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

Os Efeitos da Redução da Intuitividade nas Decisões de Gestores de Tecnologia da Informação através da Gestão de Riscos

Clayton da Silva Lobato

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

Orientador
Prof. Dr. Simone Borges Simão Monteiro

Brasília
2017

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

da Silva Lobato, CLAYTON
dC622e Os Efeitos da Redução da Intuitividade nas Decisões de Gestores de Tecnologia da Informação através da Gestão de Riscos / CLAYTON da Silva Lobato; orientador Simone Borges Simão Monteiro. -- Brasília, 2017.
113 p.

Dissertação (Mestrado - Mestrado Profissional em Computação Aplicada) -- Universidade de Brasília, 2017.

1. Multicritério,. 2. Indicadores de Decisões. 3. Teoria da Opção Real. 4. Gestão de Riscos. 5. Tomada de Decisão. I. Borges Simão Monteiro, Simone, orient. II. Título.

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

Os Efeitos da Redução da Intuitividade nas Decisões de Gestores de Tecnologia da Informação através da Gestão de Riscos

Clayton da Silva Lobato

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

Prof. Dr. Simone Borges Simão Monteiro (Orientador)
EPR/UnB

Prof. Dr. João Mello da Silva
Universidade de Brasília

Dr. Paulo Angelo Alves Resende
Presidência da República

Prof. Dr. Marcelo Ladeira
Coordenador do Programa de Pós-graduação em Computação Aplicada

Brasília, 14 de Dezembro de 2017

Dedicatória

Eu dedico esse trabalho a Deus, que em tudo tem me acompanhado me sustentado, à minha esposa Simone Matsuoka, meus filhos Tainá, Alice, Eduardo e Akemi, aos meus pais Telma e Jorge Lobato, obrigado pelo sacrifício que fizeram para dar oportunidade de estudos. Dedico aos meus avós Mário, Moroza, Eduardo e Diquinha.

Dedico à Albert Eisten e Michael Faraday pelo exemplo de perseverança e o quanto acreditar em um sonho pode ser sacrificante e ao mesmo tempo gratificante.

Que Deus abençoe todos !

Agradecimentos

Agradeço à Professora Simone por toda a paciência e por compreensão desde o início e todas as oportunidades oferecidas para continuidade de meus estudos.

Agradeço ao Professor Marcelo Ladeira pelas palavras de carinho e incentivo, ao Professor André Drummond por todo apoio e incentivo, ao Professor Guilherme Ramos pela oportunidade.

Resumo

Este trabalho apresenta um estudo que avalia o impacto do uso da gestão de riscos como ferramenta de apoio das decisões estratégicas de gestores de Tecnologia da Informação - TI. Pretende-se atender a carência identificada na literatura referente a modelos de possam apoiar ao processo de tomada de decisões e que extrapolem os aspectos da análise, avaliação e a mitigação dos riscos. Assim, serão observados os desafios das decisões baseadas em riscos, por conta do comportamento humano quando deparados com os processos de decisões complexas e a tendência intuitiva para os processos decisórios. Para isso, será apresentada uma revisão da literatura relacionada à gestão de riscos, sobre os aspectos do comportamento humano para os processos decisórios e o impacto do uso de novas abordagens de riscos para apoiar as decisões. São descritas as principais técnicas e metodologias usadas para gerenciamento de riscos, além de avaliar o quanto os modelos adotados apoiam os processos decisórios dos gestores de TI. Conseguinte, é realizado um estudo de campo com o objetivo de identificar o comportamento da gestão de riscos e o nível de suporte às decisões, visão que vai além dos aspectos da análise e mitigação dos riscos, demonstrando o nível de efetividade e eficiência dos modelos adotados e os desafios relacionados com o uso da gestão de riscos e seus limitadores para as decisões de alto nível dos gestores de TI. O estudo fornece uma reflexão sobre a complexidade dos processos de decisões e o quanto estes tornam-se intuitivos nas instituições quando sustentados em riscos e seus impactos. Como resultado, será demonstrado como o uso de um modelo proposto, apoiado em novas abordagens, pode retratar de forma mais objetiva as necessidades dos gestores de TI enquanto direcionamentos decisórios, tornando-as mais assertivas e promovendo a economicidade em suas decisões.

Palavras-chave: Multicritério, Indicadores de Decisões, Teoria da Opção Real, Gestão de Riscos, Tomada de Decisão, Decisões e Intuitividade, Cisne Negro, Antifrágil

Abstract

This paper presents a study that evaluates the impact of the use of risk management as a tool to support the strategic decisions of IT managers. The objective is to address the literature's lack of models that can support the decision-making process and extrapolate aspects of analysis, evaluation and risk mitigation. Thus, the challenges of risk-based decisions will be observed, due to human behavior when faced with complex decision processes and the intuitive tendency for decision-making processes. For this, a review of the literature related to risk management, aspects of human behavior for decision making processes and the impact of using new risk approaches to support decisions will be presented. The main techniques and methodologies used for risk management are described, as well as evaluating how the models adopted support the decision-making processes of IT managers. Consequently, a field study is carried out with the objective of identifying the behavior of risk management and the level of decision support, a vision that goes beyond the aspects of risk analysis and mitigation, demonstrating the level of effectiveness and efficiency of the models adopted and the challenges related to the use of risk management and their constraints to the high-level decisions of IT managers. The study provides a reflection on the complexity of decision processes and how they become intuitive in institutions when they are sustained by risks and their impacts. As a result, it will be demonstrated how the use of a proposed model, supported by new approaches, can more objectively portray the needs of IT managers as decision-making, making them more assertive and promoting the economics of their decisions.

Keywords: Multicriteria, Indicators Decisions, Theory of Real Option, Risk Management, Decision Making, Intuitive Decisions, Black Swan, Antifrágil

Sumário

1 Introdução **1**
1.1 Contextualização 1
1.2 Definição do problema 3
1.3 Objetivos do Trabalho 3
1.3.1 Objetivo Geral 4
1.3.2 Objetivos Específicos 4
1.4 Justificativa do Trabalho 4
1.5 Estrutura do trabalho 5

2 Revisão da literatura **7**
2.1 Conceitos e princípios da gestão de riscos 7
2.2 Complexidade do processo de tomada de decisão 39
2.2.1 Sistemas de apoio à decisão (SAD/DSS) 49
2.3 Considerações sobre o referencial teórico 51

3 Metodologia **54**
3.1 Estruturação da pesquisa 55
3.1.1 Formulação do problema 55
3.1.2 Pesquisa bibliográfica 55
3.1.3 Construção do modelo 55
3.1.4 Aplicação do modelo proposto 56
3.1.5 Avaliação dos resultados 56

4 Estruturação de um Modelo de apoio à tomada de decisão **57**
4.1 Motivação para escolha das principais técnicas e ferramentas adotadas . . . 58
4.2 Visão geral da arquitetura e transversalidade organizacional 59
4.2.1 Descrição da etapa de análise do ecossistema 63
4.3 Ciclo IATD/RCS para tomada de decisões 69

5 Estudo de caso **72**
5.1 Execução do modelo 72
5.1.1 Estrutura de negócio 72
5.1.2 Análise de resiliência e limitadores 75
5.1.3 Análise da capacidade e nível de sustentação 78
5.1.4 Integração dos processos organizacionais 79

6 Conclusão e Trabalhos futuros **83**

Referências **86**

Apêndice **89**

A Resultados do estudo proposto **90**

Lista de Figuras

2.1 Interação do processo de gestão de riscos.. 9
2.2 Atividade de tratamento de risco.. 10
2.3 Alinhamento do processo SGSI e do processo de gestão de riscos 27015.. . 11
2.4 Relacionamento entre os princípios, estrutura e processo da gestão de riscos.. 13
2.5 Relação entre as governanças e estrutura da governança organizacional.. . 14
2.6 Implementação da governança de segurança da informação.. 15
2.7 O objetivo da governança: Criação de Valor. 17
2.8 Categorias de riscos de TI.. 18
2.9 Fatores de Riscos.. 19
2.10 Perspectivas de riscos.. 21
2.11 Relacionamento entre a arquitetura organizacional e a arquitetura de segurança da informação. 23
2.12 Processo de riscos de TI. 27
2.13 Relacionamento entre as práticas de governança. 29
2.14 Visão geral da gestão de riscos. 34
2.15 Etapas de implementação do OBRiM. 35
2.16 Visão da gestão de riscos e a auditoria interna. 37
2.17 Gestão de riscos e a sustentação dos processos de decisões. 38

3.1 Formas de classificação das pesquisas científicas.. 54
3.2 Estruturação da pesquisa. 55

4.1 Pilares do IATD/RCS.. 58
4.2 Estrutura organizacional do IATD/RCS. 61
4.3 Fluxo detalhado Análise do Ecossistema Organizacional IATD/RCS. . . . 64
4.4 Ciclo de decisões IATD/RCS.. 70

5.1 Organograma da instituição.. 73
5.2 Planejamento estratégico.. 74
5.3 Estrutura do formulário SIPOC. 76

5.4 Capacidade de sustentação orçamentária.. 78

A.1 Processo de elaboração do PDTI 91
A.2 Nível de dependência das áreas aos sistemas 92
A.3 Sistemas utilizados pelas áreas de negócio 93
A.4 Sistemas que causam maior impacto 94
A.5 Sistemas mais importantes para a organização 95
A.6 Distribuição do 13 sistema obtidos pela simulação 96
A.7 MAHP dos sistemas mais utilizados 97
A.8 MAHP dos sistemas que causam maior impacto em caso de indisponibilidade 98
A.9 MAHP dos sistemas mais importantes para a organização 99
A.10 Hierarquia dos sistemas por critérios de avaliação mediante a aplicação do MAHP 100
A.11 Sistemas que satisfazem simultaneamente os critérios de avaliação e sistemas mais relevantes para a instituição 101
A.12 Comparação entre os sistemas mais relevantes identificados pelo Diagrama de Pareto e pelo método MAHP 102

Capítulo 1

Introdução

Neste capítulo são apresentadas as abordagens iniciais, contextualização e a caracterização do tema da pesquisa. São apresentados os aspectos de formulação do problema, os objetivos e hipóteses da pesquisa, a justificativa que indica a contribuição do estudo para a construção do conhecimento e sua utilidade para a prática profissional. Por fim, será demonstrada a estruturação que descreve como o trabalho de pesquisa está organizado.

1.1 Contextualização

A análise de riscos tornou-se uma área cada vez mais importante pelo fato de decisões serem tomadas em cenários de incertezas, sendo estas de diversas fontes e abrangendo riscos das mais variáveis formas[11].

Seja decidir o caminho de retornar para casa ou a escolha do caixa que será usado ao ir ao banco, todos os dias há necessidade de decisões que envolve perdas e ganhos. Apesar de aspectos como o tempo possuir relevância na vida cotidiana, há uma compreensão limitada quando observadas as perspectivas para tomada de decisões quando os riscos estão envolvidos no processo. A teoria da perspectiva é a mais popular para decisões baseadas em riscos. [16].

Independente do papel exercido em uma organização, o processo de tomar decisões é uma atividade de grande importância e a capacidade de executá-la é uma das competências básicas e deve ser praticada constantemente. Porém, pode-se sugerir que existe pouca habilidade em tomar decisões, principalmente as que possuem caráter complexo e de nível estratégico. Mais de cinquenta por cento das decisões são desprezadas e julgadas impróprias pelos tomadores de decisões. Tal fato se dá por conta da compreensão sobre o que realmente é a tomada de decisões e a forte influência das habilidades cognitivas sobre a forma como são praticadas, podendo levar a práticas defeituosas[43].

Segundo Venkat[28], os seres humanos evoluíram muito pouco quando tratados as aspectos de decisões baseadas em riscos. Decisores têm a tendência de avaliar suas opções em relação a um ponto de referência, ou seja, se eles podem realizar ganhos sem nenhum risco. Dessa forma, tomar decisões ótimas em situações complexas de riscos, como aquelas em que os pontos de referência ou os critérios que determinam a decisão são variáveis demais para a capacidade cognitiva dos indivíduos, se torna uma tarefa praticamente impossível e tão rudimentar quanto a forma que os primatas decidem. Desta maneira, pode-se esperar que os seus resultados sejam tão precários quanto aqueles provenientes das decisões tomadas por macacos, além de apoiados em um apelo na intuição [28].

Para Benaroch[9], o comportamento para os processos de decisões costumam seguir modelos intuitivos, levando a práticas com baixo retorno e contraproducentes. Por isso, o uso de técnicas de análise multicritérios apoiam na construção de informações mais consistentes acerca do nível de impacto dos sistemas para a organização. Dessa forma, é possível evitar investimentos contraproducentes baseados em modelos intuitivos, possibilitando a priorização das ações direcionadas aos sistemas mais críticos e oportunizando a economicidade em contratações [9].

Faggini[15] descreve que os modelos empíricos/intuitivos para tomada de decisão assumem que os tomadores de decisões atuam com racionalidade ao fazer escolhas, objetivando otimizar sua utilidade ou lucro de tal ação. Em uma observação mais formal, os tomadores de decisões possuem preferências transitivas e consistentes procurando maximizar a utilidade que derivam de suas escolhas, sujeito a várias restrições e atuando conforme o senso comum observado. Tal senso está baseados no conceito que, dado um conjunto de alternativas, escolha o melhor.

Já lucarelli[31] demonstra que, de uma forma geral, os indivíduos simplesmente não seguem uma estratégia de minimização de riscos por visarem uma condição de eficiência pessoal. Isso é motivado quando o "valor"fornecido pelo dinheiro é mediado ou ponderado pelo reforço emocional do indivíduo, o que apoia a importância de uma perspectiva muito "pessoal"na compreensão dos comportamentos de risco.

Um dilema enfrentado por muitas organizações é encontrar uma forma de estruturar investimentos de Tecnologia da Informação - TI para controlar o risco de forma otimizada, possibilitando maximizar o valor das estratégias usadas. Investimentos em sistemas empresariais e armazenamento de dados envolvem altos riscos e alto retorno que podem criar diversas opções das visões estratégicas para decisões.[8].

Quando observados os conceitos usados como referências de riscos, há um senso comum apoiado em dois direcionamentos principais. O primeiro é a definição da ABNT NBR ISO/IEC 27005:2011[3] onde riscos é o efeito da incerteza sobre os objetivos que se desejam alcançar em uma organização. O segundo é a definição descrita na ABNT NBR

ISO 31000:2009[2] onde risco é a relação entre os eventos potenciais e as suas consequências ou avaliando a combinação da consequência de um evento (incluindo mudanças nas circunstâncias) e a probabilidade de ocorrência associada. Assim, a incerteza entende-se como estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, conhecimento, sua consequência ou sua probabilidade.

É possível observar um conjunto de eventos que, depois de ocorridos, as pessoas procuram fazer com que pareçam mais previsíveis do que realmente seriam. Esse conjunto de eventos improváveis, chamados de Cisnes Negros, possuem características como a imprevisibilidade e a extensão do impacto causado. Com a ausência da consciência prévia destes eventos há certa dificuldade de uma avaliação clara das oportunidades [46].

Assim, segundo o The Committee of Sponsoring Organizations of the Treadway Commission - COSO[39], quando observados o nível de aderência da gestão de riscos por parte de altos gestores, é possível identificar que o acompanhamento do processo de gerenciamento de riscos não é feito ou é feito de forma ADHOC. Metade dos envolvidos em um estudo desenvolvido pelo COSO informou que os seus conselhos não têm processos formais para analisar periodicamente o nível de eficiência de seus processos de gestão de riscos e os resultados sugerem que, embora muitas empresas tenham um processo para prover informações sobre risco, em poucas delas este processo é suficientemente definido e rigoroso[39].

1.2 Definição do problema

Apesar da gestão de risco ser um conceito muito discutido por meio de artigos, livros, normas e *frameworks*, há uma lacuna na literatura sobre como a gestão de riscos pode apoiar aos gestores de TI na criação modelos de decisões que possam ser usados para apoiar em suas decisões estratégicas, reduzindo a abordagem intuitiva em tal processo, apoiado pelo uso de novas abordagens sobre riscos e suas consequências.

Pretende-se demonstrar como o modelo desenvolvido para atender aos requisitos de um projeto de apoio aos processos decisórios, que observe a transversalidade das atividades organizacionais, apoiados por uma visão de riscos, tendo como foco a definição de fronteiras através dos limitadores estratégicos e operacionais e na observação da capacidade e a sustentação do ecossistema de sustentação dos processos de negócios.

1.3 Objetivos do Trabalho

Esta seção apresenta os objetivos do presente trabalho e a contribuição esperada com seu desenvolvimento.

1.3.1 Objetivo Geral

Propor um modelo que, a partir da análise das fronteiras, da capacidade e da sustentação dos processos de negócios, que apoie nos processos decisórios de gestores de TI, aumentando a assertividade e maximizando os resultados de investimentos em TI.

1.3.2 Objetivos Específicos

1. Demonstrar a lacuna existente na literatura para o uso da gestão de riscos como ferramenta de apoio aos processos decisórios de gestores de TI;
2. Identificar as características do comportamento humano e seus efeitos para os processos decisórios.
3. Identificar como novas abordagens de riscos podem modificar o processo decisório dos gestores de TI para o planejamento de infraestrutura de TI.
4. Demonstrar o impacto do uso do modelo proposto nos projetos desenvolvidos no Ministério do Planejamento, Desenvolvimento e Gestão;

1.4 Justificativa do Trabalho

Enquanto conceito, riscos podem ser descritos como o efeito da incerteza sobre os objetivos do negócio, segundo a definição da ABNT NBR ISO/IEC 27005:2011[3]. Segundo a ISO 31000 ABNT NBR ISO 31000:2009, risco é a combinação de consequências de um evento e a probabilidade de ocorrência associada, e que a incerteza é a deficiência, mesmo que de forma parcial, das informações de um evento, devendo ser observadas as deficiências para a compreensão, o conhecimento, a consequência e a probabilidade do evento[2].

Em relação ao domínio sobre a incerteza, quanto maior o tempo entre a decisão e suas consequências, maior será o campo da incerteza para a decisão. Ainda no campo das decisões, descreve que o entendimento e o conhecimento de como a incerteza pode ser mensurada são relevantes, e que a incerteza é uma das principais justificativas para a dificuldade de decisões nos negócios, além de não ser usada para diferenciar o que era desconhecido ou simplesmente improvável. Assim, define que a incerteza é consequência da forma como um indivíduo percebe o mundo[30].

O uso clássico da gestão de riscos, somados às características humanas para o processo de tomada de decisões, geram resultados contraditório, observando um ponto de extrema relevância para que indicadores de riscos retratem muito mais a realidade do ecossistema institucional. Tal fenômeno ocorre por haver um forte apelo no comportamento empírico e a confiança nessa lógica, fortemente baseada apenas na intuição, pode levar a práticas

de gerenciamento de risco subótimo ou contraproducentes. Assim, a gestão de riscos deve ser complementada com o uso de modelos de opções reais formais, permitindo uma melhor compreensão dos alertas de riscos a serem seguidos e combinados, a fim de efetivamente enfrentar os riscos mais críticos[9].

A questão-chave para tomada de decisões baseadas em riscos tem sido a capacidade de avaliação de risco e teoria das probabilidades para capturar tais eventos, questionando sobre a profundidade da significância do cisne negro em relação ao risco, incerteza e probabilidade. Assim, indaga se um cisne negro é apenas um evento extremo com uma probabilidade muito baixa ou é um evento mais surpreendente, como por exemplo, um desconhecido, propondo que a observação desses eventos pode afetar a dimensão do conhecimento sobre os riscos[6].

É melhor evitar o perigo com um modelo alternativo que possa eliminar ou reduzi-lo usando uma abordagem inerentemente mais seguros. Além disso, há uma descrição para retratar o risco relacionado a um tipo de cisnes negros, ou seja, surpresas em comparação com as crenças dos especialistas e analistas envolvidos na avaliação de risco. Uma lista de tais eventos pode ser criada por uma equipe de análise especial com o objetivo de realizar uma revisão de todos os argumentos possíveis e provas para a ocorrência de eventos que têm baixo risco por referência às três dimensões sendo a probabilidade atribuída, as consequências, e a força do conhecimento. A questão é observar se uma surpresa (cisne negro) ainda pode ocorrer[26].

Por fim, quanto ao comportamento humano para as decisões baseadas em riscos, os mecanismos que conduzem o comportamento em seres humanos podem ser evolutivamente antigos e se estende amplamente em toda a ordem dos primatas. Dessa forma, demonstram que seres humanos possuem uma aversão natural aos riscos, quando estes estão relacionados à ganhos e um natural apego aos mesmos quando perdas são descritas, mudando a forma como são tomadas as decisões[28].

Sendo assim, observados os aspectos de decisões apresentados sobre decisões estratégicas organizacionais baseadas em riscos, pela forma como o uso de tais aspectos são afetados pelo comportamento humano faz com que um estudo mais amplo para o desenvolvimento de uma pesquisa que demonstrem alguns processos de decisões que reduzam o apelo intuitivo e que promova economicidade seja desenvolvido.

1.5 Estrutura do trabalho

Este trabalho está estruturado em quatro capítulos. O primeiro capítulo trata da introdução, onde foi delimitada a caracterização do tema, o problema e os objetivos da pesquisa, as hipóteses e a justificativa. No Capítulo 2 são abordados conceitos inerentes

do problema apresentado. O Capítulo 3 descreve a metodologia de pesquisa. O Capítulo 4 demonstra a estrutura de um modelo de apoio a tomada de decisões. O Capítulo 5 demonstra a execução do estudo de caso e, por fim, o Capítulo 6 são apresentados os resultados obtidos e tratadas as considerações finais.

Capítulo 2

Revisão da literatura

A revisão está estruturada sobre dois tópicos: (*i*) Conceitos e princípios da gestão de riscos;(*ii*) Complexidade do processo de tomada de decisão. De forma a facilitar a compreensão do objeto deste estudo, a apresentação de cada tópico está ordenado de forma estruturada.

2.1 Conceitos e princípios da gestão de riscos

Vários modelos para gerenciamento de riscos foram desenvolvidos e adotados como resultado de estudos sobre o efeito e controle de riscos aos processos organizacionais. Os modelos desenvolvidos é voltado para a identificação e tratamento das diferentes formas de riscos, avaliando a importância e impacto relativo para os processos organizacionais. Essa seção apresenta os principais modelos de análise de riscos em diversos contextos utilizados como ferramenta de controle de riscos organizacionais e de TI.

Aos aspectos que tratam de conceitos, há dois caminhos básicos que podem ser trilhados. O primeiro define risco como o efeito da incerteza sob os objetivos organizacionais, sendo que o efeito deve ser entendido como um desvio em relação ao esperado, podendo ser positivo e/ou negativo [3]. Para o segundo caminho, risco é a combinação entre a probabilidade da ocorrência de um evento e sua consequência para os processos de negócios[1] e [2].

Diversos *frameworks* e guias de referência sobre gestão de projetos, governança de Tecnologia da Informação (TI), gestão e governança organizacional definem risco usando um dos caminhos apresentados, podendo ser observado que:

- Risco é a combinação entre a probabilidade de um evento e sua consequência, sendo risco de SIC o potencial de uma ameaça explorar vulnerabilidades de um ativo ou conjunto de ativos e, desse modo, causar dano à organização[35];

- Risco de TI associa o risco aos objetivos de negócio com o uso, propriedade, operação, envolvimento e influência da adoção de TI na organização, consistindo em eventos relacionados com a TI e que podem afetar ao negócio das organizações, podendo ocorrer com frequência o impactos incertos e afetar o cumprimento das metas e objetivos estratégicos[17];

- Riscos são eventos que possam afetar afetar a entidade em seus objetivos estratégicos e negócios. Incertezas representam riscos e oportunidades, com potencial para destruir ou agregar valor, sendo risco uma parte inerente ao cotidiano do negócio e da estratégia organizacional[38];

- Risco é um possível evento que pode causar danos ou perdas, ou afetar a capacidade de uma organização alcançar seus objetivos. Um risco é medido pela probabilidade de uma ameaça, a vulnerabilidade do ativo a essa ameaça e o impacto que teria se ocorresse. O risco também pode ser definido como incerteza do resultado, e pode ser usado no contexto para medição da probabilidade de resultados positivos, bem como resultados negativos[29];

- Risco do projeto é um evento ou condição incerta que, se ocorrer, provocará um efeito positivo ou negativo em um ou mais objetivos do projeto tais como escopo, cronograma, custo e qualidade[24];

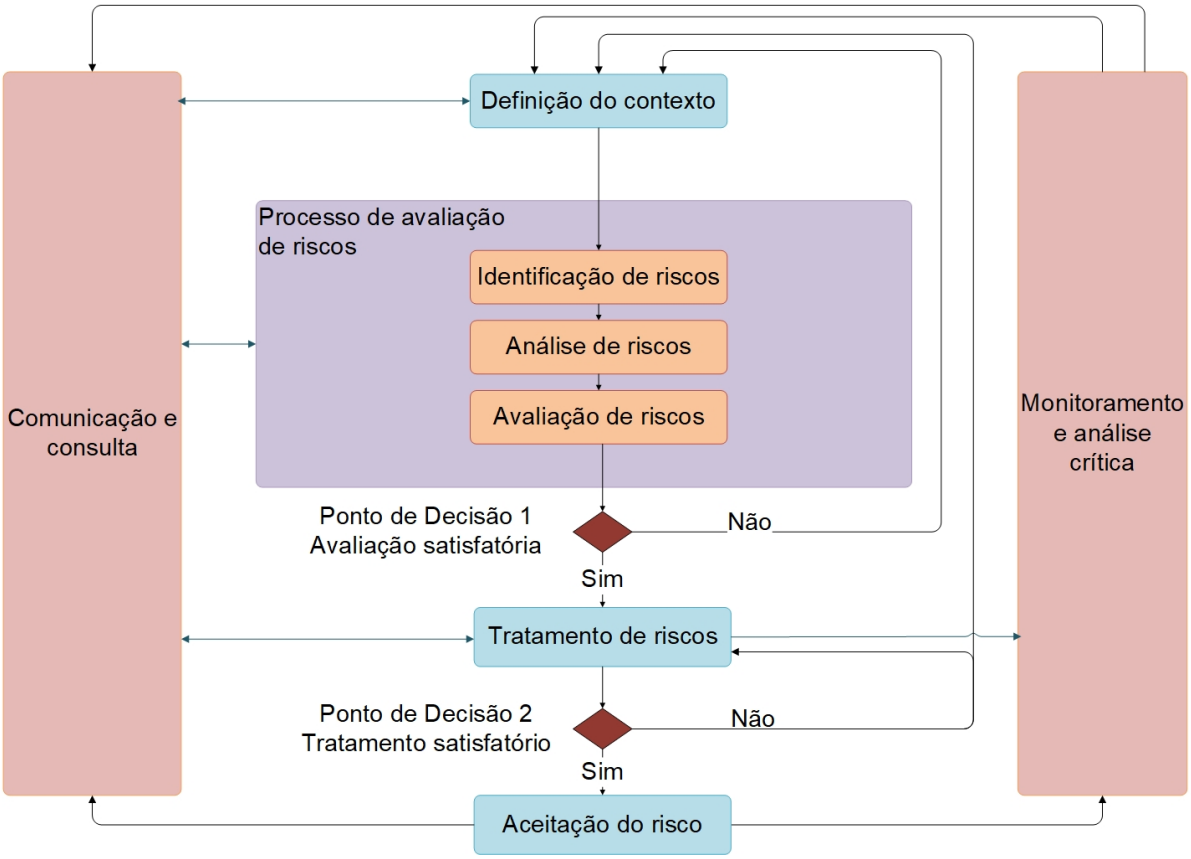
- Risco é o efeito que a incerteza tem na consecução dos objetivos de negócios. Dada a quantidade limitada de informações para tomar decisões de negócios, a incerteza está preocupada com a previsão de futuros resultados. Apesar da crença de que informações de melhor qualidade possibilite uma tomada de decisão de melhor qualidade, a previsibilidade nunca poderá ser perfeita. Risco pode ser visto em nível estratégico a longo prazo (direcionamento global de negócio), a médio prazer em nível tático (projetos e programas) e no nível operacional em processos e práticas operacionais cotidianas e nas decisões[23];

- Risco é qualquer evento para o qual não se tem certeza de forma prévia, ou seja, antes do tempo de ocorrência, sendo possível encontrar duas características básicas onde a primeira é a exclusão de eventos que já ocorreram e foram observados e a segunda tem o tempo como a característica fundamental do risco, enfatizando a dimensão temporal do risco[11].

A gestão de riscos de segurança da informação deve possuir alinhamento com o processo de gestão de riscos corporativos. Isso demonstra que as diretrizes definidas nas norma de segurança da informação, devem ser complementares ao processo de gestão de riscos organizacionais, para a qual haverá outras matérias que integram a visão de riscos

institucionais, como riscos financeiros, riscos de investimentos, de perdas nos processos produtivos, dentre outros. A Figura 2.1 demonstra como as atividades da gestão de riscos estão estruturadas[3].

Figura 2.1: Interação do processo de gestão de riscos.



(Fonte: Adaptado de [3])

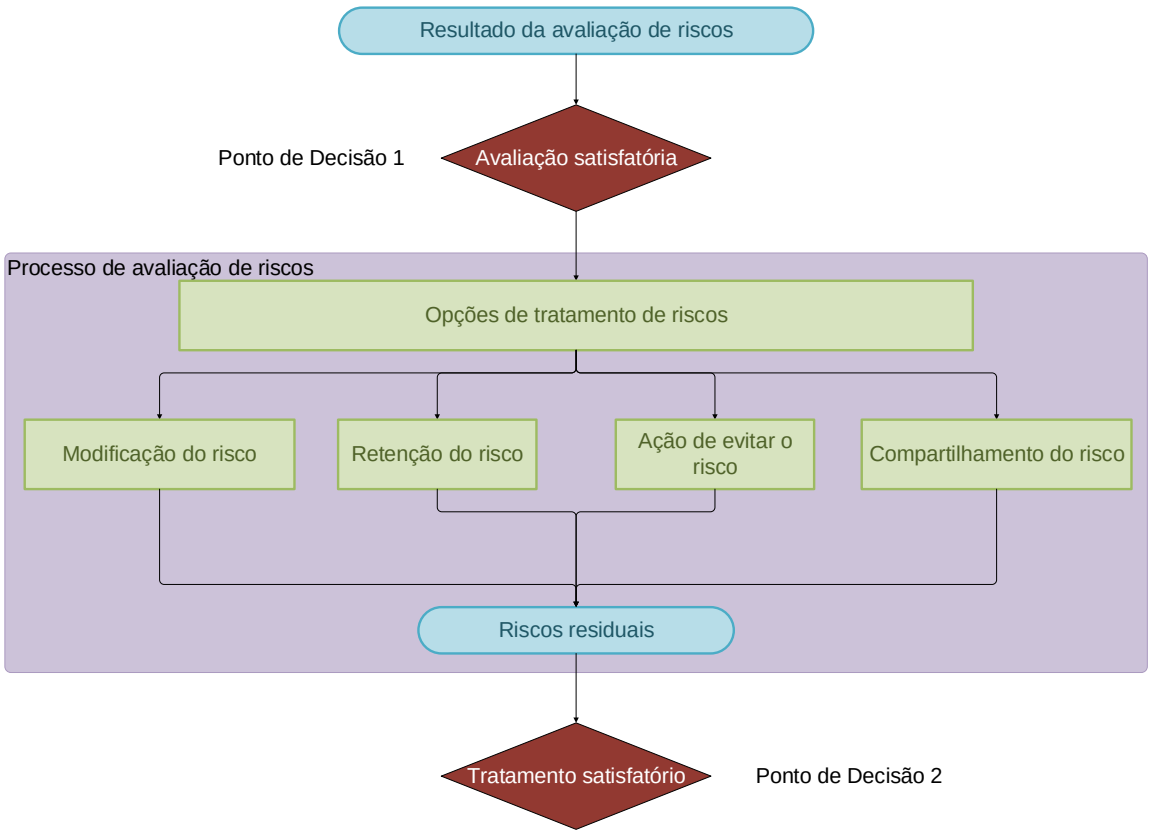
A Figura 2.1, demonstra as 5 macro atividades da gestão de riscos que visam desde o entendimento organizacional através do estabelecimento do contexto até o tratamento de riscos. Se considerados os conceitos e princípios descritos, a gestão deve avaliar os aspectos que direcionam os processos de decisões e não objetiva a definição de controles. O processo de gestão de riscos de segurança da informação possui um caráter iterativo nas etapas de avaliação de riscos e/ou para o tratamento de riscos, possibilitando o detalhamento e aprofundamento da avaliação em cada ciclo de execução. Assim, é possível minimizar o tempo e esforço na identificação de controles e assegurando que riscos de alto impacto ou de alta probabilidade possam ser adequadamente avaliados. O tratamento de riscos está estruturado em um ciclo de avaliação para o tratamento de riscos, decidindo se os níveis de riscos residuais são aceitáveis, promovendo um novo tratamento de riscos em caso de riscos não aceitáveis e avaliando a eficácia do tratamento proposto. O detalhamento de

cada atividade do processo de gestão de riscos de segurança da informação e as decisões sobre o processo de avaliação de riscos, somados aos aspectos de tratamento do risco devem ser documentados[3].

