma: *Computing with words in decision making: foundations, trends and prospects*. Fuzzy Optimization and Decision Making, 8(4):337–364, dezembro 2009, ISSN 1568-4539, 1573-2908. 2, 5, 30

[30] Society, The Risk and Insurance Management: *ERM RIMS Risk Maturity Model (RMM) for Enterprise Risk Management - Executive Summary*, novembro 2006. 3, 13, 15, 16, 17, 18, 19, 20, 22, 25, 29

[31] Tomas, Robson Nogueira e Rosane Lúcia Chicarelli Alcantara: *Models for risk management in supply chains: review, analysis, and guidelines for research*. Gestão & Produção, 20(3):695–712, janeiro 2013, ISSN 0104-530X. 3, 29

[32] Coetzee, G. P. e D. Lubbe: *The risk maturity of South African private and public sector organisations*. Southern African Journal of Accountability and Auditing Research, 14(1):45–56, janeiro 2013, ISSN 1028-9011. 3, 14

[33] Mendonça, Cláudio Márcio Campos de, Lenin Cavalcanti Brito Guerra, Manoel Veras de Souza Neto e Afrânio Galdino de Araújo: *Governança de tecnologia da informação: um estudo do processo decisório em organizações públicas e privadas*. Revista de Administração Pública, 47(2):443–468, abril 2013, ISSN 1982-3134. 3, 29

[34] Wieczorek-Kosmala, Monika: *Risk management practices from risk maturity models perspective*. Journal of East European Management Studies, 19(2):133–159, 2014, ISSN 0949-6181. 4, 11, 14, 15, 16, 17, 18, 19, 20, 24, 26

[35] Internacional, KPMG: *Expectations of Risk Management Outpacing Capabilities – It's Time For Action*. página 60, 2013. 4, 10, 16, 17, 18, 19, 20

[36] Solution, Aon Risk: *Aon Risk Maturity Index Insight Report*, 2015. `http://www.aon.com/risk-services/thought-leadership/report-rmi-insight-nov-2015.jsp`, acesso em 2018-06-11TZ. 4, 5

[37] Solution, Aon Risk: *Global Risk Management Survey - Full Report*, 2017. `http://www.aon.com/2017-global-risk-management-survey/download-reports.jsp`, acesso em 2018-06-11TZ. 5, 10, 16, 17, 18, 19, 20

[38] Deloitte: *Global risk management survey, 10th edition*, 2017. `https://www.deloitte.com`, acesso em 2018-06-11TZ. 5, 10, 13, 16, 17, 18, 19, 20

[39] Souza, Girlene Santos de, Anacleto Ranulfo dos Santos e Viviane Borges Dias: *Metodologia da pesquisa científica: a construção do conhecimento e do pensamento científico no processo de aprendizagem*. Animal, outubro 2013, ISBN 978-85-67375-10-6. 6, 7

[40] Cervo, Amado Luiz, Pedro Alcino Bervian e Roberto da Silva: *Metodologia cientifica*. Pearson Prentice Hall, 2006, ISBN 978-85-7605-047-6. 7

[41] Baraglio, Gisele Finatti: *Metodologia CientÍfica*. Clube de Autores, setembro 2008. 7

[42] Belton, Valerie e Theodor Stewart: *Multiple Criteria Decision Analysis: An Integrated Approach*. Springer Science & Business Media, 2002, ISBN 978-0-7923-7505-0. 7, 8, 9, 31, 32, 34, 35, 36, 37, 42, 51, 58

[43] Normas Técnicas, Associação Brasileira de: *ABNT NBR ISO/IEC 31000 - Gestão de Riscos*, 2009. 10, 12, 13, 16, 17, 18, 19, 20, 22, 23

[44] Normas Técnicas, Associação Brasileira de: *ABNT ISO GUIA 73 - Gestão de Riscos - Vocabulário*, 2009. 10, 12

