Pontifícia Universidade Católica
do Rio de Janeiro

Rafael de Siqueira Tenório Cavalcanti

O USO DA LINGUAGEM INTENCIONAL PARA APOIAR A GESTÃO DE RISCOS EMPRESARIAL

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Informática da PUC-Rio.

Orientador: Prof. Julio Cesar Sampaio do Prado Leite

Rio de Janeiro
Dezembro de 2020

PUC-Rio - Certificação Digital Nº 1721463/CA

Pontifícia Universidade Católica
do Rio de Janeiro

Rafael de Siqueira Tenório Cavalcanti

O USO DA LINGUAGEM INTENCIONAL PARA APOIAR A GESTÃO DE RISCOS EMPRESARIAL

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-Graduação em Informática da PUC-Rio. Aprovada pela Comissão Examinadora abaixo.

Prof. Julio Cesar Sampaio do Prado Leite
Orientador
Departamento de Informática – PUC-Rio

Profª. Simone Diniz Junqueira Barbosa
Departamento de Informática – PUC-Rio

Prof. Henrique Prado de Sá Sousa
Departamento de Informática – UNIRIO

Rio de Janeiro, 16 de Dezembro de 2020

PUC-Rio - Certificação Digital Nº 1721463/CA

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do autor e do orientador.

Rafael de Siqueira Tenório Cavalcanti

Atua no mercado de Engenharia de Software em grandes corporações desde 2007. Graduou-se em Ciência da Computação pela Universidade Federal do Rio de Janeiro em 2007. Ingressou no Mestrado em Informática na Pontifícia Universidade Católica do Rio de Janeiro em 2018.

Ficha Catalográfica

De Siqueira Tenório Cavalcanti, Rafael

O uso da linguagem intencional para apoiar a gestão de riscos empresarial / Rafael de Siqueira Tenório Cavalcanti; orientador: Julio Cesar Sampaio do Prado Leite. – 2020.

76 f. : il. color. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Informática, 2020.

Inclui bibliografia

1. Informática – Teses. 2. Gestão de riscos. 3. Linguagem intencional. 4. Engenharia de requisitos. 5. Biblioteca digital. I. Leite, Julio Cesar Sampaio do Prado. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Informática. III. Título.

CDD: 004

PUC-Rio - Certificação Digital Nº 1721463/CA

PUC-Rio - Certificação Digital Nº 1721463/CA

A meus familiares, em especial a minha mãe.

Agradecimentos

Aos meus pais, pilares da minha formação como ser humano.

Ao meu orientador, Professor Julio Cesar, pelos conhecimentos, orientação e por ser uma inspiração para a conclusão deste trabalho. É um grande exemplo pessoal e profissional.

A todos os meus familiares que sempre me incentivaram muito para que eu obtivesse mais um sucesso nessa etapa.

Aos meus colegas da PUC-Rio, UFRJ, IBMEC, Accenture e Petrobras que de alguma forma contribuíram para que eu percorrece toda esta trajetória.

A todos os funcionários do Departamento de Informática por toda ajuda durante o tempo que estive na PUC-Rio.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

Em especial, dedico esta pesquisa a Deus, causa primordial de tudo.

PUC-Rio - Certificação Digital Nº 1721463/CA

Resumo

Cavalcanti, Rafael de Siqueira Tenorio; Leite, Julio Cesar Sampaio do Prado (Orientador). **O uso da linguagem intencional para apoiar a gestão de riscos empresarial**. Rio de Janeiro, 2020. Dissertação de Mestrado – Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Em função do ritmo acelerado com que tem surgido inovações de mercado, com as incertezas econômicas, a ascensão de mídias sociais, violações cibernéticas, e diversos outros fatores, os riscos organizacionais tem se tornado cada vez mais complexos e difíceis de serem geridos. É necessário que pensemos em modelos mais completos de representação de informações que possam interpretar os riscos aos quais as empresas estão expostas da maneira mais clara e detalhada possível. A modelagem i-estrela permite que informações sejam representadas sem que sejam excluídos detalhes relevantes para a gestão de riscos das organizações. Este artigo propõe uma modelagem de gestão de riscos por meio do modelo i-estrela, de forma a atender a necessidade de representação de informações complexas no atual ambiente de negócios empresarial.

PUC-Rio - Certificação Digital Nº 1721463/CA

Palavras-chave

Gestão de Riscos; Engenharia de Requisitos; Requisitos Não-Funcionais; Modelos Intencionais; Modelos Organizacionais.

Abstract

Cavalcanti, Rafael de Siqueira Tenorio; Leite, Julio Cesar Sampaio do Prado (Advisor). **Using Intentional Modeling to Enhance Enterprise Risk Management**. Rio de Janeiro, 2020. 76p. Dissertação de Mestrado – Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Due to the accelerated pace with which market innovations have emerged, with economic uncertainties, the rise of social media, security issues, and many other factors, organizational risks have become increasingly complex and challenging to manage. It is essential to think about more complete models of information representation that can interpret the risks to which companies are exposed, as clearly, and detailed as possible. The intentional modeling approach allows information to be represented without excluding details relevant to organizations' risk management. This paper proposes a risk management modeling strategy using the iStar language to address the need for enhanced information representation in today's enterprise business environment.

Keywords

Risk Management; Requirements Engineering; Requirements Non-Functional; Intentional Models; Organizational Models.

PUC-Rio - Certificação Digital Nº 1721463/CA

Sumário

1 INTRODUÇÃO 1

1.1 Motivação 1

1.2 Trabalhos relacionados 3

1.3 Estratégia para solução do problema 5

1.4 Estrutura da dissertação 6

2 FUNDAMENTOS 8

2.1 Modelagem de Requisitos Orientada a Meta 8

2.1.1. Modelagem com i* (i-estrela) 8

2.1.2. Modelagem SD (Strategic Denpendency) 9

2.1.3. Modelo SR (Strategic Rationale) 10

2.1.4. Modelo SA (Strategic Actor) 11

2.2 Estrutura de processos em Tecnologia da Informação 11

2.2.1. Gestão de demandas 11

2.2.2. Introdução ao COBIT 12

2.2.3. Governança e Gestão de TI 13

2.2.4. Atores envolvidos no processo 14

2.2.5. Processos de Tecnologia da Informação 14

2.3 Gestão de riscos 16

2.3.1. Evolução histórica 16

2.3.2. Princípios e diretrizes 17

2.3.3. Processo gestão de riscos 18

2.3.4. Matriz de riscos 21

2.3.5. Medição e desempenho na gestão de riscos 22

3 MODELO CONCEITUAL 24

3.1 Modelagem de gestão de riscos em engenharia de requisitos 24

PUC-Rio - Certificação Digital Nº 1721463/CA

3.2 Processo para construção do modelo de gestão de riscos 24

3.3 Representação da gestão de TI 26

3.4 Matriz de riscos para análise 28

3.5 Exemplo de aplicação da Matriz 29

4 MODELAGEM PARA GESTÃO DE RISCOS 31

4.1 Strategic Actor (SA) 31

4.2 Modelo NFR de gestão de riscos 32

4.3 Strategic Dependency (SD) 33

4.4 Uso do modelo SD para apoiar os gestores de riscos 34

5 AVALIAÇÃO DA ESTRATÉGIA 37

5.1 Objetivo 37

5.2 Execução da avaliação 38

5.2.1. Coleta dos dados 39

5.2.2. Limitações do estudo 39

5.3 Análise do questionário 39

5.3.1. Perfil do respondente 40

5.3.2. Avaliação da modelagem elaborada pelo autor 42

5.4 Sintese dos resultados 46

6 CONCLUSÃO 48

6.1 Resumo 48

6.2 Contribuições 48

6.3 Trabalhos futuros 49

7 REFERÊNCIAS BIBLIOGRÁFICAS 50

PUC-Rio - Certificação Digital Nº 1721463/CA

APÊNDICE..... 54

Apêndice I. Avaliação aplicada..... 54

Apêndice II. Contextualização do método para modelagem 57

PUC-Rio - Certificação Digital Nº 1721463/CA

Lista de Figuras

Figura 1 - Tipos de representações em um modelo SD 10
Figura 2 – Normas e padrões considerados no COBIT 13
Figura 3 – Processos de TI (COBIT, 2012) 15
Figura 4 – Princípios para gestão de riscos (ABNT-ISO 31000, 2009) 18
Figura 5 – Processos de riscos (ABNT-ISO 31000, 2009) 20
Figura 6 – Processo geral de gestão de riscos 20
Figura 7 – Matriz de riscos (IBGC) 21
Figura 8 – Processos de definição dos riscos empresariais de TI 24
Figura 9 – Matriz de riscos com métricas 29
Figura 10 – Exemplo de matriz de riscos 30
Figura 11 – Valores sugeridos para riscos de TI 30
Figura 12 – Diagrama SA para processos empresariais de TI 32
Figura 13 – Diagrama NFR (Invulnerabilidade) 33
Figura 14 – Diagrama SD para processos empresariais de TI 34
Figura 15 – Representação do risco 3 35
Figura 16 – Representação do risco 4 36
Figura 17 - Caracterização pela experiência profissional 41
Figura 18 - Caracterização por área de atuação 41
Figura 19 - Caracterização pelo tamanho da empresa que trabalha 41
Figura 20 – Caracterização pelo método do processo que utiliza 42
Figura 21 - Visualização dos riscos de forma geral 42
Figura 22 - Percepção de facilidade em visualizar separação de responsabilidades 43
Figura 23 - Percepção de facilidade em visualizar transparência das informações 43
Figura 24 - Possibilidade de ajudar no trabalho rotineiro dos profissionais 43
Figura 25 - Possibilidade de perceber os fatores associados a um risco 43

PUC-Rio - Certificação Digital Nº 1721463/CA

Lista de Tabelas

Tabela 1 - A crescente complexidade dos riscos 2
Tabela 2 - Atores envolvidos nos processos do COBIT (ISACA, 2012) 14
Tabela 3 – Histórico dos padrões sobre riscos (IBGC, 2017) 17
Tabela 4 - Medidas de meta e desempenho (COSO, 2017) 23
Tabela 5 - Os grupos de atores para modelagem i-estrela 26
Tabela 6 – Processos de Tecnologia da Informação para modelagem 27
Tabela 7 - Questionário de perfil dos avaliadores 40

PUC-Rio - Certificação Digital Nº 1721463/CA

1 Introdução

O objetivo deste capítulo é estabelecer o contexto do trabalho realizado, tendo sido estruturado com: motivação do estudo, objetivo, referências pesquisadas e a estrutura da dissertação.

1.1 Motivação

Há diversos fatores aos quais as organizações estão expostas que tornam o atingimento de seus objetivos incerto. Em função disso, é necessário que essas entidades tomem uma série de medidas com a finalidade de responder da melhor maneira às possíveis incertezas que se apresentam e que colocam em risco a continuidade do negócio (ABNT-ISO 31000, 2009).

Um amplo conjunto de diretrizes que orientam a gestão de riscos empresarial foi publicado em 2018, sendo este conjunto a atualização da ISO 31000 (ABNT-ISO 31000, 2009). A organização responsável pelo normativo internacional é a International Organization Standardization (ISO), e no Brasil a gestão do normativo bem como de sua tradução oficial fica a cargo da ABNT (Associação Brasileira de Normas Técnicas).

No Brasil, por exemplo, as organizações com operações de compartilhamento em NYSE devem seguir a lei Sarbanes-Oxley (SOX, 2002). Há um grande acervo sobre maneiras de mitigar os tipos de riscos. A própria atualização da ISO 31000:2009 evidencia a sensibilidade das organizações em adotar culturas e processos de *compliance* mais robustos, adicionando-se a isto também a percepção do custo-benefício da disseminação empresarial de uma mentalidade preventiva de gestão de riscos.

O *ERM Initiative in the Poole College of Management e American Institute of Certified Public Accountants – AICPA* – publicaram em março de 2019 um relatório sobre Gestão de Riscos Empresariais (BEASLEY, 2019) que contou com a participação de 445 organizações das quais 142 possuem receita igual ou superior US $1 bilhão. Dentre os principais pontos do relatório,

PUC-Rio - Certificação Digital Nº 1721463/CA

observou-se que a maioria dos executivos entrevistados percebe que, atualmente, as incertezas no ambiente de negócio estão tornando os riscos empresariais mais complexos. Dos entrevistados, 59% acreditam que o volume e complexidade dos riscos está aumentando extensivamente ao longo dos últimos anos.

Outra informação importante observada no relatório é que apesar das preocupações sobre uma série de questões de potenciais riscos no horizonte, poucos executivos descrevem a abordagem de suas organizações à gestão de riscos como madura. Apenas 23% dos entrevistados descrevem sua gestão de riscos como "madura" ou "robusta" e, ainda, com a percepção que o nível de maturidade diminuiu nos últimos 2 anos. O quadro abaixo mostra a percepção dos entrevistados sobre como o volume e complexidade dos riscos têm aumentado nos últimos cinco anos.

Tabela 1. A crescente complexidade dos riscos

O aumento da complexidade dos risco nas organizações					
QUESTAO	Não houve alteração	Minima mente	Um pouco	Na maioria das vezes	Extensiva mente
Até que ponto o volume ea complexidade dos riscos aumentou nos últimos cinco anos?	2%	7%	32%	42%	17%

Trazendo a análise para o escopo de Tecnologia da Informação, o presente estudo pretende fazer uma reflexão de melhoria na disciplina de engenharia de requisitos, para que as demandas de TI tenham seu atendimento de uma maneira mais precisa.

Em função do aumento crescente da complexidade dos riscos nas organizações, nota-se que é necessário um maior investimento em modelos e métodos que especifiquem os processos e metas organizacionais de uma forma mais precisa e completa. A inferência que está sendo feita neste caso é que, com um melhor entendimento dos processos organizacionais, a gestão dos riscos empresarial poderá ser aperfeiçoada.

PUC-Rio - Certificação Digital Nº 1721463/CA

Neste sentido, entendemos que se as organizações são orientadas a missões e objetivos, a gestão de riscos corporativo também deve ser orientada a objetivos e metas. Além disso, trazer a visão de riscos para uma modelagem organizacional orientada a meta fará com que os requisitos de demandas de Tecnologia da Informação sejam aprimorados.

1.2 Trabalhos relacionados

Os trabalhos utilizados pelo autor para comparar com a proposta de dissertação podem ser divididos em dois grupos, dentre os quais: normativos e frameworks sobre gestão de riscos empresarial; e trabalhos que fazem uso de linguagem intencional para apoiar o processo de gestão de riscos no ambiente corporativo.

Os normativos de gestão de riscos mais adotados apresentam muitas semelhanças em seus princípios e definições. A norma ISO 31000 (ABNT-ISO 31000, 2009) traz um processo macro das etapas da gestão de riscos e relaciona o risco com o impacto em sua ocorrência e também sua probabilidade. A norma ERM COSO (COSO, 2017) contem também um macroprocesso da gestão de riscos, mas também traz uma abordagem sobre como aferir valores nas relações dos impactos dos riscos com os objetivos organizacionais. Neste sentido, há outras normas muito utilizadas no tema como o The Orange Book, trazendo relações do risco com a incerteza da obtenção de resultados empresariais (ORANGE BOOK, 2004). É possível citar também outros frameworks de mercado que seguem a mesma linha de princípios e macroprocessos sobre riscos como o COBIT (COBIT, 2012) e o ITIL (MENKEN, 2011).

Os frameworks e normativos citados no parágrafo anterior fortalecem o fato de que o padrão na literatura de riscos é que as estruturas são visualizadas sempre sob uma perspectiva de processos e de procedimentos.

Ao compreender isso o autor identificou a necessidade de trazer um viés intencional às modelagens organizacionais no processo de gestão de riscos, pois o enfoque de uma modelagem intencional está no nível mais abstrato de metas e

PUC-Rio - Certificação Digital Nº 1721463/CA

objetivos, com uma visão menos procedimental e mais voltada às políticas da estrutura (LEITE, 2013).