Analisar risco é um processo que envolve a compreensão e determinação do nível de riscos, sendo a base para a avaliação e para as decisões sobre o tratamento de riscos. Comunicação e consulta, é um processo de impacto para as decisões que envolvem o tratamento e aceitação de riscos através de influência, ao invés de poder, sendo uma entrada para o processo de tomada de decisões, e não uma tomada de decisões em conjunto[3].

O tratamento de risco está embasado em evitar o risco através da decisão de não iniciar ou descontinuar a atividade de origem do risco, sendo possível observar em seu processo dois pontos de decisões que são parte das atividades deste processo. O primeiro está no final da avaliação de riscos para determinar se houve uma avaliação satisfatória e o segundo pós tratamento, para determinar o nível de satisfação para o tratamento de riscos[3].

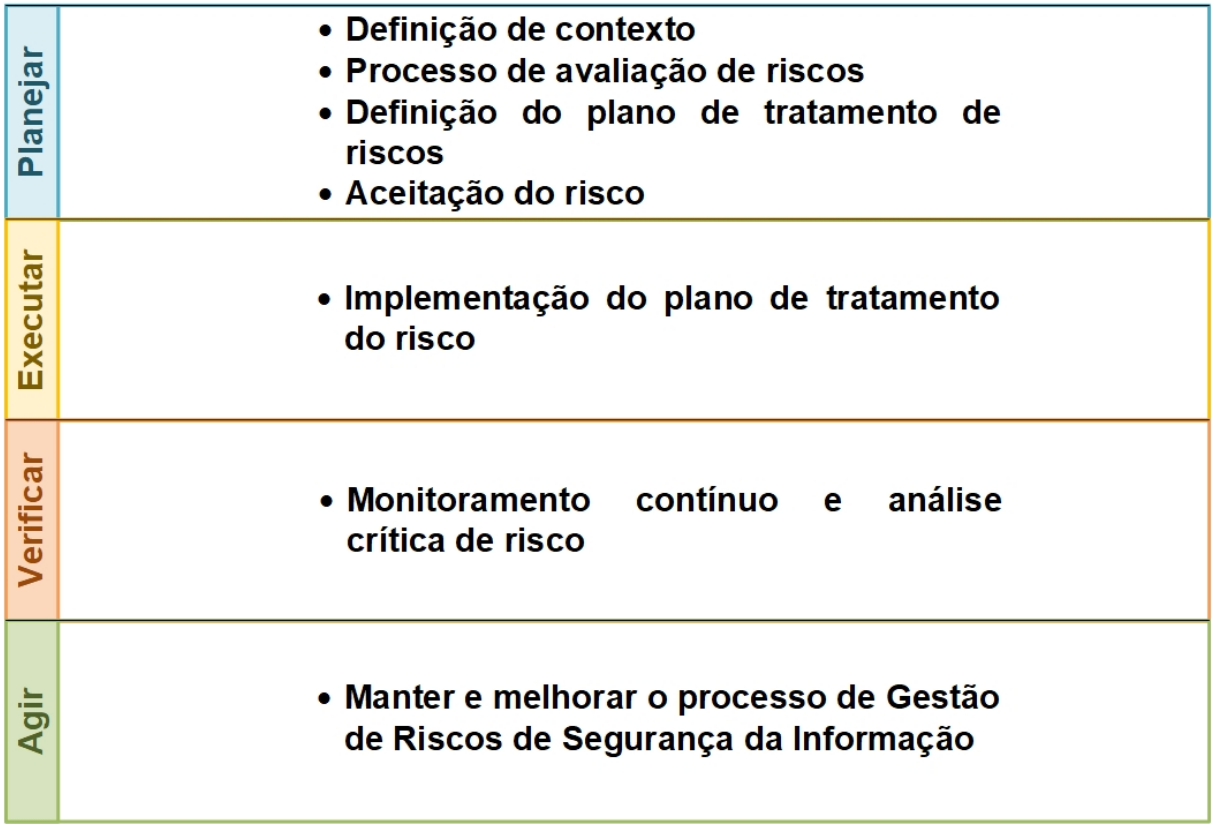
Figura 2.2: Atividade de tratamento de risco.



(Fonte: Adaptado de [3])

A Figura 2.2, demonstra que o processo decisório para o tratamento de risco é inerente ao processo de gestão de riscos e para tal, é necessário que sejam levadas em consideração a percepção e as formas mais adequadas de comunicação com as partes afetadas. Os gestores devem considerar os riscos improváveis, porém graves e a implementação dos controles, definição dos limites e do contexto do sistema de gestão de segurança da informação - SGSI devem ser apoiados por um processo de gestão de riscos, já que estes devem ser baseados em riscos[3].

Figura 2.3: Alinhamento do processo SGSI e do processo de gestão de riscos 27015.



(Fonte: Adaptado de [3])

A Figura 2.3 mostra que é possível traçar um alinhamento entre o ciclo PDCA do SGSI e o processo de gestão de riscos, apoiando na construção de um processo uníssono[3].

A gestão de riscos possibilita a uma organização o aumento da probabilidade de atingir seus objetivos, viabilizando a identificação e tratamento dos riscos através de toda a organização e ao estabelecimento de uma base confiável para a tomada de decisões e o planejamento institucional, melhorando o aprendizado organizacional e aumentando a resiliência e a governança[2].

Sendo o risco o efeito da incerteza para os objetivos organizacionais, onde, incerteza é a deficiência, mesmo que parcial, das informações relacionadas a um evento, devem ser observadas as deficiências para a compreensão, o conhecimento, a consequência e a probabilidade do evento[2].

A gestão de riscos contribui para o alcance dos objetivos organizacionais e para melhoria do desempenho da eficiência nas operações e à governança. Dessa forma, a gestão de riscos não é uma atividade adhoc, separada das demais atividades e processos da organização. Ela é parte integrante de todos os processos organizacionais, incluindo o planejamento estratégico e demais processos de gestão de projetos e mudanças. Assim, torna-se parte das tomadas de decisões, apoiando aos gestores e tomadores de decisões a fazerem escolhas conscientes[2].

A gestão de riscos trata de forma explícita a incerteza, levando em consideração a natureza e como ela pode ser tratada. Assim, deve haver uma abordagem sistêmica e estruturada para que contribua com a eficiência e para os resultados comparáveis e confiáveis. Dentre outras coisas, a gestão de riscos deve considerar fatores humanos e culturais, os contextos internos e externos e deve ser dinâmica, iterativa e capaz de reagir a mudanças e deve ser um ponto de facilitação para a melhoria contínua da organização sendo aplicada em todas as tomadas de decisões, seja qual for o nível de sua importância ou significância[2].

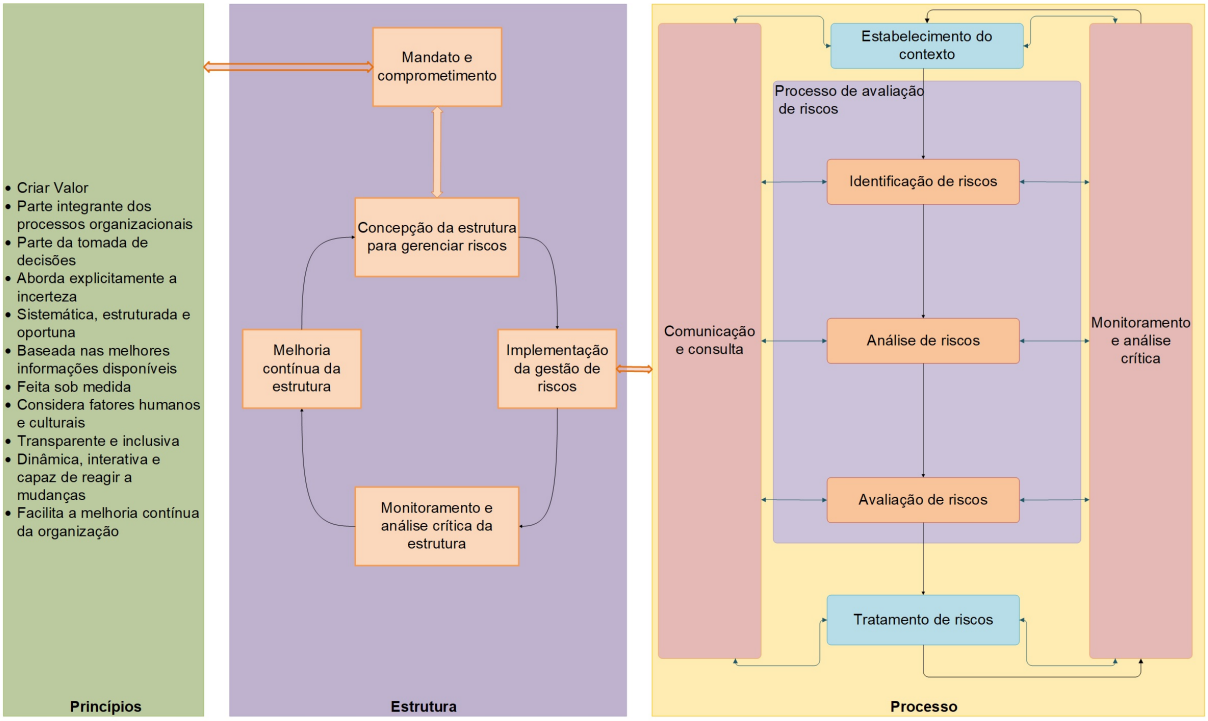
Para que seja eficiente, a gestão de riscos deve possuir alinhamento de seus objetivos com os objetivos e estratégias da organização, alinhando seus indicadores de desempenho com os indicadores de desempenho da organização e incorporada a todas as práticas e processos organizacionais, tornando-na parte integrante de todos os processos. A gestão de risco deve ainda ser absorvida no desenvolvimento de políticas, análise crítica e no planejamento estratégico e de negócios. Por isso, a gestão de riscos deve assegurar que a tomada de decisões para o estabelecimento dos objetivos organizacionais esteja alinhado com os resultados dos processos de gestão de riscos, assim como, os processos organizacionais justaponham à política e aos processo de gestão de riscos[2].

O processo de gestão de riscos deve ser parte integrante da gestão e adaptado aos processos de negócios organizacionais, sendo aplicada em todas as tomadas de decisões, já que estas envolvem explicitamente a consideração de riscos e o processo e a estrutura de governança são baseados na gestão de riscos a qual é considerada como essencial para o alcance dos objetivos da organização[2].

Os componentes da gestão de riscos devem ser representados dentro dos processos-chave para a tomada de decisão na organização, fornecendo a base para a governança eficaz através de uma base sólida da gestão de riscos na organização. Assim, a gestão de riscos é vista como um ponto central para os processos de gestão organizacional tendo em

vista o efeito da incerteza sobre os objetivos[2].

Figura 2.4: Relacionamento entre os princípios, estrutura e processo da gestão de riscos.



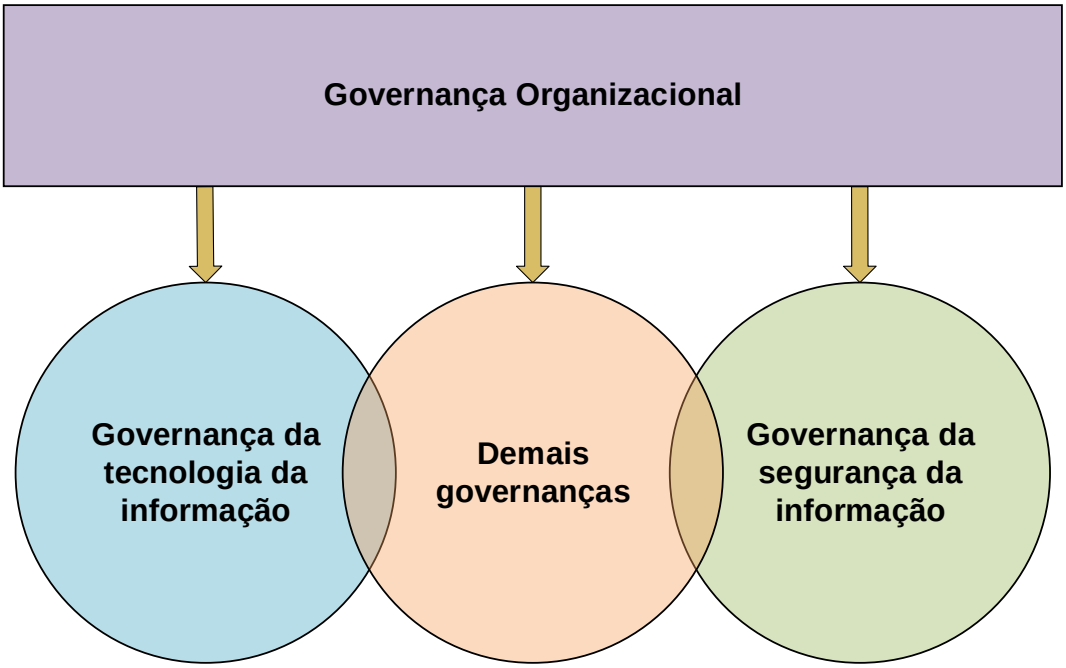
(Fonte: Adaptado de [2])

É necessário o entendimento dos princípios para que a gestão de riscos tenha efeito e traga retornos para as organizações. Além de parte integrante da gestão e dos processos de negócios organizacionais, a gestão de riscos deve ser parte parte integrante de todos os processos operacionais em busca de uma visão clara das incertezas, de forma dinâmica e capaz de reagir à mudanças, acompanhando o dinamismo do ecossistema organizacional, conforme Figura 2.4. A escolha de controles e medidas de proteção à impactos deve ser visto como consequência e não causa, haja vista que a gestão de riscos deve ser feito sob medida e, para isso, é necessário que as fronteiras organizacionais sejam estabelecidas e compreendidas[2].

A alta gestão é a maior responsável pelas decisões de uma organização, apoiados por processo de governança organizacional, sendo importante para as decisões que haja uma visão holística e integrada da governança de segurança da informação com o modelo de governança organizacional. Conforme demonstrado na Figura 2.5, diversos modelos de governança formam um conjunto de componentes integrantes da governança organizacional, enfatizando a importância do alinhamento com os objetivos de negócios, perfilando os objetivos e estratégias de segurança da informação com os objetivos e estratégias dos

negócios organizacionais. A governança de segurança da informação deve ser fundamentada em decisões baseadas em riscos e a gestão de riscos da informação deve ser integrada à abordagem de gestão de riscos da organização, tendo como base para o estabelecendo da estratégia de investimentos para segurança da informação os resultados de negócios. A governança de segurança da informação deve compatibilizar os requisitos de negócios organizacionais com os requisitos de segurança da informação, otimizando os investimentos de segurança da informação no apoio aos objetivos da organização. Dessa forma, a governança de segurança da informação deve ter seu desempenho mantido de forma à atender aos requisitos de negócios atuais da organização, analisando o desempenho em relação ao impacto no negócio e não simplesmente avaliando a eficácia e eficiência dos controles de segurança, associando o desempenho de segurança da informação com os desempenhos dos negócios organizacionais[4].

Figura 2.5: Relação entre as governanças e estrutura da governança organizacional.

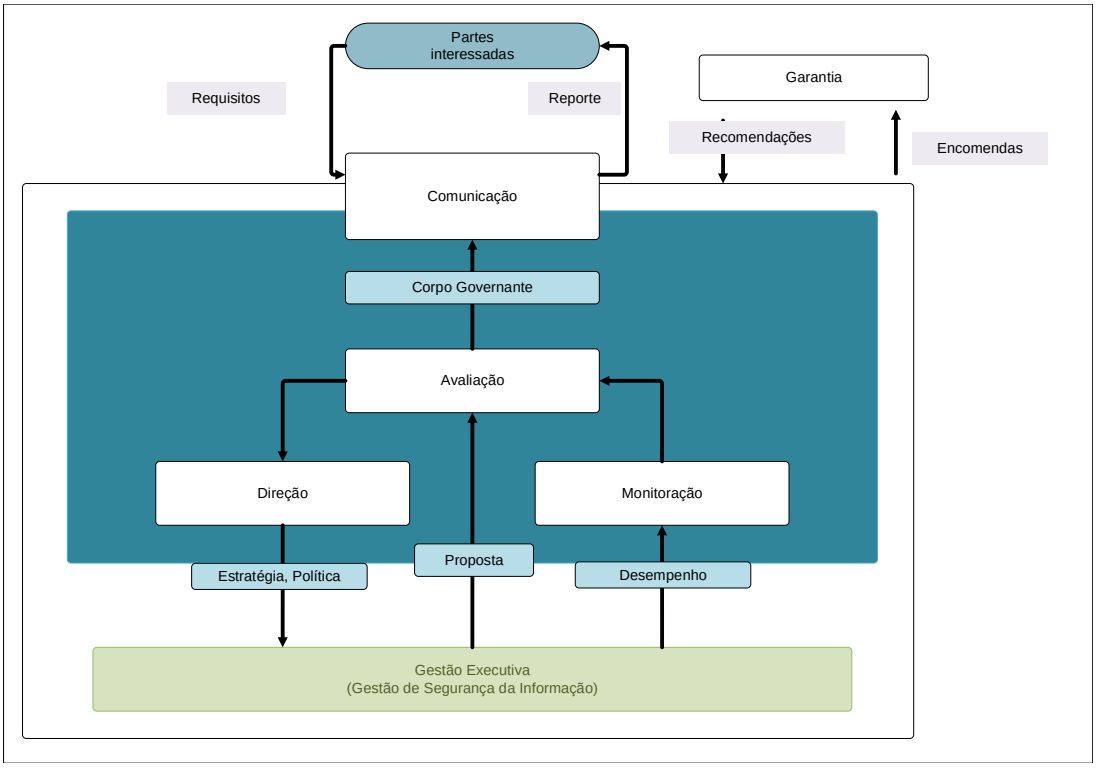


(Fonte: Adaptado de [4])

A Figura 2.6 demonstra o processo de governança de segurança da informação no qual a avaliação considera os objetivos de segurança da informação baseados nos processos,

determinando os ajustes necessários para otimizar o alcance dos objetivos estratégicos organizacionais. Assim, o corpo diretivo deve que as iniciativas de negócios estejam considerando as questões de segurança da informação, respondendo aos desempenhos de segurança da informação, garantindo que a segurança da informação suporte e sustente os objetivos de negócios organizacionais. O corpo diretivo deve, no processo de direção, determinar o apetite de riscos organizacionais, alinhar os objetivos de segurança da informação com os objetivos de negócios, promovendo uma cultura positiva de segurança da informação. Já no monitoramento, o corpo diretivo avalia o alcance dos objetivos estratégicos, avaliando a eficácia e considerando as alterações no ambiente de negócio e seus impactos sobre o risco de informação. Para isso, as métricas de desempenho devem ser fundamentadas em uma perspectiva de negócios, demonstrando os impactos sobre toda a organização[4].

Figura 2.6: Implementação da governança de segurança da informação.



(Fonte: Adaptado de [4])

As definições de aceitação dos riscos devem ser baseadas em perspectivas de perdas, como por exemplo, a perda de vantagem competitiva, de interrupções operacionais, de danos à reputação e perdas financeiras. Uma gestão de riscos de segurança da informação adequada para a organização, é aquela que esteja integrada à abordagem global de gestão

de riscos organizacionais, com base nos resultados em negócios, promovendo a harmonia entre os requisitos de negócios e os da segurança da informação. Dessa forma, é necessário que a governança de segurança da informação estabeleça uma estratégia de investimentos otimizado pela integração entre os processos atuais da organização e a segurança da informação, cumprindo os requisitos internos e externos[4].

Além das exigências por desempenhos, investidores de organizações e stakeholders estão cada vez mais envolvidos com o gerenciamento de riscos nas organizações. Tal informação ratificada por um estudo realizado pela Ernst&Young em 2008 que revelou a penalização por parte de investidores e stakeholders de empresas que não estão envolvidas com a eficiência da gestão de riscos. Nesse cenário, 61% dos investidores e stakeholders entrevistados evitaram investimentos em tais empresas e, além disso, 82% dos entrevistados afirmam que organizações que atendem de forma eficiente a gestão de riscos devem ter o valor de suas ações valorizados como forma de premiação. Tal comportamento é decorrente dos escândalos corporativos do início do século XXI, assim como, um maior cuidado para a implementação de controles eficientes de TI em suas operações, decorrente do aumento das operações automatizadas[41].

Toda organização precisa de uma observação transversal de riscos que extrapole as questões técnicas para evitar uma falsa sensação de segurança ou de urgência. Uma observação transversal permite uma revisão adequada de aspectos importantes como o apetite e a tolerância ao risco, evitando que se tenha somente pontos de vista de risco isolados ou de forma parcial. Os gestores precisam identificar e entender o impacto agregado do risco para toda a organização e não de forma isolada nos ativos de TI. A gestão de riscos perde valor quando uma visão parcial do risco é obtida e só pode entregar todo potencial de resultados se o risco for gerenciado em toda a organização. Existem obstáculos que impedem uma visão coerente e transversal de riscos, podendo citar a imaturidade em termos de gerenciamento de processos, levando à falha da medição do desempenho da gestão de riscos e os seus resultados, proporcionando a incapacidade de ter uma visão precisa dos fatores de risco e a falha na compreensão e a capacidade de detectar uma ocorrência e promover uma resposta satisfatória[17].

A governança tem o propósito a criação de valor para qualquer instituição obtendo benefícios com o aprimoramento de recursos ao otimizar riscos, podendo assumir várias formas, como otimização dos serviços para entidades públicas. É possível observar diferenças claras entre a governança e a gestão. A governança está relacionada à garantia do alcance dos objetivos de negócios através da avaliação das necessidades, condições e opções das partes interessadas. Dessa forma, a governança estabelece a direção através da priorização e tomada de decisão e acompanha o desempenho, conformidade e progresso em relação a direção e objetivos definidos. Em grande parte das empresas, a governança

está sob a responsabilidade de um conselho administrativo liderado por um presidente. É necessário que haja a otimização do risco como parte dos arranjos de governança implantados e que as informações de risco sejam incluídas no processo de tomada de decisão e, para isso, os processos e função de risco deve ser governada, fornecida com direção e monitorada. Levando em consideração as diversas partes interessadas existentes em uma organização, criar valor torna-se um processo conflitante, haja vista o entendimento e interesses dessas partes. Assim, os componentes inerentes a otimização de riscos para criação de valor demonstram que ela é parte essencial de qualquer sistema de governança, não podendo ser vista de uma forma isolada, tendo as ações para gerenciamento de riscos como ponto de influência para os benefícios e otimização de recursos, conforme demonstrado na Figura 2.7. O processo de gestão planeja, executa, constrói e monitora as atividades, de acordo com as definições e direções da governança da organização, para o alcance dos objetivos de negócios. Tal processo é de responsabilidade de de uma gestão executiva, liderada por um CEO[17].

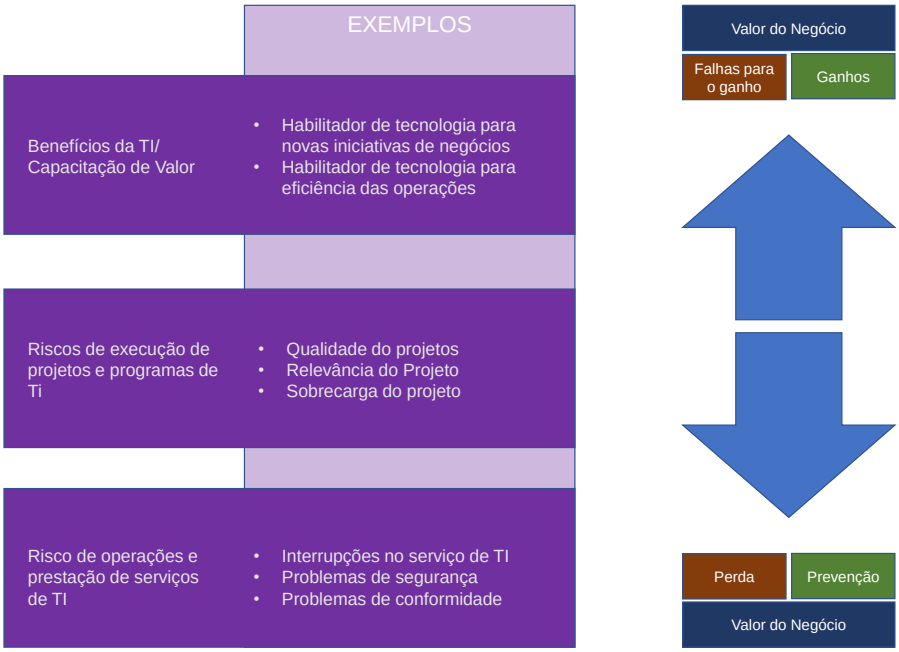
Figura 2.7: O objetivo da governança: Criação de Valor

(Fonte: Adaptado de [17])

Riscos sempre existem, mesmo que não detectados ou reconhecidos pelas organizações

e podem ser categorizados, associando-os a oportunidades de melhoria da eficiência ou eficácia dos processos de negócios, através do uso da tecnologia, às operações e entregas de serviços de TI. Isso demonstra o apoio da TI para melhoria ou implementação de novas soluções sob forma de projetos e programas como parte de uma carteira de investimentos e associando a todos os aspectos do desempenho comercial com o uso de tecnologias, possibilitando a redução de valor para a organização. Nota-se que há uma relação demonstrando que para toda categoria de risco há uma equivalência entre os aspectos negativos (downside) e positivos ou favoráveis (upside), vide Figura 2.8[17].

Figura 2.8: Categorias de riscos de TI.



(Fonte: Adaptado de [17])

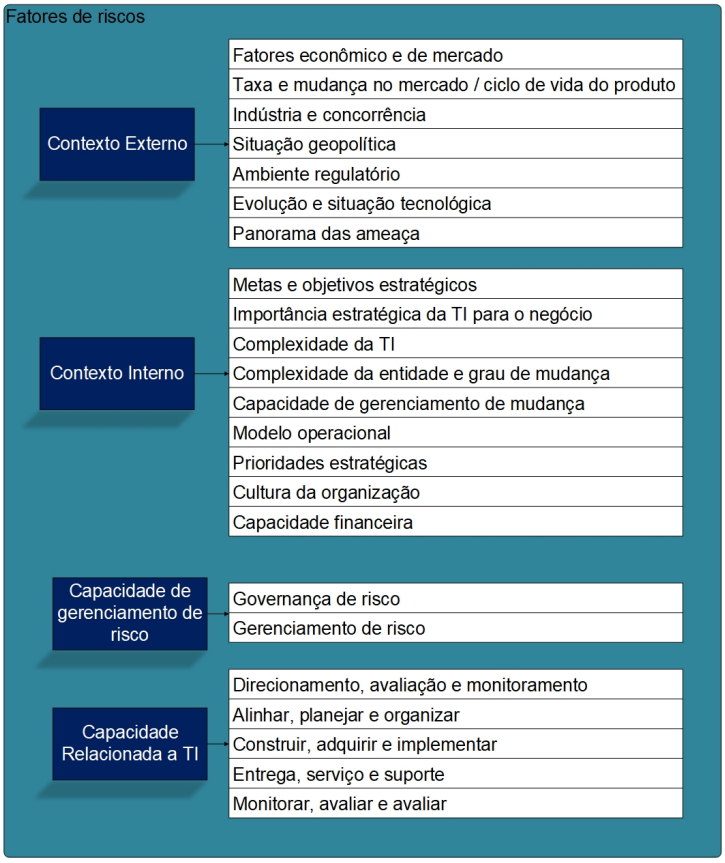
Esta dualidade de perdas e ganhos é importante e deve ser considerada para todas as decisões baseadas em riscos pois, para todas as decisões baseadas em riscos, essa dualidade deve ser presente, tendo em vista que o desenvolvimento dos processos de negócios da organização assumem o apetite de riscos, e por isso nem sempre os riscos devem ser evitados. Quando a informação e a tecnologia são bem governadas oferecem benefícios empresariais e, sendo que o contrário representa prejuízo para a organização [17].

Levando em consideração a existência de três possibilidades para riscos, sendo eles, o riscos inerente, o atual e o residual, o risco considerado é o corrente ou atual. Apesar de uma correlação entre ambos, somente o risco atual é o ponto focal pois este é, na prática, é o usado[17].

Segundo COBIT 5 for RISK[17], Os fatores são as condições que influenciam a frequência e / ou o impacto dos cenários de riscos podem ser classificados em fatores contextuais e fatores de capacidade. Para a identificação e mesmo a descrição de tais fatores, deve-se identificar, dentre outras coisas:

- Quais são as necessidades dos stakeholders e como isso pode ser afetado pelo risco ?
- Qual é a filosofia de risco da empresa (aversão ao risco ou atração ao risco) e, em relação a isso, quais os valores da empresa para tal percepção ?
- Quais são as prioridades estratégicas da organização ?
- Se o uso da TI é um diferencial estratégico, um capacitador funcional ou um processo de suporte ?

Figura 2.9: Fatores de Riscos.



(Fonte: Adaptado de [17])

A capacidade de gerenciamento de riscos é extremamente significante para a frequência e impacto de eventos, haja vista, ser responsável pelas decisões ou a falta de decisões

baseadas em riscos pelos processos de governança e pela presença ou ausência de controles, assim como por sua eficácia. Tal demonstra o quão eficiente é a execução dos principais processos de gerenciamento de riscos, podendo ser medido usando um scorecard de risco. Esse fator está correlacionado com a capacidade da empresa de reconhecer e detectar eventos adversos de risco, portanto, não deve ser negligenciado. A Figura 2.9 demonstra alguns fatores de riscos, de forma clara e ordenada entre contextuais e de capacidade[17].

Há duas perspectivas que demonstram o contexto de riscos, a perspectiva funcional e a de gerenciamento. Tais perspectivas descrevem as necessidades para a criação e sustentação de atividades eficientes e eficazes de governança e gerenciamento de riscos e como o processo de gestão de risco auxilia as atividades de identificação, análise, resposta e informação dos riscos. Para a perspectiva funcional, a otimização de risco é considerado um objetivo chave, considerando a governança e gerenciamento de riscos como parte integrante da governança e do gerenciamento de TI da organização, descrevendo a contribuição para a governança e gerenciamento de risco. A perspectiva de gerenciamento de risco aborda os aspectos de identificação, análise e resposta aos riscos. A Figura 2.10 demonstra a relação entre estas perspectiva e a intersecção entre os processos de gestão e governança de riscos [17].