[45] Normas Técnicas, Associação Brasileira de: *ABNT NBR ISO/IEC 31010 - Técnicas de Avaliação de Riscos*, 2009. 10, 12, 20

[46] Bharathy, Gnana K. e Michael K. McShane: *Applying a Systems Model to Enterprise Risk Management*. Engineering Management Journal, 26(4):38–46, dezembro 2014, ISSN 1042-9247, 2377-0643. 10, 13, 16, 17, 19, 20

[47] Institute, Project Management: *Um guia do conhecimento em gerenciamento de projetos. Guia PMBOK. (6 Ed)*, 2017. 11, 12, 14, 16, 17, 18, 19, 20, 22, 26, 29

[48] European Risk Management Associations, Federation of: *A Risk Management Standard*, 2002. 11, 12, 16, 17, 18, 20

[49] Treadway Commission, Committee of Sponsoring Organizations of the: *Enterprise Risk Management - Integrated Framework.*, 2004. `https://www.coso.org`, acesso em 2018-06-11TZ. 12, 15, 21, 22, 25, 29

[50] Normas Técnicas, Associação Brasileira de: *ABNT NBR ISO/IEC 27005 - Tecnologia da Informação - Técnicas de Segurança - Gestão de Riscos de Segurança da Informação*, 2011. 12, 16

[51] Group, Open Compliance and Ethics: *A Governance, Risk and Compliance Capability Model (Red Book) 3.0*. 3ª edição, 2015. 12, 16, 17, 18, 19, 20, 27, 29

[52] Dubois-Pelerin, Emmanuel, Li Cheng, Miroslav Petkov, Howard L Rosen, Rodney A Clark, Eric E Hedman, Jackson E Griffith e Andy Chang: *Enterprise Risk Management*. Standard & Poor's Ratings Services, página 29, julho 2013. 12, 16, 22

[53] Directors Southern Africa, Institute of: *The King IV Report on Corporate Governance for South Africa 2016*. Relatório Técnico, LexisNexis South Africa, janeiro 2016. 12, 16, 17, 18, 20

[54] International Settlemens, Bank for: *Basel III: Finalising post-crisis reforms*. Basel Comittee on Baking Supervision, página 162, dezembro 2017. 12

[55] Raz, Tzvi e David Hillson: *A Comparative Review of Risk Management Standards*. Risk Management, 7(4):53–66, outubro 2005, ISSN 1460-3799, 1743-4637. 12

[56] Carcary, Marian: *IT risk management: A capability maturity model perspective*. Electronic Journal of Information Systems Evaluation, 16(2):3–13, 2015. 13, 16, 17, 18, 19, 20

[57] Deloitte: *Os cinco pilares dos riscos empresariais: Como gerenciá-los em um cenário econômico e de negócios desafiador*. Relatório Técnico, junho 2017. `https://www.deloitte.com`, acesso em 2018-03-26TZ. 13

[58] Monda, Barbara e Marco Giorgino: *An ERM maturity model*. Em *Enterprise Risk Management Symposium. Chicago, IL, IL: Management, Economics and Industrial Engineering Department*, 2013. 13, 16, 17, 18, 19, 20

[59] Njagi, Caroline: *Evaluation of the Level of Enterprise Risk Management Adoption and Maturity of Insurance Companies in Kenya*. Thesis, United States International University - Africa, 2015. 13, 14, 16, 17, 18, 19, 20

[60] Merna, Tony e Faisal F. Al-Thani: *Corporate Risk Management: An Organisational Perspective*. John Wiley and Sons, julho 2005, ISBN 978-0-470-01588-9. 14, 17, 18, 19, 20

[61] Siqueira, Jairo: *O Modelo de Maturidade de Processos: como maximizar o retorno dos investimentos em melhoria da qualidade e produtividade*. IBQN Brasil, 2005. 14, 29