A partir desse entendimento, o autor passou a pesquisar trabalhos que utilizassem a linguagem intencional no contexto de gestão de riscos em ambientes empresariais. Nesta abordagem, o livro Social Modeling for Requirements Engineering em seu capítulo 7 apresenta os benefícios de usar o framework i-estrela para apoiar a melhoria da gestão da segurança de tecnologia da informação por meio de uma análise de gestão de riscos (YU, 2011). No artigo "Engenharia de Requisitos e Desenvolvimento de Projetos Globais" (LOPEZ, 2009) foi feita uma revisão sistemática da literatura para identificar os riscos de RE no processo de desenvolvimento de projetos globais, juntamente com as formas de mitigação desses riscos.

Em "Goal-driven risk assessment in requirements engineering" (ASNAR, 2011) há uma abordagem que é baseada em uma estrutura conceitual composta por três camadas principais: ativos, eventos e tratamentos. No artigo "Multi-Objective Risk Analysis with Goal Models" é feita uma porposta de estrutura de análise de risco orientada a objetivos que inclui interdependências entre tratamentos e riscos em termos de probabilidade e soluções ótimas em relação a múltiplos objetivos, como recompensas de meta, custos de tratamento ou fator de risco (BASAK, 2016).

No trabalho "A Goal-Driven Risk Management Approach to Support Security and Privacy Analysis of Cloud-Based System" os autores fornecem um exemplo ilustrativo da aplicação da abordagem proposta em um estudo de caso industrial em que um serviço de nuvem é implantado para compartilhar dados entre parceiros do projeto (ISLAM, 2013).

Os artigos: "Using i* to represent OSS ecosystems for risk assessment" (MARTINEZ, 2013) e os "Empirical Principles and an Industrial Case Study in Retrieving Equivalent Requirements via Natural Language Processing Techniques", também abordam a gestão de riscos nos projetos de TI (FALESSI, 2013).

O artigo "Risk management in software projects: an approach based on non-functional requirements" (ANDRADE, 2019) traz uma modelagem de riscos

PUC-Rio - Certificação Digital Nº 1721463/CA

utilizando a linguagem i* mas com foco apenas em riscos de projetos, fazendo menções ao framework PMBOK. Por fim, há o artigo o artigo “Modeling Organizational Alignment” (SOUZA, 2014) que propõe um processo para integrar objetivos estratégicos e operacionais, inclusive entre linguagens distintas.

Os trabalhos citados na seção 1.2 são os que merecem destaque para efeito de comparação com a proposta de dissertação cujo tema é o uso de linguagem intencional para apoiar o processo de gestão de riscos empresarial.

1.3 Estratégia para solução do problema

Portanto, diante do problema mencionado que é o aumento da complexidade dos riscos empresariais, este trabalho tem como objetivo:

Propor uma estratégia de modelagem de gestão de riscos, com uso de linguagem intencional, para atender à necessidade de representar com uma maior completude as informações as quais os ambientes de negócio estão exposotos. Os objetivos para a estratégia de modelagem são:

a) Separar as responsabilidades entre a área de *compliance*, as áreas de tecnologia da informação, a área de negócios e a alta administração empresarial;

b) Certificar-se que as decisões estratégicas sejam tomadas com base na transparência da organização.

Para elaborar a modelagem foi utilizado um catálogo inicial de requisitos a partir dos processos de Tecnologia da Informação constantes do framework COBIT-5 (COBIT, 2012). O framework foi utilizado por ser bastante abrangente em termos de atividades e processos de TI e por ser usado há bastante tempo entre grandes empresas, portanto com bastante maturidade.

A utilização do framework permitiu ter uma visão holística dos processos e atividades utilizados pelas áreas de TI em um ambiente corporativo. Dessa forma, com essa visão mais completa da estrutura empresarial, é possível que a

PUC-Rio - Certificação Digital Nº 1721463/CA

Administração e os gestores visualizem com mais clareza os processos e, por consequência, os riscos de TI.

O trabalho traz também a sugestão de um processo genérico para a criação de uma modelagem intencional utilizando a linguagem i-estrela, representando as dependências da organização, suas funções, recursos, metas e softgoals (metas de qualidade, NFRs). Os softgoals, no modelo, refletirão as qualidades relacionadas com os riscos.

A escolha pelo framework i-estrela deve-se ao fato da linguagem ter entre suas funcionalidades pontos que fazem parte do objetivo do modelo proposto nesta dissertação de mestrado: a) modelar estruturas onde há diversos relacionamentos entre agentes; b) explicitar o funcionamento individual de cada ator pertencente ao processo (YU, 1995).

A hipótese sustentada pela pesquisa é que a modelagem criada, a partir do processo genérico sugerido, apoie os gestores de riscos a entenderem melhor os riscos empresariais de forma a tomarem decisões mais precisas quando da análise de riscos de TI em um ambiente corporativo.

O escopo do trabalho se limita à criação de uma modelagem que permita aos gestores visualizarem os processos de TI elencados em uma matriz de riscos. Mitigar riscos não é o objetivo da dissertação.

É importante destacar que também não faz parte dos objetivos do trabalho fazer um comparativo entre linguagens intencionais. O que se pretende é avaliar, por meio de uma pesquisa de opinião, os benefícios do uso de uma linguagem intencional no processo de gestão de riscos empresarial. Participaram da pesquisa de opinião pesquisadores e profissionais das áreas de TI e de riscos.

1.4 Estrutura da dissertação

Diante do aumento da complexidade dos riscos empresariais, esta dissertação apresenta uma proposta de modelagem para gestão de riscos empresarial, no contexto de Tecnologia da Informação, utilizando a linguagem i-estrela. A

PUC-Rio - Certificação Digital Nº 1721463/CA

avaliação conduzida durante a pesquisa é a hipótese de que a proposta citada é positiva.

No capítulo 2 são mostradas algumas definições do modelo i-estrela que foi utilizado para modelar a estrutura de gestão de riscos empresarial, uma análise do framework COBIT e um histórico sobre normas e padrões de gestão de riscos.

O capítulo 3 contém uma aboradagem das referências apresentadas relacionando-as com o modelo de gestão de riscos que será proposto.

No capítulo 4, é apresentado a instanciação da abordagem definida no capitulo 3.

O capítulo 5 é apresentada a avaliação do modelo por meio de entrevistas e questionários.

No capitulo 6 contém o desfecho do trabalho relacionado com as contribuições obtidas e uma introdução sobre possíveis trabalho futuros.

PUC-Rio - Certificação Digital Nº 1721463/CA

2 Fundamentos

2.1 Modelagem de Requisitos Orientada a Meta

O conhecimento das abordagens de modelagens orientadas a metas tornou-se mais amplamente divulgado após as pesquisas realizadas por Van, Yu e Mylopoulos no fim dos anos 90 (Van Lamsweerde, 2000; Yu e Mylopoulos, 1998). O ponto central na concepção do presente trabalho é que muitos requisitos não funcionais são, em geral, deixados de fora das especificações na área de Tecnologia da Informação, sobretudo no ambiente empresarial. A modelagem de sistemas orientados a meta tenta resolver este problema (Lapouchnian, 2005).

Além disso, um outro diferencial para o uso do método orientado a meta é que a análise de sistemas tradicional foca em quais características um sistema irá suportar, já as abordagens orientadas a meta focam no porquê sistemas são construídos, justificando assim os requisitos originários dos sistemas (Anton, 1996).

Baseado nas definições de Van e Yu (Van Lamsweerde, 2000; Yu e Mylopoulos, 1998), em 2007, em sua dissertação de mestrado, Cunha descreveu de forma estruturada vários dos conceitos para sistema orientados a meta (CUNHA, 2007). Algumas dessas descrições citadas por Cunha serão sintetizadas nos próximos tópicos para um melhor entendimento sobre a modelagem, que será exposta na presente dissertação a partir do capitulo 3.

2.1.1. Modelagem com i* (i-estrela)

O i-estrela (Yu, 1995) é bastante adequado para modelagem de requisitos orientada a meta, a decomposição do sistema é feita por atores, que podem ser estendidos em agentes de software. É possível representar dependências entre atores, a estrutura interna de um ator, com objetivos individuais, e as possibilidades de satisfazer ou não esses objetivos.

PUC-Rio - Certificação Digital Nº 1721463/CA

Além da cadeia de relacionamentos citada acima, é possível representar requisitos não funcionais e inserí-los em uma modelagem criada. Este último ponto é a principal característica adicionada a representação de gestão de riscos criada nesta dissertação.

É importante destacar que a mesma abordagem produzida neste trabalho poderia ser feita com outra linguagem intencional que atendesse aos requisitos de instanciação em um modelo organizacional. O i-estrela pode ser dividido em modelos: o Strategic Dependency (SD) e o Strategic Rationale (SR), descritos a seguir.

2.1.2. Modelagem SD (Strategic Denpendency)

É um modelo de representação que possui um conjunto de nós (atores) dependentes entre si. Essas dependências são criadas para que uma determinada meta seja satisfeita, um recurso seja concedido, uma tarefa seja realizada ou uma meta-flexível seja satisfeita a contento. Há quatro possíveis tipos de dependências entre atores. Essas dependências podem ser por:

– Meta: quando um ator depende de outro para que determinado objetivo seja alcançado.

– Tarefa: quando um ator depende de outro para que este outro execute uma tarefa.

– Recurso: quando um ator depende de outro para que um objeto seja concedido.

– Meta-flexível: quando um ator depende de outro para que este desempenhe alguma tarefa. Esta ligação servirá de base para que uma meta flexível seja satisfeita de forma adimissível, considerando as partes interessadas no modelo elaborado.

A Figura 1 ilustra como são representados os quatro tipos de relação em um modelo SD, esta figura será a legenda que utilizaremos na modelagem criada nesta dissertação.

PUC-Rio - Certificação Digital Nº 1721463/CA

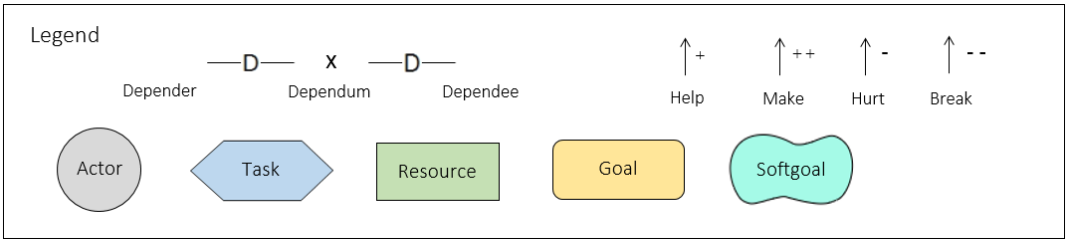


Figura 1 - Tipos de representações em um modelo SD

2.1.3. Modelo SR (Strategic Rationale)

Este modelo representa as estratégias internas de um ator, trazendo um detelhamento do processo em termos de componentes. No SR o principal objetivo é a identificação de quais metas, tarefas, recursos e metas-flexíveis foram dispostas naquele contexto do diagrama.

No modelo SR há dois tipos de decomposição, por tarefa e por meio-fim. No presente trabalho não haverá uma instanciação de um modelo SR mas, como haverá uma decomposição de metas-flexíveis no contexto da gestão de riscos, é importante destacar que na decomposição de metas-flexíveis há um atributo para identificar o tipo de contribuição da meta-flexível que está sendo decomposta.

Conforme já mencionado na seção 2.1, o uso das contribuições das metas-flexíveis foi baseado na dissertação de mestrado de Herbet Cunha (CUNHA, 2007), que utilizou o software OpenOME (OPENOME, 2011), que tratava essas relações como próprias.

Portanto, as contribuições a serem utilizadas podem ser classificadas como:

- MAKE representa a situação positiva em que o elaborador entende que o meio é suficiente para permitir satisfação do fim.

- BREAK representa a situação positiva em que o elaborador entende que o meio é suficiente para impedir do fim.

- HELP ("+") e HURT ("-") são contribuições parciais para satisfação da meta, podedondo ser contribuições positivas e negativas, respectivamente.

PUC-Rio - Certificação Digital Nº 1721463/CA

2.1.4. Modelo SA (Strategic Actor)

O modelo SA (Leite, 2007) foi concebido para apoiar na modelagem dos atores auxiliando no entendimento da relação entre esses atores por uma visão holística da estrutura. A base da sintaxe utilizada no modelo SA é a mesma contida nas modelagens proposta por Yu (Yu, 1995) nos modelos SD e SR. Os conceitos constantes do modelo SA estão descritos a seguir:

Ator: é um componente da estrutura que alcança metas por meio de ações desempenhadas e com uso de seu conhecimento sobre o modelo.

Papel: é uma abstração do ocmportamento do ator em um determinado domínio. Pode representar um conjunto de comportamentos similares de um grupo de atores específico.

Agente: é um ator com manifestações físicas específicas, podendo ser usado no lugar de uma determinada pessoa com características iguais a sua.

No presente trabalho será explorada a instanciação de um modelo SA considerando grupos de atores organizacionais simbolizados por papéis específicos na gestão de riscos.

PUC-Rio - Certificação Digital Nº 1721463/CA

2.2 Estrutura de processos em Tecnologia da Informação

2.2.1. Gestão de demandas

Para a APICS (associação norte americana de gestão empresarial e gerenciamento da cadeia de suprimentos) a gestão de demandas é um processo vinculado ao reconhecimento de todas as demandas de mercadorias e serviços necessários para atender ao mercado.

A gestão de demandas impõe a necessidade de estabelecer uma hierarquização dos pedidos a serem atendidos para a obtenção de resultados do negócio. No contexto de TI, a gestão de demandas é um processo que objetiva identificar e priorizar solicitações e iniciativas do departamento de tecnologia da informação.

2.2.2. Introdução ao COBIT

Trata-se de um manual de boas práticas para implementação de processos de governança e gestão de TI, mantido pela *Information Systems Audit and Control Association* – ISACA. É um padrão com diretrizes que deve ser ajustado para cada entidade onde é implantado. Neste tópico serão descritos a estrutura e os processos utilizados pelo framework COBIT.

Uma das principais características do COBIT é que o guia possui uma vasta interseção de conceitos e princípios com outros guias de mercado, conforme destacado na Figura 2 (COBIT, 2012). Além disso, o padrão propõe o alinhamento da TI às áreas de negócio, melhorando a governança e gestão de TI corporativa, permitindo uma visão geral de toda a entidade.

Contudo, a abrangência do padrão contemplando de forma detalhada muitas áreas torna-o contraproducente quando se planeja desenhar a estrutura de processos empresarial que permeie todos os processos e recomendações. Para isso, é necessário haver um método de modelagem eficiente para representação das informações.

O motivo pelo qual será utilizado o COBIT como base para o catálogo de processos da modelagem a ser proposta, é pelo fato do COBIT ser mais orientado a objetivos, monitorização e controle, e não só para operações. O framework também é bastante focado nas áreas de negócio, monitoração e na estratégia das entidades (SILVA, 2012).

Há algumas pesquisas na literatura que fazem uso do COBIT para aprimorar outros métodos na área de Tecnologia da Informação, como é o caso da pesquisa sobre a implementação do COBIT nas empresas de TI para apoiar no desenvolvimento de softwares (FIDALGO, 2017).

A necessidade de busca por uma modelagem apropriada para representação dos processos de uma empresa deve-se ao fato do COBIT ser bastante extenso em termo de especificação e ter como pretensão apenas a reposta sobre “o que deve ser feito” e não “como deve ser feito”. A figura 2 mostra os modelos com os quais o COBIT possui interseção para descrever os processos de TI (COBIT, 2012).