Figura 2.10: Perspectivas de riscos.

Estapa	Perspectiva da função de risco	Perspectiva da Gestão de Riscos
Fase de configuração da função de risco	A empresa configura uma série de estruturas organizacionais, entre outras, uma função de risco e atribui responsabilidades relacionadas ao risco para algumas funções existentes, por exemplo, o diretor executivo (CEO) e o conselho. A empresa define um orçamento para a função de risco, atribui responsabilidade e responsabilidade a pessoas com as habilidades relevantes, etc.	
Configuração do processo de gerenciamento de risco	A empresa define e mantém um processo de governança de risco, ou seja, COBIT 5 processa EDM03, no contexto de uma estrutura de gerenciamento de risco, que inclui a definição de apetite de risco e níveis de tolerância, promovendo uma cultura consciente de risco, monitorando o perfil de risco, etc. A empresa define e implementa um processo de gerenciamento de risco, ou seja, COBIT 5 processo APO12. Uma política de gerenciamento de risco está escrita	A empresa executa os processos definidos (EDM03 e APO12), que são suportados pelos facilitadores que foram implementados. Com base nos processos listados acima e no apetite de risco definido, a empresa determina que a qualidade de seus aplicativos de software e a segurança do software e hardware são questões de risco principais que requerem ação apropriada. A empresa responde ao risco, ou seja, executa a prática do processo COBIT 5 APO12.06. Esta resposta requer a implementação de todas as ações de resposta ao risco previamente definidas e aprovadas. Na prática, essas ações de resposta ao risco consistem em muitos dos facilitadores COBIT 5, agora aplicados ao ambiente geral de TI.
Operações de gerenciamento de riscos		Em resposta a problemas com a qualidade do software, a empresa implementa / melhora o seguinte: • Processos APO09 e APO10 para gerenciar fornecedores e contratos de serviços com seus fornecedores • Processar o APO11 para gerenciar a qualidade do desenvolvimento de software • Todos os processos no domínio construir, adquirir e implementar (BAI) • Processo DSS01 para fornecer operações de TI • Processo DSS04 para fornecer continuidade de negócios Além disso, os outros facilitadores relacionados, por exemplo, itens de informações, estruturas organizacionais, políticas, são definidos e implementados. Em resposta a problemas com segurança, a empresa implementa / melhora o seguinte: • Processo APO13 Gerenciar Segurança • Processo DSS05 Gerenciar Serviços de Segurança Além disso, os outros facilitadores relacionados (por exemplo, informações, estruturas organizacionais, políticas) são definidos, implementados e relatados.

(Fonte: Adaptado de [17])

Um aspecto importante para a gestão de risco está relacionado à aquisição da informação. Quanto mais for o domínio e aprendizado sobre o ecossistema, menor será o volume de incertezas enfrentado durante o processo decisório e sempre haverá riscos em qualquer esforço para mudanças na arquitetura ou direcionamentos dos negócios. Risco está relacionado ao impacto à organização e deve ser abordado por certos níveis de governança, sendo normalmente classificados como tempo, custo, e alcance. Sua classificação deve observar categorizações como, por exemplo, negócios, de informações, de aplicativos e tecnologia. Tal classificação é útil, mas podem haver características organizacionais que demandem formas específicas de expressar o risco e estas devem ser consideradas, sendo uma forma de gerenciamento dos riscos a classificação por domínio de arquitetura, à medida que as organizações, as informações, as aplicações e a tecnologia são utilizadas, podendo haver formas específicas de expressar o risco[22].

Em uma estrutura organizacional, existem quatro domínios aceitos como subconjuntos de sua arquitetura. Aa arquitetura empresarial define a estratégia de negócios, a governança, a organização e os principais processos comerciais. A arquitetura de dados, trata da estrutura dos ativos lógicos e físicos de uma organização, já a arquitetura de aplicativos envolve um modelo para os aplicativos que devem ser implementados, suas interações e as relações com os principais processos de negócios da organização e, por fim, a arquitetura de tecnologia descreve toda a infraestrutura tecnológica corporativa necessária para suportar a implantação de serviços de negócios[22].

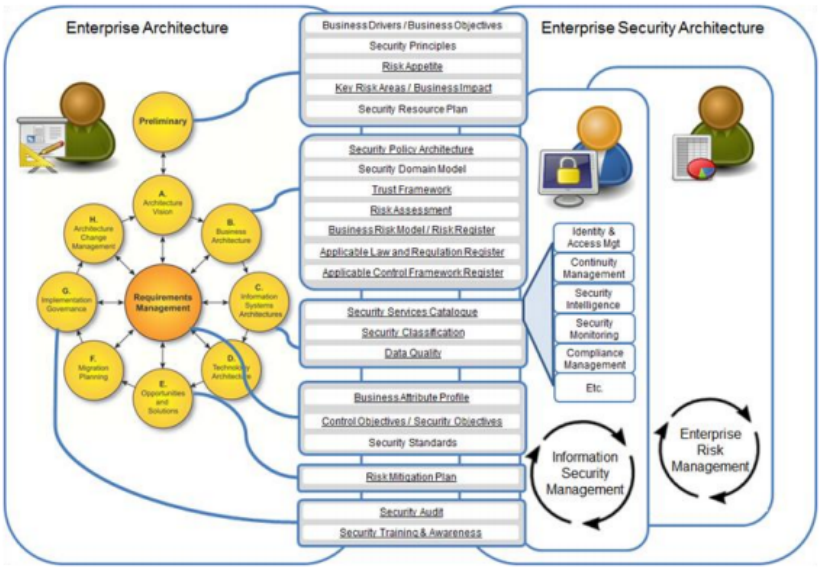
Para realizar efetivamente a governança baseada em arquitetura numa organização, é necessário que haja a capacidade de atendimento ao negócio de forma apropriada através da organização de estruturas, funções, responsabilidades, habilidades e processos. Uma prática de arquitetura corporativa bem sucedida deve estar fundamentada em uma base operacional bem estruturada, sendo executada como qualquer outra unidade operacional e sendo tratado como parte do negócio. Por isso, segundo o TOGAF [22], uma prática de arquitetura empresarial deve estabelecer capacidades para:

- a gestão financeira;
- a gestão do desempenho;
- o gerenciamento de serviços;
- o gerenciamento de riscos;
- a gestão de recursos;
- a gestão das comunicações e das partes interessadas;
- a gestão da qualidade;

- a gestão de fornecedores;
- o gerenciamento de configuração;
- a gestão do ambiente.

A Arquitetura Empresarial consiste em um alinhamento dos sistemas empresariais e de informação de suporte para alcançar objetivos de negócios de forma eficaz e eficiente. Tais sistemas são a combinação entre os processos, as pessoas e a tecnologia, sendo a segurança da informação um aspecto importante, assim como a maneira como pode ser gerenciado, apesar de ter sido considerada por muito tempo uma disciplina descolada, isolada dos demais processos de negócios e da arquitetura corporativa[23].

Figura 2.11: Relacionamento entre a arquitetura organizacional e a arquitetura de segurança da informação



(Fonte: Adaptado de [22])

Uma arquitetura de segurança é uma estrutura formada por componentes organizacionais, conceituais, lógicos e físicos interligados para alcançar e manter um estado de gerenciamento de riscos e segurança, sendo não somente um habilitador de segurança, resiliente e confiável, bem como para abordar áreas de riscos em toda a organização, não existindo isoladamente. Baseia-se em informações da organizações disponíveis e produz informações que influenciam toda a organização, sendo a integração entre a arquitetura de segurança e a arquitetura organizacional benéfica. Porém, para que haja retornos benéficos, as duas arquiteturas precisam estar alinhadas e seguir o mesmo direcionamento. A Figura 2.11, demonstra como a arquitetura organizacional e a arquitetura de segurança

organizacional estão relacionadas, demonstrando os principais conceitos de segurança, de riscos usados para o gerenciamento de segurança da informação e no gerenciamento de riscos organizacionais. A gestão de riscos em uma arquitetura organizacional centra-se em diversos aspectos, podendo destacar negócios, sistema, informação, projeto, privacidade, conformidade e risco de mudança organizacional, entre outras categorias[23].

A arquitetura de segurança da informação promove uma visão equilibrada sobre os riscos, mantendo as consequências negativas sob controle a um nível aceitável e explorando ao máximo as oportunidades e consequências positivas. Uma abordagem orientada ao negócio é uma alavanca importante para a arquitetura da segurança. Os drivers de negócios promovem uma visão de contexto para a avaliação de riscos, definindo se a adoção e nível de cumprimento de qualquer guia ou *framework* de referência é necessário e justificam a necessidade das medidas de segurança[23].

A governança tornou-se um requisito cada vez mais sensível e visível para a gestão organizacional, sendo a execução de uma governança bem definida e efetiva um ponto central para a noção do ecossistema em que todas as atividades arquitetonicamente significativas são controladas e alinhadas em uma única estrutura em busca da garantia de um nível de visibilidade, orientação e controle que suporte todos os requisitos e obrigações das partes interessadas de todo o ecossistema organizacional. Assim, segundo TOGAF[22], pode-se destacar os seguintes benefícios de uma governança baseada em estrutura de arquitetura:

- Maior transparência da responsabilidade e delegação de autoridade informada;
- Um controlado gerenciamento de risco;
- Proteção da base de ativos existente através da maximização da reutilização de componentes da arquitetura existentes;
- Mecanismos proativos de controle, monitoramento e gerenciamento;
- Processo, conceito e reutilização de componentes em todas as unidades de negócios organizacionais;
- Criação de valor através de monitoramento, medição, avaliação e feedback;
- Maior capacidade de suporte dos processos internos e os requisitos das partes externas;
- Uma maior visibilidade da tomada de decisões em níveis mais baixos assegura a supervisão a um nível apropriado de decisões que podem ter consequências estratégicas de longo alcance para a organização;
- Um maior valor para os acionistas haja vista que a arquitetura empresarial representa cada vez mais a principal propriedade intelectual de uma organização, tendo

sido demonstrado por alguns estudos uma correlação entre o aumento do valor de ecossistemas bem governadas para os acionistas;

- A capacidade de integração com os processos e metodologias existentes e complementa a funcionalidade, adicionando capacidades de controle;

Qualquer arquitetura empresarial possui dois elementos-chave, sendo um elemento voltado para a definição dos entregáveis que devem produzir e o outro relacionado a uma descrição do método usado para que isso possa ser feito. A maioria dos *frameworks* se concentra nos entregáveis, sendo omissos, em alguns casos de forma intencional, sobre os métodos que devem ser usados para desenvolvê-los. Em todo caso, espera-se que o responsável pelo desenvolvimento da arquitetura organizacional se adapte para definir um método personalizado, transversal e integrado nos processos e estruturas da organização, podendo incluir a adoção de elementos de diversos *frameworks*, alinhados em uma visão de arquitetura, integrando os métodos apresentados no TOGAF com outros *frameworks* padrão, como ITIL, CMMI, COBIT, PRINCE2, PMBOK e MSP. A estrutura baseado em arquitetura fornece a capacidade para integração com os outros *frameworks*, usando domínios de negócios verticais, com áreas de tecnologia horizontal ou áreas de aplicação produzindo uma arquitetura competitiva, viabilizando a maximização das oportunidades de negócios[22].

Risco pode ser medido avaliando a probabilidade de uma ameaça, a vulnerabilidade do ativo e o impacto caso ocorresse. Dentre outras formas, risco pode ser descrito como a incerteza do resultado podendo ser usado no contexto para medição da probabilidade dos resultados positivos e negativos. Apesar das organizações sempre gerenciarem seus riscos, nem sempre é de uma forma visível, repetitiva e aplicada de forma consistente para apoiar a tomada de decisões[20].

Todas as organizações devem promover esforços para que informações necessárias para apoio aos processos decisórios sejam reunidas e validadas. O gerenciamento de riscos visa que uma organização desenvolva o uma eficiência econômica de uma estrutura de riscos, com uma série de atividades ou etapas bem definidas e objetiva o apoio a melhores decisões através de uma compreensão dos riscos e seu possível impacto. Para isso, existem duas importantes etapas, sendo uma responsável pela coleta de informações sobre a exposição ao risco para que se possa tomar decisões apropriadas e a segunda envolve a implementação de processos para monitorar os riscos e a busca pelo equilíbrio entre do controle adequado para lida com os riscos e apoiar aos processos de decisões embasados na avaliação e estimativa de riscos. Diversos tópicos abrangem o gerenciamento de riscos e o gerenciamento de continuidade de negócios, segurança, gerenciamento de riscos de programas, projetos e serviços operacionais devem ser observados e cuidadosamente tratados e colocados no contexto organizacional para que haja o gerenciamento de riscos[20].

Apesar de percebido como algo que deve ser evitado, risco também deve ser associado a oportunidades. Convém que o portfólio de serviço seja elaborado para um portfólio subjacente de riscos que devam ser gerenciados. Dessa forma, quando o gerenciamento de serviços é efetivo, os serviços no catálogo representam oportunidades e a possibilidade da criação de valor para as partes interessadas. De forma contrária, os serviços podem se tornar uma ameaça pela possibilidade de falha associada com as necessidades das demandas atraídas por eles, aos compromissos que tais serviços exigem e aos custos gerados. Para que os benefícios potenciais produzam mais valor para a organização do que o custo para enfrentar o risco, as decisões sobre o risco precisam ser equilibradas. Assim, é necessário uma avaliação precisa dos riscos em uma determinada situação e analisar os benefícios potenciais. Para cada objetivo apresentado é necessária uma avaliação precisa dos riscos em uma determinada situação e analisar os benefícios potenciais. Riscos e oportunidades apresentados por cada cenário e ação deve ser definidos para identificar respostas mais apropriadas[20].

Segundo ITIL Service strategy[20], existem dois tipos de níveis de riscos que devem ser considerados a partir de uma perspectiva do gerenciamento de serviços, sendo:

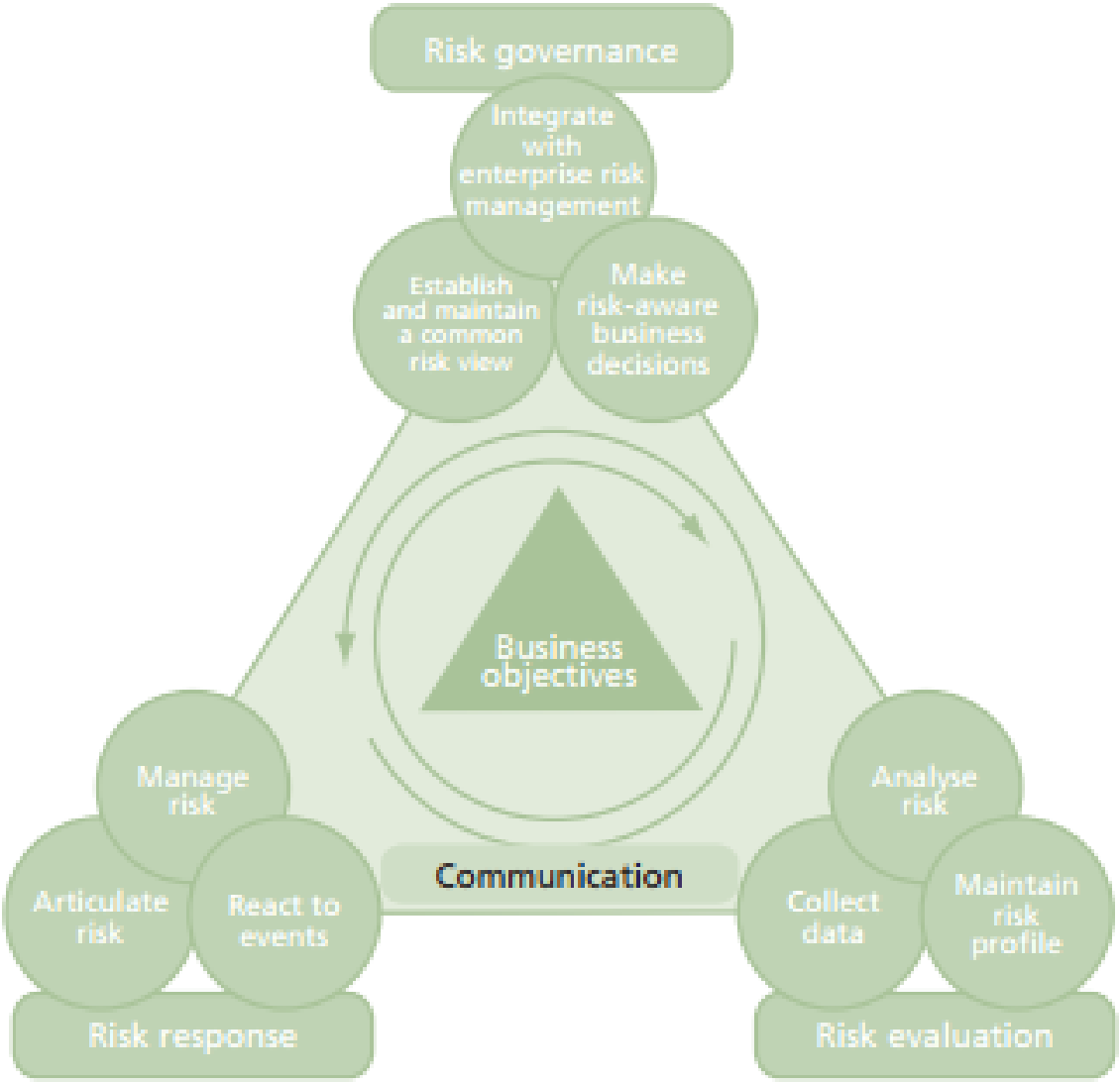
- Os riscos enfretados pelo negócio e os serviços comerciais usados por ele;
- Os riscos para os serviços de TI que sustentam o negócio e seus processos.

Para possibilitar uma visão mais completa dos riscos, é necessário que os dois níveis apresentados devam ser considerados simultaneamente já que interagem constantemente entre si. Dessa forma, o efeito da remoção dos riscos para os negócios é a principal proposta de valor dos serviços. Definido como a incerteza do resultado, seja uma visão de oportunidade (positiva) ou uma ameaça (negativa), o fato da existência da incerteza que cria a necessidade de atenção e gerenciamento formal de risco. A gestão de riscos exige a identificação e o controle da exposição aos riscos que possam ter impacto no alcance dos objetivos de uma organização. O objetivo do gerenciamento de risco é permitir uma melhor tomada de decisões com base em uma sólida compreensão dos riscos e seu provável impacto aos objetivos organizacionais[20].

Segundo ITIL Service Strategy[20], controlar os riscos de TI faz parte do portfólio de produtos de governança de TI e fornece um guia para uma governança e gerenciamento eficazes do risco, incluindo o risco comercial relacionado ao uso de TI, tendo como principais fundamentos da efetiva governança corporativa e o gerenciamento do risco de TI. Dessa forma, é necessário que:

- Sempre se conectar aos objetivos estratégicos e de negócios;
- Alinhar a gestão do risco de negócios relacionados à TI com o gerenciamento de riscos global corporativo;

Figura 2.12: Processo de riscos de TI



(Fonte: Adaptado de [20])

- Balancear os custos e os benefícios da gestão do risco de TI;
- Promover a comunicação aberta e clara do risco de TI;
- Estabeleça uma definição correta dos interesses, metas e objetivos da alta gestão, ao mesmo tempo a definição e responsabilização pessoal para a operação dentro deos níveis de tolerância aceitáveis;
- E deve ser um processo contínuos e parte de todas as atividades cotidianas da organização.

A Figura 2.12 demonstra uma estrutura de gestão de risco em TI, na qual a governança de risco promove a integração das práticas de gestão de risco de TI integradas a uma visão organizacional, permitindo que se obtenha um melhor retorno. Com a avaliação de riscos, é possível identificar as oportunidades e riscos relacionados à TI, analisando e descritos em termos de metas e objetivos de negócios e a resposta ao risco, garante que questões as questões de risco, oportunidades e eventos relacionados a TI sejam abordados de forma mais eficientes economicamente e de acordo com os objetivos e metas dos organizacionais, sendo o centro de todo o processo os objetivos de negócios[20].

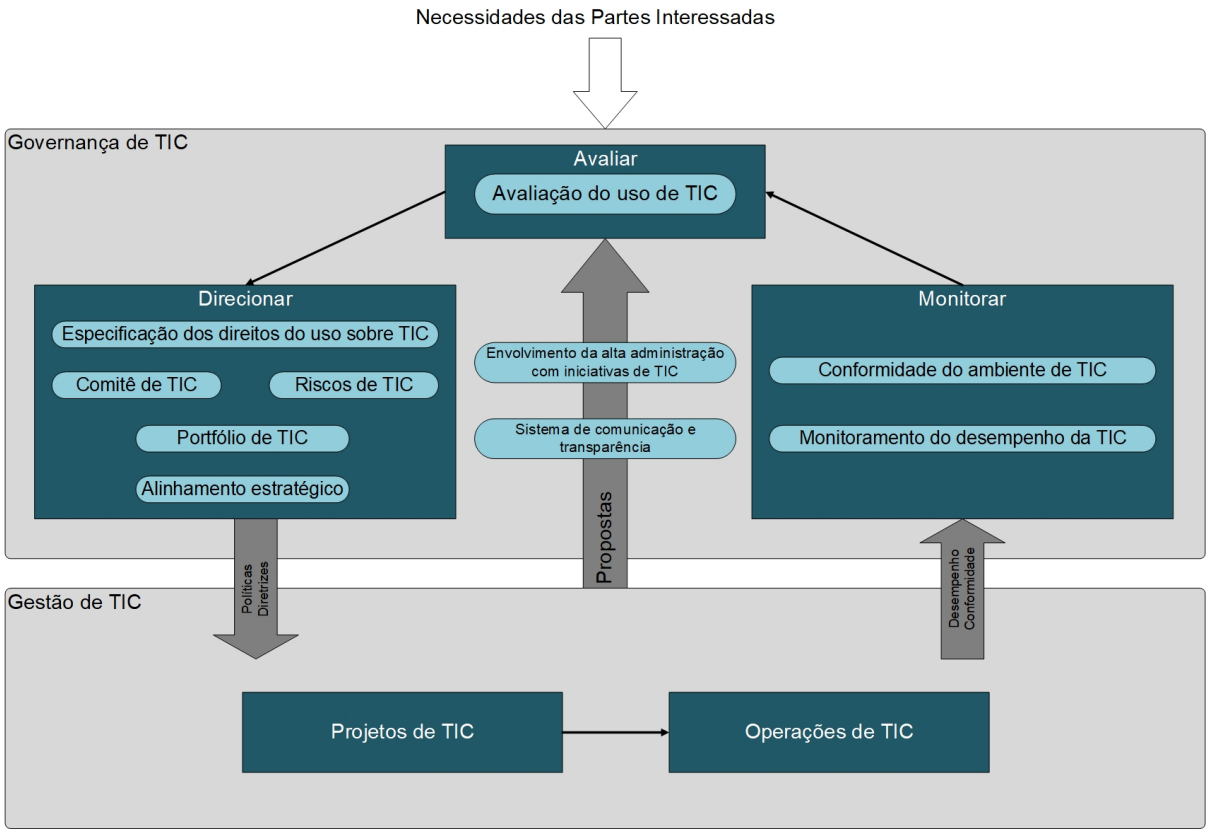
Apesar de várias referências, é um grande desafio para as organizações manter a TIC alinhada ao negócio de forma a agregar valor e obtendo melhores resultados. O fato de haver modelos para governança de TIC elaborados não significa, necessariamente, que a governança de TIC seja efetiva na organização. Quando os processos de governança são mal projetados ou estão desatualizados, eles acabam não sendo eficientes. A gestão de riscos necessita da responsabilidade da alta administração e um planejamento rigoroso e estratégico para se obter comprometimento em todos os níveis organizacionais. Antes de iniciar a concepção e a implementação da estrutura organizacional em gestão de riscos de TIC, é importante avaliar e compreender os contextos externo e interno da organização, uma vez que podem influenciar significativamente a concepção da estrutura, conforme demonstrado na Figura 2.13 [36].

Para que organizações possam identificar possíveis ameaças aos seus negócios, estabelecendo medidas eficazes de proteção. É necessário que haja uma abordagem sistemática para a gestão da Segurança da Informação e Comunicações (SIC). A missão da organização e os seus objetivos principais devem ser a base para o estabelecimento de práticas para a promoção da SIC. Um elemento importante nos esforços voltados à SIC é abordar os riscos de maneira efetiva, devendo ser parte integrante do sistema de gestão de SIC. A gestão de riscos deve ser alinhada às práticas gerais de gestão de riscos da organização, objetivando atingir níveis satisfatórios de segurança e racionalizar os investimentos pela priorização de ações e por evitar redundâncias na gestão de riscos.[35].

É necessário identificar os setores da organização que tratam com atividades e informações que envolvem requisitos de segurança, isto é, atividades e informações para as quais é importante que haja disponibilidade, integridade e confidencialidade. O ideal é que a organização mapeie os seus processos de negócio e suas informações para que haja uma efetiva identificação e mapeamento de tais informações. De uma forma geral, busca-se racionalizar o uso de recursos, aumentando a efetividade das proteções e a proteção dos recursos de sustentação dos negócios organizacionais[35].

Se considerado a cultura popular, a qual fala que "... sem governar não há gestão e sem gestão não há decisões corretas...", é de extrema importância que o processo de

Figura 2.13: Relacionamento entre as práticas de governança



(Fonte: Adaptado de [36])

governança possa entregar aos tomadores de decisões insumos consistentes e capazes de apoiar aos processos decisórios. Dessa forma, a governança organizacional deve possuir uma visão holística dos processos de governança e gestão[40].

Governance é o domínio do conselho de administração e está ligada a um conjunto de regras e práticas pelas quais um conselho supervisiona a configuração da estratégia e a gestão da organização. Uma governança efetiva assegura a prestação de contas, a justiça e a transparência nos relacionamentos da organização com suas diversas partes interessadas. Strategy Setting define o contexto do planejamento de negócios, fornecendo o plano de gerenciamentos de alto nível que deverá ser alcançado ao longo do planejamento estratégico selecionado, incluindo sua direção geral, análise do ecossistema, capacidades, limitadores e a infra-estrutura necessária para tornar as capacidades de entrega. A estratégia é muitas vezes apresentada sob a forma de metas gerais, iniciativas e táticas, podendo haver outras formas de apresentação[40].

Business Planning articula formalmente as metas específicas estabelecendo a forma como o gerenciamento operacional contribuirá para o alcance dos objetivos estratégicos

organizacionais, explicando as razões pelas quais esses objetivos são realizáveis e fornece um processo habilitador para implementar e executar a estratégia corporativa em toda a organização dentro do horizonte de planejamento especificado. Execution são as operações principais da organização necessárias para projetar, construir e operar os processos que fazem funcionar o plano de negócios e entregar o desempenho esperado de acordo com os valores e a estratégia organizacionais estabelecidos[40].

Monitoring são as atividades estabelecidas pela alta estão para avaliar e supervisionar a execução das operações da organização em relação ao planejamento estratégico, incluindo o nível de risco aceitável. As atividades de monitoramento consideram tanto nas métricas de desempenho que demonstram progresso na consecução de objetivos de negócios quanto metas estratégicas de longo prazo e nas métricas de risco para garantir que o risco permaneça em níveis aceitáveis[40].

Adapting descreve os processos organizacionais que foram avaliados pela atividade de Monitoring e requerem o acompanhamento da gestão, identificando ações corretivas que promoverão mudanças implementáveis na estratégia corporativa, no plano de negócios e / ou em táticas de execução (incluindo respostas de risco e / ou controles internos). A adaptação é importante quando se considera a resiliência e a agilidade da organização tão vitais para o sucesso em um ambiente de negócios em rápida mudança, incluindo as melhorias nos processos para reduzir as lacunas de desempenho relacionadas às expectativas das partes interessadas, bem como as correções decorrentes de mudanças no ambiente externo e interno que podem alterar as premissas da estratégia e / ou plano de negócios[40].

A gestão de riscos organizacionais é o processo efetuado pelo conselho de alta gestão, administração e outros funcionários de uma entidade, aplicado na definição de estratégias e em todas as camadas da organização. A gestão de riscos é projetada para identificar eventos potenciais que podem afetar a entidade, objetivando atuar dentro do seu apetite de risco para fornecer a garantia razoável da realização dos objetivos estratégicos. Controle interno é um processo realizado pela alta gestão, camada de gerenciamento e operacional de uma organização, podendo ainda ser entendido como um processo que fornece uma garantia razoável quanto à realização de objetivos relacionados a operações, relatórios e conformidade [40].

A gestão de riscos é aplicada para apoiar na definição da estratégia, abordando os objetivos de negócios. O controle interno tem um caráter mais tático, direcionado à execução do negócio e à redução do risco para a consecução dos objetivos, fazendo com que a gestão de riscos tenha um impacto maior no direcionamento estratégico e no planejamento de negócios. Dessa forma, os objetivos de negócios, incluindo tolerâncias de risco, são uma condição prévia para projetar e avaliar o sistema de controle interno. Os ele-

mentos inerentes às definições estratégicas, identificação de eventos, avaliação e resposta ao risco possui um direcionamento baseado no impacto nas definições estratégicas e no planejamento de negócios[40].

Como benefício do uso de um processo integrado, é possível observar que para as definições estratégicas e os objetivos estratégicos estabelecidos, o apetite e a tolerância de riscos são considerados. Isso se dá por risco ser parte inerente de qualquer direcionamento estratégico para a organização, desde decidir um processo de expansão para novos mercados, quanto investir em atividades de pesquisa e desenvolvimento de um nicho inexplorado e toda a avaliação de riscos leva em consideração a aceitação ou não aceitação para o negócio.

Definir o apetite de risco é um fator de suma importância. Ao determinar o apetite de riscos, é necessário considerar as atividades de desenvolver, comunicar, monitorar e atualizar o apetite de risco, sendo necessário a revisão e concordância da alta gestão. A definição de aceitação de riscos tem um caráter fundamental para as organizações e são inerentes ao modelo de negócio e estratégica atuais, criando valor para a organização e estes riscos são aqueles que "compensam"para o planejamento de execução efetiva da estratégia organizacional[40].

A gestão de riscos inclui o planejamento estratégico como parte, incorporando o apetite de riscos como ferramenta para o gerenciamento de riscos corporativos, sendo parte das definições estratégicas organizacionais. Como demonstrado, há uma superposição significativa entre a gestão de riscos e o controle interno. Afinal, o controle interno é um subconjunto do gerenciamento de riscos e ambos os abordam metas e objetivos de forma distinta. A implementação de controles não elimina a necessidade e benefícios da implementação da gestão de riscos[40].

Planejamento estratégia, gerenciamento de riscos e controles são afetados por decisões de gestão e decisões da alta gestão e, dessa forma, o apetite de risco de uma organização pode ser diferente de outra organização. Planejameto estratégico e o gerenciamento de riscos estão intimamente relacionados, haja vista que cada organização assume riscos de acordo com a busca de seus objetivos de negócios. É imperativo que as decisões de gestão sejam tratadas para possibilitar que as respostas de risco e os controles internos adequados sejam selecionados para o alcance dos objetivos da organização, dentro dos parâmetros do apetite de risco estabelecidos em seu processo de estabelecimento da definições e planejamentos estratégicos[40].

O ecossistema organizacional deve ser alinhado com o processo estratégico da administração e a supervisão da alta gestão. O ecossistema abrange o direcionamento estratégico, estabelecendo o contexto de como o risco é visto e abordado por todos. É necessário incluir a filosofia de gerenciamento de risco e o apetite de risco, integridade e valores éticos

e o meio ambiente em que operam. O ambiente operacional é incorporado pela supervisão da alta gestão e pelo compromisso da organização com a competência, estrutura organizacional, atribuição de autoridade e responsabilidade, e padrões de recursos humanos. Esses elementos do ambiente interno fornecem a base para os demais componentes da gestão de riscos e têm um efeito significativo na tomada de decisões organizacionais[40].