[62] Becker, Joerg, Bjoern Niehaves, Jens Poeppelbuss e Alexander Simons: *Maturity Models in IS Research*. ECIS 2010 Proceedings, página 42, 2010. 14, 19, 20

[63] Öngel, Begüm: *Assessing Risk Management Maturity: a Framework for the Construction Companies*. Tese de Doutoramento, Middle East Technical University, dezembro 2009. 14

[64] Zhao, Xianbo, Bon Gang Hwang e Sui Peng Low: *Developing Fuzzy Enterprise Risk Management Maturity Model for Construction Firms*. Journal of Construction Engineering and Management, páginas 1179–1189, setembro 2013. 14, 29

[65] Junior, Jucá, Antonio da Silva, Edivandro Carlos Conforto e Daniel Capaldo Amaral: *Maturity project management in small software development firm's of the Technological Pole of São Carlos*. Gestão and Produção, 17(1):181–194, janeiro 2010, ISSN 0104-530X. 14

[66] Association, Information Systems Audit and Control: *COBIT Process Assessment Model (PAM): Using COBIT 5*, 2013. `http://www.isaca.org`, acesso em 2017-06-05. 15, 22, 26, 29

[67] Aksu, Halil: *BT Yoneticisinin El Kitabı: Kurumsal Bilisim Olgunluk Modeli*. Pusula Yayıncılık, 2013, ISBN 978-9944-711-67-8. 16, 23, 28, 29

[68] Hartono, Budi, Deo F. N. Wijaya e Hilya M. Arini: *An empirically verified project risk maturity model: Evidence from Indonesian construction industry*. International Journal of Managing Projects in Business, 7(2):263–284, abril 2014, ISSN 1753-8378. 16, 25

[69] Goksen, Yılmaz, Eda Cevik e Huseyin Avunduk: *A Case Analysis on the Focus on the Maturity Models and Information Technologies*. Procedia Economics and Finance, 19:208–216, 2015, ISSN 22125671. 17, 18, 19, 20, 21, 24, 28, 29

[70] Farrokh, J e Azhar K. Mansur: *Project Management Maturity Models and Organizational Project Management Maturity Model (OPM3): A Critical Morphological Evaluation*. International Journal of Economics and Management Engineering, 7(5):4, 2013. 21, 24, 25, 29

[71] Crawford, J. Kent: *Project Management Maturity Model, Second Edition*. Auerbach Publications, Boca Raton, FL, 2 edition edição, julho 2006, ISBN 978-0-8493-7945-1. 21, 24

[72] Hopkinson, Martin e Graham Lovelock: *The project risk maturity model-assessment of the U.K. MoD's top 30 acquisition projects*. 2004. 21, 25

[73] Government Commerce, Office of: *Portfolio, Programme and Project Management Maturity Model (P3m3)*, 2010. 23, 29

[74] Institute, CMMI: *Capability Maturity Model Integration*, 2018. `https://www.cmmiinstitute.com/cmmi`, acesso em 2018-06-12TZ. 24

[75] Certo, Samuel C.: *Administração moderna*. Prentice Hall, 2003, ISBN 978-85-87918-12-3. 30

[76] Robbins, Stephen, Tim Judge e Filipe Sobral: *Comportamento organizacional: teoria e prática no contexto brasileiro*. Pearson Brasil, 2010, ISBN 978-85-7605-569-3. 30

[77] Souza, Fernando Menezes Campello de: *Decisoes racionais em situaçoes de incerteza*. Fernando Menezes Campello de Souza, 2007, ISBN 978-85-905006-2-9. 30

[78] Chiavenato, Idalberto: *Introdução a Teoria Geral da Administração*. Elsevier Brasil, 8ª edição, maio 2011, ISBN 978-85-352-4791-6. 30

[79] Zavadskas, Edmundas Kazimieras e Zenonas Turskis: *Multiple criteria decision making (MCDM) methods in economics: an overview*. Technological and Economic Development of Economy, 17(2):397–427, junho 2011, ISSN 2029-4913. 31