PUC-Rio - Certificação Digital Nº 1721463/CA

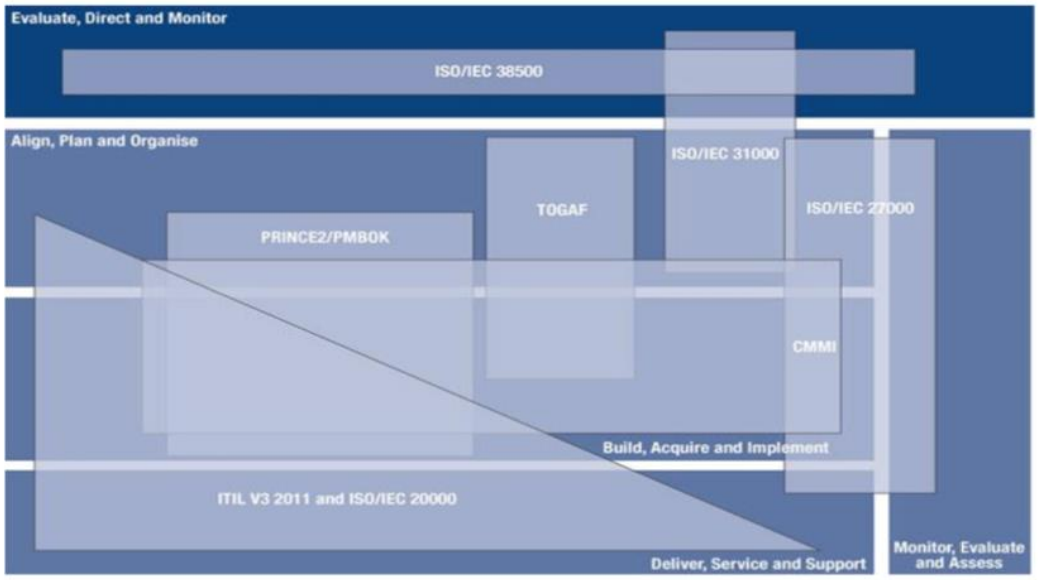


Figura 2 – Normas e padrões considerados no COBIT (COBIT, 2012)

2.2.3. Governança e Gestão de TI

Na abordagem do framework, a Governança de TI é responsável pelo planejamento, implantação, controle e monitoramento de programas e projetos de TI, de uma maneira mais abstrata, contemplando assim as seguintes atribuições:

- Estrutura o planejamento e as normas em um nível mais alto na entidade;
- Elenca e prioriza as decisões as serem tomadas por meio de um processo decisório;
- Controla a execução das atividades de acordo com o planejamento estratégico.

Cabe a governança de TI um olhar mais estratégico sobre os processos de TI voltados aos objetivos de negócio e, por sua vez, cabe a gestão de TI estruturar os processos meio para serem executados com intuito de atingir as metas estratégicas da organização. A Gestão planeja, constrói, organiza e monitora as atividades operacionais, conforme a estratégia da administração da empresa a fim de atingir os objetivos corporativos (ISACA, 2012).

PUC-Rio - Certificação Digital Nº 1721463/CA

2.2.4. Atores envolvidos no processo

O COBIT 5 contém em uma extensão de seus guias uma matriz com papéis e responsabilidades pelo catálogo de processos contido no framework. Os atores envolvidos no processo consideram as atividades exercidas essencialmente pela área de TI e também as atividades necessárias para o cumprimento dos objetivos de negócio, neste caso, nos casos que há alguma participação da área de TI (COBIT e ISACA, 2012). A Tabela 2 traz os atores mencionados pelo COBIT no catálogo de processos de TI.

Tabela 2 – Atores envolvidos nos processos do COBIT (ISACA, 2012)

Board	Enterprise Risk Committee
Chief Executive Officer	Head Human Resources
Chief Financial Officer	Compliance
Chief Operating Officer	Audit
Business Executive	Chief Information Officer
Business Process Owners	Head Architect
Strategy Executive Committee	Head Development
Steering Committee	Head IT Operations
Project Management Officer	Head IT Administration
Value Management Officer	Service Manager
Chief Risk Officer	Information Security Manager
Chief Information Security Officer	Business Continuity Manager
Architecture Board	Privacy Officer

2.2.5. Processos de Tecnologia da Informação

O framework possui 37 macroprocessos separados por 4 categorias, conforme exposto na Figura 3.

PUC-Rio - Certificação Digital Nº 1721463/CA

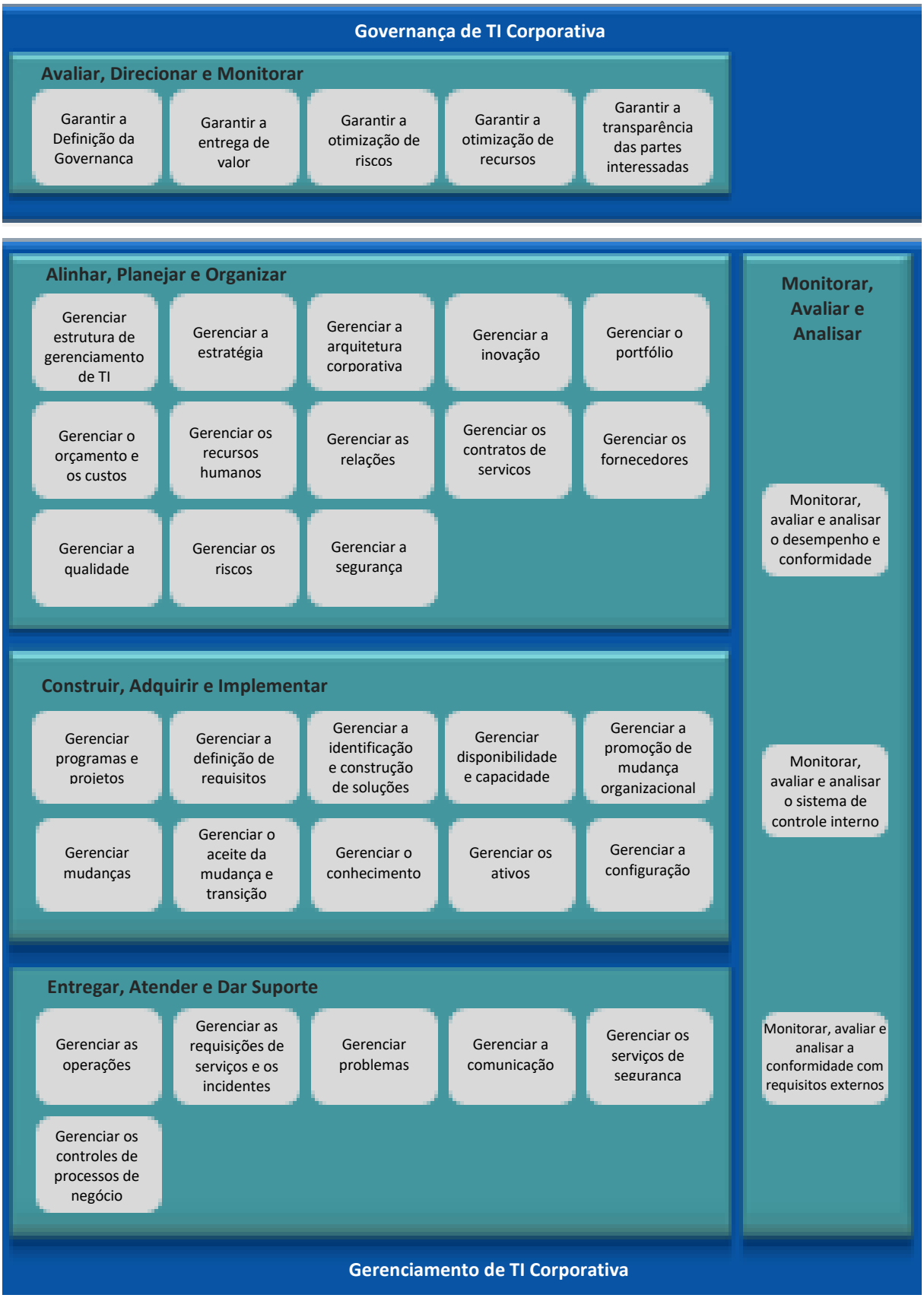


Figura 3 – Processos de TI (COBIT, 2012)

PUC-Rio - Certificação Digital Nº 1721463/CA

Esses são os processos que servirão de base para a construção da modelagem a ser proposta nesta dissertação de mestrado.

2.3 Gestão de riscos

2.3.1. Evolução histórica

O Instituto Brasileiro de Governança Corporativa - IBGC - em seu guia intitulado *Gerenciamento de Riscos Corporativos* (IBGC, 2017) descreve o histórico dos padrões de riscos no mundo desde o início do século passado, a seguir são citados alguns desses padrões constantes do histórico bem como uma linha do tempo resumida contendo alguns dos padrões referenciados.

As principais normas sobre o tema atribuem a Frank Knight a publicação, em 1921, do material precursor sobre gestão de riscos e que se tornou a primeira referência que introduziu alguma sistematização sobre o tema (FRASER; SIMKINS, 2010). Houve poucos avanços sobre o tema nas décadas seguintes e apenas em 1975 a revista Fortune publicou o artigo The Risk Management Revolution, sendo este um dos primeiros documentos a tratar do tema sob um enfoque mais corporativo, voltado a objetivos empresariais (FRASER; SIMKINS, 2010).

O IBGC (IBGC, 2017) traz ainda referências de padrões que trouxeram os princípios e diretrizes dos padrões de riscos que seguimos atualmente. No início dos anos 90, as bases para o que conhecemos como gestão de risco foram estabelecidas, mediante a publicação de dois documentos que se tornaram referência internacional sobre o tema: o Cadbury (CADBURY, 1992) e a AS/NZS 4360:1995 (AUSTRALIA, 2004).

Já no início do Século XXI, houve a consolidação de práticas de gestão de risco corporativo. Em 2001 foi iniciado aquele que se tornou o principal guia de gestão de riscos britânico, o The Orange Book. Na mesma época, em 2002, os Estados Unidos aprovaram a chamada Lei Sarbanes-Oxley, por meio dela, buscaram mitigar riscos, evitar a ocorrência de fraudes e proteger investidores

PUC-Rio - Certificação Digital Nº 1721463/CA

(USA, 2002). Ainda no mesmo período, em 2004, o COSO publicou o Enterprise Risk Management - Integrated Framework.

Nos últimos anos, um dos padrões mais adotados internacionalmente foi lançado em 2009, a norma técnica ISO 31000 Risk Management – Principles and Guidelines, que provê princípios e boas práticas para um processo de gestão de riscos corporativos. No Brasil a norma também é amplamente utilizada, sua tradução e edição é divulgada pela Associação Brasileira de Normas Técnicas (ABNT-ISO 31000, 2009).

A Tabela 3 contém parte dos padrões de riscos citados no guia de riscos corporativos do IBGC com suas respectivas datas de publicação no cenário mundial.

Tabela 3 – Histórico dos padrões sobre riscos (IBGC, 2017)

1921	Estudo de Frank Knight
1947	ISO
1977	FCPA
1985	Criação Coso
1988	Acordo Basileia I
1992	Coso I – Internal Controls CadBurry VaR
1996	Cobit
1999	Emendas ao Basileia I
2004	Proposta de uma nova adequação de capital: Basileia II
2005	Sarbanes-Oxley Coso II – ERM ISO 27.001
2009	ISO 31.000
2010	UK Bribery Act Basileia III / Lei Dodd-Frank
2013	Coso 2013 – atualização
2014	Lei n. 12.846 – Anti-Corrupção
2017	Decreto n. 8.420 / ISO 9.000 – Mentalidade de Riscos

PUC-Rio - Certificação Digital Nº 1721463/CA

2.3.2. Princípios e diretrizes

A ISO 31000 fornece princípios e diretrizes para gerenciar os riscos de forma geral, não especificando o setor ou área de atuação da organização. Além disso a norma pode ser aplicada no nível operacional, tático ou estratégico para serviços, projetos ou produtos (ABNT-ISO 31000, 2009).

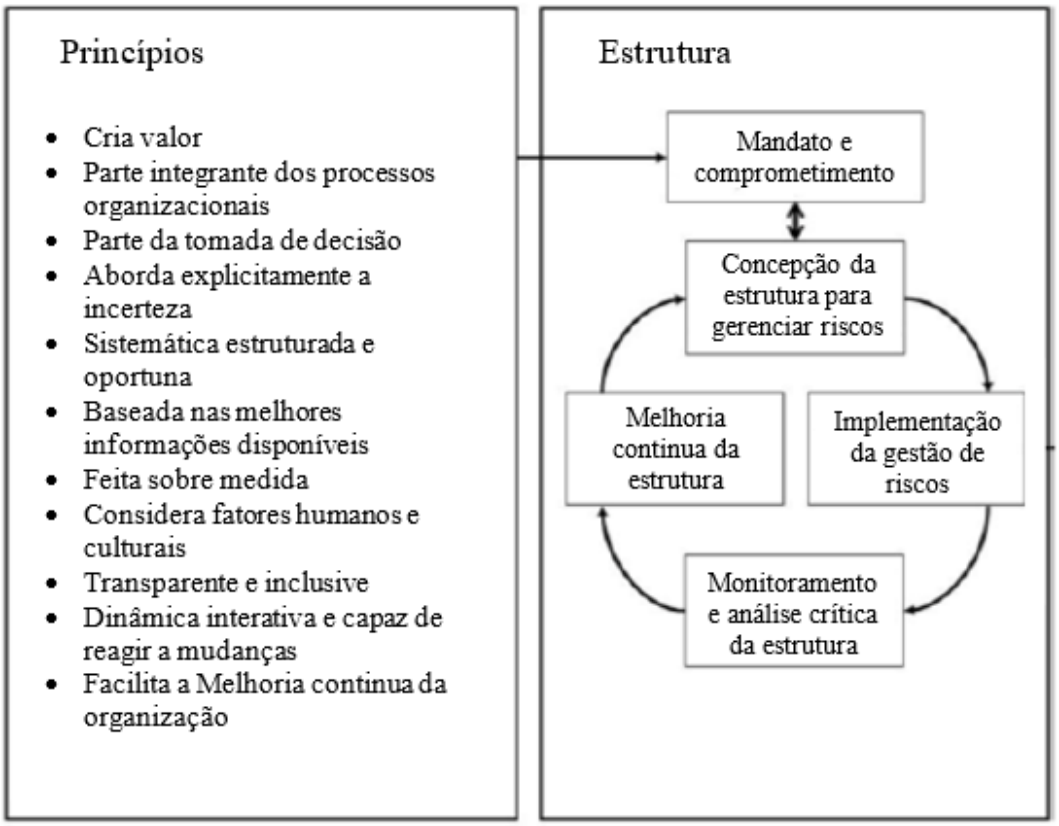


Figura 4 – Princípios para gestão de riscos (ABNT-ISO 31000, 2009)

Em linhas gerais, o fluxo do risco segue uma primeira análise pela diretoria, visto que primeiramente é necessário entender a área responsável da empresa por tratar cada risco. Após a fase inicial, cada gestor faz uma mensuração mais detalhada do risco, levando em consideração os objetivos de negócio e a tolerância para entidade suportar a concretização do risco analisado. Após a análise do gestor, os riscos são colocados em uma visão de carteira para que a alta administração possa avaliar a gravidade do risco e as interdependências existentes.

2.3.3. Processo gestão de riscos

Uma iniciativa de gestão de riscos bem implementada depende das diretrizes, metas e objetivos traçados pela alta administração na matriz organizacional. Os registros e ações reportadas na cadeia de gestores da empresa serve como origens para tomadas de decisão mais precisas nos níveis hierárquicos mais elevados.

PUC-Rio - Certificação Digital Nº 1721463/CA

A Figura 5 descreve as interrelações entre as áreas no processo de gestão de riscos, além disso, contempla de forma macro o processo de riscos conforme a norma ISO 31000.

De acordo com a norma da ISO 31000 (ABNT-ISO 31000, 2009), o planejamento do gerenciamento de riscos segue as etapas para compor o processo geral de gerenciamento de riscos. As etapas contidas na norma estão descritas abaixo de forma resumida:

a) Estabelece o contexto: classificação se os riscos e ameaças são internos ou externos;

b) Identificação de riscos: busca, reconhecimento e descrição de riscos, gerando uma lista de eventos que impactam os objetivos organizacionais;

c) Análise de risco: avaliação das causas e fontes de risco, suas consequências positivas e negativas e a probabilidade de que essas conseqüências possam ocorrer;

d) Avaliação de Riscos: auxilia na tomada de decisões quanto ao tratamento, estabelecendo prioridades e possíveis ações a serem tomadas para posterior processamento;

e) Riscos de tratamento: processo usado para modificar o risco, incluindo mitigação de riscos, táticas de prevenção de riscos e planos de contingência, caso o risco se concretize;

f) Comunicação e consulta: processo contínuo e iterativo que fornece informações compartilhadas, dialogando com as partes interessadas;

g) Monitoramento e Análise Crítica: processo contínuo de verificação, supervisão, observação crítica ou identificação da situação para identificar mudanças.