As organizações existem para um propósito, com um objetivo que é a entrega de um serviço ou para alcançar resultados específicos. Tal conceito aplicado em ao setor privado, faz com que o objetivo seja o aprimoramento do valor para o acionista. Quando inserido no contexto do setor públicos, o objetivo é relacionado com a entrega do serviço ou com a entrega de um resultado benéfico no interesse público. Seja qual for o propósito da organização, a entrega de seus objetivos está cercada de incerteza.[19]

O risco é definido como esta incerteza do resultado, seja a oportunidade (caráter positivo) ou ameaça (caráter negativo), de ações e eventos e deve ser avaliado em relação à combinação da probabilidade de algo acontecer e do impacto que ocorre se realmente acontecer. Os recursos disponíveis para gerenciar o risco são finitos e, portanto, o objetivo é alcançar uma resposta ótima ao risco, priorizado de acordo com uma avaliação dos riscos. O risco é inevitável e todas as organizações precisam agir para gerenciar o risco de forma que ele possa estar a um nível tolerável e seja justificado. Dessa forma, apetite de risco é a quantidade de risco que é julgada tolerável e justificável por uma organização[19].

Organizações possuem um ecossistema complexo onde outras instituições contribuem para os seus objetivos estratégicos e uma gestão de riscos eficaz deve levar em consideração o ecossistema em que a organização está inserida e as prioridades de risco das organizações parceiras. Quando observada aos níveis estratégicos, de programas e operacionais, a gestão de riscos precisa ser integrada para que os níveis de atividade se apoiem mutuamente. Desta forma, a estratégia de gerenciamento de riscos da organização será conduzida na esfera mais alta e incorporada nas rotinas e atividades normais de trabalho da organização. Todos os funcionários devem estar conscientes da relevância do risco para o alcance dos seus objetivos[19].

Independente de qual camada de decisões organizacionais, há incertezas inerentes aos processo. Dessa forma, os tomadores de decisões em cada nível, precisam de habilidades apropriadas que lhes permitam gerir riscos de forma eficaz, e a organização como um todo precisa de meios para garantir que a gestão de riscos esteja sendo implementada de forma apropriada em cada nível. Assim, a aplicação da gestão de riscos deve ser incorporada aos sistemas de negócios da organização, incluindo processos de definição de estratégias e políticas, para garantir que o gerenciamento de riscos seja uma parte intrínseca da forma como os negócios são conduzidos[19].

Não há um padrão para o gerenciamento de riscos em organizações governamentais,

porém, mais importante do que o cumprimento de qualquer padrão específico é a capacidade de demonstrar que o risco é gerenciado na organização de forma a apoiar efetivamente a entrega de seus objetivos, como ao apoio no processo de decisões organizacionais[19].

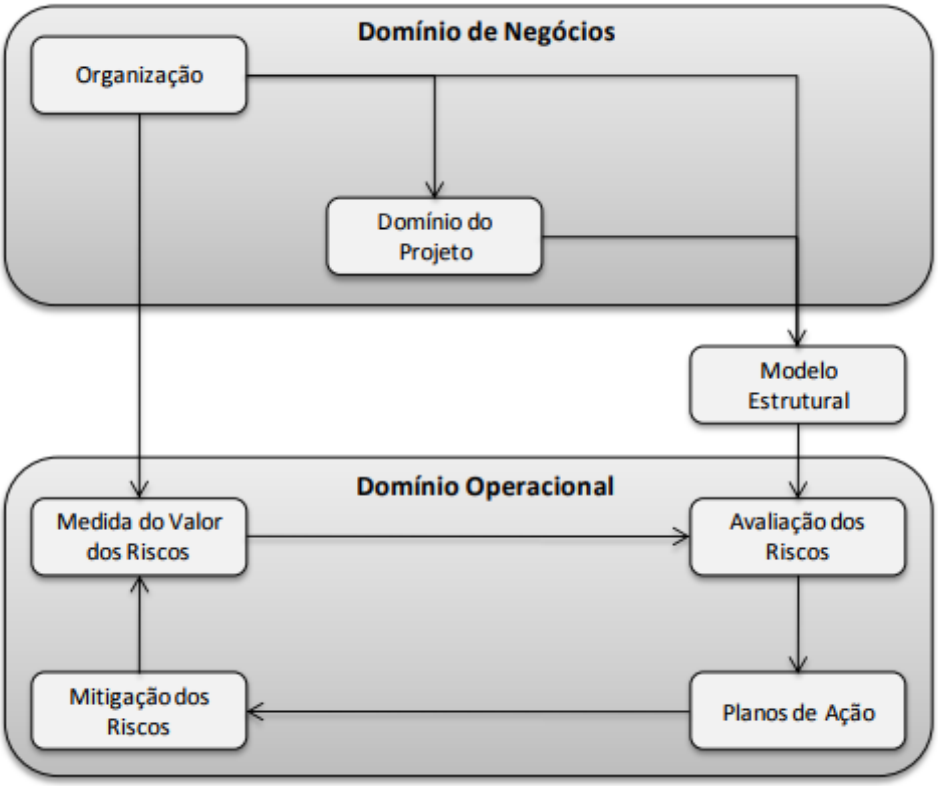
O conceito de apetite de risco é fundamental para uma gestão de riscos efetiva, sendo essencial considerá-lo antes de uma consideração de abordagem o riscos. Dessa forma, pode-se dependendo da tipo de consequência da incerteza (risco), podendo ser uma oportunidade ou uma ameaça. Dessa forma, quando risco for considerado uma ameaça, o apetite de risco abrange o nível de exposição que é considerado tolerável e justificável se for realizado, comparando o custo (seja financeiro ou não) de restringir o risco com o valor da exposição caso esta se torne uma realidade e encontrar um saldo aceitável. Considerado como uma oportunidade, o apetite de risco considera o quanto a organização está preparada para lidar com o risco e obter os benefícios da oportunidade, enfatizando o valor (financeiro ou não) da oportunidade potencial com as perdas que podem ser incorridas (algumas perdas ocorrer com ou sem a realização dos benefícios). É de extrema importância considerar que risco é sempre inevitável e não está dentro da capacidade da organização gerenciá-lo completamente a um nível tolerável. Nesses casos, a organização precisa fazer planos de contingenciamento para lidar com as incertezas (riscos) e seus efeitos[19].

Independente de qual seja a circunstância, o apetite de risco será melhor expresso como uma visão de fronteiras, em concordância e aprovação da alta gestão. Essa fronteiras dão a cada nível da organização uma orientação clara sobre os limites de risco que devem ser considerados, seja o risco considerado ameaça ou uma oportunidade. Isto significa que o apetite de risco será expresso de maneira similar aos feito avaliação do risco. O apetite de risco de uma organização não é necessariamente estático tendo a alta gestão a liberdade para definir o nível de risco que está preparado para suportar, considerando as circunstâncias[19].

O gerenciamento de riscos está estruturada em duas camadas, sendo a primeira ligada ao negócio e a segunda exclusivamente operacional, vide Figura 2.14. A camada de Negócio foca nas perspectivas da organização e do projeto, tendo duas etapas de responsabilidades fundamentais sendo a identificação do ambiente econômico no qual está inserido o projeto e a susceptibilidade da organização com relação ao desempenho da equipe de projeto, e a exposição a fatores de riscos externos como etapas de responsabilidades fundamentais e a estima do conhecimento associados à experiência da organização para o desenvolvimento de um projeto, assim como, o nível de confiança para uma implantação bem sucedida. Já a camada operacional está centrada na modelagem dos diferentes aspectos do projeto, tendo como responsabilidade cinco etapas para quantificar os riscos como guia para as políticas da empresa, fornecer uma análise detalhada que identifique

os fatores chaves de risco, identificar e descrever planos de ação para reduzir o impacto dos riscos chaves, implementar tais planos e reavaliar os fatores de risco afetados e manter um ciclo contínuo destas etapas durante a execução do projeto[37].

Figura 2.14: Visão geral da gestão de riscos



(Fonte: Adaptado de [37])

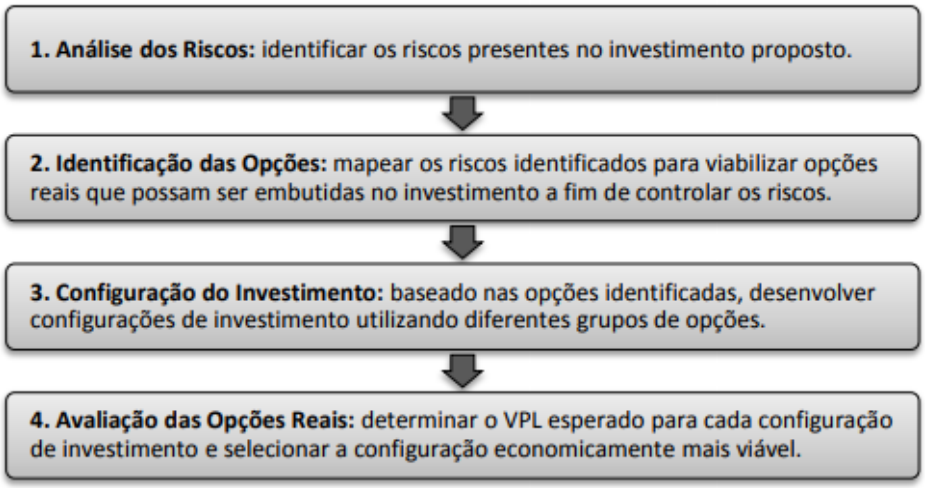
Miorando[37] afirma que a estruturação de modelos baseados em hierárquica prevê as seguintes atividades:

- Identificação dos Stakeholders: identificar diferentes maneiras de avaliar interesses de um grande número de stakeholders;
- Identificação dos fatores de risco: para a obtenção de melhores resultados, o uso de técnicas como brainstorming ou do método Delphi podem ser usados;
- Construção de um modelo de árvore de risco: onde o agrupamento dos fatores de risco relacionados em uma estrutura hierárquica que se alinhe as perspectivas dos stakeholdes deve ser desenvolvido;
- Calibração do modelo: é realizada com a estimativa dos pesos dos fatores de risco;

- Estimativa das probabilidades dos eventos de risco: onde cada fator de risco deve ser avaliado pela sua probabilidade de ocorrência;
- Desenvolvimento de planos de ação: é importante que estes forneçam suporte para a documentação, gerenciamento e reavaliação dos eventos de risco durante o desenvolvimento do projeto.

Há uma conjunto de guias de referência baseados em uma visão de portfólios e que podem ser explorados como ferramentas de apoio à decisões em diversas situações. Tais modelos possuem uma visão de modelagem de indicadores baseados em questionário e técnicas multicritérios, sendo possível destacar os modelos SERIM – Software Engineering Risk Model; SRAM – Risk Assessment Model; Modelo de Tiwana e Keil; Modelo BRisk[37].

Figura 2.15: Etapas de implementação do OBRiM



(Fonte: Adaptado de [37])

A gestão de riscos deve focar na formas de abordagem do gerenciamento de risco em TI a partir de um viés econômico e na escolha de mecanismos de mitigação adequados, combinando-os para combater de forma eficaz alguns riscos específicos. De forma complementar, deve buscar ao atendimento destas questões utilizando a teoria das opções reais como uma estratégia de alto nível para mitigação de riscos, proporcionando diferentes formas de flexibilidade necessárias para desenvolver as ações corretivas quando os riscos ocorrerem, sendo possível encontrar a combinação de opções que adicionem o máximo valor relativo a um investimento sob ameaça de um risco especifico. Vide Figura 2.15 para entendimento das etapas de implementação do OBRiM[37].

Rogério[37] demonstra que, como forma de apoiar em decisões de investimentos e na obtenção de melhores resultados para estes, é necessário que se parta do pressuposto de que os investimentos em TI envolva uma associação dos riscos externos e riscos internos existentes à organização, estando o modelo dividido em:

- Definição dos objetivos do investimento e identificação dos riscos: onde deve-se definir os objetivos e requisitos do investimento, identificando as fontes críticas de fatores de risco, sendo que estas podem estar relacionadas tanto ao desenvolvimento do projeto quanto ao comportamento do mercado;
- Avaliação dos riscos externos: onde são avaliados os riscos externos à organização e os riscos públicos são representados como a volatilidade do retorno financeiro do projeto;
- Avaliação dos riscos internos: é executada a avaliação dos riscos, constituídos por fatores internos a organização, e devem ser observados a experiência da equipe, a complexidade do projeto, o planejamento e controle, entre outros aspectos;
- Avaliação das opções reais: onde é analisado o valor das opções reais para o projeto, baseado no resultado das etapas anteriores e o método de Opções Reais para a análise, dependerá do número de opções a serem avaliadas.

Assumir a responsabilidade pela realização dos objetivos na implementação de políticas públicas é o elemento basilar da accountability pública, sendo o dever das pessoas e/ou entidades às quais se tenha confiado a gestão de recursos públicos demonstrar os resultados obtidos e o uso apropriado dos recursos. De forma complementar, ainda há a necessidade de demonstrar a administração e controle dos recursos mediante estratégias que permitiriam segurança razoável do alcance desses objetivos e o não cumprimento dessas obrigações de accountability é cada vez mais percebido pela sociedade como quebra de responsabilidades confiadas[13].

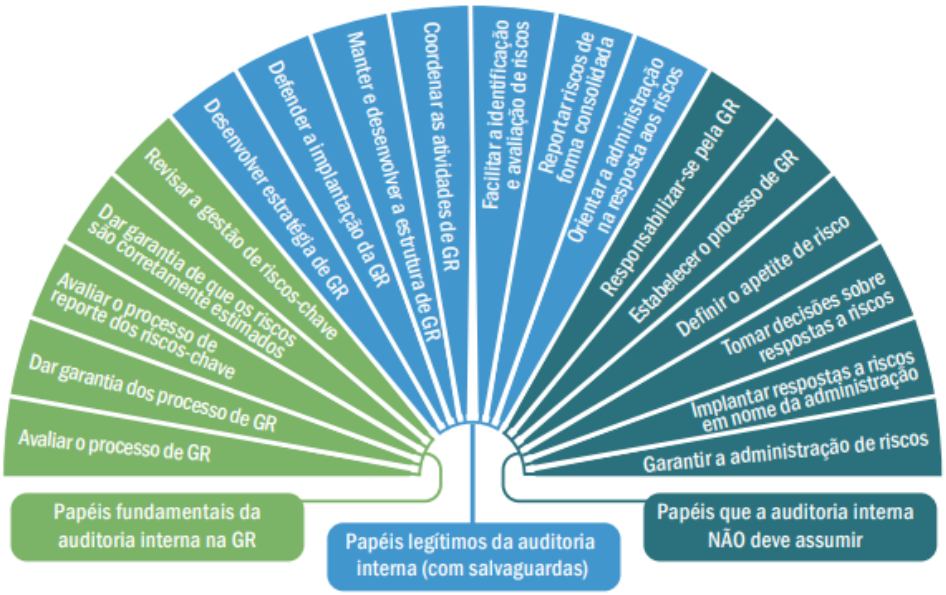
O objetivo da integração da governança e da gestão é entregar o melhor valor para os cidadãos na forma de políticas, bens e serviços públicos que atendam às suas necessidades e expectativas, e apresentem um retorno condizente com os recursos públicos usados para tal fim. O cumprimento dos objetivos inerentes às obrigações de accountability, tanto a tomada de decisão na definição da estratégia, por parte dos órgãos de governança e da alta administração, e a sua implementação, por parte da gestão executiva, enfrentam influências de fatores inerentes ao ecossistema, que tornam incerto se e quando tais objetivos serão atingidos. Tais incertezas e seus efeitos sobre os objetivos finalísticos da organização é chamado de risco[13].

Como desafio, a governança nas organizações públicas precisam determinar quanto de risco aceitar na busca da maximização do valor para os cidadãos e outras partes

interessadas, significando prestar o serviço de interesse público da melhor maneira possível, equalizando os riscos e os benefícios. A gestão de risco é processo estratégico e fundamental para as organizações do setor públicove um componente relevante de seus sistemas de governança tornando-se a ferramenta usada pela governança para lidar com tal desafio[13].

Quando implementada e executada de forma eficaz, a gestão de riscos melhora as informações para o direcionamento estratégico e para as tomadas de decisões de responsabilidade da governança e contribui para a otimização do desempenho e na realização dos objetivos de políticas e serviços públicos e, consequentemente, para o aumento da confiança dos cidadãos nas organizações públicas, além de prevenir perdas e auxiliar na gestão de incidentes e no atendimento a requisitos legais e regulamentares[13].

Figura 2.16: Visão da gestão de riscos e a auditoria interna



(Fonte: Adaptado de [13])

O relatório “Avaliação da OCDE sobre o Sistema de Integridade da Administração Pública Federal Brasileira - Gerenciando riscos por uma administração pública mais íntegra” recomenda a integração da gestão de riscos como elemento-chave da responsabilidade gerencial, desenvolvendo uma abordagem de controle interno baseada em riscos e inclusão da gestão de riscos nos programas de apoio ao desenvolvimento das competências dos gestores públicos, enfatizando a necessidade de promoção de uma liderança comprometida com a criação de uma cultura de gestão que promova a gestão de riscos como ferramenta estratégica do sistema de governança[13].

A Figura 2.16 demonstra o papel da auditoria interna na gestão de riscos em instituições quando as organizações não possuem uma estrutura formal para o gerenciamento de riscos. O papel da auditoria é fornecer aos órgãos de governança e à alta administração, bem como aos órgãos de controle e regulamentação, garantias de que os processos de gerenciamento de riscos operam de maneira eficaz e que os riscos significativos do negócio são gerenciados adequadamente em todos os níveis da organização. A auditoria interna deve ter uma compreensão clara da estratégia da organização e as formas como é executada, quais os riscos associados e como esses riscos estão sendo gerenciados[13].

Figura 2.17: Gestão de riscos e a sustentação dos processos de decisões

(Fonte: Adaptado de [13])

As organizações adotam abordagens informais e, em alguns casos, altamente estruturadas e sistematizadas de gestão de riscos, possibilitando lidar com riscos e aumentar a chance de alcançar objetivos. A implantação da gestão de riscos em uma organização é um processo de aprendizagem organizacional, que começa com o desenvolvimento de uma consciência sobre a importância de gerenciar riscos e avança com a implementação de práticas e estruturas necessárias à gestão eficaz dos riscos. O desenho e a implementação de estruturas e processos de gestão de riscos devem levar em consideração as necessidades específicas da organização em face dos objetivos que dão suporte à sua missão e dos riscos associados e em qualquer situação, é importante que a organização se apoie em modelos reconhecidos. A Figura 2.17 demonstra como a gestão de riscos está envolvida com o ecossistema de negócios organizacionais[13].

2.2 Complexidade do processo de tomada de decisão

Pela grande quantidade de informações e variáveis que necessitam ser analisadas e avaliadas, tomar decisões pode ser descrito como uma atividade complexa. Além dos aspectos inerentes ao entendimento e direcionamento para a gestão de riscos e os processos decisórios, há o desafio do comportamento e limitações do ser humano para os processos decisórios. À seguir serão apresentados os desafios para tomada de decisão.

Tomadores de decisões precisam abordar a natureza crítica do risco e da incerteza no processo de tomada de decisão. A identificação dos riscos e incertezas inerentes a uma ação proposta, a avaliação do seu impacto sobre os possíveis resultados e a elaboração de planos de contingência para gerenciá-los são essenciais para a tomada de decisões eficientes, sendo que a ausência de tais atividades geram resultados subótimos para os processos decisórios. Isso demonstra que a gestão de riscos e as suas implicações para a governança organizacional tornaram-se cada vez mais críticas. Os tomadores de decisões estão cada vez mais apegados aos aspectos qualitativos de projetos relacionados à incertezas e os problemas de definições relacionadas aos riscos e à incertezas perseguem cada vez a gestão estratégica[5].

A variedade de riscos e incertezas podem afetar a escolha de modelos, técnicas e processos utilizados para os processos de tomada de decisões. Não há uma definição clara ou consenso sobre os significados de risco e incerteza, assim, observa-se que risco e incerteza são pontos distintos onde risco pode ser mensurado probabilisticamente e incerteza é um conjunto de eventos que não podem ser associados com uma dada probabilidade. Risco e incerteza têm sido utilizado de forma alternada, porém são construções teóricas distintas e, quando considerados risco e incerteza de forma conjuntas, é dominante o efeito da incerteza em relação ao riscos. Por isso, dada tal mixórdia, se faz necessário definir como serão usados os termos risco e incerteza de forma adequada[5].

Apesar de usados de forma permutável na literatura, riscos e incertezas são concepções teóricas distintas e, por conta desse desarranjo conceitual, é necessário que haja uma definição clara para o uso de tais conceitos, podendo aplicar ao risco a distribuição de probabilidade das consequências de cada alternativa, sendo que a distribuição implica na capacidade de quantificar as consequências e a incerteza apresenta a consequência de cada alternativa, a qual pertence a um subconjunto de todas as possíveis consequências sem que seja possível, ao tomador de decisão, atribuir probabilidades à ocorrência de resultados particulares. Isso sugere que fatores quantificáveis representam riscos e fatores qualitativos afetam a confiança dos decisores e representam incertezas. Decisores não agem segundo os princípios da racionalidade quando são confrontados com decisões baseadas em riscos, pois a presença das incertezas parece afetar o processo de tomada de decisões pela dificuldade de coleta e de processamento de informações[5].

Uma prática comum no planejamento estratégico é a apresentação de uma imagem precisa do futuro ou um resultado mais provável escondendo as incertezas subjacentes. Quando usada uma ferramenta qualitativa, oriunda da área estratégica há a capacidade de tomadores de decisões analisar e avaliar de forma estruturada incertezas e contingências. Tal associação de ferramentas de estudos de cenários e opões reais, proporciona aos tomadores de decisões a capacidade de avaliar qualitativamente os riscos e incertezas, podendo ser um ponto de apoio para o desenvolvimento de um programa corporativo de gerenciamento de riscos, promovendo a capacidade da identificação e integração das exposições ao nível das divisões. Argumentamos que ambas as abordagens também podem ser utilizadas no nível do projeto para ajudar a gerenciar a incerteza em projetos de capital complexos. Tomadores de decisões tendem a usar abordagens quantitativas e analíticas para identificar a decisão ótima diante de riscos, porém, mesmo que haja uma tentativa de uso de uma análise analítica e quantitativa, à medida que a incerteza aumenta, cria-se uma dependência para um julgamento e experiência em maior medida, buscando apoio em uma abordagem mais qualitativa para tomar decisões (apelo intuitivo). Considerando que a distribuição de aproximação implica em uma capacidade de quantificar a consequência de um dado evento e a incerteza representa a incapacidade de um tomador de decisões em atribuir probabilidades definidas à ocorrência de resultados particulares, cada alternativa pertence a um subconjunto de todas as possíveis consequências, implicando em uma falta de confiança em relação às estimativas de probabilidade ou a incapacidade de atribuir estimativa causando uma ambiguidade completa[5].

À medida que a incerteza aumenta e as previsões tornam-se difíceis, diminui o valor das técnicas das modelagens de decisão. Problemas de definição relacionados ao risco e à incerteza têm perseguido a gestão estratégica e decisores não podem agir de acordo com os princípios da racionalidade quando confrontados com decisões baseadas em riscos, já que, devido à dificuldade de coleta e processamento de informações, a presença de incerteza parece também afetar o processo de tomada de decisão. Assim, quanto maior a incerteza, maior será a abordagem comportamental para os processos decisórios[5].

Riscos e incertezas são considerados aspectos distintos, impactando distintamente quando sozinhos ou conjugados, no processo de tomada de decisão, demonstrando que tomadores de decisões enxergam diferença entre estes conceitos e respondem de forma distinta a cada um deles. Tomadores de decisões são sensíveis aos riscos e costumam usar abordagens analíticas e quantitativas, visando encontrar a melhor decisão. Quando confrontados com incertezas, são utilizadas abordagens de julgamento, os quais dependem da intuição ou da experiência para os processo decisórios[5].

Independente do nível de riscos, os tomadores de decisões confiam em seus julgamento e experiência para justificar suas decisões, quando há altos níveis de incertezas. Deve-

se ressaltar que algumas noções de incertezas representam a falta de informação. Dessa forma, tomadores de decisões precisam de uma abordagem crítica do risco e da incerteza para o processo de decisão, sendo necessárias a identificação dos riscos e incertezas, a avaliação do seu impacto sobre os resultados, somados a elaboração de planos de contingências para gerenciá-los. Dessa forma, sem que haja uma complementação de tais atividades, as decisões tomadas provavelmente sejam subótimas, tornando crítica a implicação da gestão de riscos para a governança corporativa[5].

Sendo risco qualquer situação em que não há a certeza do conhecimento de alguns eventos ou relacionados com eventos que são relativamente raros, é difícil considerar qualquer situação em que riscos não esteja desempenhando algum papel. Desenvolver uma lista de riscos é um trabalho extensivo e cria um desafio significativo para medir os eventos de risco por sua complexidade[11].

Jean-Paul Chavas[11] faz dois questionamentos importantes sobre a capacidade de um domínio dos riscos:

- Como é possível medir o que não se tem certeza ou, como pensar em uma medição de riscos tendo em vista a quantidade de eventos de riscos ?
- Risco e incerteza são equivalentes ou há um significado diferente entre eles ?

Segundo Chavas[11] não há um consenso claro sobre as definições de riscos e incertezas, porém, duas escolas de pensamento são encontradas. Uma escola argumenta que risco e incerteza não são equivalentes e uma maneira de distinguir entre ambos depende da capacidade de fazer avaliações de probabilidade. Risco corresponde a eventos que podem ser associados a determinada probabilidade e a incerteza são eventos aos quais a avaliação de probabilidade é impossível e, seguindo tal conceito, eventos de riscos são de fácil avaliação, porém, eventos incertos são bem mais complexos. A avaliação de riscos é simples, entretanto, avaliar incerteza segue um caminho antagônico e tão complexo quanto mensurar a incerteza é a sua separação de risco dependendo, de certa forma, do significado dado à probabilidade. A probabilidade é comumente entendida como a possibilidade de mensurar algo que não se tem certeza, assim o conhecimento pode mudar entre os indivíduos possibilitando diversas interpretações alternativas. A segunda escola define os riscos como a exposição às consequências da incerteza. Um outro aspecto do risco está ligado ao tempo, já que pode ser descrito como qualquer evento para o qual não se tem certeza de forma prévia, ou seja, antes do tempo de ocorrência. Dessa forma, duas características básicas do risco são observadas. A primeira é a exclusão de eventos que já ocorreram e foram observados, considerados eventos seguros. A segunda característica sugere que o tempo é a característica fundamental do risco, enfatizando a dimensão temporal do risco. A prevalência de eventos de riscos demonstra que há muitos eventos desconhecidos no

momento atual, demonstrando a importância de uma avaliação do efeito dos riscos para a tomada de decisões sob incertezas[11].

Apoiado por tais conceitos, Chavas[11] provê dois pontos de reflexão, questionando como lidar com a grande extensão da incerteza no ecossistema organizacional, sendo que a racionalização de eventos de risco conflitará com a crença científica de que qualquer evento pode ser explicado em uma relação de causa-efeito e se é possível, através de tal crença, negar a existência de riscos e, sendo isso verdade, por que há eventos de riscos ?

O predomínio e a existência de eventos de riscos podem ser explicadas por três fatores principais. O primeiro descreve que a existência de risco está relacionada à nossa incapacidade de controlar e / ou medir de forma precisa alguns fatores causais dos eventos. O segundo denota que risco existe devido a capacidade limitada que temos de processar informações, reforçando a importância do processamento de informações para a escolha das opções de decisões e o terceiro demonstra que custos podem assumir várias formas, podendo ser monetário, operacional, em tempo gasto para a aprendizagem associado ao alto custo de obtenção e processamento de informações. Tendo a informação um custo tão alto, nem sempre a sua obtenção e processamento será de grande valia. Para o terceiro fator, mesmo que haja a capacidade de obtenção e processamento da grande quantidade de informações inerentes à incerteza ou aos riscos, isso não significa que haverá o uso de tais informações[11].

As informações devem ser obtidas quando seus benefícios forem maiores do que seu custo e há muitas razões para as imperfeições das informações sobre eventos, independente do motivo. Todos os eventos de riscos têm uma característica única que é o fato de não haver a certeza sobre sua existência ou conhecimento antes do tempo de sua ocorrência, demonstrando que há sempre diversas possibilidades de ocorrência do mesmo[11].

Jean-Paul[11] demonstra que o comportamento ao risco pode ser descrito matematicamente e, dependendo da natureza das preferências de riscos individuais, é possível classificar o risco como positivo, zero ou negativo. Dessa forma é possível afirmar que o processo de decisão tem um comportamento em relação ao risco.

Intuitivamente, um tomador de decisão será averso ao risco quando este for prejudicado pelo riscos e está disposto a pagar uma quantia positiva para eliminação de riscos ($R > 0$). De forma contrária, é propenso ou atraído pelo risco se este for compensado pela eliminação da exposição ao riscos ($R < 0$), demonstrando a atração ao risco, sendo cada vez maior sua atração quando há a remoção do risco. Caso não haja um efeito da exposição do risco não desenvolva um efeito nem positivo nem negativo, o tomador de decisão é indiferente ao risco ($R = 0$). Na ausência de riscos, tomadores de decisões tem um potencial incentivo para maximização do lucro, podendo esperar que haja uma tomada de decisão de forma consciente com a maximização do lucro. Porém, o mesmo

comportamento não ocorre com a presença de riscos para os processos decisórios[11].

A análise estatística de um período do comportamento dos riscos como mecanismo para o apoio da decisão possui limitações importantes, podendo citar que não há a captura dos aspectos dinâmicos de grande parte dos processos de tomada de decisão, a incerteza é tratada como um dado e como tudo aquilo que não foi possível aprender antes da tomada de decisão[11].

O estresse e a tomada de decisão estão intimamente ligados, não apenas no nível comportamental, sendo que o estresse afeta o resultado da tomada de decisão[45].

Para os processos de decisões das organizações, os dados e os modelos usados para os processos decisões desempenham cada um papel cada vez mais importante. Os processos de decisões podem ser melhorados, tornando-os mais rigorosos e analíticos, apoiados pela aplicação de modelos quali-quantitativos, apesar da compreensão limitada de como a modelagem realmente pode afetar o comportamento de tomada de decisão organizacional, seja para o lado positivo ou para o lado negativo, porém, qualquer método produzirá benefícios para uma organização apenas na medida em que ele realmente altera o comportamento de seus atores de maneiras que melhoram o desempenho organizacional. Considerando o processo de tomada de decisões baseados em modelos, qualquer processo de tomada de decisão que seja suportado pelo uso de métodos analíticos quantitativos ou qualitativos [33].

Sendo a tomada de decisão uma escolha racional, baseado em uma análise lógica e sequencial de causa e efeito e supondo que as organizações eram conhecidas e previsíveis, os tomadores de decisões seguiam um processo baseado em identificar o problema quantificáveis, encontrar as opões plausíveis priorizando-as de acordo com critérios pré definidos e selecionando a escolha, sendo esta, otimizada pela certeza. O pressuposto está sustentado na ideia de que regras definidas, relacionamentos previsíveis, tarefas estabelecidas e linhas claras de autoridade permitem tomar decisões racionais com eficiência semelhante a máquina. Porém, gerentes buscam atitudes e comportamentos estáveis e previsíveis, assumindo que tomar decisões seja um processo relativamente direto, enleado por parâmetros estabelecidos e dessa forma, decisões são moldadas, controladas e coordenadas por um conjunto de regras cuidadosamente construídas, direitos de decisões e normas de condutas[43].