[80] Costa, Carlos A. Bana e e Jean Claude Vansnick: *MACBETH - An interactive path towards the construction of cardinal value functions*. International Transactions in Operational Research, 1(4):489–500, outubro 1994, ISSN 0969-6016. 31, 39

[81] Gomes, Carlos Francisco Simões e Luiz Flávio Autran Monteiro Gomes: *A Função de Decisão Multicritério*. Revista do Mestrado Em Administração e Desenvolvimento Empresarial,, 2:77–88, 2002. 31, 32, 33, 36

[82] Ensslin, Leonardo, Ademar Dutra e Sandra Rolim Ensslin: *MCDA: a constructivist approach to the management of human resources at a governmental agency*. International Transactions in Operational Research, 7(1):79–100, janeiro 2000, ISSN 0969-6016. 31

[83] Roy, Bernard e Patrice Bertier: *La methode ELECTRE II: Une methode de classement en presence de criteres multiples.* Paris: SEMA (Metra International) Paris, página 45, 1971. 32, 36

[84] Mousseau, V., R. Slowinski e P. Zielniewicz: *A user-oriented implementation of the ELECTRE-TRI method integrating preference elicitation support*. Computers and Operations Research, 27(7):757–777, junho 2000, ISSN 0305-0548. 32

[85] Brans, Jean Pierre, Philippe Vincke e Bertrand Mareschal: *How to select and how to rank projects: The Promethee method*. European Journal of Operational Research, 24(2):228–238, fevereiro 1986, ISSN 0377-2217. 32, 38

[86] Edwards, Ward: *How to use multiattribute utility measurement for social decisionmaking.* IEEE Transactions on Systems, Man and Cybernetics, SMC-7(5):26–340, 1977. 32, 38

[87] Keeney, Ralph L. e Howard Raiffa: *Decisions with Multiple Objectives: Preferences and Value Trade-Offs*. Cambridge University Press, 1976, ISBN 978-0-521-43883-4. 32, 38

[88] Antunes, C. e M. Alves: *Programação linear multiobjetivo-métodos interativos e software*. Em *Anais do Congreso Latino-Iberoamericano de Investigación Operativa*, volume 24, páginas 4725–4736, 2012. 33

[89] Herva, Marta e Enrique Roca: *Review of combined approaches and multi-criteria analysis for corporate environmental evaluation.* Journal of Cleaner Production, 39:355–371, janeiro 2013, ISSN 0959-6526. 33

[90] Roy, Bernard: *Decision-Aid and Decision-Making.* Em *Readings in Multiple Criteria Decision Aid*, páginas 17–35. Springer, Berlin, Heidelberg, 1990, ISBN 978-3-642-75937-6 978-3-642-75935-2. 33, 34

[91] Roy, Bernard: *Classement et choix en présence de points de vue multiples.* RAIRO - Operations Research - Recherche Opérationnelle, 2(V1):57–75, 1968, ISSN 0399-0559. 34, 36

[92] Roy, Bernard e Jean Christophe Hugonnard: *Classement des prolongements de lignes de stations en banlieu parisienne.* Cahiers du LAMSADE., página 45, 1981. 34, 36, 37

[93] Roy, Bernard e Jean Michel Skalka: *ELECTRE IS: Aspécts Methodologiques et Guide d'Utilization.* Cahiers du LAMSADE., 1985. 34, 37, 44, 50

[94] Rodriguez, Dey Salvador Sanchez, Helder Gomes Costa e LFRRS Do Carmo: *Métodos de auxílio multicritério à decisão aplicados a problemas de PCP: Mapeamento da produção em periódicos publicados no Brasil.* Gestão e Produção, 20(1):134–146, 2013. 36