O padrão ainda trata das funções e responsabilidades que os atores organizacionais devem cumprir nos ambientes corporativos. A abordagem contém três linhas de defesa, onde na primeira linha estão os operadores do processo de gestão de riscos (controles internos), já na segunda linha estão os profissionais que

PUC-Rio - Certificação Digital Nº 1721463/CA

apoiam a primeira linha em suas atribuições. Por fim, a terceira linha contém os profissionais da auditoria interna, que são mais independentes da execução do processo.

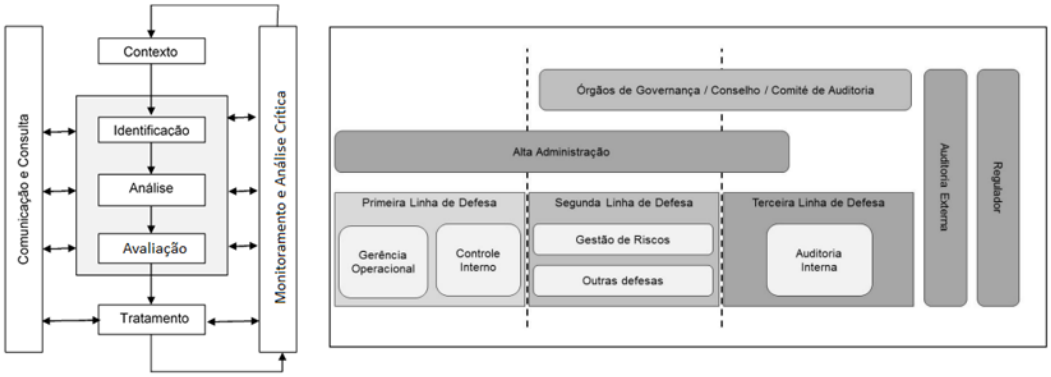


Figura 5 – Processos de riscos (ABNT-ISO 31000, 2009)

Há também no normativo ISO uma especificamente à Matriz de Riscos que é mais um componente para a gestão de riscos que permite a identificação e priorização dos riscos em uma tabela geral. A matriz de riscos consiste em uma tabela de duas dimensões com objetivo de calcular a severidade do risco e exibi-lo em um diagrama gerencial.

A Figura 6 traz o processo de gestão de riscos empresarial, de acordo com as normas apresentadas. O processo é uma interpretação do autor em relação à literatura já apresentada.

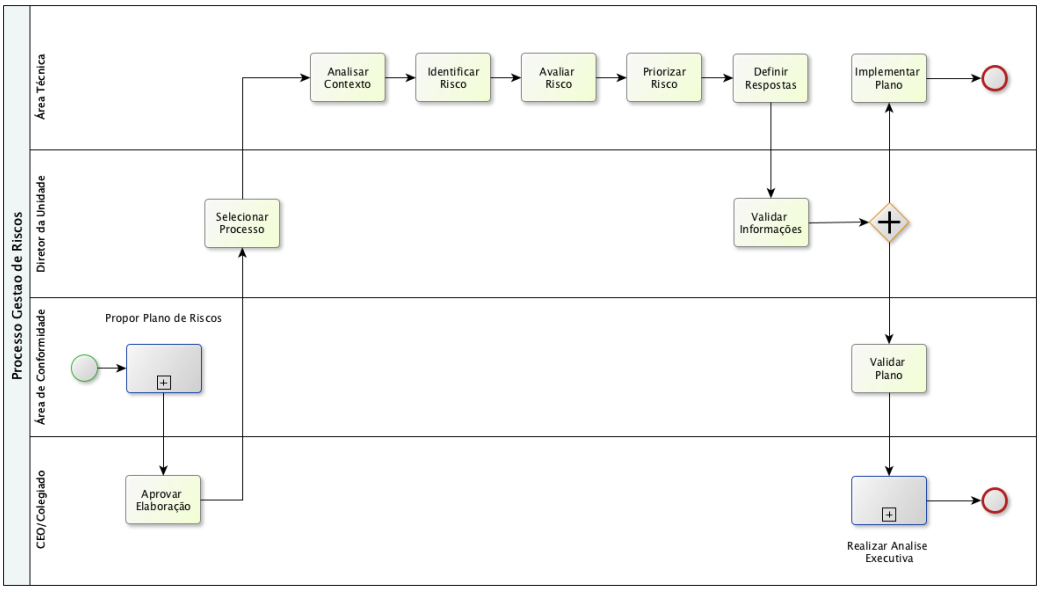


Figura 6 – Processo geral de gestão de riscos

PUC-Rio - Certificação Digital Nº 1721463/CA

2.3.4. Matriz de riscos

Este tópico contém os conceitos trazidos pela norma ISO 31000 para, após entender o processo da gestão de riscos, compreender sua categoria e identificar sua severidade, para assim subsidiar as decisões dos gestores (ABNT-ISO 31000, 2009).

De acordo com a norma, o risco é uma composição de probabilidade de ocorrência com o impacto por ele causado, no caso da ocorrência se confirmar:

Risco = Probabilidade X Impacto

O resultado dessa operação estabelece o nível de risco para a organização. A análise de riscos pode ser qualitativa ou quantitativa, em função do cenário apresentado. Métodos qualitativos usam escalas como baixa, média e alta. Já os métodos quantitativos são representados por valores para suas consequencias e probabilidades, dependendo do conhecimento do gestor sobre os processos empresariais.

Extraída do guia sobre riscos do Instituto Brasileiro de Governança Corporativa, a Figura 7 exemplifica a relação entre os riscos, que pode ser ilustrada por meio de uma matriz bidimensional simples, como a que segue:

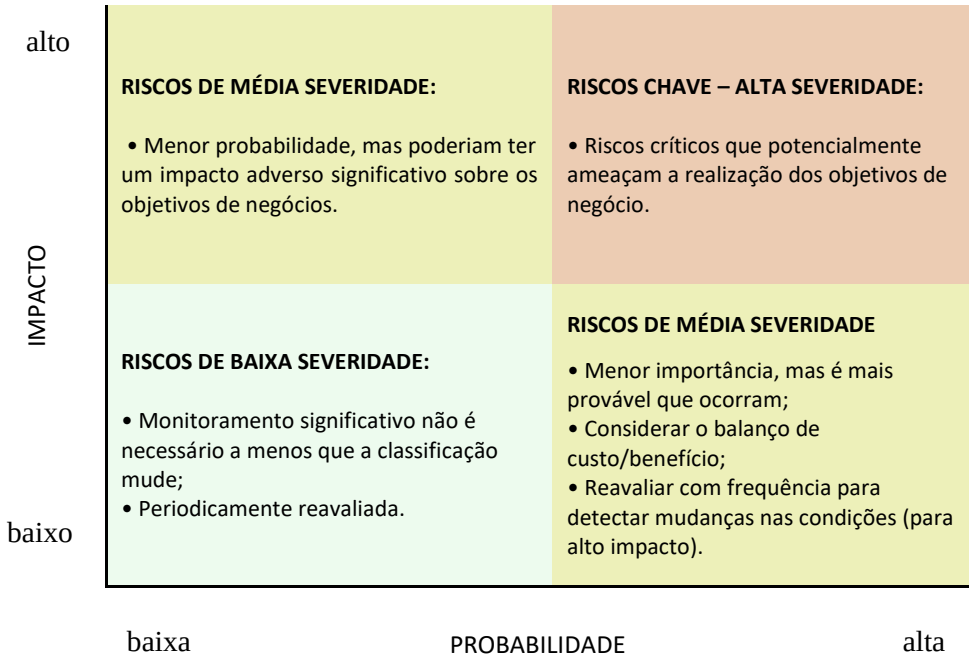


Figura 7 – Matriz de riscos (IBGC, 2017)

PUC-Rio - Certificação Digital Nº 1721463/CA

2.3.5. Medição e desempenho na gestão de riscos

Em relação à medição e desempenho dos riscos, a norma editada pelo *Committee of Sponsoring Organizations of the Treadway Commission*, COSO (COSO, 2017), trouxe uma atualização em suas definições tratando o tema de uma forma mais estruturada. No material, algo que é bastante pontuado é que as estratégias de abordagens à tomada aos riscos não são homogêneas, quando comparadas de uma organização para outra.

Em alguns casos, os Conselhos das empresas se envolvem mais com a estratégia de risco definida pela Administração, em outros casos os Conselhos fazem um papel menos questionador, tendendo a aceitar a visão definida pela Administração sobre os riscos. Entretanto, independente da estratégia tomada para o apetite a riscos, a missão e visão da empresa são sempre um direcionador para as decisões sobre os riscos.

O que a norma traz também como informação sobre a mensuração de riscos é que, além de ser uma definição que é refinada pelos gestores de cada área, o melhor tipo de abordagem de estruturação dos riscos é aquele que está alinhado a estratégia da empresa.

Extraída da norma COSO editada em 2017, a Tabela 4 traz um exemplo de tabela que define os níveis de riscos aceitos por uma organização após a definição das metas estratégicas e a análise dos riscos indicados pela Administração e detalhado pelos gestores das áreas.

PUC-Rio - Certificação Digital Nº 1721463/CA

Tabela 4 – Medidas de meta e desempenho (COSO, 2017)

Objetivo de Negócio	Meta	Tolerância
Retorno sobre os investimentos para um gerente de ativos	Meta de 5% de retorno anual sobre a carteira	3% a 7% de retorno anual
Pedidos online de entrega em domicílio de um restaurante	Meta de entrega em 40 minutos	Tempo de entrega entre 30 e cinquenta minutos
Diminuir o número de ligações perdidas em um call center	Meta de 2% do número total de ligações	1% a 5% do número total de ligações

O que se pretende pontuar para esta dissertação com as definições de medição e desempenho na gestão de riscos é que, para a Administração definir os riscos de cada área, é necessário o conhecimento dos processos de negócio da empresa no nível de detalhe que cada processo possui. Dessa forma, modelos que representem bem os processos possibilitam que os administradores e gestores possam elencar os riscos de forma correta e prever as medidas de tolerância necessárias para cada risco elencado.

PUC-Rio - Certificação Digital Nº 1721463/CA

3 Modelo conceitual

3.1 Modelagem de gestão de riscos em engenharia de requisitos

Em função da importância que as informações possuem sobre a estratégia de gestão de riscos nas organizações, torna-se claro que as áreas de TI desempenham um papel central na avaliação de riscos. O ponto mais importante é que em um processo de gestão de riscos há várias informações que não são valoradas de forma objetiva, e para isso a representação dos requisitos não funcionais por meio de um framework de metas flexíveis (CASTRO, 2002) pode ser uma boa aliada ao processo de gestão de riscos. Dessa forma, o que pretendemos aqui é utilizar um catálogo de metas flexíveis (CHUNG, 2000) para auxiliar na análise da gestão de riscos empresarial.

PUC-Rio - Certificação Digital Nº 1721463/CA

3.2 Processo para construção do modelo de gestão de riscos

Neste tópico ilustramos o processo utilizado para criação do modelo proposto, que tem por objetivo representar as dependências da organização, suas funções, recursos, metas e softgoals (metas de qualidade, NFRs). Os softgoals, no modelo, refletem as qualidades relacionadas com os riscos.

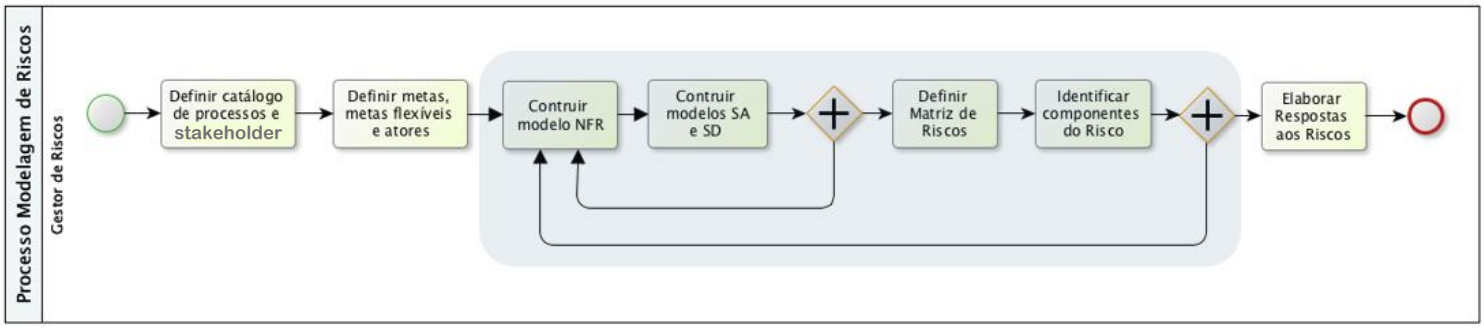


Figura 8 – Processos de definição dos riscos empresariais em TI

- ***01. Definir catálogo de processos e stakeholders:***

  Nesta etapa utilizamos o framework COBIT-5 (COBIT, 2012) para obter a base dos processos e stakeholders de TI. O COBIT faz integração dos principais frameworks de mercado como o ITIL, PMBOK e TOGAF, além disso, também propõe o alinhamento da TI ao negócio, permitindo uma visão holística da organização.

- ***02. Definir metas, metas flexíveis e atores:***

  Nesta etapa reduzimos a base de processos do COBIT com a premissa que as seguintes áreas estivessem representadas: a) governança, planejamento, implantação, suporte e monitoração. Também extraímos os atores do framework com o obejtivo de termos as seguintes áreas representadas: a) alta administração, área de negócio, *compliance* e áreas de TI.

- ***03. Construir modelo NFR:***

  A partir dos processos mapeados no passo 02, identificamos quais seriam as metas que não teriam critérios estritamente claros para terem seus objetivos satisfeitos e, a partir desses, construímos o modelo NFR.

- ***04. Construir modelos SA e SD:***

  Construção do modelo de gestão de riscos, considerando a rede de dependências e elos entre os atores, de acordo com a linguagem i*, descrevendo as metas, tarefas, recursos e metas flexíveis.

- ***05. Definir Matriz de Riscos:***

  Nesta etapa, para tornar mais compreensível a identificação dos componentes do risco (passo 06), foram considerados apenas 2 riscos de TI, muito comuns a uma matriz de riscos empresarial: I – Falha no desenvolvimento de projeto e II – Falha na gestão de mudanças.

- ***06. Identificar componentes do Risco:***

  Foi utilizado o modelo SD para identificar os riscos escolhidos no passo 05. As metas, atores, recursos, tarefas e metas flexíveis associadas ao risco foram elencadas pelo autor, de acordo com a natureza do risco analisado. A etapa tem como finalidade ser um exercício para percepção do uso real da modelagem, avaliando se é possível visualizar de forma holística as partes envolvidas em um determinado risco empresarial.

PUC-Rio - Certificação Digital Nº 1721463/CA

- ***07. Elaborar plano de respostas aos Riscos:***
  Nesta etapa, é elaborado pelos gestores um plano de ação para os riscos identificados, que é aprovado posteriormente pelos altos executivos da organização.

Conforme mencionado no primeiro capítulo, o objetivo desta pesquisa é que a modelagem criada apoie os gestores de riscos a entenderem melhor os riscos empresariais de forma a tomarem decisões mais precisas quando da concepção e aprovação de um plano de resposta aos riscos.

3.3 Representação da gestão de TI

A tabela 5 representa os atores responsáveis pela gestão organizacional no contexto de Tecnologia da Informação, os 6 agrupamentos de responsabilidades representam os 6 atores que serão utilizados no modelo SD a ser criado. A origem dos dados de responsáveis é do framework COBIT-5.

Tabela 5 – Os grupos de atores para modelagem i-estrela

1	Diretoria	Board
		Chief Executive Officer
		Chief Financial Officer
		Chief Operating Officer
2	Negócios	Business Executive
		Business Process Owners
		Strategy Executive Committee
		Steering Committee
3	Auditoria	Project Management Officer
		Value Management Officer
		Chief Risk Officer
		Chief Information Security Officer
		Architecture Board

3	Auditoria	Enterprise Risk Committee
		Head Human Resources
		Compliance
		Audit
4	Plan.	Chief Information Officer
		Privacy Officer
		Head IT Administration
5	Desen.	Head Architect
		Head Development
		Information Security Manager
6	Oper.	Head IT Operations
		Service Manager
		Business Continuity Manager

Para compreender melhor os processos que seriam usados para criação do modelo SD, foi criada a Tabela 6 que é um resumo de todos os processos constantes do COBIT-5 (COBIT, 2012). O objetivo do modelo é representar as dependências

PUC-Rio - Certificação Digital Nº 1721463/CA

da organização, suas funções, recursos, metas e softgoals (metas de qualidade, NFRs). Os softgoals refletem as qualidades relacionadas aos riscos mapeados.