Todos os dias decisões que envolve perdas e ganhos são tomadas. Apesar de aspectos como o tempo possuir relevância na vida cotidiana, há uma compreensão limitada quando observadas as perspectivas para tomada de decisões nos quais os riscos estão envolvidos no processo. Por isso, decidir de forma eficiente tornou-se cada vez mais importante, apesar de haver uma compreensão limitada da tomada de decisão quando os resultados do risco são envolvidos e uma das razões para este comportamento é a máxima "tempo é

dinheiro", onde a suposição econômica de que, com base no tempo, as decisões apoiados em risco devem respeitar os mesmos princípios que as decisões monetárias[16].

Festjens[16] assume que a Teoria da Perspectiva (PT) é a descrição mais popular para o processo de decisões baseados em riscos. As principais características da PT reconhecem que os indivíduos são mais sensíveis às mudanças do que aos estados mais absolutos e menos dinâmicos. Os indivíduos valorizam o tempo e as perdas monetárias de forma diferente, sendo possível observar que as descobertas para o domínio monetário nem sempre se traduzem para o domínio temporal. Os resultados de tal comportamento são codificados em uma relação de perdas e ganhos em vista a certo referencial e estes pontos de referência desempenham um papel fundamental na avaliação de tempo. A PT ainda apresenta a suposição do fenômeno da aversão a perda, ou seja, as perdas são maiores do que os ganhos[16].

Assumindo que U é composto por uma utilidade básica u, refletindo o valor dos resultados e pela aversão à perda que reflete a diferente avaliação de ganhos e perdas, onde λ é o parâmentro de aversão a perdas e os tomadores de decisões possuem uma percepção subjetivas da probabilidade[16].

É possível medir as atitudes em relação às decisões baseadas em riscos, sem impor um modelo de escolhas. Utilizando a Teoria da Perspectiva - PT, é possível reconhecer que os tomadores de decisões são mais sensíveis às mudanças do que aos estados absolutos e que os resultados são codificações de perdas e ganhos em relação a um ponto de vista e que "perdas são maiores que ganhos", o fenômeno da aversão à perda[16].

A importância das mudanças e da aversão a perdas é capturada por uma função que é definida sobre ganhos e perdas, tendo uma acentuação maior para as perdas, assumindo que (U) utilidade é composta por uma utilidade básica (u), onde são refletidos os valores dos resultados e λ é a aversão à perda, a qual dará a diferença entre as avaliações de ganhos e perdas. Cada indivíduo tem uma percepção subjetiva da probabilidade, capturada por pesos de decisões, fazendo com que pequenas probabilidades sejam superestimadas, enquanto probabilidades grandes e moderadas tendem a ser subestimadas[16].

Tais tendências são representadas pela função de ponderação de probabilidade, onde a atitude global para riscos está ligada à curva de utilidade, a ponderação de probabilidade e a aversão à perda. Considerando uma perspectiva (x,y,p), onde um indivíduo receba o resultado de x com a probabilidade de p, recebendo o resultado de y de uma outra forma. Entendendo que u(.) é uma função de utilidade, $\pi^{(+/-)}$ são os pesos de decisão associados aos resultados e λ é o coeficiente de aversão às perdas.

Tal descoberta reforça as exploração de Lakshminarayanan[28] que demonstra haver pouca evolução quando observado o processo de decisão baseado em riscos. A análise do comportamento de humanos e primatas, ao serem apresentados à cenários que retratam

a maneira como fazem escolhas entre opções de riscos apresentam uma tendência de avaliação em relação a um ponto de referência, e de agir em busca de risco quando são apresentadas perspectivas de perdas. De forma antagônica, quando os mesmos aspectos representam ganhos, seres humanos demonstram uma aversão natural ao risco[28].

Os mecanismos que norteiam o comportamento em seres humanos podem ser evolutivamente antigos, demonstrando que o padrão de tomada de decisão baseado em riscos denominado "efeito de reflexão", no qual os seres humanos passam de um comportamento de afinidade para um comportamento de aversão ao risco, depende simplesmente de como os mesmos resultados são apresentados e isso é determinante para suas decisões[28].

É possível afirmar que tomadores de decisões procuram a certeza de obter ganhos ou algo que os agradam, assim como a certeza de evitar perdas ou algo que não os agradam. A aversão ao risco é um fenômeno recorrente quando a perspectiva de perda para elevados valores estão em foco[14].

Seres humanos possuem comportamento fortemente apoiado na intuitividade quando se trata em tomar decisão e possui um amplo suporte na intuição para os mapeamentos de opções de riscos na construção das opções de investimentos baseados em riscos. Os gerentes de TI seguem a lógica do Gestão de Riscos Baseado em Opções - OBRiM embora seja puramente apoiado na intuição. A confiança nessa lógica, fortemente baseada apenas na intuição, pode levar a práticas de gerenciamento de risco subótimo ou contraproducentes[9].

A lógica existente no OBRiM está sustentada sobre um conjunto de mapeamentos normativos de opção de riscos, possibilitando escolher quais das opções reais devem ser incorporadas em um investimento para controlar riscos específicos. Esses mapeamentos são observados na prática propondo que a intuição gerencial deve ser complementada com o uso de modelos de opções reais formais, permitindo uma melhor compreensão dos alertas de riscos a serem seguidos e combinados a fim de efetivamente enfrentar os riscos mais críticos[9].

Há algumas implicações importantes como o fato de que o comportamento natural dos gerentes de TI correspondem bem à lógica das opções reais e abre oportunidades para o uso do ROT como forma de estudar uma série de questões comportamentais e econômicas no gerenciamento de riscos de TI. Os gerentes de TI continuam tendo dificuldades em aplicar conceitos de opção real na prática, apesar de demonstrado que o escopo da ROT pode e deve ser expandido para a gestão do risco de TI e á razões para acreditar que o mesmo raciocínio pode ser aplicado para organizações com práticas de gerenciamento de riscos bem estabelecidas, possibilitando que as organizações possam ganhar ao adotar formalmente o OBRiM[9].

Nos últimos anos, a gestão de riscos tem tido um suporte cada vez maior dos chamados

cisnes negros, quando estes estão relacionados à gestão de risco e a tomada de decisão sob incerteza. Há um grande desafio na capacidade de avaliação de risco e o uso da teoria da probabilidade para captura dos cisnes negros. Uma definição de qual real significado do Cisne Negro para os riscos, à incerteza e à probabilidade deve ser adotado, podendo sugerir que o cisne negro seja apenas um evento extremo com probabilidade muito baixa ou que pode ser um evento mais surpreendente em algum sentido, como por exemplo, um desconhecido, desconhecido. Outro ponto de observação é sobre a relação entre os cisnes negros e a concepção de risco, aos valores e as probabilidades esperados à distinção comum entre incertezas aleatórias e epistêmicas. O esclarecimento dessas questões podem apoiar no fortalecimento das bases do significado e na caracterização do risco, sendo este o aspecto de maior importância e fornecendo uma base para a melhor gestão do risco[6].

Existem duas formas mais adequadas para a definição do cisne negro. A primeira descreve o cisne negro como um evento raro com consequências extremas e a segunda o descreve como um termo para expressar um evento extremo e surpreendente quando comparado ao conhecimento atual do ecossistema. É possível usar o termo "cisne negro"nos dois sentidos apresentados, porém, o emprego do segundo é mais adequado pois a compreensão do primeiro conceito resultaria em uma classe muito grande de eventos, incluindo aqueles que são simplesmente raros, mas bem compreendidos. A segunda abordagem está em consonância com a definição de Nassim Nicholas Taleb, porém não se concentra apenas em surpresas relativas ao passado. O campo de riscos necessita de conceitos adequados para refletir o fenômeno do cisne negro e que esses conceitos não podem e não devem ser limitados pelo pensamento e ideias baseados em probabilidade pois os fenômenos que foram caracterizados se estendem além deste paradigma e que um cisne negro deve ser visto como um evento surpreendentemente extremo em relação ao conhecimento e crenças atuais[6].

Nos últimos anos, vários autores têm defendido a adoção de novos tipos de perspectivas de risco que evidenciam incertezas e não probabilidades na forma como o risco é compreendido e medido. Apesar de haver uma boa fundamentação teórica e estas perspectivas estarem bem estabelecida, há pouco que demonstre as implicações práticas para possa ser demonstrado claramente, sendo necessário mostrar como as novas perspectivas alteram a maneira como o risco é descrito e comunicado em situações reais e, por sua vez, os efeitos sobre a gestão de riscos e a tomada de decisões. Risco tem sido considerado como a perda esperada ou como a associação de perdas e probabilidades. O conceito de riscos deve ser substituído por uma perspectiva mais ampla e que não sejam ligadas a uma medida de incerteza específica, a chamada probabilidade[6].

O conceito de risco deve permitir diferentes formas de descrever as incerteza e a dimensão da falta de conhecimento. A probabilidade usada como medida de incerteza ou

grau de crença, não é capaz de refletir a força do conhecimento em que as probabilidades se baseiam. As suposições que a análise probabilística está construída podem esconder aspectos importantes das incertezas e sugere que as perspectivas recentemente desenvolvidas sobre o risco, afetam a forma como o risco é avaliado e descrito na prática[6].

As mudanças observadas estão relacionadas aos aspectos da dimensão do conhecimento e das possíveis surpresas, consideradas como cisnes negros. Dessa forma, é possível observar que as probabilidades atribuídas e os valores esperados fornecem uma ferramenta importante para refletir informações, incertezas e graus de crença. Tal aspecto demonstra a necessidade de explorar muitas abordagens diferentes de riscos pois a simples mudança na descrição do risco afetará o gerenciamento de riscos e a tomada de decisões de diferentes maneiras. Os procedimentos baseados em probabilidade precisam ser ajustados ao ponto de refletir adequadamente as dimensões de conhecimento e das surpresas. As novas perspectivas de risco influenciam na descrição tradicional de muitas maneiras, em particular, a maneira como a dimensão do conhecimento é descrita e tratada[6].

Para Ludvig e Spetch[32], a forma como as pessoas tendem a avaliar o risco e tomam decisões entre as alternativas apresentadas é um problema fundamental na tomada de decisões. Quando confrontadas com decisões que envolvam riscos, tomadores de decisões tendem a ser avessos ao risco em cenários de ganhos e tendem a um interesse ao risco em um cenário de perdas (o efeito de reflexão). Esse comportamento para tomada de decisão sensível ao risco é observado quando perguntado diretamente às pessoas quais escolhas fariam em situações hipotéticas. Quando essas decisões são baseadas em riscos e incluem resultados raros, as pessoas possuem comportamentos diferentes em suas escolhas, notando o apego explícito à probabilidades descritiva e experimental. É notório que os eventos raros são sobreponderados, quando tratados pela probabilidade descritiva, e subponderados quando tratados pela probabilidade experimental. É possível observar que a tomada de decisão é sensível ao risco quando a opção de risco possui dois resultados igualmente prováveis. Para as decisões baseadas na experiência, há uma reversão do efeito de reflexão com maior risco para ganhos do que para perdas, em comparação com decisões baseadas em descrição. Ao tomar decisões com base em descrições verbais, os tomadores de decisão super valorizam os eventos cisne negro, mas eles subestimam o valor desses eventos raros ao tomar decisões com base na experiência[32].

A teoria da escolha sob incerteza visa proporcionar uma estrutura coerente de princípios do comportamento racional para analisar e orientar as atitudes do tomador de decisões em relação a potenciais perdas ou ganhos. Quase todas as teorias de decisão consideram a aversão ao risco como um princípio fundamental do comportamento racional afirmando que, dada a escolha entre um resultado qualquer e uma remuneração segura igual ao valor esperado, um tomador de decisão avesso ao risco sempre irá preferir os

ganhos. Enquanto algumas teorias de decisões exibem um progresso constante para a compreensão e modelagem das atitudes do indivíduo em relação ao risco, há uma evidência cada vez maior que questiona sua aplicabilidade na tomada de decisões sob risco caracterizados como eventos raros com consequências extremas. De fato, em todas essas teorias, as premissas do comportamento racional são projetados da perspectiva de um único poto, através da aversão ao risco coletivo, cujo objetivo é alcançar ganhos além de um retorno livre de risco e quem, se desejar, pode limitar ou eliminar completamente a exposição a ativos de risco.[21]

Para Benaroch[7], há a necessidade de um conjunto de mapeamentos normativos de opções de riscos para escolher quais seriam as opções reais específicas que deveriam ser incorporaradas em um investimento afim de controlar os riscos. Apensar de um grande conjunto de pesquisas sobre gerenciamento de ricos de sistemas de informações, não há condições de demonstrar que existe uma proposta que satisfaça as necessidades práticas. Opções operacionais reais, incorporadas ao processo de investimento em tecnologia são importantes por permitir que os tomadores de decisões possuam um comportamento racional e de valor agregado, os quais afetam favoravelmente as características operacionais do investimento, observando tempo, escala, escopo e demais características. Porém, tais opções não são inerentes aos investimentos na área de tecnologia da informação. Os gestores afirmam que os investimentos devem ser cuidadosamente planejados e projetados para atender cada necessidade de forma diferente, além de serem observados os conceitos da área de gestão de risco financeiro, como forma de propor uma metodologia para planejamento, observando as opções operacionais específicas, projetadas para maximizar o valor de um investimento em tecnologia à luz dos riscos subjacentes a esse investimento. As opções de crescimento estão relacionadas aos investimentos em estratégia, descrito por infraestrutura, e que os retornos são indiretos e de longo prazo sob a forma de oportunidades de negócios futuras. Estas opções de crescimento são frutos de investimentos para o desenvolvimento de tecnologias essenciais ou para a construção de experiências com tecnologias que poderiam impulsionar futuras capacidades organizacionais. Ao contrário das opções de crescimento, as opções operacionais são comuns a todos os tipos de investimentos em tecnologia, principalmente para os que geram retornos diretos e mensuráveis. Tais opções oferecem aos tomadores de decisão a flexibilidade para adaptar as características como tempo, âmbito, escala, e outras características que possam afetar o investimento tecnológico levando em consideração a imprevisibilidade de certas condições. A avaliação de investimentos é, a priori, assumida para incorporar uma única opção operacional, porém, na execução prática as opções operacionais não são inerentes aos investimentos em tecnologia[7].

Os tomadores de decisões podem sempre considerar maneiras diferentes de estruturar

investimentos em tecnologia usando formas versáteis, havendo a viabilidade da aplicação de uma estrutura de gestão de risco baseada em opções (OBRiM) para os problemas de investimento em tecnologia de informação (TI). Tais problemas envolvem alternativas de modelos para investimento apoiados e desenvolvidos na observação de diferentes riscos e que podem melhorar os resultados dos projetos associados e o desempenho da organização[7].

O ato de tomar decisões, é importante para todos os indivíduos e acontece ao longo do dia, às vezes sem que seja notado. Tomar decisões é um ato complexo, aumentando sua complexidade quando a decisão está em um ambiente que, por si, possui características complexas por envolver dados imprecisos ou incompletos, múltiplos critérios e inúmeros agentes de decisão, somados aos vários objetivos organizacionais que acabam sendo conflitantes entre si. A tomada de decisão necessita buscar uma opção que apresente um melhor desempenho, uma melhor avaliação, ou o melhor acordo entre as expectativas do tomador de decisão, considerando a relação entre os elementos e é um processo de análise e escolha entre várias alternativas disponíveis de ações que a pessoa deverá executar[34].

O modelo racional de tomada de decisão geralmente é descrito como um processo de construção de opções. Dessa forma, devem ser calculados os níveis de risco e escolher a alternativa que tiver maior chance de sucesso, identificando o processo decisório como uma questão de maximização de utilidades, somados a racionalidade econômica. Os gestores tomam as decisões mais racionais que podem dentro das restrições impostas por informações e capacidades limitadas. A alternativa escolhida normalmente representa apenas a mais adequada entre as opções disponíveis e, portanto, não representa a intenção de se atingir os objetivos visados em toda a sua plenitude. A tomada de decisão consiste de um inter-relacionamento entre as pessoas, com a presença de diversos fatores intuitivos, provenientes de experiência pessoal e personalidades envolvidas no processo decisório, onde a importância destes fatores, na qualidade de decisão, diferenciam o bom do mau decisor. O processo decisório significa optar entre diversas alternativas viáveis oferecidas e, muitas vezes, influenciado pela qualidade, fluxo de informações, recursos e tempo disponíveis[34].

2.2.1 Sistemas de apoio à decisão (SAD/DSS)

Teoricamente, é notório e até um consenso que as decisões que utilizam sistemas de suporte à decisão (DSSs) podem ser mais eficientes e ágeis do que as decisões sem ajuda. Porém, quando observado o comportamento de tomadores de decisões, é surpreendente como nem sempre aproveitem o DSS para suportar sua tomada de decisões[10].

O suporte efetivo à decisão tornou-se mais importante devido ao aumento do fortalecimento dos funcionários, elevados requisitos para a velocidade e a qualidade em decisões gerenciais e maior acessibilidade a uma grande quantidade de informações, somados ao

surgimento de uma economia eletrônica que aumentou profundamente a necessidade de apoio à decisão. Motivos por tais circunstâncias, o desenvolvimento de sistema de suporte à decisão (DSS) deixou de ser uma organização tradicional do sistema de "caixa de ferramentas"e passou a ser um paradigma extremamente colaborativo e ativo. Dessa forma, os pesquisadores relacionados à processos de decisões salientam a importância de um maior suporte ao nível cognitivo, proporcionando o encorajamento de processos divergentes de alternativas de decisão, criticando automaticamente as alternativas[47].

Pessoas de deparam com situações que é necessário um posicionamento sobre como agir, sobre o melhor caminho à ser seguido e qual decisão deve tomar dentro de seu cotidiano nas organizações e, por conta do número de objetivos que se pretende atingir, tomar decisões torna-se um problema complexo e a escolha do melhor caminho pode ser um problema de difícil solução. Dessa forma, o uso de técnicas do uso de múltiplos critérios visa reduzir a subjetividade das decisões, recomendando um conjunto de ações que reflitam medidas objetivas, apoiando as preferências do decisor. Tais técnicas demonstram-se importantes, haja vista que o ser humano se depara com a necessidade de decidir, tendo como base, a associação de parâmetros qualitativos e quantitativos, com extrema característica subjetiva[42].

As decisões que utilizam sistemas de suporte à decisão (DSSs) podem ser feitas de forma mais rápida e precisa do que as decisões sem qualquer ajuda ou suporte e, surpreendente, grande parte dos decisores nem sempre aproveitem o DSS para suportar sua tomada de decisões. Tal comportamento aumenta a necessidade de entender como encorajar o uso de sistemas de apoio à decisões, porém, alguns estudos concluíram que nem sempre há um ganho ou aumento de desempenho com uso de DSS. É importante que seja medido o uso real do DSS, em vez da intenção de uso. Isso se dá porque as baixas correlações relatadas entre a intenção e o uso do sistema sugerem que a intenção pode não ser adequada para o uso real. O aumento da motivação do DSS que incorpora uma estratégia de decisão compensatória precisa, deve levar a um melhor desempenho de decisão. A estratégia de decisão compensatória de diferença aditiva exige que os usuários se envolvam em comparações iterativas de todas as alternativas disponíveis para chegar a uma escolha final. Tomadores de decisão preferem a estratégia de decisão compensatória quando um DSS oferece um alto suporte para esta estratégia. Um DSS que incorpora esta estratégia normativa aumenta a precisão e mitiga a quantidade de esforço cognitivo necessário para avaliar cada atributo e alternativa e o tempo necessário para tomar uma decisão. Uma estratégia de decisão precisa que atenua o esforço de processamento de informações e, ao mesmo tempo, atende às expectativas dos usuários em alcançar seus objetivos, proporcionam o aumento da motivação do DSS e o uso subsequente do DSS para completar uma tarefa, levando a um melhor desempenho de decisão, fazendo com

que o desempenho da decisão melhore quando um DSS é adequado para uma tarefa e suporta o usuário através de um esforço reduzido[10].

Seres humanos são propensos a tomar decisão de forma errada e muitas vezes sujeita a preconceitos, causado pela má ponderação de informações importantes e os atrasos de *feedback*, o que dificulta a aprendizagem. A informação de tarefas se mostrou valiosa para melhorar a tomada de decisões, mesmo que essas informações raramente estejam disponíveis. Uma abordagem de "diagnóstico de qualidade de decisão"(DDQ) pode ajudar os decisores a descobrir as informações necessárias, podendo identificar erros sistemáticos específicos do contexto na tomada de decisões de forma a facilitar mudanças adaptativas e melhorar o desempenho. Uma das preocupações do ser humano é avaliar a qualidade das decisões tomadas, porém, há raros estudos sistemáticos para que se possa mensurar o nível de conhecimento. Em geral, há uma tendência para julgar decisões com base em seus resultados - se o resultado for bom então, a decisão foi boa. Outro ponto de vista é a percepção de que decisões devem ser julgadas boas ou ruins de acordo com a qualidade do processo pelo qual elas foram feitas. A literatura baseada na análise de julgamento demonstrou que melhorar os processos de tomada de decisão humana é um exercício nada trivial. Os seres humanos, enquanto são adaptativos, muitas vezes ignoram informações relevantes ou pesam de forma inadequada e, consequentemente, fornecer ferramentas de suporte a decisões úteis também não é uma solução de certeza-ganha, pois os usuários geralmente descartam erroneamente o valor dos modelos quantitativos que eles incorporam. Para melhorar o desempenho das decisões, informações de diagnóstico e *feedback* devem ser fornecidos aos tomadores de decisão - informações que podem ajudá-los na revisão de seus processos de decisão ao invés de simplesmente informar seu desempenho[12].

2.3 Considerações sobre o referencial teórico

Analisando o referencial teórico pela perspectiva dos objetivos descritos no capítulo 1, observa-se que a análise de risco, apesar de ser um tema amplamente discutido e com métodos estabelecidos, ainda mantém certo afastamento e pouca interação com os modelos de arquitetura e apoio ao planejamento e tomadas de decisões estratégico. É possível notar que há uma descrição para processos decisórios, porém, inerente à avaliação e o tratamento de riscos organizacionais.

Apesar de ser um consenso entre os referenciais apresentados no capítulo 2, onde se demonstra que a gestão de riscos necessita atuar como uma ferramenta de sustentação para o planejamento estratégico organizacional, subsidiando ao processo de entendimento das fronteiras e limitações relevantes aos direcionamentos organizacionais, não há uma descrição de como ou quais aspectos devem ser observar para alcance de tal princípio.

Esta característica promove o distanciamento dos tomadores de decisões na observação e no uso da gestão de riscos como parte dos processos de sustentação direta dos processos de negócios e aos seus princípios, destacando o apoio aos processos decisórios e direcionamentos estratégico, maximizando os resultados e os retornos dos investimentos, além dos alcances para os objetivos de negócio.

Os métodos são focados em descrições para a redução do efeito de eventos, porém, há margem para um entendimento intuitivo sobre como classificar tais eventos. É notório que a incerteza é o ponto crucial para o sucesso ou insucesso de uma gestão de riscos, desde que, tais incertezas sejam relacionadas ao efeito de eventos (previstos e conhecidos ou incertos) e não à incerteza de ocorrência de um evento, já que este último cenário é intangível, já que a incerteza é o desconhecimento, mesmo que imparcial sobre um determinado assunto.

Apoiados pela ausência de uma descrição formal e de uma definição clara da relação entre risco, incerteza, evento, consequência e impacto, o ser humano se apoia cada vez mais na intuição para tomar decisões. A probabilidade como ferramenta de mensuração de ocorrência de um evento não demonstra os aspectos incertos de suas consequências e impactos, sendo limitada na sua capacidade de refletir a dinâmica dos ecossistemas institucionais.

Tais métodos assumem que os cenários institucionais e as premissas adotadas para prospecção de riscos permanecerão estáticos durante toda a sua vida. Tempo é um fator de extrema relevância para um processo decisório, podendo ser preponderante para o aumento do estresse e um apego cada vez maior à intuição nos processos decisórios. Considerando que o ser humano possui uma tendência natural para considerar riscos como perdas, ignorando as perspectivas de ganhos ou oportunidades, ser tomadores de decisões possuem limitações naturais para o uso da gestão de riscos como ferramenta de decisão.

Dadas as limitações dos métodos tradicionais e do comportamento humano para os processos decisórios, o método de Opções Reais, Cisne Negro, análise multicritérios são apontadas como a solução adequada para análise de riscos em ambientes de incerteza, reduzindo o nível da intuição e aproximando a gestão de riscos aos processos organizacionais. No entanto, apesar de tais ferramentas conseguir valorar a flexibilidade da incerteza e melhorar os processos decisórios, enfrentam certa resistência por parte de gerentes e tomadores de decisão devido ao desconhecimento, o forte apego pela busca à conformidade e a complexidade no seu uso. Um dos caminhos alternativos entre as limitações dos métodos tradicionais e a complexidade das Opções Reais é a avaliação de todas as opções no inicio do projeto pelos métodos tradicionais. Quando observados os riscos envolvidos nos projetos de TI, estes se mostram complexos, envolvendo efeitos potencialmente graves,

por serem parte do ecossistema sustentação dos processos de negócios das organizações. Contudo, apesar das altas taxas de falhas em projetos e do alto volume de investimentos realizado em TI, os modelos de análise de risco para projetos de TI não oferecem uma avaliação clara do impacto para os processos de um ensaio para demonstrar a curva de discrepância dos processos decisórios e o apoio para a gestão de riscos como ferramenta de decisões.

Tão importante quando definir qual ferramenta usar, apoiar-se em um sistema de suporte à decisões possibilita ao tomador de decisões melhores resultados. Para melhorar o desempenho dos processos decisórios, informações de diagnóstico e *feedback* devem ser fornecidos aos tomadores de decisão. Tais informações devem ajudá-los na revisão de seus processos de decisão ao invés de simplesmente informar seu desempenho.

Considerando que as decisões estão sustentadas por uma visão de riscos (mesmo que de forma muito subjetiva, quando pensamos em perdas), podemos entender que a gestão de riscos dever ser considerada como elo de ligação entre os componentes organizacionais, apoiando na construção de informação baseadas na visão do ecossistema, na capacidade e no nível de sustentação dos processos de negócios, podendo defletir a transversalidade dos processos organizacionais.

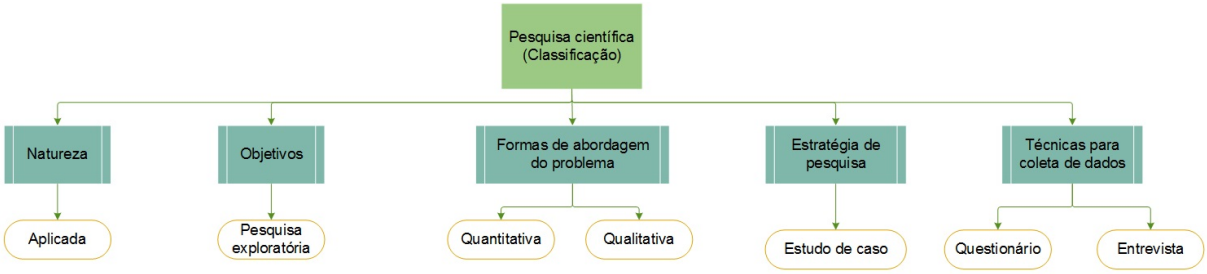
Capítulo 3

Metodologia

Os objetivos para este trabalho buscam descrever os efeitos da redução da intuitividade para os processos de decisões, através da gestão de riscos.

Baseado nas definições de Gil[18] , Marconi e Lakatos[27] e Silva e Menezes[44], essa pesquisa pode ser classificada como: (a) quanto a natureza, pesquisa aplicada; (b) no que diz respeito aos objetivos, pesquisa exploratória; (c) qualitativa, quanto a abordagem.

Figura 3.1: Formas de classificação das pesquisas científicas.



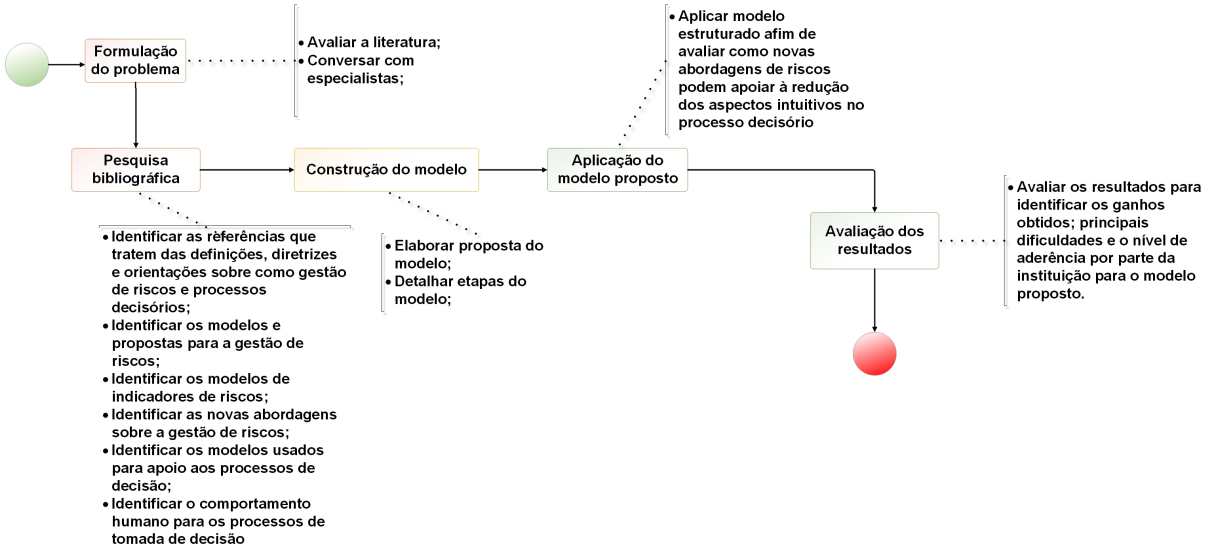
A coleta dos dados se dará no âmbito da administração pública federal, através da análise do ranking de governança por meio do relatório de levantamento de governança do Tribunal de Contas da União - IGOV-TCU complementada por uma um questionário estruturado para gestores de TI e pelo estudo de caso em uma entidade escolhida à partir do cruzamento dos dados coletados.

Assim, pode-se observar a estrutura da pesquisa, conforme descrito à seguir:

3.1 Estruturação da pesquisa

Afim de demonstrar as etapas que serão adotadas para execução da pesquisa, será observado o fluxo, conforme Figura 3.2.

Figura 3.2: Estruturação da pesquisa



3.1.1 Formulação do problema

Através do levantamento da revisão bibliográfica e da necessidade de melhoria da eficiência dos processos decisórios para investimentos em TI, foi possível identificar características no processo de decisão que traduz um dos objetivos deste trabalho, o qual retrata as características intuitivas para o comportamento de tomadores de decisões.

3.1.2 Pesquisa bibliográfica

Foi realizada pesquisa bibliográfica afim de demonstrar a coerência do problema proposto, assim como contextualizar, justificar e demonstrar como podem ser

3.1.3 Construção do modelo

Foram realizadas as atividades de estudo da aplicação combinada de técnicas de BPM, tomada de decisões, análise de riscos, técnicas de redução da intuição, com o objetivo de desenvolver e descrever um modelo apoio à decisões contendo orientações práticas para sua aplicação.

3.1.4 Aplicação do modelo proposto

Foi realizada a aplicação da metodologia desenvolvida em um estudo de caso com o objetivo de verificar a sua viabilidade de uso e descrever os resultados obtidos.

3.1.5 Avaliação dos resultados

Foi realizada a análise dos resultados da aplicação da metodologia com o propósito de avaliar sua utilidade e aplicabilidade.

Com isso, no próximo capítulo será elaborado uma análise crítica baseada nos resultados obtidos e, por fim, apresentados os resultados finais.