[95] Yu, Wei: *ELECTRE TRI - Aspects Methodologiques et Guide d'Utilisation.* Document du LAMSADE., 1992. 37, 51, 52

[96] Roy, Bernard e Denis Bouyssou: *Aide multicritère à la décision : méthodes et cas.* London School of Economics and Political Science, 1993, ISBN 978-2-7178-2473-5. 37, 51, 52

[97] Almeida-Dias, J., J. R. Figueira e B. Roy: *Electre Tri-C: A multiple criteria sorting method based on characteristic reference actions.* European Journal of Operational Research, 204(3):565–580, agosto 2010, ISSN 0377-2217. 37

[98] Bouyssou, Denis e Thierry Marchant: *On the relations between ELECTRE TRI-B and ELECTRE TRI-C and on a new variant of ELECTRE TRI-B.* European Journal of Operational Research, 242(1), 2015. 38, 43

[99] Costa, Helder e André Freitas: *Aplicação do método ELECTRE TRI à classificação da satisfação de clientes. Um estudo de caso em um curso de extensão universitária.* Revista Portuguesa e Brasileira de Gestão, 4(4):66–76, 2005, ISSN 1645-4464,. 38, 44, 50, 57

[100] Fishburn, Peter C.: *Utility theory for decision making.* Wiley, New York, janeiro 1970. 38

[101] Edwards, Ward e F. Hutton Barron: *SMARTS and SMARTER: Improved Simple Methods for Multiattribute Utility Measurement.* Organizational Behavior and Human Decision Processes, 60(3):306–325, dezembro 1994, ISSN 0749-5978. 38

[102] Saaty, Thomas L: *The Analytic Hierarquic Process.* RWS Publications, Pittsburg, 1980. 38

[103] Saaty, Thomas L.: *Decision Making with Dependence and Feedback: The Analytic Network Process.* Rws Publications, Pittsburg, 1996, ISBN 978-0-9620317-9-3. 39

[104] Hwang, Ching Lai e Kwangsun Yoon: *Multiple Attribute Decision Making - Methods and Application.* Springer-Verlag, New York, 1981. 39

[105] Yoon, Kwangsun: *A Reconciliation among Discrete Compromise Solutions.* The Journal of the Operational Research Society, 38(3):277–286, 1987, ISSN 0160-5682. 39

[106] Hwang, Ching Lai, Young Jou Lai e Ting Yun Liu: *A new approach for multiple objective decision making.* Computers & Operations Research, 20(8):889–899, outubro 1993, ISSN 0305-0548. 39

[107] Gomes, Luiz Flavio Autran Monteiro e Monica Marcondes Porto Pedrosa Lima: *From modeling individual preferences to multicriteria ranking of discrete alternatives: A look at prospect theory and the additive difference model.* Foundations of Computing and Decision Sciences, 17(3):171–184, janeiro 1992. 39

[108] Gomes, Luiz Flávio Autran Monteiro, Carlos Francisco Simões Gomes e Adiel Teixeira de Almeida: *Tomada de decisão gerencial: enfoque multicritério.* Atlas, 2009, ISBN 978-85-224-5351-1. 44, 58

[109] Likert, Rensis: *Novos padrões de administração.* Pioneira, 1971. 45

[110] Hare, A. Paul: *Consensus Versus Majority Vote : A Laboratory Experiment.* Small Group Behavior, 11(2):131–143, maio 1980, ISSN 0090-5526. `https://doi.org/10.1177/104649648001100201`, acesso em 2018-08-02TZ. 45

[111] *Decision Deck - diviz.* `https://www.diviz.org`, acesso em 2018-06-04TZ. 53, 54, 55, 56, 57

[112] Costa, Helder Gomes, André Fernando Uébe Mansur, André Luís Policani Freitas e Rogério Atem de Carvalho: *ELECTRE TRI applied to costumers satisfaction evaluation.* Production, 17(2):230–245, agosto 2007, ISSN 0103-6513. 55