Tabela 6 – Processos de Tecnologia da Informação para modelagem

Macroprocessos para gestão de TI
1 – Alinhar a TI ao negócio
1.1 - Gerenciar a estratégia e o planejamento de TI
Desenvolver estratégias de TI
Desenvolver planejamento de TI
1.2 - Gerenciar o desempenho da TI
Monitorar o desempenho financeiro
Gerenciar o desempenho dos processos de TI
Gerenciar o desempenho operacional de TI
1.3 - Alinhar arquitetura de TI ao negócio
Desenvolver arquitetura de TI
Prospectar novas tecnologias de TI
Padronizar tecnologias existentes
..4 - Gerenciar a prestação de serviços aos clientes
Gerir os recursos de ambientes informatizados
Gerenciar o catálogo de serviços de TI
Gerenciar o portfólio de serviços de TI
..5 - Fornecer inovação através de processos e tecnologia
2 - Gerenciar o relacionamento com as áreas de clientes
2.1 - Avaliar novas soluções de TI
Estruturar o planejamento das ideias de TI
Identificar benefícios e requisitos de TI das ideias
Identificar necessidade das soluções de TI
Consolidar soluções propostas
2.2 – Gerenciar o portfólio de TI
Identificar projetos de TI
Priorizar os projetos de TI
Controlar os projetos de TI
2.3 – Monitorar os serviços de TI
Desenvolver relatórios e indicadores de serviços
Controlar os serviços de TI
Realizar reuniões de acompanhamento com clientes
Avaliar mudanças em projetos
Avaliar pós implantação dos projetos
2.4 - Executar consultoria de serviços de TI
Aprofundar as relações com os clientes
Prospectar soluções de clientes
Executar consultoria a serviços solicitados
2.5 - Gerenciar modelo de informação de TI

4 – Sustentar os serviços de TI
4.1 – Controlar solicitações de ativos e incidentes
Tratar eventos e solicitações de TI
Tratar incidentes
Controlar ativos de TI
4.2 - Gerenciar a qualidade na passagem para a produção
Documentação mudança de infra-estrutura
Controlar documentação de requisitos de sistemas
Gerir integridade e disponibilidade dos sistemas
Manter catálogo de aplicações
4.3 – Controlar ambientes e produtos de TI
Controlar a disponibilidade de ambientes de TI
Gerenciar mudanças nas configurações de TI e infra-estrutura
Gerenciar a continuidade dos serviços de TI
Executar serviços de TI
4.4 - Manter sistemas e ambientes de TI
Prover correção e manutenção de aplicações
Garantir a manutenção preventiva de ambientes de produção
Executar gestão de ambientes em produção
Preparar documento de manutenção para novos sistemas
5 - Apoiar a organização de TI
5.1 - Gerenciar a segurança, risco e conformidade
Gerenciar as políticas, normas e padrões de segurança da informação
Gerenciar arquitetura tecnológica de segurança da informação
Gerenciar os riscos de TI
Gerenciar conformidades de TI
Gerenciar perfis de acesso e identidade em TI
5.2 - Gerenciar fornecedores e contratos de TI
Gerenciar contratações e aquisições
Gerenciar relacionamentos com fornecedores
Realizar pequenas contratações
5.3 - Gerenciar a administração e orçamento de TI
Gerenciar a administração de TI
Gerir o orçamento de TI
Verificar pagamentos e contratos de TI
Gerir os recursos humanos e conhecimento de TI
Gerenciar satisfações de empregados em TI
Gerir e desenvolver funcionários de TI

PUC-Rio - Certificação Digital Nº 1721463/CA

3 – Implementar as soluções de TI
3.1 - Desenvolver protótipo de projetos
Desenvolver estrutura de soluções de TI
Reunir informações, processos e requisitos
Prototipar sistemas de informação
3.2 - Implementar soluções de software
Realizar análise e projeto de soluções de software
Desenvolver soluções de software
Testar e aprovar aplicações de TI
Prospectar ferramentas pre-existentes de software
3.3 - Implementar soluções de infraestrutura
Realizar análise e projeto de soluções de infra
Desenvolver soluções de infra
Testar e aprovar sokuções de infra
3.4 - Gerenciar métodos e documentação
Gerenciar documentação padrão de ambiente
Gerenciar recursos e ferramentas
Gerenciar métodos para desenvolvimento e manutenção
Gerenciar conhecimento de TI

5.4 – Suportar comunicação de TI
Gerir a mudança em ambientes de TI
Gerir a comunicação interna e externa

PUC-Rio - Certificação Digital Nº 1721463/CA

3.4 Matriz de riscos para análise

É geralmente usada para avaliar o risco em um nível geral, muitas vezes quando não há muitos dados ou recursos disponíveis.

Cabe destacar que a atividade de elaborar uma matriz de riscos não pode ser a única a ser executada quando os riscos forem ser priorizados, sendo necessário visualizar detalhes de cada risco.

Na elaboração de uma matriz de riscos a escala de probabilidades será classificada como:

• Muito baixa: Improvável. A conjuntura sugere essa possibilidade em um cenário extremamente atípico. (peso 1)

• Baixa: Rara. A conjuntura pouco sugere essa possibilidade. (peso 2)

• Media: Possível. A conjuntura observada sugere moderadamente essa possibilidade. (peso 5)

• Alta: Provável. A conjuntura observada sugere fortemente a possibilidade. (peso 8)

• Muito alta: A conjuntura observada sugere nitidamente essa possibilidade. (Peso 10)

A escala de consequências será classificada de acordo com a lista abaixo:

• Muito baixo: Mínimo dano aos objetivos da empresa. (Peso 1)

• Baixo: Pequeno dano à empresa. (Peso 2)

• Médio: Moderado dano aos objetivos empresariais, entretanto recuperável. (Peso 5)

• Alto: Significativo dano aos objetivos empresariais, de difícil reversão. (Peso 8)

• Muito alto: Catastróficos danos aos objetivos empresariais, de forma irreversível. (Peso 10)

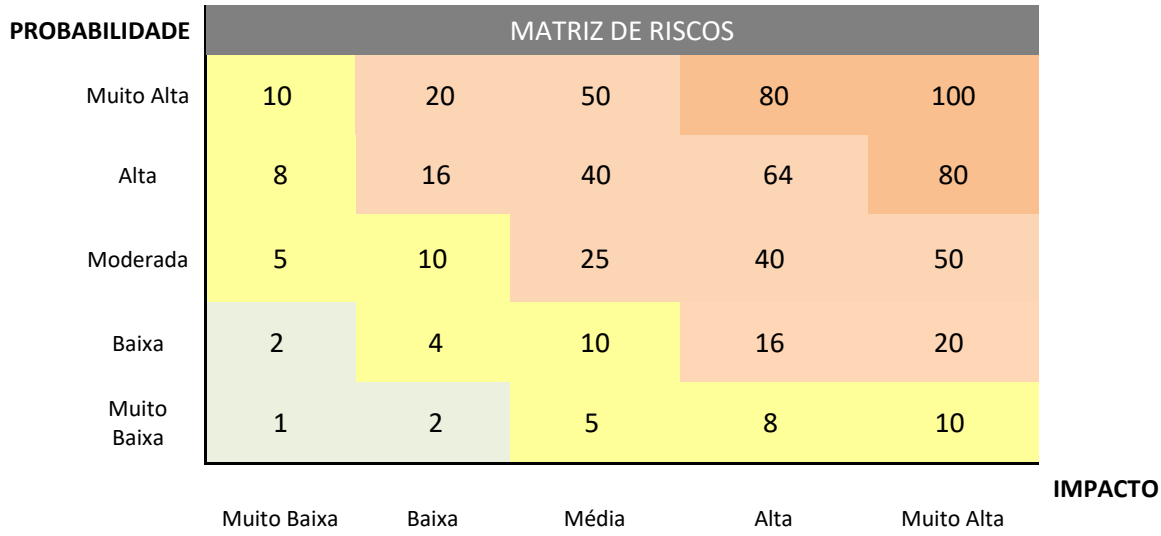


Figura 7 – Matriz de riscos com métricas (IBGC, 2017)

3.5 Exemplo de aplicação da Matriz

Neste tópico iremos utilizar o modelo SD descrito para rastrear os elementos associados aos riscos que compõem uma matriz de riscos de tecnologia da informação. Um dos principais objetivos da gestão de riscos é que os gestores tenham uma melhor compreensão da estrutura organizacional, vinculando-a às ameaças as quais a instituição está exposta.

PUC-Rio - Certificação Digital Nº 1721463/CA

A matriz de riscos abaixo contém 4 riscos básicos de tecnologia da informação. A classificação dos riscos baseada na matriz de impacto e probabilidade ajuda os gestores a planejar e acompanhar os riscos de forma mais estruturada. Contudo, é importante ressaltar que o uso único e exclusivo da matriz não é suficiente para que se tenha um entendimento do processo com completude.

#	Risco	Descrição do risco
1	Falha de segurança de TI	Perda ou roubo de informações comerciais, causadas por falhas nos sistemas de proteção, ciberterrorismo ou não conformidade.
2	Falha de Infraestrutura	Falha ou indisponibilidade de recursos de TI, resultando em falhas ou interrupções nos serviços de TI.
3	Falha na Gestão de Mudanças	Falhas no gerenciamento de demandas, permitindo erros em sistemas e / ou processos no ambiente de produção.
4	Falha em projetos de TI	Falta de controle na implementação dos projetos, causando atrasos na implementação, baixa qualidade do produto ou não conformidade com os regulamentos legais.

Figura 10 – Exemplo de matriz de riscos

A tabela abaixo contém as descrições dos riscos e seus valores de impacto e probabilidade. A resultante da composição entre os valores dos eixos I e P posicionam cada risco em sua coordenada na matriz de riscos empresarial.

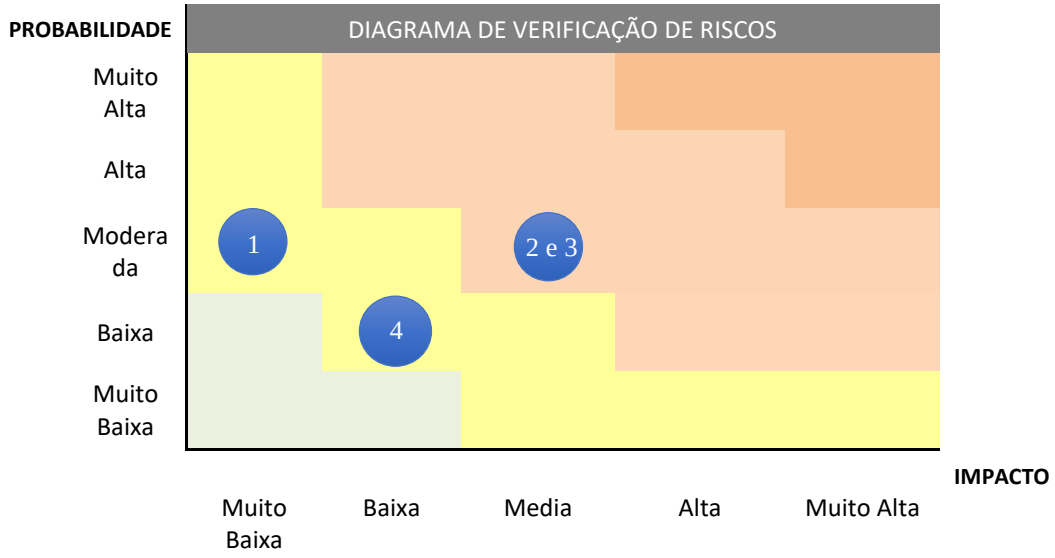


Figura 11 – Valores sugeridos para riscos de TI

PUC-Rio - Certificação Digital Nº 1721463/CA

4 Modelagem para gestão de riscos

Neste capítulo serão mostradas as atividades mais relacionadas à linguagem i-estrela especificamente, como a construção dos modelos SA, SD, o catálogo NFR, e as representações dos riscos no próprio modelo SD proposto.

Dessa forma, as etapas do processo e a sugestão de uma matriz de riscos, mencionados no capítulo 3, adicionadas às construções dos modelos descritas a seguir, servirão de base para subsidiar a hipótese do autor do uso da linguagem intencional para apoiar no processo de gestão de riscos empresarial.

4.1 Strategic Actor (SA)

Para representação dos responsáveis pelos processos organizacionais haverá seis atores relacionando os processos e metas empresariais no contexto de TI. As seis categorias são: Diretoria Executiva, Área de Negócio, Área de Riscos, Operacao de TI, Planejamento de TI e Arquitetura e Projetos de TI. Todos são derivados dos papéis e responsabilidades do framework COBIT-5 (COBIT, 2012). Conforme mencionado anteriormente, foi feito um resumo dos papéis organizacionais em seis categorias para facilitar o entendimento de uma versão inicial de um modelo SD aplicável a um ambiente empresarial. É natural que, conforme as necessidades, os papéis sejam adicionados para melhor expor as necessidades de cada empresa.

PUC-Rio - Certificação Digital Nº 1721463/CA

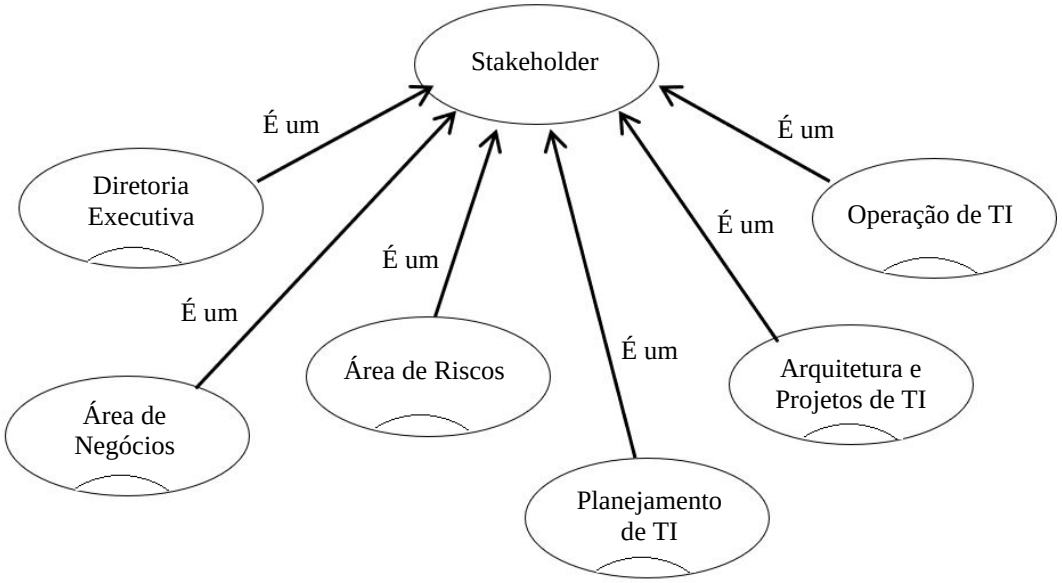


Figura 12 – Diagrama SA para processos empresariais de TI

PUC-Rio - Certificação Digital Nº 1721463/CA

4.2 Modelo NFR de gestão de riscos

Para uma melhor compreensão do papel das metas-flexíveis (NFRs) na gestão de riscos, foi criado um catálogo NFR (CHUNG, 2000) para ajudar a modelagem do conhecimento. A Figura 13 mostra um catálogo NFR parcial para a meta-flexível Invunerabilidade. O papel das metas-flexíveis na linguagem i-estrela capacita a descrição de como as qualidades interferem entre si, bem como processos e recursos da organização. O catálogo foi gerado a partir do processo de revisão do framework COBIT-5, conforme demonstrado no capítulo 3 deste trabalho.