Concluída a apresentação da metodologia da pesquisa, no próximo capítulo será apresentada a proposta do modelo de apoio à decisões.

Capítulo 4

Estruturação de um Modelo de apoio à tomada de decisão

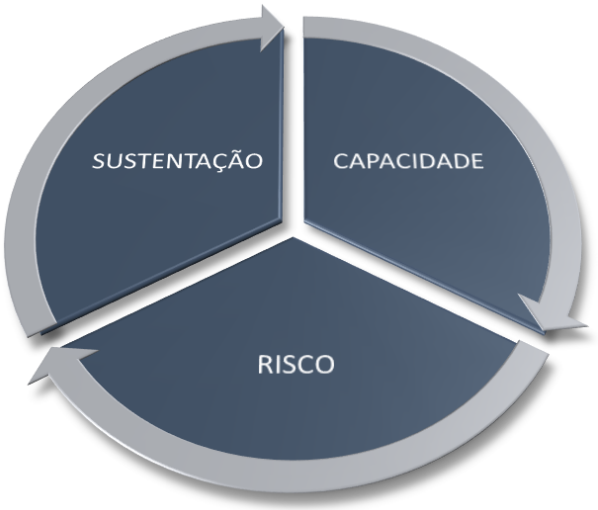
O objetivo deste capítulo é apresentar a Metodologia Indicadores de Apoio à Tomada de Decisões baseados em riscos, capacidade e sustentação (IATD/RCS) desenvolvida nessa pesquisa, apresentando inicialmente a contextualização e motivação para a escolha das principais técnicas e ferramentas adotadas; em seguida a visão geral da sua estrutura; no restante do capítulo, a descrição de cada uma das fases da metodologia e na última Seção, a descrição da compatibilidade do IATD/RCS com outras abordagens conhecidas. O IATD/RCS uma proposta para o diagnóstico da transversalidade do ecossistema organizacional com a finalidade de prover orientações que possam ser seguidas para apoiar aos processos decisórios à partir de uma visão holística da sustentação, da capacidade de atendimento dos requisitos e dos riscos de negócio.

Devido às limitações temporais relativas ao prazo para conclusão desta pesquisa, a metodologia a ser desenvolvida teve como foco apenas a descrição do processo baseado nas lacunas observadas na literatura. Portanto, questões relativas à quais técnicas ou ferramentas devem ser mais apropriadas ou mesmo um estudo comparativo entre as diversas ferramentas existentes para apoio à decisão complexa e o efeito dessas quando usadas em um contexto de riscos não farão parte do escopo, no entanto poderão ser alvo de estudos futuros. O restante desse capítulo se ocupará em detalhar cada uma das fases e respectivos subprocessos. A especificação do método vai apresentar as atividades e respectivas entradas, assim como as saídas esperadas, apoiado por uma abordagem descritiva para as técnicas e ferramentas a serem utilizadas.

4.1 Motivação para escolha das principais técnicas e ferramentas adotadas

Conforme Figura 4.1, o modelo proposto está focado na observação de 3 pilares inerentes aos processos estratégicos e operacionais organizacionais, o risco, a capacidade de entrega e o nível de sustentação do negócio.

Figura 4.1: Pilares do IATD/RCS.



Para o desenvolvimento da modelo proposto, foram selecionadas técnicas e ferramentas conhecidas e amplamente difundidas como gestão de processos de negócios, gestão de riscos e para apoio aos processos de decisões complexas. A partir da avaliação das informações obtidas com a revisão de literatura sobre as técnicas e ferramentas de apoio à decisões e análise de riscos e dos resultados das experimentações com algumas delas, foram selecionadas aquelas que se mostraram viáveis e úteis para aplicação no contexto aplicado.

Quando avaliadas as ferramentas e as necessidades inerentes aos modelo, foi possível identificar o desafio da integração dos processos de forma transversal e da possibilidade de integração dos processos estratégicos e operacionais. Dessa forma, as principais motivações para escolha delas, são as seguintes:

- Análise da arquitetura organizacional: Análise do ecossistema de sustentação do negócio observando a arquitetura organizacional buscando o entendimento da cadeia de sustentação dos processos finalísticos. Dessa forma, é possível definir a cadeia de sustentação dos processos organizacionais;

- Utilização de técnicas de apoio à decisões complexas: A decisão pela adoção dessa abordagem foi tomada levando em considerando o comportamento humano para os processos decisórios e para a forma como observam riscos. O uso de ferramentas e técnicas de decisões complexas apoiam para maximização dos resultados e reduzem o nível de intuitividade das decisões;
- Ferramentas de gestão de riscos: Considerando que a observação de riscos pode criar um conjunto de cenários tão amplo que pode ser inexequível para tomadas de decisões eficazes, é necessário que o processo decisórios se concentre em indicadores significativos para a obtenção dos resultados desejados. Para evitar a criação de muitos cenários diferentes que possam levar à perda do foco, distanciando os decisores das metas estabelecidas, foram adotadas técnicas de análise de riscos com o intuito de prover orientações para a criação e seleção dos indicadores de decisão;
- A exequibilidade da gestão de riscos: A capacidade de execução da gestão de riscos de forma eficaz, eficiente e, principalmente efetiva, capaz de gerar cenários de decisões que apoiem aos objetivos estratégicos das organizações;
- Transversalidade dos processos decisórios: A integração do gerenciamento de riscos como parte dos processos organizacionais e decisórios. Dessa forma, a gestão de riscos será parte de todo o ciclo estratégico operacional possibilitando a criação de indicadores de decisões transversais;

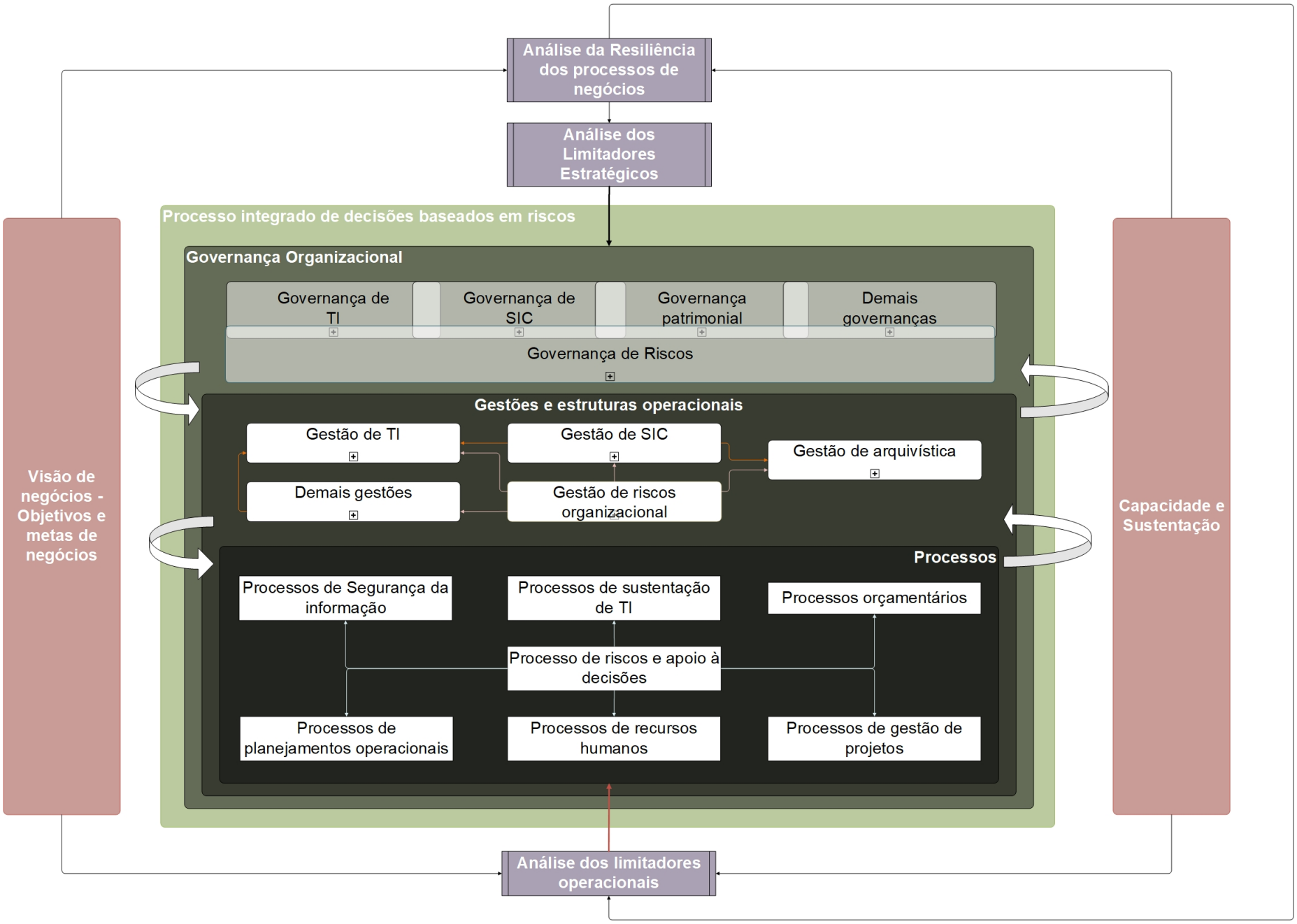
Para o modelo proposto, risco é definido como a incerteza da consequência de um evento, onde evento é todo e qualquer acontecimento, seja controlado ou não, passíveis ou não de previsão. Governar e gerir está relacionado à capacidade de controle e reação para os diversos cenários inerentes às incertezas de eventos de forma transversal, observando as camadas estratégicas, táticas e operacionais. Dessa forma, a eficiência de uma decisão está intimamente ligado à capacidade governar e gerir.

4.2 Visão geral da arquitetura e transversalidade organizacional

É necessário que haja uma visão holística da organização proporcionando um olhar transversal de toda a arquitetura que sustenta os processos de negócios. Conforme demonstrado na Figura 4.2, é necessário que a organização seja vista como um ecossistema no qual todas as camadas são integradas e complementares. Assim, a construção de processos transversais torna-se indispensável. Por consequência da transversalidade dos processos, os

indicadores gerados serão capazes de demonstrar de forma holística os cenários institucionais.

Figura 4.2: Estrutura organizacional do IATD/RCS.



Com a transversalidade dos processos é possível determinar as fronteiras institucionais que serão observados como parte dos critérios decisórios, apoiada pelo estabelecimento de uma visão voltada ao negócio, pela definição dos limites de resiliência dos processos finalísticos e operacionais, pela capacidade e nível de sustentação e pela definição dos limitadores de negócios e operacionais.

Para maximizar os resultados obtidos e minimizar o nível da erro causado pela intuição e o forte apego ao risco, quando este representa perda e a rejeição ao risco quando representa ganhos, convém que sejam usadas técnicas multicritérios como ferramenta de integração para estabelecimento das fronteiras estratégicas, táticas e operacionais. O uso de tais ferramentas possibilita a redução do desvio da intuição através dos algoritmos matemáticos usados por estas ferramentas. De forma complementar, o estabelecimento de uma visão transversal proporcionada a observação dos impactos dos eventos em toda cadeia de sustentação dos processos finalísticos, confrontando-os às fronteiras estabelecidas. Com tal abordagem o modelo propõe uma visão mais ampla das consequências de eventos, desenvolvendo indicadores de decisões baseados em riscos.

Dois aspectos devem ser considerados para o mapeamento e definição dos cenários de eventos:

- A possibilidade de previsibilidade: A probabilidade pode ser usada como uma ferramenta de medição das consequências de eventos baseados em dados históricos, porém é incapaz de prever o futuro pela mudança na dinâmica operacional e de direcionamento dos objetivos e metas. Dessa forma, apenas eventos aos quais se tem o conhecimento em sua totalidade é que há a possibilidade da previsibilidade. Para os eventos para os quais há um conhecimento parcial, é necessário que haja o apoio de técnicas de construção de cenários baseados nas informações conhecidas. Para eventos desconhecidos, para os quais não há dados históricos mas são passíveis de previsibilidade por observação de eventos externos ou indiretos, convém o uso estudo de cenários como ferramenta de proposição da previsibilidade;
- Análise de eventos externos: Necessário para que sejam observados aspectos externos (discretos ou não) que possam afetar a sustentação dos negócios. Para que não haja confusão com os contextos externos, a observação dos eventos externos tem por objetivo a construção de cenários que, direta ou indiretamente, sejam capazes de descrever possíveis eventos que venham afetar à organização. Não são tratados os aspectos de contextos, conforme descrito nos referenciais apresentados no Capítulo 2.

O IATD/RCS não trata de uma metodologia ou fluxo de atividades que devam ser seguidas. O modelo trata de aspectos que devem ser considerados para a construção de indicadores de apoio à decisão. Dessa forma, os direcionamentos do IATD/RCS foram

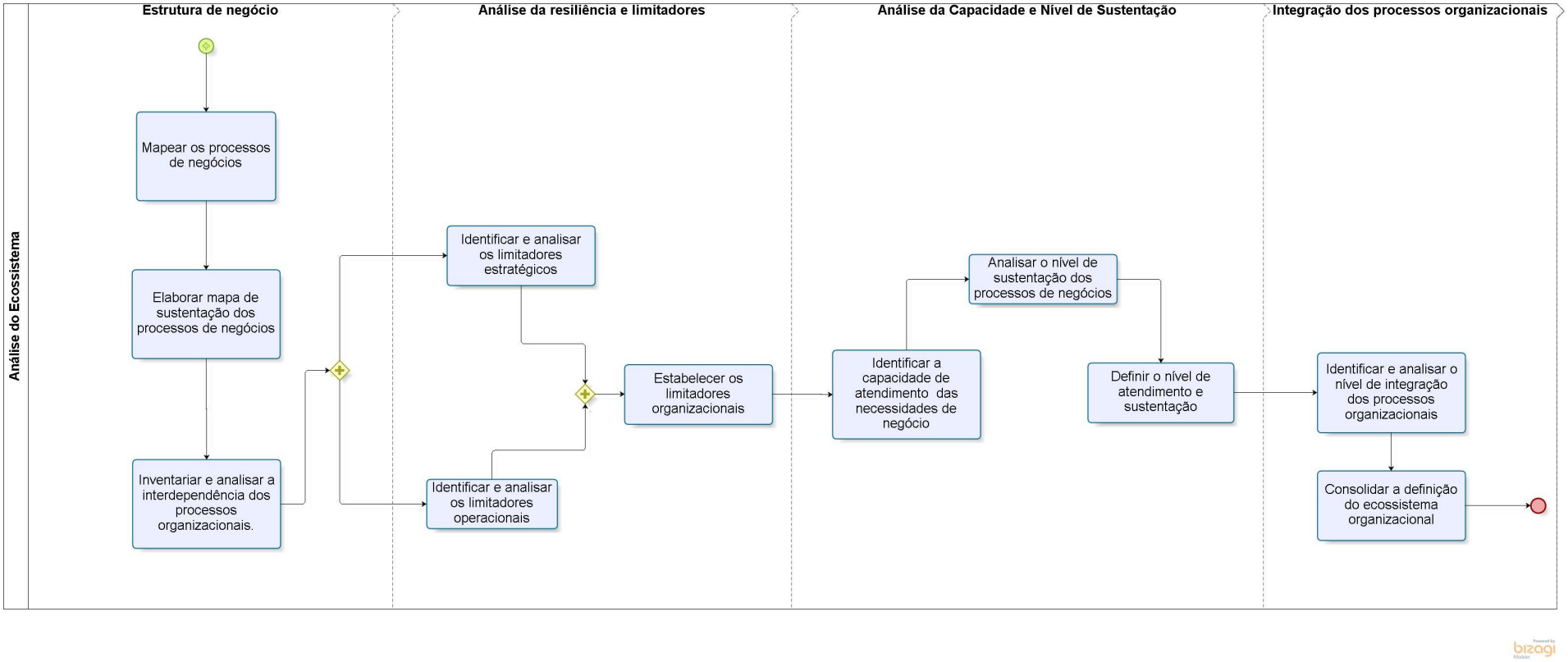
organizadas em uma estrutura com cinco fases: Identificação do Problema, definição dos critérios; análise de dependência dos processos organizacionais, definição das fronteiras estratégicas e operacionais, análise e avaliação das possíveis alternativas, análise e avaliação dos riscos, tomada de decisão. Essas fases foram ordenadas em forma de cascata, de modo que as saídas de uma fase são utilizadas como entradas nas fases subsequentes.

4.2.1 Descrição da etapa de análise do ecossistema

Como etapa inicial, serão tratados os aspectos da construção da transversalidade organizacional que será baseada em 4 fases, conforme Figura 4.3.

As fases para esta etapa estão estruturadas em (*i*) Entendimento de negócio: Criação do mapa sustentação entre os processos de negócios; (*ii*) Análise da capacidade e nível de sustentação: Análise e avaliação da capacidade de atendimento e do nível de sustentação dos processos estratégicos e operacionais; (*iii*) Análise da resiliência e limitadores: Definição dos critérios e estabelecimento da resiliência dos processos organizacionais assim como identificação dos limitadores estratégicos operacionais; (*iv*) Integração dos processos organizacionais: Elaborar o mapa de integração e sustentação dos processos organizacionais afim de demonstrar o efeito de eventos nas diversas camadas de sustentação e atendimento dos processos finalísticos;

Figura 4.3: Fluxo detalhado Análise do Ecossistema Organizacional IATD/RCS.



1. **Mapear os processos de negócios**

   Objetivos - Inventariar e estabelecer a classificação por prioridade dos processos de negócios de forma clara e objetiva.

   Entradas - Objetivo, missão e visão organizacional, inventário dos processos finalísticos, visão da alta gestão, contextos externos e internos, metas estabelecidas.

   Descrição da Atividade - Inventariar, através de entrevistas, ferramentas e técnicas estabelecidas para inventariamento de processos todos os processos finalísticos da organização. Necessário que seja utilizado técnicas de causa-efeito ou similares para definir a classificação de priorização dos processos inventariados.

   Observações - Para o inventário dos processos organizacionais, o uso de um consultor externo poderá apoiar e maximizar os resultados, haja vista que este usará ferramentas e a imparcialidade com a qual tratará as informações da alta gestão apoiará na redução da intuição.

   Saídas - Mapa dos processos organizacionais.

2. **Elaborar mapa de sustentação dos processos de negócios**

   Objetivos - Identificar o mapa de sustentação horizontal(entre os processos organizacionais) e vertical (entre os processos organizacionais e os operacionais).

   Entradas - Mapa dos processos organizacionais.

   Descrição da Atividade - Elaborar um estudo técnico para demonstrar o nível de sustentação entre os processos de negócios (identificação de "alimentação"entre os processos) e entre os processos de negócios e o ambiente operacional.

   Observações - Convém que o mapa de sustentação seja claro suficiente para identificar, com o menor tempo de resposta, a capilaridade dos impactos decorrentes de eventos.

   Saídas - Mapa de sustentação.

3. **Inventariar e analisar a interdependência dos processos organizacionais**

   Objetivos - Identificar o mapa de sustentação horizontal(entre os processos organizacionais) e vertical (entre os processos organizacionais e os operacionais).

   Entradas - Mapa de sustentação.

   Descrição da Atividade - Elaborar estudo para definição da interdependência dos processos de negócios.

   Observações - Descrição clara da interdependência dos processos, demonstrando grau de sustentação;

Saídas - Mapa de interdependência dos processos.

4. **Identificar e analisar os limitadores estratégicos**

   Objetivos - Identificar os limitadores estratégicos, sejam eles humanos, operacionais, de processos, financeiros e outros que possam ser identificados.

   Entradas - Mapa dos processos organizacionais, Mapa de sustentação, Mapa de interdependência dos processos.

   Descrição da Atividade - Identificar os limitadores estratégicos estratégicos que possam impactar aos processos decisórios estratégicos.

   Observações - Os limitadores que devem ser considerados são aqueles que, em um processo decisório, representam fronteiras para o tratamento das consequências de eventos;

   Saídas - Mapa de limitadores estratégicos.

5. **Identificar e analisar os limitadores operacionais**

   Objetivos - Identificar os limitadores operacionais.

   Entradas - Mapa de limitadores estratégicos, Mapa de interdependência dos processos, Mapa de sustentação.

   Descrição da Atividade - Identificar os limitadores operacionais, sendo eles de processos, humanos, orçamentários, técnicos, tecnológicos, dentre outros.

   Observações - Os limitadores devem ser considerados como parte dos critérios de decisões;

   Saídas - Mapa de limitadores operacionais.

6. **Estabelecer os limitadores organizacionais**

   Objetivos - Estabelecer os limitadores organizacionais que serão usados como critérios de decisões.

   Entradas - Mapa de limitadores organizacionais, mapas de limitadores operacionais.

   Descrição da Atividade - Elaborar estudo para definição da interdependência dos processos de negócios.

   Observações - Descrição clara da interdependência dos processos, demonstrando grau de sustentação;

   Saídas - Definição dos limitadores organizacionais.

7. **Identificar a capacidade de atendimento das necessidades de negócios**

   Objetivos -Avaliar a capacidade operacional de atendimento das necessidades de negócios.

   Entradas - Mapa de limitadores organizacionais, Mapa dos processos organizacionais.

   Descrição da Atividade - Com base nos limitadores organizacionais, deve-se estabelecer a capacidade de atendimento das necessidades estratégico-operacional.

   Observações - A capacidade de atendimento deve ser considerado como parte dos critérios de decisão, sendo observado como parte das fronteiras organizacionais.

   Saídas - Mapa de capacidade de atendimento.

8. **Analisar o nível de sustentação dos processos de negócios**

   Objetivos - Identificar e analisar o nível de sustentação dos processos organizacionais.

   Entradas - Mapa de capacidade, Mapa de limitadores organizacionais, Mapa dos processos organizacionais.

   Descrição da Atividade - De forma complementar ao mapa de capacidade, o mapa de sustentação deve demonstrar o nível de sustentabilidade dos processos.

   Observações - Enquanto a capacidade avalia o nível de entrega para demandas, o nível de sustentação preocupa-se com o nível de sustentabilidade e continuidade dos processos. Dessa forma, requisitos humanos, técnicos e tecnológicos. O nível de sustentação deve ser considerado como parte dos limitadores organizacionais.

   Saídas - Mapa de sustentabilidade.

9. **Definir o nível de atendimento e sustentação**

   Objetivos - Consolidar o mapa de sustentação à partir dos mapas de capacidade e sustentação o nível de atendimento e perenidade dos processos estabelecidos.

   Entradas - Mapa de atendimento .

   Descrição da Atividade - À partir da consolidação dos mapas de capacidade, mapa de sustentação e mapas de limitadores é necessário que seja descrito o nível de atendimento aos processos operacionais e estratégicos.

   Observações - A consolidação de atendimento e sustentação deve ser considerado como fator preponderante para os processos decisórios.

   Saídas - Critérios de sustentação.

10. **Identificar e analisar o nível de integração dos processos organizacionais**

    Objetivos - Analisar o nível de transversalidade dos processos organizacionais como forma de complementar os indicadores criados nas etapas de Mapear os processos de negócios e Inventariar e analisar a interdependência dos processos organizacionais.

    Entradas - Mapa de processos de negócios, Mapa de interdependência, Mapa de sustentação, Mapa de capacidade.

    Descrição da Atividade - À partir do mapeamento dos processos estratégicos e operacionais é necessário que seja avaliado o nível de integração entre os processos operacionais.

    Observações - É importante que o nível de integração seja estabelecido e analisado, haja vista a necessidade da transversalidade dos processos é considerado um critério para os processos decisórios.

    Saídas - Mapa de integração dos processos.

11. **Consolidar a definição do ecossistema organizacional**

    Objetivos - Consolidar os critérios decisórios institucionais.

    Entradas - Mapas descritos nas etapas anteriores.

    Descrição da Atividade - Definição dos critérios através da consolidação critérios parciais desenvolvidos anteriormente.

    Observações - Criação das fronteiras institucionais para os processos decisórios.

    Saídas - Critérios decisórios organizacionais.

Para que cada uma das etapas sejam cumpridas, antes de entrar em um plano de execução, é necessário observar o apoio dos membros envolvidos no projeto e o nível de aceitação de uma nova abordagem. Caso seja identificado rejeição ou mesmo negação ao processo, pode-se apoiar na andragogia para promover uma aceitação dos participantes. Para isso, deve-se observar alguns aspectos e apoiar-se nos pressupostos-chave da andragoia, podendo destacar ***(i)*** **Necessidade (aplicabilidade)** - A capacidade de demonstrar relevância demonstrando a aplicabilidade dentro de contidiano; ***(ii)*** **Autonomia (autodiretividade)** - Identificar como alcançar a cada membro participante; ***(iii)*** **Experiência prévia** - Capacidade de demonstrar interesse em ouvir e entender as experiências vividas, sejam positivas ou negativas; ***(iv)*** **Interatividade** - Demonstrar aos membros participantes o quanto sua visão, opinião e interação é importante para o desenvolvimento do projeto; ***(v)*** **Segurança e respeito** - Promover um ambiente de interação que não exponha os partícipes à constrangimentos e promova um clima de acolhedor, respeitoso

e seguro; ***(vi)*** **Feedback (Reflexão)** - Encorajar aos partícipes em praticar os novos conhecimentos e de refletir sobre sua prática, analisar e avaliar seu próprio desempenho.

O modelo é adaptativo para o uso de técnicas que devam ser usadas para a execução. Foram testadas algumas técnicas para apoiar no desenvolvimento da construção do modelo, como técnicas de causa efeito, de perdas e ganhos, espinha de peixes, *brainstorm*, simulação de monte carlo e os melhores resultados obtidos foram a associação de *brainstorm* e *monte carlo ahp*. Através de reuniões e uso brainstorm e de técnicas causa efeito foram feitos o levantamento preliminar de informações, e através do monte carlo ahp foi feita a construção correlação de uma visão institucional para que pudesse ser confrontada com visão mais operacional.

Para projetos de infraestrutura de TI, foram usadas técnicas de brainstorm, causa efeito, mapeamento da dependência para sustentação, aplicado nas camadas de negócio e operacionais, sendo possível confrontar os resultados e poder definir o melhor caminho à ser seguido. Como forma de criar uma tabulação para escolha do melhor caminho, foi ainda usado o mapeamento de resiliência como ferramenta.

Tais técnicas foram usadas por conta da limitação de informações e maturidade para levantamento de informações e a ausência de conhecimento dos atores envolvidos, quando observado a transversalidade dos processos organizacionais.

Apesar de simples, do modelo promove maior adesão e assertividade por maior interação de todas as camadas organizacionais, possibilitando uma visão holística e uma construção mais objetiva de mecanismos de decisões. Como forma de demonstrar a aplicabilidade e os benefícios do modelos, será apresentado um estudo de caso no Capítulo 5.

4.3 Ciclo IATD/RCS para tomada de decisões

Observados os limitadores e do entendimento do ecossistema organizacional, pode-se estabelecer o processo de decisões considerando os limitadores e critérios estabelecidos.

- Identificação do Problema: Definição do problema e objetivos através do uso de ferramentas e técnicas que possibilitem uma visão transversal da necessidade apresentada. Para esta fase o apoio de ferramentas necessário que seja claramente definido o escopo e a abrangência do problema;
- Definição dos critérios: Estabelecer os critérios que deverão ser usados para os processos decisórios. A Análise da capacidade de entrega e do nível de sustentação dos processos estratégicos operacionais devem ser observados como parte dos critérios;
- Análise de dependência: Analisar e avaliar o nível de dependência entre os processos de negócios, entre os processos operacionais, avaliando o nível de integração dos

Figura 4.4: Ciclo de decisões IATD/RCS.

processos de sustentação, assim como o quanto são capazes de entregar à governança informações de apoio efetivo à decisão. Esta etapa está ligada diretamente com a etapa de Inventariar e analisar a interdependência dos processos organizacionais, apresentado no entendimento do ecossistema. Dessa forma, deve ser considerado o Mapa de interdependência.

- Definição das fronteiras: Catalogar os limitadores organizacionais que podem ser determinantes para os processos de negócios ou para o apoio à decisão. Elaborar a descrição do nível de alcance organizacional para a gestão de riscos e os processos decisórios. Esta etapa está relacionada com a etapa de Estabelecer os limitadores organizacionais.
- Análise e avaliação das alternativas: Através de cenários estabelecidos, é possível desenvolver a análise e avaliação dos resultados para que haja o direcionamento de

quais são as melhoras opções para os processos decisórios.

- Análise e avaliação dos riscos: Através do uso de técnicas de gestão de riscos e decisões complexas, elaborar cenários que possibilitem a descrição das consequências do agir e não agir para cada evento descrito. Dessa forma, a gestão de riscos passa ser uma ferramenta de gestão e governança, conforme preconizado no Capítulo 2;
- Tomada de decisões: Selecionar o cenário que representa a melhor alternativa para a organização, dados os limitadores, fronteiras e metas estabelecidas;

Concluída a apresentação do modelo, será apresentado um estudo de caso, demonstrando o resultado da aplicação do modelo proposto.

Capítulo 5

Estudo de caso

Nesse capítulo serão apresentados os resultados obtidos pelo uso do modelo proposto no planejamento de contratação de uma fábrica de software de uma entidade da administração pública federal. Dessa forma, seguindo a descrição do modelo proposto, foram executadas as etapas:

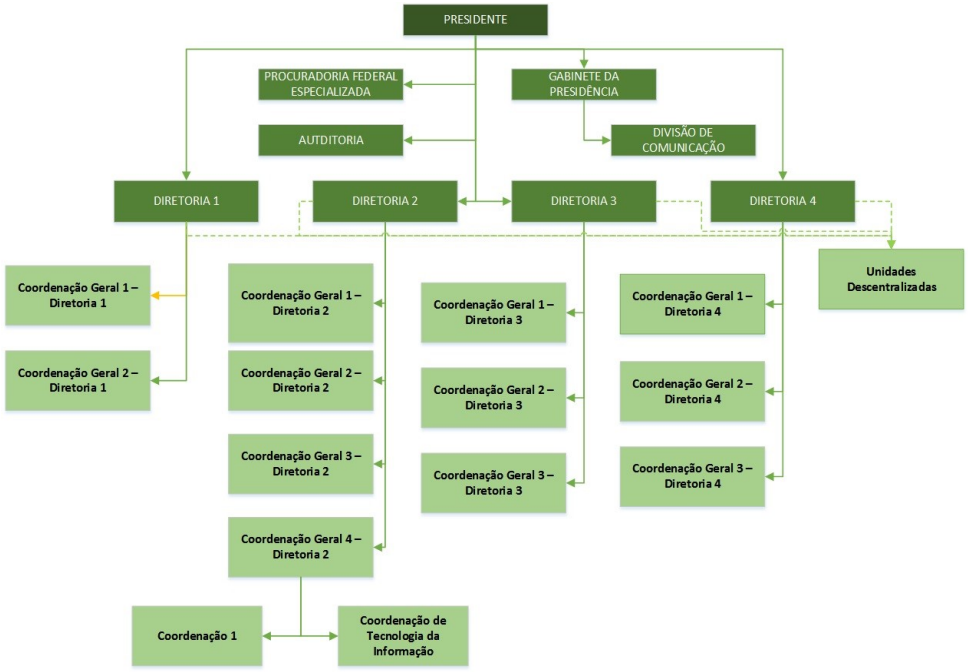
- (*i*) Estrutura de negócio: Objetivando entendimento da entidade e seus processos de negócios;
- (*ii*) Análise da resiliência e limitadores: Objetivando a identificação de possíveis limitadores estratégicos e operacionais, além da definição da resiliência. Para o estudo, resiliência foi traduzido como suporte ao tempo de parada dos sistemas;
- (*iii*) Análise da capacidade e nível de sustentação: Afim de identificar o nível de entrega e nível de sustentação dos sistemas. Nessa etapa, o ponto de análise foi a sustentação econômica;
- (*iv*) Integração dos processos organizacionais: Afim de demonstrar os impactos transversais de possíveis eventos.