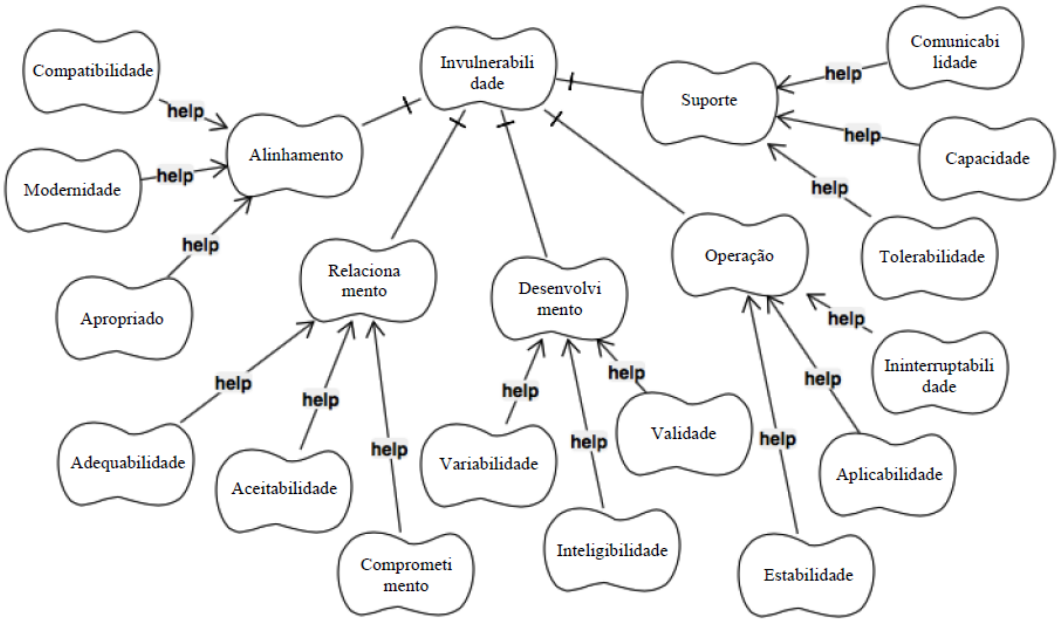


Figura 13 – Diagrama NFR (Invulnerabilidade)

PUC-Rio - Certificação Digital Nº 1721463/CA

4.3 Strategic Dependency (SD)

A partir das informações estruturadas dos processos e atores exibidos anteriormente foi construído o modelo SD para avaliação dos riscos de TI. Embora não tenham sido cobertos todos os processos de TI do framework, o modelo foi construído para também ser avaliado por pesquisadores e profissionais da área. A modelagem possui a base para mostrar as possíveis vantagens de usar uma linguagem intencional para representar o objetivo definido no capitulo inicial da dissertação.

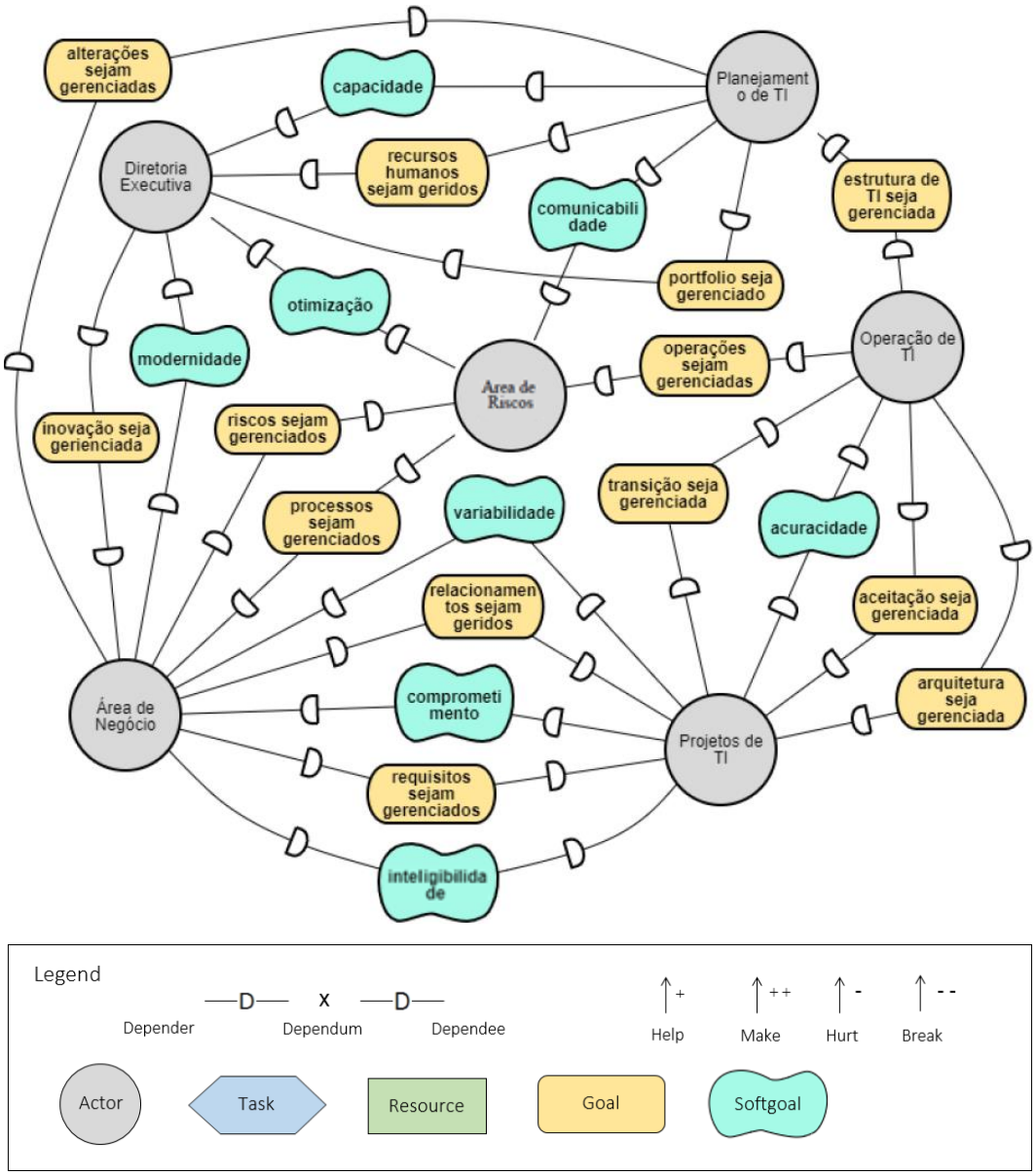


Figura 14 – Diagrama SD para processos empresariais de TI

A linguagem i-estrela também fornece outro diagrama, o diagrama SR, para ampliar os detalhes de como cada ator tenta cumprir as suas responsabilidades de acordo com o diagrama SD. Entretanto, para validação da modelagem foi elaborado apenas o diagrama SD e o catálogo NFR.

4.4 Uso do modelo SD para apoiar os gestores de riscos

As figuras 15 e 16 foram elaboradas a partir de riscos de TI, com base no diagrama SD para rastrear elementos associados a riscos que compõem uma TI. Um

PUC-Rio - Certificação Digital Nº 1721463/CA

dos principais objetivos da gestão de riscos é que os gestores tenham uma melhor compreensão da estrutura organizacional relacionando-a com as ameaças que a instituição está exposta, dessa forma o diagrama SD torna-se um poderoso aliado na gestão de riscos. *"A implantação e o aprimoramento da gestão de riscos começa com a conscientização sobre a importância de gerenciar riscos e avança com a implementação de práticas e estruturas necessárias*. " (TCU-SEPLAN, 2014).

Os riscos selecionados para aplicação do modelo SD estão demonstrados nas Figuras 15 e 16, sendo estes respectivamente: "A falha de projetos de TI" e "Falha na gestão de mudanças".

A avaliação do modelo irá comparar as Figuras 15 e 16 com o diagrama SD e verificar se elas auxiliam na visualização da rede de dependências organizacional, e se capacitam os gestores a avaliar melhor a cadeia de responsabilidades, metas, metas-flexíveis, tarefas e recursos envolvidos em um risco específico.

PUC-Rio - Certificação Digital Nº 1721463/CA

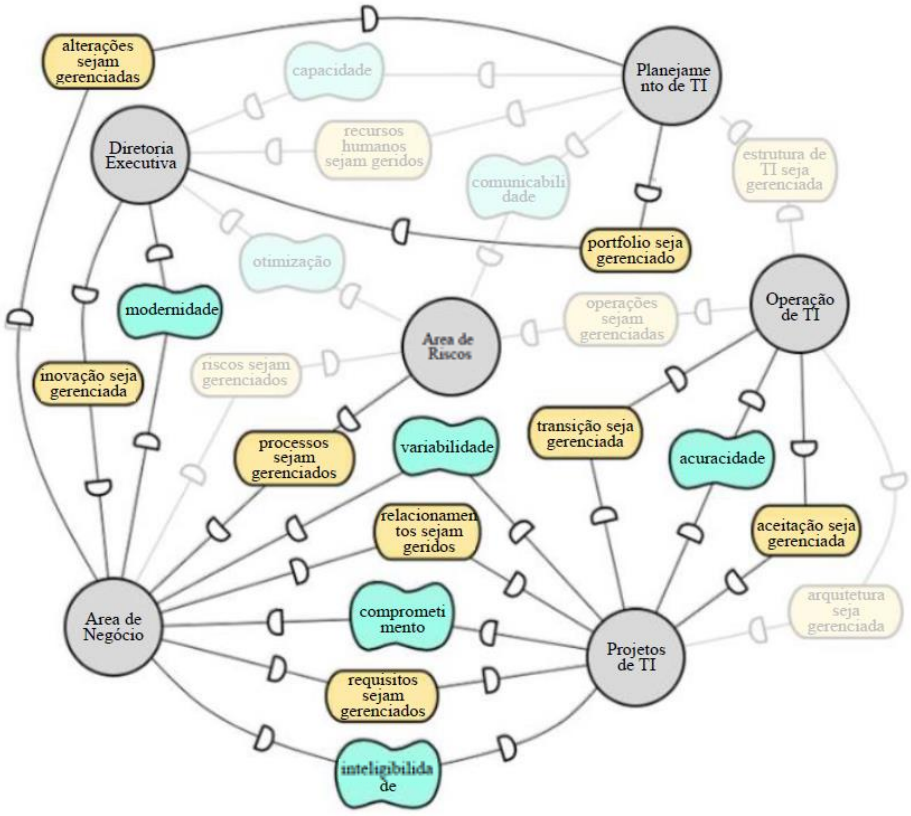


Figura 15 – Representação do risco 3

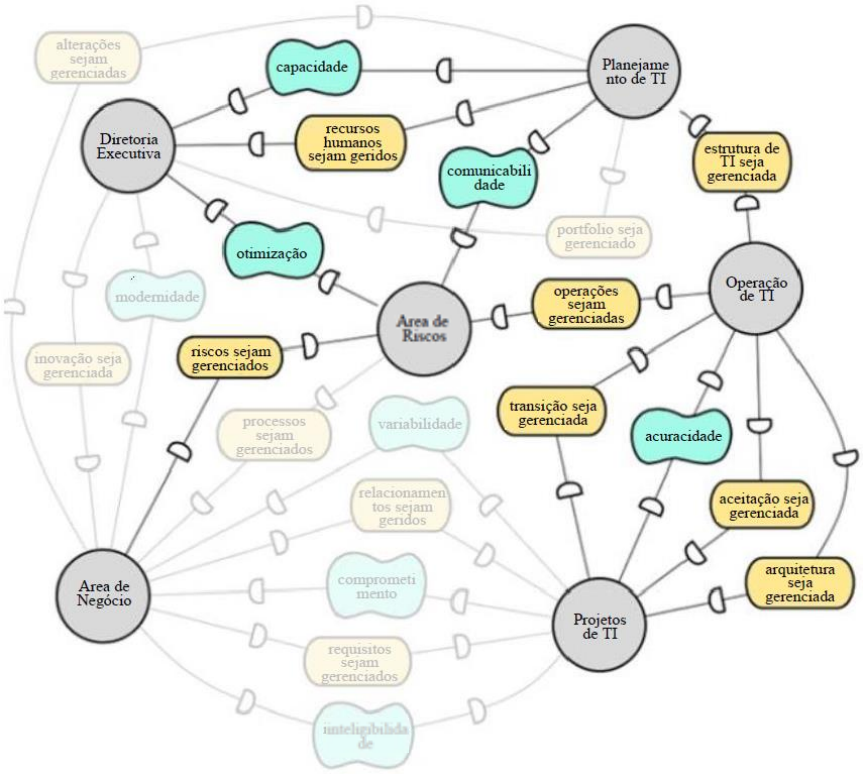


Figura 16 – Representação do risco 4

PUC-Rio - Certificação Digital Nº 1721463/CA

5 Avaliação da estratégia

Este capítulo descreve a avaliação da modelagem organizacional que visa apoiar os riscos de TI com os quais as empresas estão expostas, a partir do uso da linguagem intencional i-estrela.

5.1 Objetivo

Com a finalidade de obter percepções sobre a modelagem elaborada, o autor realizou uma pesquisa de opinião entre profissionais que atuam na área da pesquisa [1]. Conforme explicado ao longo do trabalho, o autor elaborou uma modelagem de gestão de riscos com uso de linguagem intencional para atender à necessidade de representar a contento as informações às quais os ambientes de negócio estão expostos.

Como resultado da avaliação, os participantes reportaram suas impressões sobre modelagem construída pelo autor e a eventual usabilidade desta modelagem. É importante ressaltar que os participantes apenas avaliaram única e exclusivamente a modelagem construída, não havendo participação no processo de construção da modelagem.

Durante a avaliação foram enviadas as documentações descritas abaixo, que continham o conhecimento sintetizado da linguagem i-estrela, o processo de construção da modelagem e a análise dos riscos a partir da modelagem:

> **Documento 1**: Contextualização sobre a linguagem i-estrela, o processo de construção da modelagem e por fim a análise dos riscos a partir da modelagem

[1] Submeteu-se à Câmara de Ética em Pesquisa da PUC-Rio o Projeto de Pesquisa 61/2020, para obtenção de parecer ético favorável para pesquisa de opinião envolvendo pessoas.

PUC-Rio - Certificação Digital Nº 1721463/CA

Documento 2: Questionário que aborda tanto questões sobre o perfil profissional do respondente, quanto aspectos sobre conhecimento adequado e usabilidade da modelagem. O questionário contém um grupo de questões profissionais e um grupo questões a respeito da modelagem.

Com as respostas ao questionário pretendeu-se cobrir os objetivos traçados para um entendimento sobre o processo de modelagem bem como a avaliação da modelagem em si, levando-se em consideração os riscos escolhidos e seus fatores associados.

5.2 Execução da avaliação

Para seleção dos participantes, a amostra da avaliação foi determinada pela quantidade de convites aceitos entre engenheiros de requisitos, arquitetos de TI e gestores de riscos. O total de convites feitos pelo autor foi de 43 (por meio eletrônico: e-mail ou Whatsup), dos quais o autor obteve resposta de 14 participantes, com o questionário efetivamente respondido. Nesta etapa foi solicitado aos participantes informar a quantidade de anos de experiência nas respectivas áreas de atuação.

Inicialmente o autor enviou a explicação textual para os 43 participantes que continha o objetivo da pesquisa e os documentos 1 e 2 citados anteriormente. Nesta etapa houve alguns questionamentos dos participantes para um melhor entendimento da pesquisa e, ainda nesta etapa, o autor efetuou pequenas correções nos documentos da pesquisa.

Após a etapa incial de entendimento, o autor enviou novamente para os 43 participantes a documentação ajustada para que se manifestassem com a resposta ao questionário. Houve então 14 respostas efetivas com o questionário preenchido pelos participantes.

Foi possível identificar no processo a importância da etapa incial no nivelamento do conhecimento entre os envolvidos na pesquisa. Na etapa, além de atingir o objetivo de explicação sobre o processo de criação da modelagem, foi possível identificar lacunas na documentação que impediam que os participantes

PUC-Rio - Certificação Digital Nº 1721463/CA

tivessem um melhor entendimento dos conceitos. Essa etapa foi necessária pois nem todos os participantes possuíam conhecimento sobre a linguagem i-estrela.