5.1 Execução do modelo

5.1.1 Estrutura de negócio

O órgão selecionado para este estudo é uma autarquia vinculada ao Governo Federal. Este é um órgão de abrangência nacional, composto por aproximadamente 378 unidades, dentre estas, uma sede administrativa situada em Brasília e 377 unidades descentralizadas distribuídas em todo território brasileiro. A Figura 5.1 ilustra o organograma da autarquia em questão:

Figura 5.1: Organograma da instituição.

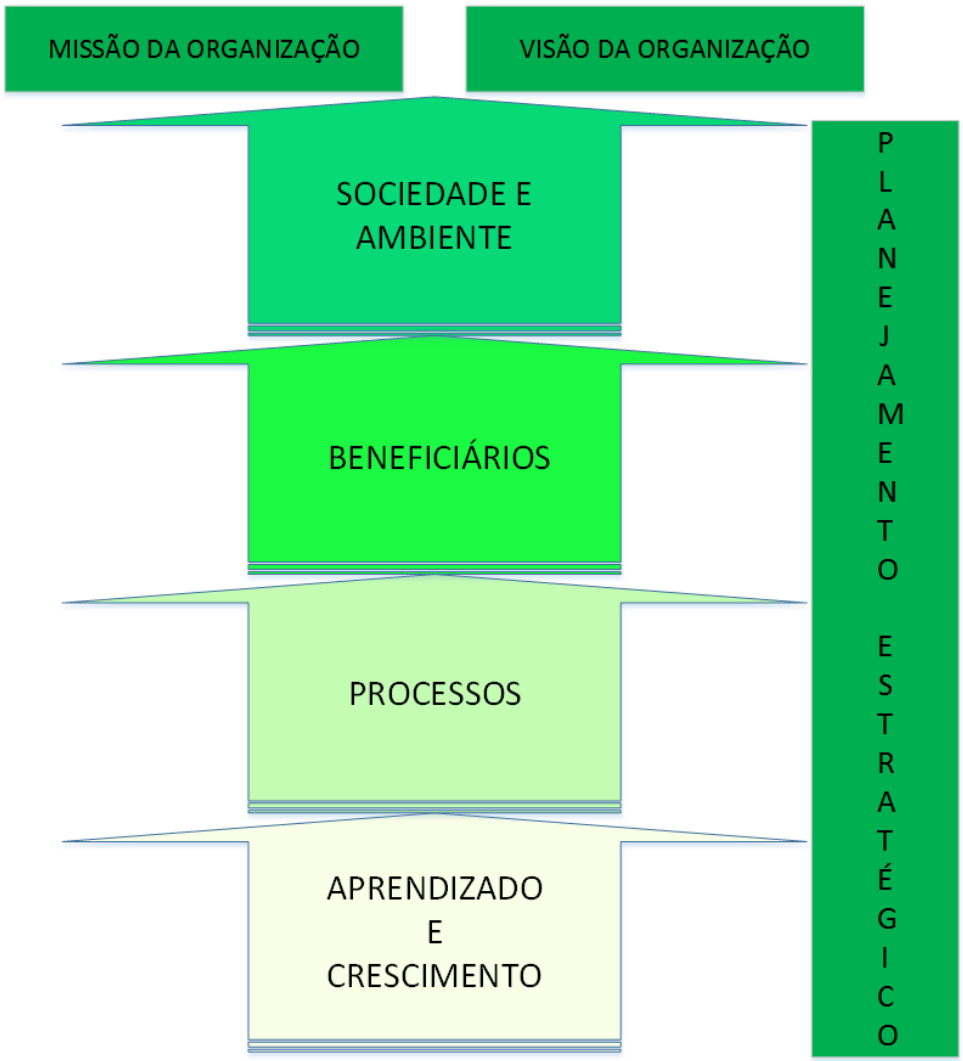


Conforme demonstrado, a instituição está dividido em 5 grandes áreas organizacionais, sendo:

- Órgão colegiado - Comitê Gestor: formado pelo Presidente, Diretores, Procurador Federal, Auditoria e Divisão de Comunicação;
- Gabinete: órgão de apoio a presidência
- Órgãos seccionais: Procuradoria Federal Especializada (PFE), Diretoria 2 e Auditoria interna;
- Órgãos específicos singulares: formado pelas 03 outras diretorias;
- Unidades descentralizadas: São ao todo 377 unidades espalhadas por todo território brasileiro, excetuando-se a sede que está situada na capital federal.

A instituição possui um conjunto de objetivos estratégicos (resultados prioritários), que são pressupostos para que ela alcance sua visão de futuro e cumpra sua missão. Por essa razão estes são atualizados periodicamente considerando as principais demandas da sociedade, do governo e das comunidades interessadas para a atuação do órgão. Os objetivos estratégicos precisam se articular mutuamente constituindo-se em um conjunto lógico, equilibrado e integrado. Dessa forma, conforme demonstrado na Figura 5.2, pode-se observar todas as esferas do planejamento estratégico.

Figura 5.2: Planejamento estratégico.



Para o período de 2015 a 2018, o planejamento está focado em 4 grandes grupos, sendo estes: sociedade e ambiente, beneficiário, processos e, por fim, aprendizado e crescimento. Desse modo, 10 metas estratégicas foram estabelecidas e assim, a instituição demonstra grande preocupação com a missão e visão para ele estabelecidos.

Sendo assim, considerando a estrutura altamente capilarizada do órgão, para o sucesso do monitoramento da gestão orientada para os resultados, a autarquia investiu no desenvolvimento de um sistema informatizado que pudesse abranger todas as suas unidades organizacionais em todo o território nacional, tendo sido então implantado no ano de 2012, um sistema de gestão, que tem por objetivo das apoio à realização e registro de todo o ciclo PDCA (Planejar, Executar, Checar e Agir Corretivamente). Nesse sistema, com

base nos objetivos estratégicos do órgão, são definidos indicadores e metas para cada uma das unidades organizacionais onde há desdobramento de atividades vinculadas de forma a garantir as entregas previstas. Com dimensões tão grandes, a necessidade de uma infraestrutura de TI que possa apoiar na sustentação de seus negócios torna-se imprescindível. Dessa forma, a Tecnologia da Informação exerce papel fundamental no apoio a autarquia para execução de sua missão, por meio do fornecimento de suporte às áreas finalísticas. Ademais, apoia aos processos de trabalho e a área administrativa.

Por conseguinte, em um esforço para prover tal infraestrutura, a autarquia vem a cada ano investindo mais em sua infraestrutura de TI. Porém, para que as ações da TI sejam mais assertivas, se faz necessário um perfeito alinhamento entre a estratégia organizacional e a estratégia da área de TI. Assim, tais investimentos devem promover o retorno e a aproximação cada vez maior entre as áreas de tecnologia com as áreas de negócio. Dessa forma, o órgão, apoiado pelas orientações do Guia do PDTI do SISP (SLTI, 2015), desenvolveu seu Plano Diretor de TI - PDTI, tendo-o como um mecanismo de apoio e justificativas de aquisições em TI e controles dos riscos a este ambiente e ao processo de sustentação de seus negócios.

5.1.2 Análise de resiliência e limitadores

A fim de promover alinhamento das ações de TI com o planejamento estratégico, sua missão e visão, o órgão, por intermédio da Coordenação de Tecnologia da Informação, observando as orientações da Secretaria de Logística e Tecnologia da Informações - SLTI, por meio do GUIA de Elaboração do PDTI (SLTI, 2015), desenvolveu seu Plano Diretor de TI. Desta maneira, os investimentos de TI respeitam as orientações e etapas nele definidas, o qual será descrito abaixo.

O PDTI não se refere apenas como um Plano de Informática e/ou normatização tecnicista. Tampouco estático com ciclo de vida determinado e ao fim do qual se começa tudo novamente, às vezes partindo-se da fase inicial, apropriando custos desnecessários e onerosos. Não é, portanto, um plano para ou da área de TI, mas para apoio e sustentação operacional para todas as suas unidades organizacionais. Dessa forma, o PDTI torna-se uma forma de alinhar as aquisições e ações da área tecnológica da instituição aos processos finalísticos organizacionais.

A Coordenação de Tecnologia da Informação foi o setor responsável por elaborar o PDTI no órgão em questão. Com o objetivo de fornecer o suporte a todas as unidades da autarquia, todos os sistemas de computadores, telefonia e demais serviços fornecidos foram levados em consideração.

Para demonstrar de forma sistemática a estrutura da elaboração do PDTI, foi elaborado o formulário SIPOC, uma abreviação de Suppliers (Fornecedores) – Inputs (En-

tradas) – Process (Processo) – Outputs (Saídas) – Customer (Clientes) como forma de levantamento preliminar do fluxo de planejamento para elaboração. Dessa forma, conforme demonstrado na Figura 5.3, é possível observar os envolvidos, os insumos, as fontes de dados coletados e as áreas interessadas pelo PDTI.

Figura 5.3: Estrutura do formulário SIPOC

SIPOC - Elaborar PDTI				
S Suplier	I Input	P Process	O Outputs	C Costumer
• Coordenadores Gerais • Procurador Chefe • Auditor Chefe • Chefe da Divisão de Comunicação • Colaboradores da Coordenação de Tecnologia da Informação	• Entrevistas • Processos de contratação • Relatórios • Sistemas utilizados na Autarquia • Legislação vigente • Orientações SLTI • Recomendações dos órgãos de controle • Contratos de TI • Questionários	• Elaborar PDTI	• Plano Diretor de Tecnologia da Informação (PDTI)	• Autarquia do Governo Federal

Complementar ao SIPOC, usou-se a notação BPMN - Business Process Management and Notation em inglês, para desenhar o fluxo de atividades que estão compreendidas no processo de elaboração do PDTI, conforme demonstrado na Figura A.1. Dessa forma, foi possível identificar o fluxo operacional utilizado pelo órgão estudado no desenvolvimento de seu PDTI.

Para que fosse possível elaborar tal documento, a coordenação efetuou um levantamento da situação da TI na autarquia. Dessa maneira, diagnosticou as carências de infraestrutura de tecnologia da informação e dos sistemas nas diversas áreas do órgão. Como insumos para gerar este diagnóstico, foram realizados levantamentos através de questionários, com as diretorias e foram coletados dados de colaboradores da Coordenação de Tecnologia da Informação. Levou-se em consideração as recomendações de órgãos reguladores e de fiscalização, os contratos de TI existentes e todos os sistemas que o órgão possui em produção atualmente. O diagrama do processo de elaboração do PDTI, demonstrado no Anexo I, foi construído com base em questionários que foram enviados a todas as diretorias, procuradoria federal especializada, auditoria e divisão de comunicação. Os coordenadores gerais foram os responsáveis por responder os relatórios em cada diretoria, na procuradoria o responsável foi o próprio procurador chefe, o mesmo ocorreu na auditoria, onde o auditor chefe quem respondeu os questionários, por fim o chefe da divisão de comunicação da instituição foi o responsável por responder por sua divisão.

Os questionários continham 11 perguntas e visaram obter informações sobre utilização de sistemas, necessidades de novos sistemas ou sistemas especializados, equipamentos de informática, serviços de manutenção de TI, sobre a dependência de cada área com relação a TI, sobre o planejamento da área e a relação deste com a TI e uma área para reclamações e sugestões. Complementar aos questionários, relatórios da situação do parque tecnológico, fornecidos pelas empresas responsáveis pela sustentação de software e suporte de infraestrutura de TI, também foram levados em consideração. Cada colaborador da Coordenação de TI elencou pontos que acreditavam que deveriam ser melhorados, todos estes pontos foram consolidados em uma única planilha e, posteriormente, cada colaborador foi entrevistado para que se obtivesse um entendimento sobre o que foi especificado, bem como retirar itens que poderiam ser redundantes.

Como resultado, foi possível identificar os seguintes limitadores organizacionais:

- Ausência da autoridade máxima na aprovação e publicação do PDTI;
- Inefetividade do Comitê Gestor de Tecnologia da Informação e Comunicação;
- PDTI incompleto:

  Ausência de plano de investimento e custeio;

  Ausência de proposta orçamentária consolidada;

  Ausência de um plano de gestão de riscos;

  Ausência de uma política de descarte de equipamentos; e

  Ausência de um inventário de TI.
- Ausência do processo de acompanhamento do PDTI;
- Ausência de uma Política de Segurança da Informação e Comunicação;
- Insuficiência do número de servidores lotados na TI;
- Contratações de serviços específicos de outros órgãos;
- Com relação a gestão contratual:

  Ausência de definição formal de fiscais técnico, requisitante e administrativo;

  Ausência de registro formal do histórico do gerenciamento dos contratos de TI;

  Ausência da gestão dos níveis de serviço;

  Inexistência de gestão de acordos de níveis de serviço; e

  Ausência de plano de inserção da contratada.

- Com relação a fiscalização contratual:

  Emissão de ordens de serviço sem requisitos essenciais;

  Ausência de elaboração do termo de recebimento provisório e do termo de recebimento definitivo; e

  Ausência de participação da área de negócio no recebimento dos serviços.

- Contratos caracterizados por disponibilidade de mão de obra.

5.1.3 Análise da capacidade e nível de sustentação

Com a redução de investimentos decorrentes de uma crise econômica enfrentada pelo Brasil, foi solicitado que houvessem cortes em diversas áreas da instituição. No ano de 2015, após auditoria por parte dos órgãos de fiscalização, constatou-se diversos itens de não conformidade com os cumprimentos legais e orçamentários. Sendo assim, como forma de determinar as prioridades para o PDTI, foi definido que todas as recomendações dos órgãos de fiscalização deveriam ser cumpridas imediatamente e de forma complementar, foram elencadas todas as necessidades de todas as áreas da autarquia para que fosse possível realizar o planejamento.

Figura 5.4: Capacidade de sustentação orçamentária.

ANO	CONTRATAÇÃO	VALOR/ANO	
2016	Empresa para prover serviços de links de comunicação **Valor mensal: 1.375.000,00**	R$	16.500.000,00
	Empresa para sustentação de infraestrutura de TI **Valor mensal: 833.333,33**	R$	10.000.000,00
	Empresa para desenvolvimento e sustentação de sistemas **Valor mensal: 816.666,67**	R$	9.800.000,00
2017	Empresa para prover serviços de links de comunicação (9 meses de 2017, com correção de 10%) **Valor mensal: 1.512.500,00**	R$	13.612.500,00
	Empresa para sustentação de infraestrutura de TI (9 meses de 2017, com correção de 10%) **Valor mensal: 916.666,67**	R$	8.250.000,00
	Empresa para desenvolvimento e sustentação de sistemas (9 meses de 2017, com correção de 10%) **Valor mensal: 898.333,33**	R$	8.085.000,00
TOTAL 2016/2017		**R$**	**66.247.500,00**

Como resultado, foi gerado um plano de investimento e custeio, onde constam todas as necessidades e seus respectivos valores para aquisição. O orçamento total necessário,

previsto pela equipe do PDTI para atingir todas as metas requeridas no período proposto, foi de R$120.630.170,24 reais, divididos entre investimento (aquisição de bens) e custeio (aquisição de serviços). Apenas com a contratação de serviços de TI, que passa por suporte de infraestrutura, sustentação de sistemas, fornecimento de links de comunicação, entre outros, serão gastos em dois anos R$ 84.805.126,85, o equivalente a 70,3% do total previsto.

Dentre todas as contratações de serviços, destacam-se 03 grandes contratos, sendo um para suporte a infraestrutura de TI (incluindo telefonia), um para fornecimento de links de comunicação em todo território brasileiro e o último para sustentação de software, que somados são responsáveis pelo maior investimento da TI, totalizando R$ 66.247.500,00, perfazendo 78% do previsto para o período de vigência do PDTI, como pode ser visto na Figura 5.4

Com tal cenário, foi possível observar o comprometimento da capacidade de sustentação financeira, levando em consideração a existência de dívidas com fornecedores, reduzido número de servidores de carreira para os processos operacionais e ausência de mecanismos de sustentação operacional.

5.1.4 Integração dos processos organizacionais

Para o desenvolvimento deste estudo, foi necessário conhecer os objetivos estratégicos e missão do órgão. Dessa maneira, o passo inicial para tal entendimento foi a avaliação do planejamento estratégico, além das declarações de missão e objetivo. Como passo seguinte, verificou-se a necessidade da identificação dos sistemas e qual a visão das áreas de negócios da autarquia sobre seus processos, impactos aos processos e dependência dos sistemas. Assim, elaborou-se um questionário aplicado à 9 (nove) gestores de áreas estratégicas como forma de coleta inicial de dados e insumos para os passos seguintes. Para prospecção de investimentos, é necessário que se tenha uma visão clara da relação dos sistemas e suas necessidades para o órgão. Devido ao grande volume de sistemas se fez necessários classificá-los de forma objetiva. Dessa maneira, a classificação dos 41 sistemas teve como direcionamento o impacto e relevância institucional. Para isso, foi questionado aos gestores quais são os mais utilizados pela sua área, que tem maior impacto caso haja indisponibilidade, e quais os mais importantes para organização.

Desta forma, o questionário composto com 7 (sete) questões foi enviado e, com as respostas coletadas, houve a possibilidade de identificar qual a percepção dos gestores sobre a importância, dependência e criticidade de tais sistemas para suas áreas e para a autarquia como um todo. Com a identificação da percepção dos gestores sobre os sistemas, foi necessário identificar os principais sistemas para a instituição.

Então, considerando, o método de Pareto preconiza que vinte por cento das causas implicam em 80% dos problemas, empregou-se, mediante as respostas coletadas, tal método para realizar a referida identificação. Os dados coletados por meio dos questionários enviados aos gestores, foram separados tendo como base os critérios: utilização, indisponibilidade e importância dos sistemas. Assim foi possível priorizar os sistemas dentro de cada um dos critérios acima citados. Posteriormente, para obter uma visão geral da relevância de cada sistema, foi aplicado o método do ótimo de Pareto sobre o conjunto de sistemas em cada um dos critérios. Entretanto, esse resultado não foi suficiente para justificar como fazer investimentos de forma mais assertivas, bem como foi incapaz de estabelecer uma ligação entre os critérios adotados e a definição da sustentação dos processos finalísticos.

Nesse compasso, o método de Monte Carlo AHP foi introduzido na metodologia visando estabelecer tal hierarquia entre os sistemas segundo os critérios citados. Para tanto, primeiramente os dados foram submetidos a uma simulação de Monte Carlo com 10.000 iterações, utilizando uma distribuição do tipo Beta-PERT. Foi considerada como medida aceitável um intervalo de confiança de 95%. Sobre o resultado obtido com as simulações foi aplicado o AHP tendo como resultado a definição considerada ótima para priorização de investimentos em TI no órgão estudado.

Como primeiro resultado do método descrito foi possível identificar a alta dependência das áreas de negócio da instituição com relação aos sistemas computacionais. A Figura A.2 demonstra que 62,5% dos entrevistados acreditam que suas áreas de negócios possuem alto nível de dependência dos sistemas computacionais atualmente utilizados na autarquia.

De acordo com a Figura A.3, quando perguntado sobre o viés da utilização, 7 sistemas aparecem através do uso da análise sobre o princípio de Pareto, sendo eles o Sistema 13, Sistema 14, Sistema 10, Sistema 41, Sistema 32, Sistema 33 e Sistema 38. Dessa forma foi observado que, apesar de grande dependência tecnológica, apenas sete sistemas demonstram, na visão dos diversos gestores, causar um nível de dependência institucional.

O segundo ponto verificado foi a identificação dos sistemas que causam maior impacto em caso de indisponibilidade. Na Figura A.4, da mesma maneira do critério anterior, verifica-se que 5 sistemas causam maior impacto institucional em caso de inoperância. Estes podem ser listados, em ordem crescente: Sistema 20, Sistema 13, Sistema 14, Sistema 10 e Sistema 41.

Do ponto de vista dos gestores, classificando os sistemas por nível de importância institucional e não mais focada em suas áreas de negócios, foi possível identificar, como demonstrado na Figura A.5, que 16 sistemas detêm a maior importância dentro do universo estudado, sendo estes o Sistema 14, Sistema 20, Sistema 41, Sistema 11, Sistema 13, Sistema 15, Sistema 32, Sistema 33, Sistema 25, Sistema 4, Sistema 5, Sistema 6, Sistema

7, Sistema 8, Sistema 23 e Sistema 22.

Alguns resultados demonstram que a possível visão institucional dos sistemas de TI pode causar certos conflitos. Analisando o resultado, o Sistema 14 foi classificado como o de maior relevância para a instituição.

Porém, quando confrontado com os processos de negócios, o Sistema 41 (website da autarquia) em um primeiro momento, pode ser visto como a página institucional sem muita relação com os processos de negócios institucionais. Entretanto, navegando pela página, observa-se que nele encontram-se os links dos sistemas usados pelas diversas áreas. Dessa forma, verifica-se uma grande dependência dos usuários para o portal, até mesmo pela facilidade de acesso aos sistemas institucionais. Desse modo, justifica-se o Sistema 41 estar como um dos sistemas mais usados e de maior importância para as áreas de negócio. Sendo assim, tomando por base o cenário operacional apresentado, podemos observar que a indisponibilidade do portal poderá causar considerável impacto operacional, haja vista cultura dos colaboradores da autarquia. Assim, mesmo que os sistemas estejam em pleno funcionamento, podem vir a não ser acessados pela simples indisponibilidade do portal.

Após as análises realizadas por meio dos Diagramas de Pareto, aplicou-se a AHP mediante simulação de Monte Carlo. Esta abordagem manteve estrita coerência do MAHP descrito pela literatura.

A cada um dos gestores foi solicitado que pontuassem a importância de cada um dos sistemas considerando a escala entre 1 e 9, sendo 1 menos importante e 9 o mais importante. Assim, foi estabelecida uma relação de relevância entre cada sistema de acordo com as pontuações de cada gestor, ou seja, se o sistema A recebeu uma pontuação de importância igual a 9 e o sistema B recebeu uma pontuação de importância igual à 3, é possível extrair que para um determinado gestor o sistema A é 3 vezes mais significativo para a instituição do que o sistema B. Portanto, a partir das informações fornecidas pelos gestores do órgão, foram produzidas matrizes de preferências entre todos os pares de opções de sistemas.

Considerando que o julgamento dos especialistas apresenta uma distribuição Beta-PERT [25], foram realizadas algumas simulações de Monte Carlo para determinar o julgamento mais provável do gestor em relação à relevância dos sistemas entre si. Assim, as preferências dos gestores entrevistados foram modeladas de acordo com a distribuição Beta-PERT visando à simulação de 10.000 julgamentos a respeito da relevância dos sistemas de TI dois a dois. Desta forma, com um nível de confiança igual a 95%, obteve-se para os critérios de interesse os julgamentos mais prováveis para cada um dos sistemas confrontados. A Figura A.6 destaca como exemplo o resultado obtido para a simulação de Monte Carlo relativa ao Sistema 13.

No gráfico acima é possível observar que o julgamento mais provável atribuído ao

Sistema 13 por 10.000 gestores, com 95% de confiança, seria 8,92, ou seja, é um dos sistemas mais relevantes para a instituição. Assim, para cada um dos critérios, foram analisados todos os sistemas utilizando a abordagem MAHP com grau de confiança de 95%. A partir dessa análise foi possível observar que o número de sistemas mais utilizados subiu para 8 e agora destacam-se os sistemas Sistema 14, Sistema 10, Sistema 25, Sistema 17, Sistema 13, Sistema 41, Sistema 33 e o Sistema 32, conforme observado na Figura A.7.

Da mesma forma, foram analisados quais sistemas causam maior impacto à instituição em caso de indisponibilidade. Neste cenário, conforme demonstrado na Figura A.8, a quantidade de sistemas que causam grande impacto caso estejam indisponíveis aumenta para 7, a saber: Sistema 17, Sistema 13, Sistema 32, Sistema 10, Sistema 41, Sistema 25 e Sistema 14.

A Figura A.9 demonstra o resultado do estudo quando visto sob a ótica do grau de importância institucional de cada sistema. Neste cenário a quantidade de sistemas considerados como os mais importantes, cai para 11, em oposição aos cenários anteriores onde houve acréscimo na quantidade de sistemas, sendo estes o Sistema 41, Sistema 14, Sistema 33, Sistema19, Sistema 13, Sistema 36, Sistema 25, Sistema 20, Sistema 10, Sistema 17 e o Sistema 32.

Sendo assim, dentro do contexto do Processo Analítico Hierárquico, essa matriz permitiu a manipulação de diversos julgamentos simultaneamente visando determinar os sistemas mais prioritários para a instituição segundo os critérios de avaliação. A Figura A.10 apresenta a priorização resultante da simulação em relação a cada um dos referidos critérios.

A partir dos resultados da Figura A.10, foram identificados os sistemas que satisfazem simultaneamente os três critérios e aqueles que, complementarmente, representam a maior relevância para a instituição, conforme demonstrado na Figura A.11

Concluída a apresentação do estudo de caso, no próximo capítulo serão apresentados a conclusão e os trabalhos futuros.

Capítulo 6

Conclusão e Trabalhos futuros

O modelo proposto neste trabalho busca demonstrar os efeitos da redução da intuição para os processos decisórios de gestores de TI. O objetivo é atender uma carência da literatura para modelos que utilizem a análise de riscos e os processos decisórios, apoiados na transversalidade da capacidade de atendimento, nível de sustentação e os riscos inerentes aos processos organizacionais. O modelo busca estabelece critérios de decisões e reduzir os efeitos da intuição nos processos decisórios.

Ao finalizar a avaliação dos resultados do modelo proposto, pode se afirmar que esta pesquisa alcançou seu objetivo de desenvolver um modelo de apoio à decisões baseados na redução da intuição, e validá-lo por meio de sua aplicação em um estudo de caso de investimentos em contratação de serviços de desenvolvimento de software em uma entidade da administração pública federal. Os resultados obtidos evidenciaram a aplicabilidade no cenário em estudo como também em cenários similares, pois permitiu maximizar os resultados das decisões e minimizar os efeitos contraproducentes causados pelo forte apego à intuição.

A adoção da IATD/RCS demonstrou seu potencial de ajudar a superar as principais dificuldades de gestão e governança enfrentadas cotidianamente. Os principais benefícios da sua adoção são:

- Proveu os recursos para atender a demanda por conhecimento, ferramentas e técnicas adequadas para apoiar aos processos decisórias;
- Proveu uma abordagem transversal na observação dos três pilares estruturantes de uma organização, sendo estes os riscos, a capacidade e o nível de sustentação dos processos finalísticos organizacionais;
- Minimizou os resultados contraproducentes e os seus impactos;
- Facilitou a fiscalização dos contratos de prestação de serviços de TI terceirizados;

- Apoiou na construção de justificação institucional;
- Proveu informações para subsidiar a tomada de decisão sobre as medidas a serem adotadas para a melhoria desses processos e para monitorar e avaliar se as decisões tomadas tiveram os efeitos esperados.

De acordo com os dados alcançados, cabe apresentar uma comparação entre os resultados obtidos pelo Princípio 20-80 de Pareto e pelo método Monte Carlo AHP. A Figura A.12 ilustra o quanto os resultados obtidos são semelhantes. Dos 16 (dezesseis) sistemas indicados como os mais relevantes pelo Diagrama de Pareto, com caráter mais intuitivo, apenas 11 (onze) foram contemplados pelo método MAHP, ou seja, é possível afirmar que houve um refinamento da pesquisa em decorrência da utilização do método.

O Diagrama de Pareto dispôs de 9 (nove) entrevistados para formar o conjunto de sistemas de TI relevantes enquanto o MAHP produziu 10.000 julgamentos para realizar o mesmo propósito. Além disso, os 3 (três) sistemas que o método MAHP agregou ao conjunto produzido pelo Diagrama de Pareto são sistemas muito próximos da faixa de 20% do ótimo de Pareto.

Neste contexto, parece coerente inferir que, se o Diagrama de Pareto pudesse contar com 10.000 entrevistados, os 3 (três) sistemas supracitados receberiam melhores pontuações e alçariam a faixa dos 20%. Portanto, o MAHP agregou valor à análise tanto por permitir a manipulação simultânea de vários julgamentos quanto por melhorar a acurácia, a precisão e o coeficiente de revocação da informação.

De toda forma, é válido afirmar que tais abordagens indicam uma redução aproximada de 73% no espectro dos sistemas que são relevantes para a tecnologia da informação da autarquia, demonstrando a importância e relevância da redução da intuição para os processos decisórios.

Ao utilizar as técnicas de Pareto e MAHP, foi possível demonstrar os efeitos das tomadas de decisão por modelos empíricos, principalmente para os prospectos financeiros. Assim, de um universo de 41 sistemas, aferimos a grande dependência do órgão em relação aos 11 sistemas priorizados. Ademais, do total de investimentos feitos para a sustentação dos sistemas, é plausível considerar a viabilidade de grande redução de investimentos de aquisições e contratações, haja vista a redução no número de sistemas críticos. Apesar de não ter sido possível especificar, para este estudo, o valor total da redução se observarmos o universo dos sistemas priorizados após uso das técnicas abordadas, a redução do universo foi de 73% dos sistemas. Diante do exposto é possível verificar que apenas 27% dos sistemas de TI atualmente implantados na autarquia, são efetivamente críticos para os processos de negócios do Instituto.

Se observarmos todo o ecossistema que suporta os processos finalísticos do Instituto, há uma redução da perspectiva de sustentação do ambiente e sistemas tecnológicos. Le-

vando em consideração, desde os contratos e investimentos para alta disponibilidade, recuperação de desastres e demais contratos de manutenção e sustentação dos sistemas, a economicidade aumenta consideravelmente.

Por fim, demonstramos que decisões empíricas podem efetivamente levar a decisões subótimas ou contraproducentes, reduzindo assim os retornos e aumentando a incerteza para os investimentos de TI.