Com isso, o documento sobre a contextualização da modelagem foi mais bem detalhado para o entendimento dos participantes. Esta atividade reduziu o risco de o nível do conhecimento não ser uma ameaça no preenchimento do questionário de Avaliação Final.

5.2.1. Coleta dos dados

O questionário foi elaborado e armazenado por meio da ferramenta do *google forms*, para que o acesso às questões pelos participantes fosse mais fácil e para que o autor pudesse extrair as informações, tabular e armazenar com maior celeridade e precisão.

5.2.2. Limitações do estudo

Entre as limitações do estudo identificadas pelo autor estão:

a) a quantidade de perguntas pode não ter sido suficiente para capturar os resultados desejados, em função de tratar-se de um tema muito amplo e de difícil síntese em um pequeno número de perguntas;

b) o elaborador das perguntas ser um pesquisador em engenharia de requisitos com conhecimento na linguagem i-estrela, e, ao mesmo tempo, ter vivenciado profissionalmente os mesmos problemas de representação de informações ao mapear riscos de TI.

5.3 Avaliação do questionário

Para a Avaliação Final houve 14 questionários respondidos, dos 43 enviados. O grau de escolaridade dos respondentes é composto por 71% de pós-graduandos e os 29% restantes tem grau superior. O perfil complementar dos respondentes segue descrito nos tópicos subsequentes.

PUC-Rio - Certificação Digital Nº 1721463/CA

5.3.1. Perfil do respondente

O questionário preenchido após de execução da avaliação é evidenciado na Tabela 7. As perguntas visam avaliar, de modo geral, o perfil dos respondentes.

Tabela 7 - Questionário de perfil dos avaliadores

P.I – Há quanto tempo você atua em área relacionada a Engenharia/Tecnologia da Informação?
( ) Menos de 1 ano
( ) Entre 1 e 3 anos
( ) Entre 3 e 10 anos
( ) Acima de 10 anos
P.II – Qual sua área de atuação de maior especialidade?
( ) Arquiteto de Soluções / Engenheiro de Software
( ) Gestor de Riscos/TI
( ) Outros
P.III – Qual a receita anual da empresa de maior relevância que você já trabalhou (no mínimo 2 anos)?
( ) Menos de $10 milhões
( ) Entre $10 milhões e $100 milhões
( ) Entre $100 milhões e $1 bilhão
( ) Mais de $1 bilhão
P.IV – Qual método de modelagem de processos você possui maior especialidade?
( ) BPMN
( ) UML
( ) iStar
( ) Outro (Qual:_____)

PUC-Rio - Certificação Digital Nº 1721463/CA

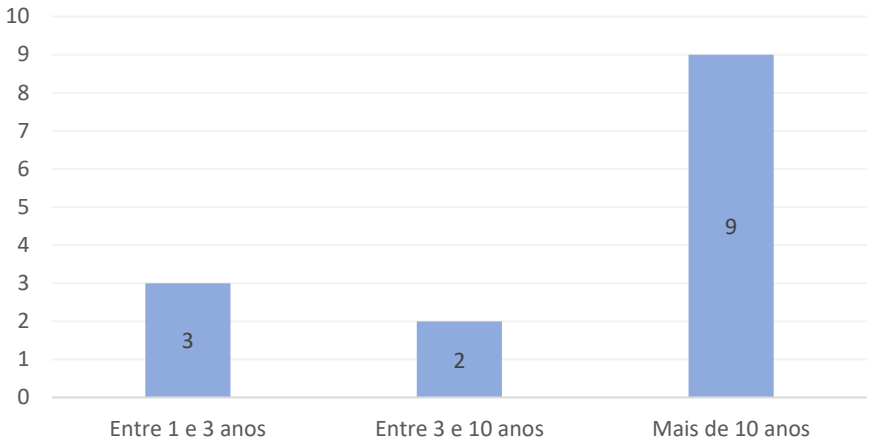


Figura 17 - Caraterização pela experiência profissional

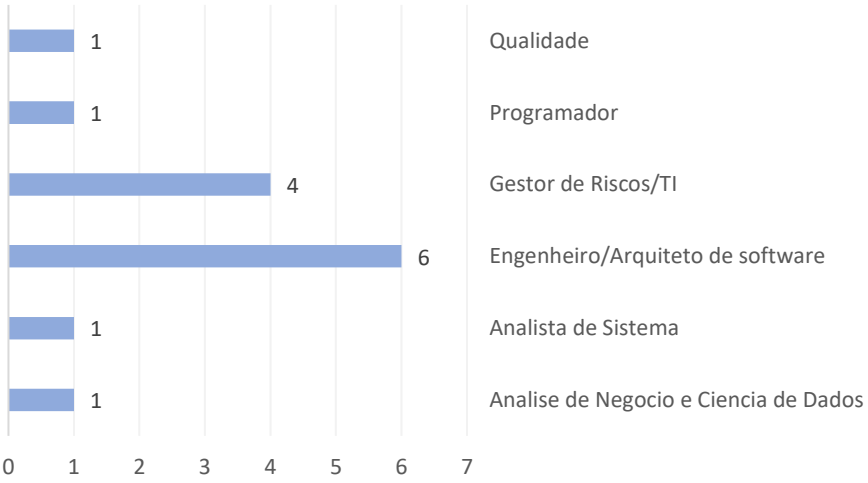


Figura 18 - Caraterização por área de atuação

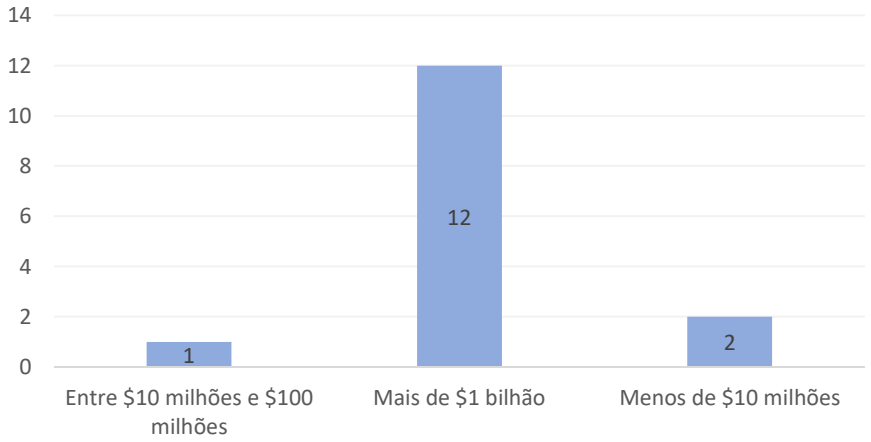


Figura 19 - Caraterização pelo tamanho da empresa que trabalha

PUC-Rio - Certificação Digital Nº 1721463/CA

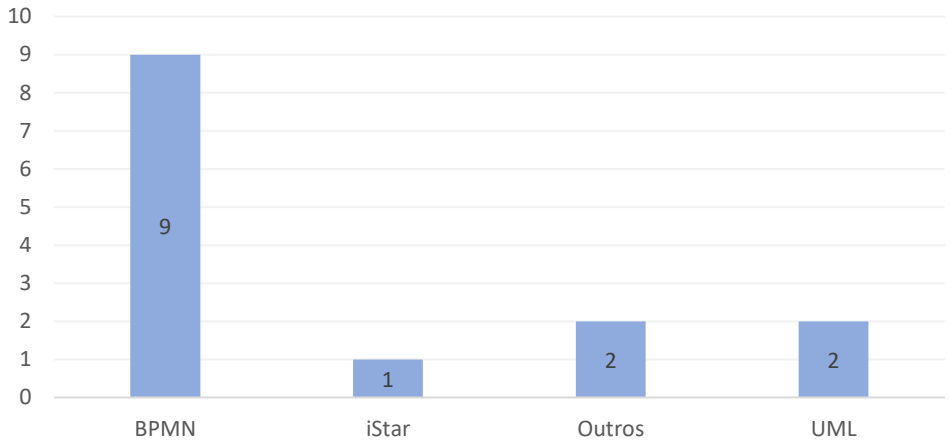


Figura 20 - Caraterização pelo metodo de processo que utiliza

Cabe destacar, a partir da caracterização dos participantes, que um grupo muito pequeno possuía conhecimento na linguagem i-estrela, conforme mencionado no gráfico acima.

5.3.2. Avaliação da modelagem elaborada pelo autor

A avaliação foi dividida em duas macroatividades para serem executadas pelos participantes do questionário. Após a leitura do documento sobre a contextualização da criação da modelagem e indicação dos riscos, foram respondidas as perguntas do documento 2, e as respostas estão tabuladas conforme segue:

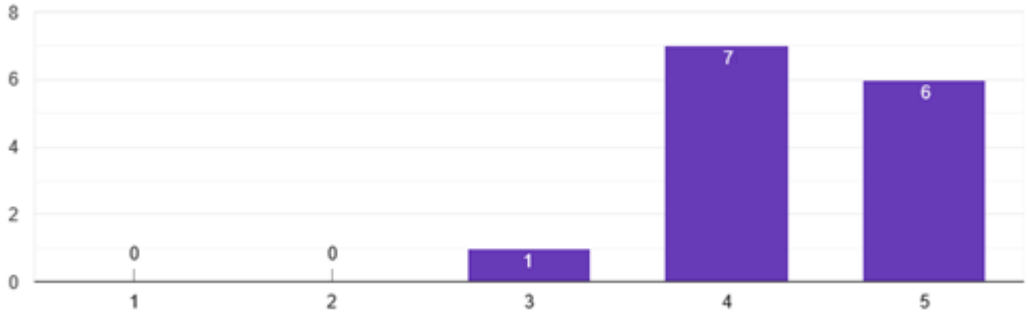


Figura 21 – Visualização dos riscos de forma geral

PUC-Rio - Certificação Digital Nº 1721463/CA

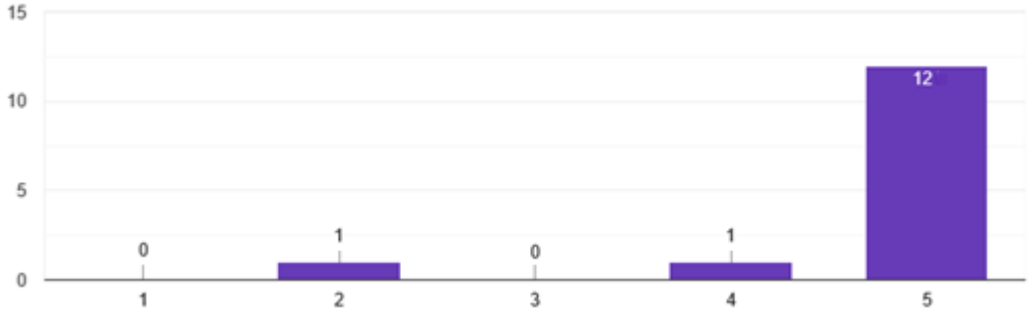


Figura 22 - Percepção de facilidade em visualizar separação de responsabilidades

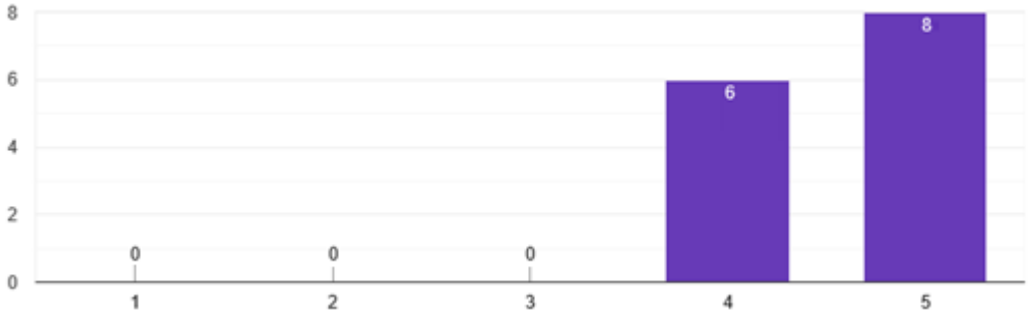


Figura 23 – Percepção de facilidade em visualizar transparência das informações

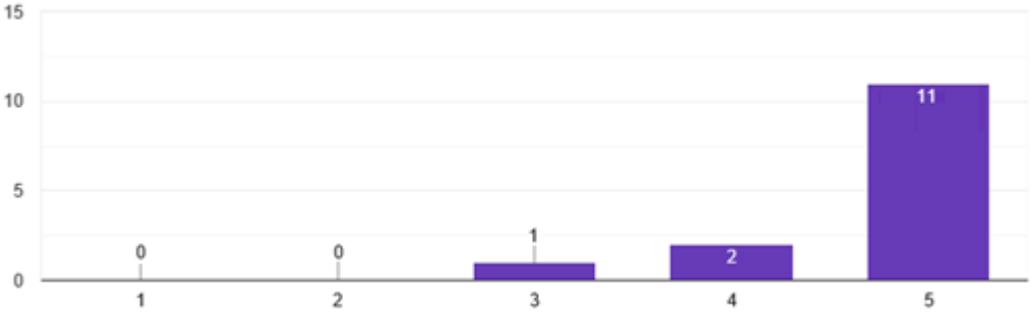


Figura 24 – Possibilidade de ajudar no trabalho rotineiro dos profissionais

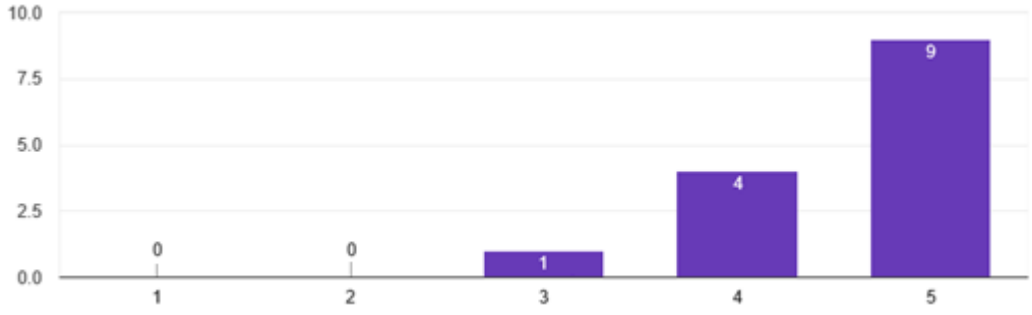


Figura 25 – Possibilidade de perceber os fatores associados a um risco

PUC-Rio - Certificação Digital Nº 1721463/CA

Foram recebidos comentários positivos e sugestões de melhoria com a finalidade de aperfeiçoar o modelo, em uma implementação posterior, conforme tabelas de resumo a seguir.

P6. Indique fatores positivos que encontrou na modelagem

Os registros no questionário evidenciam também os fatores positivos da modelagem e seguem listados abaixo:

• Ótima separação entre as reponsabilidades dos atores.
• A visualização dos riscos é bastante positiva, como se fosse um BSC (balanced score card) de riscos.
• Alto potencial para consolidação e apresentação de informações e dados complexos; Vinculação entre riscos e metas.
• Trouxe o nível de inter-relacionamento entre as áreas e as métricas relevantes.
• Tratar requisitos não funcionais junto com os funcionais; Definir metas e os meios para alcançá-las por ator.
• Atores e responsabilidades bem divididas e claras; Metas e riscos transparentes; A informação apoia decisões de maior qualidade.
• Ajuda a modelar riscos.
• Consegue de forma visual identificar os riscos e pontos de falha que podem ajudar na análise de riscos.
• Alinhamento de entendimento do processo põe todos os envolvidos.
• Em resumo ela permite o mapeamento adequado e realista do software.
• A modelagem trabalha bem no nivel operacional.
• A modelagem ajuda a visualizar de forma bastante clara e bem definida a interrelação entre os macroprocessos e entre as diferentes áreas/atores, relacionando-os com as potenciais falhas que se originam a partir disso.

P7. Indique fatores negativos que encontrou na modelagem.

Além dos fatores positivos, os respondentes registraram também os pontos negativos que encontraram na modelagem apresentada.