Referências

[1] ABNT. *ABNT ISO GUIA 73:2009 - Gestão de riscos - Vocabulário.* Associação Brasileira de Normas Técnicas, 2009. 7

[2] ABNT. *ABNT NBR ISO 31000 - Gestão de riscos — Princípios e diretrizes.* Associação Brasileira de Normas Técnicas, Rio de Janeiro, 2009. 3, 4, 7, 11, 12, 13

[3] ABNT. *ABNT NBR ISO/IEC 27005:2011 Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.* Associação Brasileira de Normas Técnicas, Rio de Janeiro, 2011. 2, 4, 7, 9, 10, 11

[4] ABNT. *ABNT NBR ISO/NRB 27014:13 Tecnologia da informação — Técnicas de segurança — Governança de segurança da informação.* Associação Brasileira de Normas Técnicas, Rio de Janeiro, 2013. 14, 15, 16

[5] Todd M. Alessandri, David N. Ford, Diane M. Lander, Karyl B. Leggio, e Marilyn Taylor. Managing risk and uncertainty in complex capital projects. *The Quarterly Review of Economics and Financeo*, iii(44):751 – 767, 2004. 39, 40, 41

[6] Terje Aven. On the meaning of a black swan in a risk context. *Safety Science*, 57:44–51, 2013. 5, 46, 47

[7] Michel Benaroch. Option-based management of technology investment risk. *IEEE Transactions on Engineering Management*, 48(4):428–444, 2001. 48, 49

[8] Michel Benaroch, Mark Jeffery, Robert Kauffman, e Sandeep Shah. Option-based risk management: A field study of sequential information technology investment decisions. *Journal of Management Information Systems*, 24(2):103–140, 2007. 2

[9] Michel Benaroch, Yossi Lichtenstein, e Karl Robinson. Real options in information technology risk management: an empirical validation of risk-option relationships. *Mis Quarterly*, pages 827–864, 2006. 2, 5, 45

[10] Siew H. Chan, Qian Song, Saonee Sarker, e R. David Plumlee. Decision support system (DSS) use and decision performance: DSS motivation and its antecedents. *Information & Management*, 54(7):934–947, 2017. 49, 51

[11] Jean-Paul Chavas. *Risk Analysis in Theory and Practice.* Elsevier Academic Press, San Diego, 2004. 1, 8, 41, 42, 43

[12] Michael J. Davern, Ravi Mantena, e Edward A. Stohr. Diagnosing decision quality. *Decision Support Systems*, 45(1):123–139, 2008. 51

[13] Secretaria de Métodos e Suporte ao Controle Externo da Secretaria-Geral de Controle Externo. *Roteiro de Auditoria de Gestão de Riscos*. Tribunal de Contas de União, 2017. 36, 37, 38

[14] Saman Eskandarzadeh e Kourosh Eshghi. Decision tree analysis for a risk averse decision maker: CVaR criterion. *European Journal of Operational Research*, 231(1):131–140, 2013. 45

[15] Marisa Faggini e Concetto Paolo Vinci. *Decision Theory and Choices: a Complexity Approach*, volume 1. Springer-Verlag, Italia, IT, 2010. 2

[16] Anouk Festjens, Sabrina Bruyneel, Enrico Diecidue, e Siegfried Dewitte. Time-based versus money-based decision making under risk: An experimental investigation. *Journal of Economic Psychology*, 50:52–72, 2015. 1, 44

[17] COBIT for Risk Task Force. *COBIT 5 for Risk*. ISACA, 2012. 8, 16, 17, 18, 19, 20, 21

[18] Antonio C. Gil. *Métodos e Técnicas de Pesquisa Social*, volume 6. ATLAS, SP, BRA, 2008. 54

[19] Great Britain e Treasury. *The orange book: Management of Risk- Principles and Concepts*. Stationery Office, 2004. OCLC: 369135994. 32, 33

[20] Cabinet Office. Great Britain. *ITIL Service strategy*. TSO, The Stationery Office, 2011. 25, 26, 27, 28

[21] Bogdan Grechuk e Michael Zabarankin. Risk averse decision making under catastrophic risk. *European Journal of Operational Research*, 239(1):166–176, 2014. 48

[22] The Open Group. *Open Group Standard TOGAF 9.1*. The Open Group., 2011. 22, 23, 24, 25

[23] The Open Group. *Integrating Risk and Security within a TOGAF Enterprise Architecture*. The Open Group., 2016. 8, 23, 24

[24] Project Management Institute. *UM GUIA DO CONHECIMENTO EM GERENCIAMENTO DE PROJETOS (GUIA PMBOK) - QUINTA EDIÇÂO*. Project Management Institute, Inc, 2013. 8

[25] Liang Jing, Bing Chen, Baiyu Zhang, Pu Li, e Jisi Zheng. Monte carlo simulation–aided analytic hierarchy process approach: Case study of assessing preferred non-point-source pollution control best management practices. *Journal of Environmental Engineering*, 139(4):618–626, 2013. 81

[26] Jim Conner John F. Murphy. Beware of the black swan: The limitations of risk analysis for predicting the extreme impact of rare process safety incidents. *Process Safety Progress*, 31(4):330–333, 2012. 5

[27] Eva M. Lakatos e MARINA DE ANDRADE Marconi. *Fundamentos da Metodologia Científica*, volume 5. ATLAS, SP, BRA, 2003. 54

[28] Venkat R. Lakshminarayanan, M. Keith Chen, e Laurie R. Santos. The evolution of decision-making under risk: Framing effects in monkey risk preferences. *Journal of Experimental Social Psychology*, 47(3):689–693, 2011. 2, 5, 44, 45

[29] The Stationery Office Limited. Itil service strategy - 2011 edition. *TSO (The Stationery Office)*, 1(1):–, 2011. 8

[30] Marta Fabiano Sambiese Lombardi e Eliane Pereira Zamith Brito. Incerteza subjetiva no processo de decisão estratégica: uma proposta de mensuração. *Anpad*, 14(6):990–1010, 2010. 4

[31] Caterina Lucarelli, Pierpaolo Uberti, Gianni Brighetti, e Mario Maggi. Risky choices and emotion-based learning. *Journal of Economic Psychology*, 49:59–73, 2015. 2

[32] Elliot A. Ludvig e Marcia L. Spetch. Of black swans and tossed coins: Is the description-experience gap in risky choice limited to rare events? *PLoS ONE*, 6(6):e20262, 2011. 47

[33] Jukka Luoma. Model-based organizational decision making: A behavioral lens. *European Journal of Operational Research*, 249(3):816–826, 2016. 43

[34] Cristiano Souza Marins, Daniela de Oliveira SOUZA, e Magno da Silva BARROS. O uso do método de análise hierárquica (AHP) na tomada de decisões gerenciais–um estudo de caso. *XLI SBPO*, 1, 2009. 49

[35] Desenvolvimento e Gestão / Secretaria de Tecnologia da Informação Ministério do Planejamento. *Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - MGR-SISP v 2.0*. Ministério do Planejamento, Desenvolvimento e Gestão / Secretaria de Tecnologia da Informação, 2016. 7, 28

[36] Desenvolvimento e Gestão / Secretaria de Tecnologia da Informação Ministério do Planejamento. *Guia de Governança de TIC do SISP do Ministério do Planejamento, Desenvolvimento e Gestão - GovTIC-SISP v 2.0*. Ministério do Planejamento, Desenvolvimento e Gestão / Secretaria de Tecnologia da Informação, 2017. 28, 29

[37] Rogerio Feroldi Miorando. Modelo econômico-probabilístico de análise de risco em projetos de TI. *UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL - ESCOLA DE ENGENHARIA*, 2010. 34, 35, 36

[38] The Committee of Sponsoring Organizations of the Treadway Commission COSO. Coso gerenciamento de riscos corporativos - estrutura integrada. *Committee of Sponsoring Organizations of the Treadway Commission*, 1(1):–, 2007. 8

[39] The Committee of Sponsoring Organizations of the Treadway Commission COSO. Board risk oversight a process report. *Protiviti*, 1(1):–, 2010. 3

[40] The Committee of Sponsoring Organizations of the Treadway Commission COSO. Improving organizational performace and governance - how the coso frameworks can help. *Protiviti*, 1(1):–, 2014. 29, 30, 31, 32

[41] Oana Diana Oprea. Improvements in the control frameworks: Coso and cobit. *International Conference "Risk in Contemporary Economy"*, 1(15):331–338, 2014. 16

[42] Ana Carla Bittencourt Reis. Modelagem multicritério e aplicação da teoria dos conjuntos fuzzy para avaliação da liderança. *UNIVERSIDADE FEDERAL DE PERNAMBUCO*, 2011. 50

[43] Brenda Barker Scott. Decision making and the limits of rationality. *Queen's IRC Facilitator*, 3, 2013. 1, 43

[44] Edna Lúcia da Silva e Estera Muszkat Menezes. *Metodologia da Pesquisa e Elaboração de Dissertação*, volume 4. UFSC, SC, BRA, 2005. 54

[45] Katrin Starcke e Matthias Brand. Decision making under stress: A selective review. *Neuroscience & Biobehavioral Reviews*, 36(4):1228–1248, 2012. 43

[46] Nassim Taleb. *A lógica do cisne negro: O impacto do altamente improvável*, volume 2015. Best.Business, RJ, BRA, 2015. 3

[47] Rustam Vahidov e Bijan Fazlollahi. Pluralistic multi-agent decision support system: a framework and an empirical test. *Information & Management*, 41(7):883–898, 2004. 50

Apêndice A

Resultados do estudo proposto

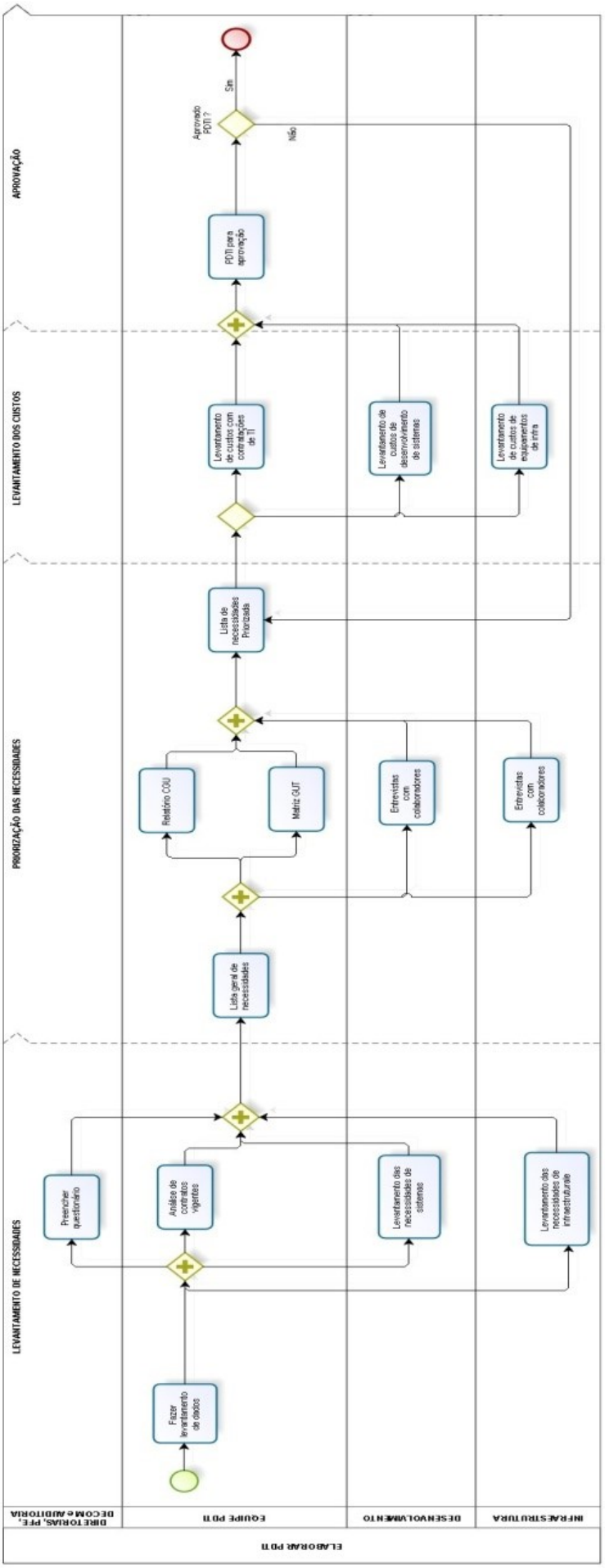


Figura A.1: Processo de elaboração do PDTI

Figura A.2: Nível de dependência das áreas aos sistemas

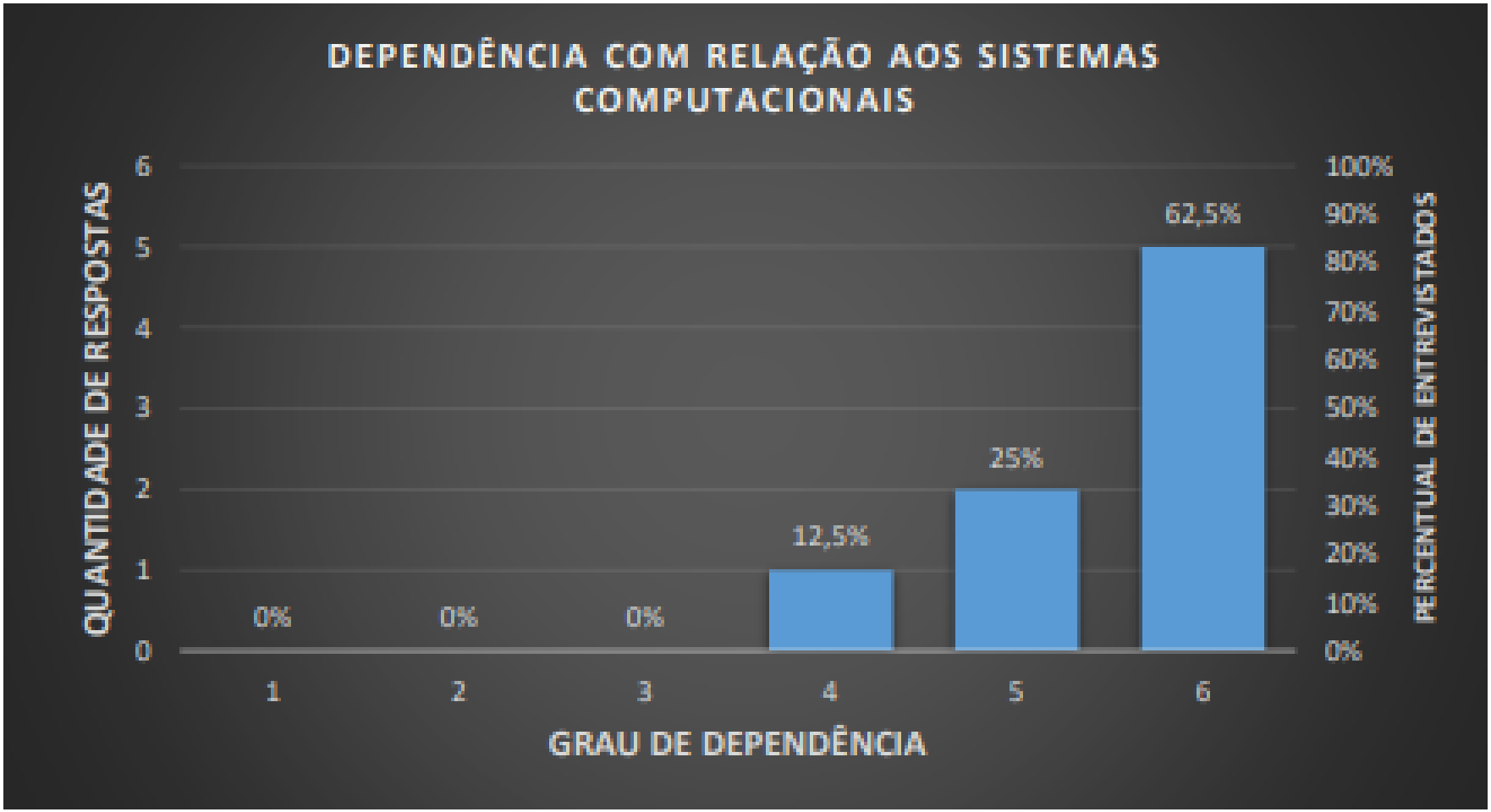


Figura A.3: Sistemas utilizados pelas áreas de negócio

Figura A.4: Sistemas que causam maior impacto

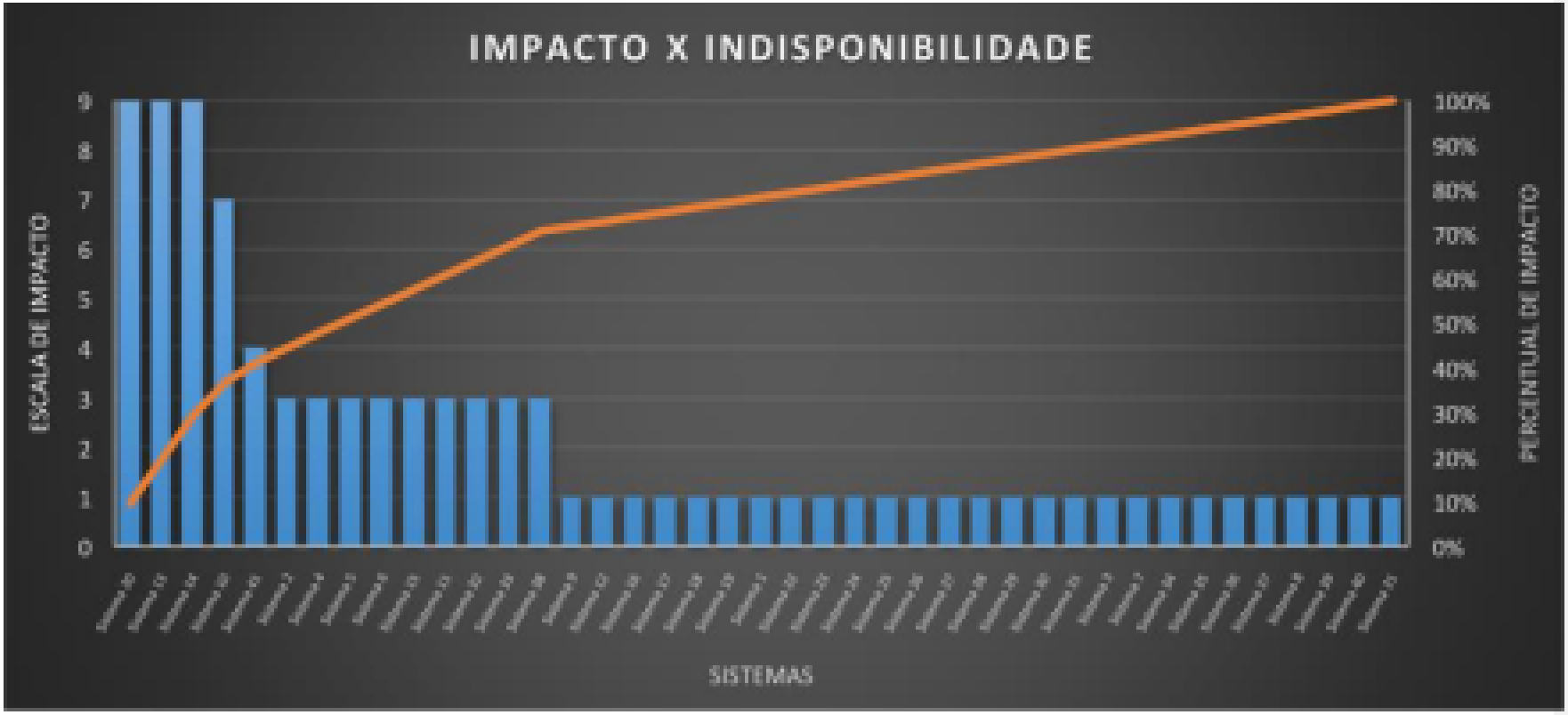


Figura A.5: Sistemas mais importantes para a organização

Figura A.6: Distribuição do 13 sistema obtidos pela simulação

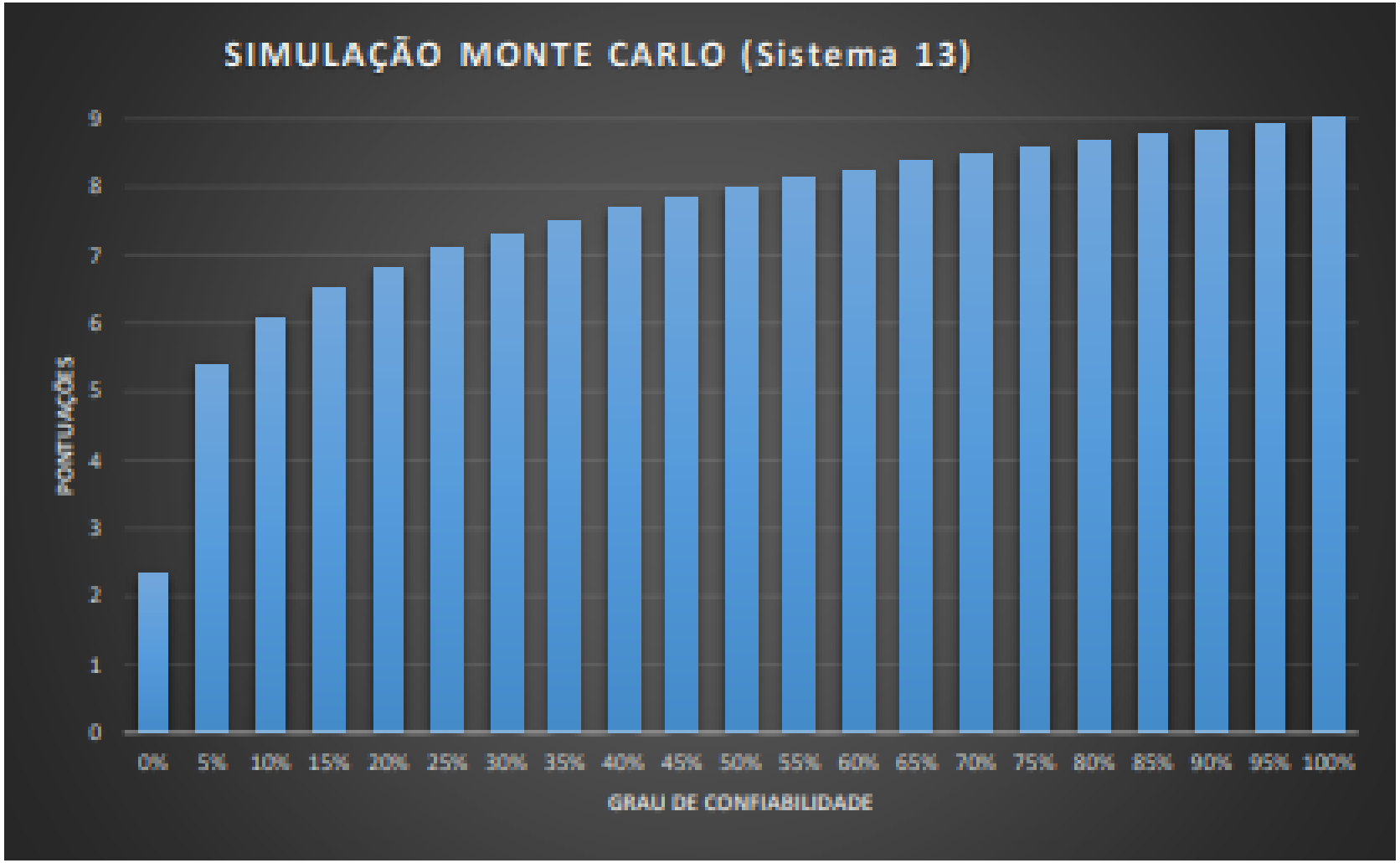


Figura A.7: MAHP dos sistemas mais utilizados

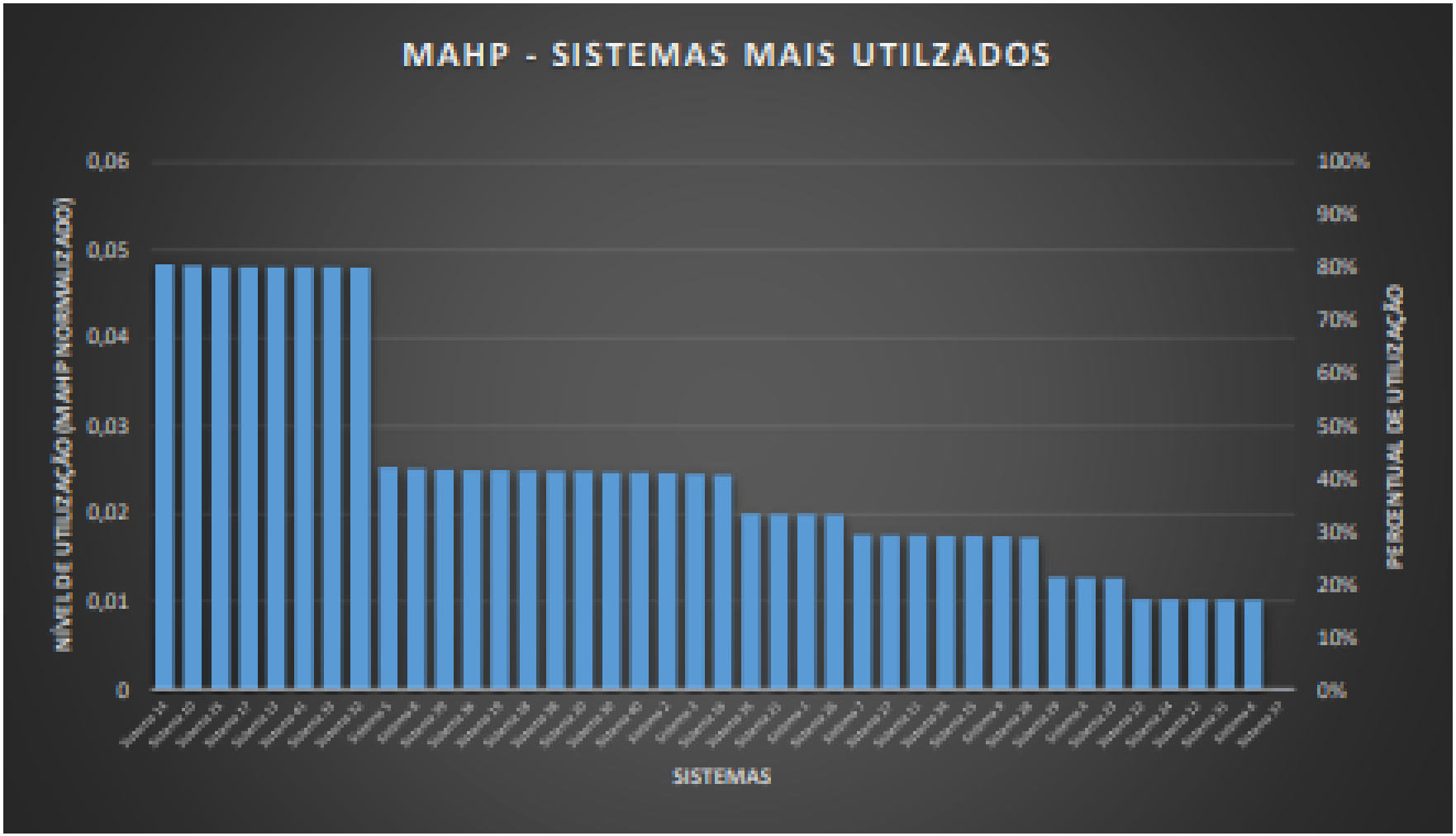


Figura A.8: MAHP dos sistemas que causam maior impacto em caso de indisponibilidade

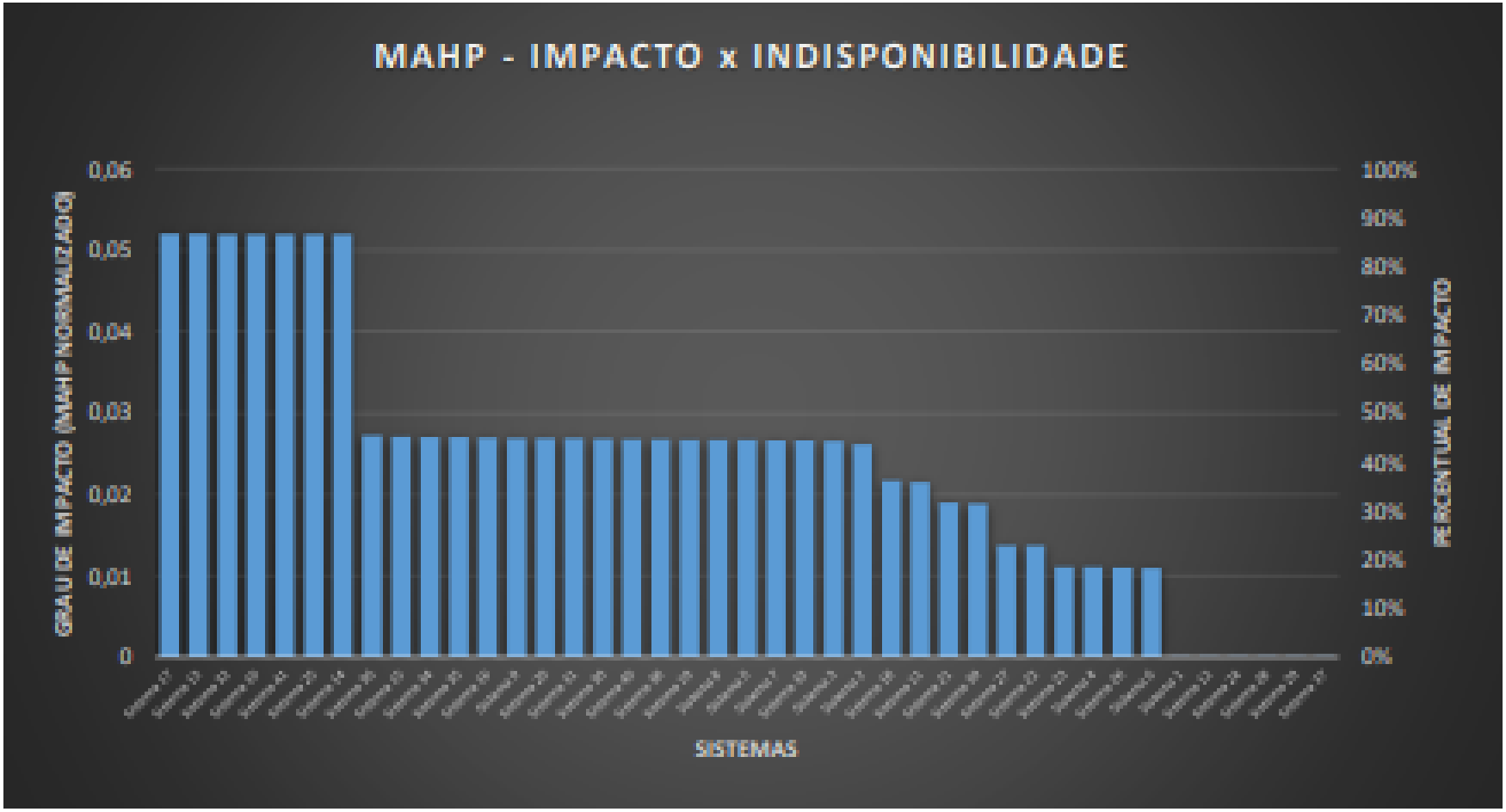


Figura A.9: MAHP dos sistemas mais importantes para a organização

Figura A.10: Hierarquia dos sistemas por critérios de avaliação mediante a aplicação do MAHP

HIERARQUIA	MAIS IMPORTANTE	MAIS USADO	IMPACTO EM INDISPONIBILIDADE
1	Sistema 41	Sistema 14	Sistema 17
2	Sistema 14	Sistema 10	Sistema 13
3	Sistema 33	Sistema 25	Sistema 32
4	Sistema 19	Sistema 17	Sistema 10
5	Sistema 13	Sistema 13	Sistema 41
6	Sistema 36	Sistema 41	Sistema 25
7	Sistema 25	Sistema 33	Sistema 14
8	Sistema 20	Sistema 32	-
9	Sistema 10	-	-
10	Sistema 17	-	-
11	Sistema 32	-	-

Figura A.11: Sistemas que satisfazem simultaneamente os critérios de avaliação e sistemas mais relevantes para a instituição

ITEM	SATISFAÇÃO SIMULTÂNEA	MAIOR RELEVÂNCIA
1	Sistema 41	Sistema 41
2	Sistema 14	Sistema 14
3	Sistema 13	Sistema 13
4	Sistema 25	Sistema 25
5	Sistema 10	Sistema 10
6	Sistema 32	Sistema 32
7	Sistema 17	Sistema 17
8	-	Sistema 19
9	-	Sistema 33
10	-	Sistema 36
11	-	Sistema 20
TOTAL:	7	11

Figura A.12: Comparação entre os sistemas mais relevantes identificados pelo Diagrama de Pareto e pelo método MAHP

ITEM	DIAGRAMA DE PARETO	MAHP
1	Sistema 33	Sistema 33
2	Sistema 32	Sistema 32
3	Sistema 41	Sistema 41
4	Sistema 14	Sistema 14
5	Sistema 13	Sistema 13
6	Sistema 25	Sistema 25
7	Sistema 20	Sistema 20
8	Sistema 4	Sistema 36
9	Sistema 6	Sistema 10
10	Sistema 7	Sistema 17
11	Sistema 8	Sistema 19
12	Sistema 11	-
13	Sistema 15	-
14	Sistema 5	-
15	Sistema 22	-
16	Sistema 23	-
TOTAL:	16	11