• Não é trivial o processo de construção da modelagem.
• Os nós deveriam apresentar outras variáveis ligadas neles, com pesos, como probabilidade, impacto, severidade e complexidade.
• Não encontrei.

PUC-Rio - Certificação Digital Nº 1721463/CA

- Modelos com um grande número de elementos são difíceis de se compreender. Não existe ferramentas muito utilizadas no mercado com essa linguagem.

- Não é simples. Requer um treinamento para conseguir entendê-la e utilizá-la de maneira consistente.

- Para uso, o especialista deve conhecer a linguagem i-star.

- Na modelagem não é possivel descrever todos os detalhes dos riscos, ou seja, não é um retrato 100 % da realidade.

- Pode ser demorado construir um modelo. Tambem é um grande desafio saber o nivel de abstracao mais adequado, pois o cliente pode estar num nivel de detalhe muito grande, mas isso pode ser importante para entender um requisito macro.

- A modelagem por vezes nao é adequada pra captar riscos exógenos ao processo.

- Apesar de ajudar na visualização dos macroprocessos e suas interações, poderia haver maior detalhamento do que leva determinado macroprocesso a não ser executado corretamente pelos atores.

Finalmente a pergunta P8 expõe sobre as sugestões de melhoria: ***P9. Pode dar alguma sugestão de melhoria da modelagem?***

- Estou habituada a utilizar a matriz de riscos de probabilidade, impacto e severidade. Este modelo tem a vantagem do visual, lembrando o BSC, portanto uma visualiação positiva para se apresentada à Alta Administração, e trazendo um modelo de rede, que quem sabe possa evoluir para redes neurais.

- Os processos de gerenciamento de riscos com os quais costumo trabalhar não têm vínculo claro entre os riscos e as metas que precisam ser alcançadas. A metodologia apresentada traz grande contribuição nesse aspecto.

- Uma evolução ao permitir sintetizar o inter-relacionamento entre as áreas e as métricas e visualização dos participantes na analise de risco.

- Eu tenho utilizado para modelar a intencionalidade de sistemas autoadaptativos legados em minha pesquisa de doutorado.

- Tenho bastante experiência no que foi apresentado.

- Para mim: inédito, muito interessante.

- O que foi apresentado é o que geralmente uso na prática.

- Eu uso bpmn e foi muito importante para entendimento do processo e dos riscos associados.

- O uso de modelagem em meu dia-a-dia se dá a partir de dados históricos e “bem-comportados”. Não há um trabalho de estruturação e clarificação das interações entre os atores e macroprocessos como na metodologia apresentada. Dessa forma, a abordagem proposta acresentaria uma camada complementar de tratamento dos dados, ajudando na visualização das falhas potenciais.

PUC-Rio - Certificação Digital Nº 1721463/CA

Cabe mencionar que as sugestões dos participantes permitirão melhorar o desenvolvimento de uma modelagem i-estrela para ser usada no modelo de gestão de riscos empresarial. Adicionalmente, os comentários dos participantes da pesquisa sugerem que a modelagem produzida na dissertação converge com os objetivos iniciais da pesquisa.

5.4 Síntese dos resultados

Com o resultado das avaliações feitas pelos respondentes sobre a modelagem de apoio à identificação de riscos de Tecnologia da Informação, pode-se observar que a proposta foi compreendida e possui aspectos relevantes para contribuir com o tema, com base nos dados estatísticos obtidos.

As estatísticas mostraram o grau de satisfação em relação à percepção da facilidade com a qual o usuário entende as características da modelagem.

Contudo, chamou atenção do autor que nas avaliações feitas pelos respondentes, alguns pontos ratificaram suposições já esperadas pelo autor, porém, houve ponderações que nem mesmo o autor havia previsto a respeito da modelagem.

Dentre os fatores que o autor havia suposto em relação à modelagem, destacaram-se:

- *Não há ferramentas de mercado que suportam a utilização da linguagem;*
- *É necessário um treinamento para uso da linguagem de maneira consistente;*
- *Um dos desafios é saber o nível de abstração mais adequado para construção de um modelo no ambiente empresarial.*

Em relação aos fatores não previstos pelo autor, os que merecem destaque em relação a uma melhoria da abordagem são:

- *O modelo poderia conter detalhes para que os gestores identifiquem as causas de um risco ser materializado;*
- *Os nós poderiam conter mais informações, como peso, severidade e complexidade.*

PUC-Rio - Certificação Digital Nº 1721463/CA

Diante da avaliação elaborada, além do aspecto positivo em relação ao resultado estatístico citado, as opiniões ajudarão em um aprimoramento do modelo e de seu processo de criação utilizado como insumo para validação da hipótese do trabalho.

PUC-Rio - Certificação Digital Nº 1721463/CA

6 Conclusão

6.1 Resumo

O objetivo desta pesquisa foi apresentar os benefícios do uso da linguagem i-estrela para apoiar a gestão de riscos de negócios, no contexto de um departamento empresarial de Tecnologia da Informação.

A utilização do diagrama SD evidencia uma melhor forma de exibir os processos de TI em um ambiente empresarial, permitido uma melhor avaliação dos riscos, bem como a adoção de contramedidas às ameaças identificadas.

Embora não tenha sido realizado um estudo sobre a introdução da línguagem i-estrela na prática real, o questionário com a percepção de profissionais e pesquisadores da área mostra argumentos que ratificam a hipótese do autor e também podem subsidiar posteriores melhorias à modelagem.

6.2 Contribuições

Ao propor uma modelagem intencional para a gestão de riscos corporativos, este trabalho traz a contribuição de mostrar a possibilidade de implementar uma modelagem multi-dimensional dos processos de TI com atores, papéis, recursos, metas e metas-flexíveis. Tal abordagem sugere uma forma de destacar as inter-relações dos processos de TI, as intenções dos atores envolvidos no processo, além de evidenciar os requisitos não funcionais para que os objetivos organizacionais sejam alcançados.

A opinião de pesquisadores e profissionais da área ratificam a hipótese do autor que é necessário um maior investimento em modelos e métodos que especifiquem os processos e metas organizacionais de uma forma mais precisa e completa.

PUC-Rio - Certificação Digital Nº 1721463/CA

6.3 Trabalhos futuros

Nesta pesquisa foram coletadas avaliações em relação à modelagem elaborada utilizando linguagem intencional para gestão de riscos empresariais de TI. Vislumbramos futuramente as seguintes melhorias:

- Detalhar o nível das tarefas das metas de acordo com os processos.
- Evoluir a modelagem incorporando novas metas e atividades de TI.
- Inserir mais atributos aos componentes do modelo de forma a trazer mais completude na representação das informações.
- Fazer uma nova avaliação sobre o processo de forma mais robusta, considerando um maior número de perguntas e uma maior quantidade de participantes.

As respostas aos questionários permitirão que o processo de criação da modelagem seja melhorado com a inclusão de novos processos, metas, metas-flexíveis e demais componentes de um modelo i-estrela para uma estrutura organizacional.

Com um amadurecimento da prospecção de metas-flexíveis para o modelo organizacional, será possível também generalizar a modelagem para a aplicação em ambientes empresariais, de acordo com a empresa.

PUC-Rio - Certificação Digital Nº 1721463/CA

7 Referências bibliográficas

ABNT - NBR ISO 31000 - Associação Brasileira De Normas Técnicas: **Gestão de riscos: Princípios e diretrizes**. Rio de Janeiro, 2009.

ABNT - NBR ISO/IEC 31010: **Gestão de riscos: Técnicas para o processo de avaliação de riscos**. Rio de Janeiro, 2012.

AMORIM, P., F.; SACRAMENTO, C.; CARPA, E., P.; TAVARES, P., Z.; FERREIRA, S., B., L.: **Submit or Not My HCI Research Project to the Ethics Committee, That is the Question** (2019). https://doi.org/10.1145/3357155.3358473.

ANDRADE, A. C. S.; Braga, J. L.; Leal, A. L. C.; Zaidan, F. H.: **Risk management in software projects: an approach based on non-functional requirements.** Revista Sistemas & Gestão - Universidade Federal Fluminense (2019). DOI: 10.20985/1980-5160.2019.v14n2.1526

ANTON, A. I. **Goal-based requirements analysis.** (1996). In Requirements Engineering, Proceedings of the Second International Conference on (pp. 136-144). IEEE.

ASNAR, Y., GIORGINI, P., MYLOPOULOS, J.: **Goal-driven risk assessment in require- ments engineering**. Requirements Eng. 16, 101–116 (2011). https://doi.org/10.1007/s00766-010-0112-x.

AUSTRÁLIA. *AS/NZS* 4360:2004 – **Risk Management, Australia Standards, 2004.** Disponível em: <http://infostore.sai-global.com/store/details.aspx?Produc- tID=381579>. Acesso em: maio, 2020.

BASAK, A., GIORGINI, P., MYLOPOULOS, J.: **Multi-objective risk analysis with goal models**. In: 2016 IEEE Tenth International Conference on Research Challenges in Information Science (RCIS). pp. 1–10 (2016). https://doi.org/10.1109/RCIS.2016.7549302.

CADBURY, A. **Report of the Committee on the financial aspects of corporate governance**. Londres: Gee and Company Ltd, 1992. Disponível em: <http://www. ecgi.org/codes/documents/cadbury.pdf>. Acesso em: maio, 2020.

CANADÁ. Secretaria do Conselho do Tesouro do Canadá. **Framework for the management of risk. Ottawa**, 2010a. Disponível em: <http://www.tbs-sct.gc.ca/pol/doc-eng. aspx?id=19422&section=text>. Acesso em: maio de 2020.

CASTRO, J., KOLP, M., MYLOPOULOS, J.: **Towards requirements-driven information systems engineering: the Tropos project**. Information Systems. 27, 365–389 (2002).

PUC-Rio - Certificação Digital Nº 1721463/CA

CHUNG, L.; NIXOS, B. A.; YU, E.; MYLOPOULOS, J.: **Non-Functional Requirements in Software Engineering** (2000).

COBIT 5: **A Business Framework for the Governance and Management of Enterprise IT** - ISACA (2012).

COSO: **Enterprise Risk Management - Integrating with Strategy and Performance** - (2017). Disponível em: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf. Acesso em: outubro, 2020.

CUNHA, H. S.: **Uso de estratégias orientadas a metas para modelagem de requisitos de segurança**. (2007). Dissertação de Mestrado. Pontifícia Universidade Católica do Rio de Janeiro.

FALESSI, D., CANTONE, G., CANFORA, G.: **Empirical Principles and an Industrial Case Study in Retrieving Equivalent Requirements via Natural Language Processing Techniques**. IEEE Transactions on Software Engineering. 39, 18–44 (2013). https://doi.org/10.1109/TSE.2011.122.

FIDALGO, J. J. C.: **Implementar COBIT em empresas de TI**. (2017) Dissertação de Mestrado. Universidade Aberta - Intituto Superior Técnico de Lisboa.

FRASER, J.; SIMKINS, B. J. **Enterprise risk management: today's leading research and best practices for tomorrow's executives**. New Jersey (EUA): John Wiley & Sons, Inc., 2010. Disponível em: <http://www.amazon.com/Enterprise-Risk-Management-Practices-Executives/dp/0470499087>. Acesso em: maio, 2020.

GESPUBLICA – Brasil - Ministério do Planejamento, Orçamento e Gestão. **Guia de Orientação para o Gerenciamento de Riscos. Secretaria de Gestão Pública**. Departamento de Inovação e Melhoria da Gestão. Brasília, 2013. Disponível em <http://www.planejamento.gov.br/secretarias/upload/Arquivos/segep/projeto/2013_03_01_Produto_VII_Risco_Oportunidade_PT.pdf>. Acesso em: março 2020.

HUBBARD, Douglas W. The Failure of Risk Management: **Why It's Broken and How to Fix It**. New Jersey (EUA): John Wiley & Sons, Inc., 2009. Disponível em: <http://www.amazon. com/Failure-Risk-Management-Why-Broken/dp/0470387955>. Acesso em: maio, 2020.

IBGC - Instituto Brasileiro De Governança Corporativa. **Guia de Orientação para Gerenciamento de Riscos Corporativos** (2017). Disponível em: < http://www.ibgc.org.br/userfiles/3.pdf>. Acessado em: outrubro, 2019.

ISACA - Information Systems Audit and Control Association - **Enabling Processess, COBIT 5,** ISACA (2012).

ISLAM, S., MOURATIDIS, H., WEIPPL, E.R.: **A Goal-Driven Risk Management Approach to Support Security and Privacy Analysis of Cloud-Based System**. Security Engineering for Cloud Computing: Approaches and

PUC-Rio - Certificação Digital Nº 1721463/CA

Tools. 97–122 (2013). https://doi.org/10.4018/978-1-4666-2125-1.ch006.

KNIGHT, K. **Risk Management: an integral component of corporate governance and good management**. ISO Bulletin, p.21-24, Out. 2003.

LAPOUCHNIAN, A. **Goal-oriented requirements engineering: An overview of the current research.** (2005). University of Toronto.

LEITE, J. C. S. P. **Política versus Procedimento**, 2013. Disponível em: <http://sisdinf.blogspot.com/2013/01/politica-versus-procedimento.html>. Acesso em: 23 dezembro. 2020

LEITE, J. C. S. P. **Livro Vivo: Engenharia de Requisitos: A Necessidade da Elicitação**, 2007. Disponível em: <http://livrodeengenhariaderequisitos.blogspot.com/2007/09/necessidade-da-elicitao.html>. Acesso em: 19 maio. 2019

LIU, L.; YU, E. **Designing information systems in social context: a goal and scenario modelling approach.** (2004) Information Systems 29, 187–203.

LOPEZ, A., NICOLAS, J., TOVAL, A.: **Risks and Safeguards for the Requirements Engineering Process in Global Software Development**. In: 2009 Fourth IEEE International Conference on Global Software Engineering. pp. 394–399 (2009). https://doi.org/10.1109/ICGSE.2009.62.

MARTÍNEZ, M.C.P. A., GUTIÉRREZ, J.F., CUESTA, L.L., MORANDINI, M., SUSI, A.: **Using i* to represent OSS ecosystems for risk assessment**. Presented at the Proceedings of the 6th International i* Workshop 2013: Valencia, Spain, June 17- 18, 2013 (2013).

Mellor, S. J., Balcer, M., Jacoboson, I.: **Executable UML: A Foundation for Model-Driven Architectures**. Addison-Wesley Longman Publishing Boston (2002)

MENKEN, I., BLOKDIJK, G.: **ITIL Foundation Complete Certification Kit** - Fourth Edition: Study Guide Book and Online Course. Emereo (2011).

OPENOME. **OpenOME, an open-source requirements engineering tool**. Disponível em: https://se.cs.toronto.edu/trac/ome/. Acesso em 23 dez. 2020.

ORANGE BOOK: Treasury, G.B.: **Management of Risk- Principles and Concepts**. Stationery Office (2004).

RESOLUÇÃO 510 - (2016) Disponível em: <http://conselho.saude.gov.br/resolucoes/2016/Reso510.pdf>. Acesso em: 05 ago. 2020.

SILVA, M. M., PEREIRA, R.; **IT Governance Implementation: The Determinant Factors**, 2012.

Silver, B.: **BPMN Method and Style: A levels-based methodology for BPM pro- cess modeling and improvement using BPMN 2.0**. Cody-Cassidy Press (2009)

PUC-Rio - Certificação Digital Nº 1721463/CA

SOUSA, H.P., DO PRADO LEITE, J.C.S.: **Modeling organizational alignment**. In Yu, E., Dobbie, G., M., Purao, S (eds) ER 2014. LNCS, 407-414. Springer, Heidelberg (2014)

TCU-SEPLAN - **Referencial básico de governança aplicável a órgãos e entidades da administração pública**. Versão 2. Brasília: TCU, Secretaria de Planejamento, Governança e Gestão (Seplan), 2014. Disponível em: <http:// www.tcu.gov.br>. Acesso em: março, 2020.

THE ORANGE BOOK - HM Treasury. **Management of Risk - Principles and Concepts** - HM Treasury do HM Government, 2004.

BEASLEY, M; BRANSON, B; HANCOCK, B.: The State of Rsik Oversight: **An Overview of Enterprise Risk Management Practices - ERM - Enterprise Risk Management Initiative** (2019) | North Carolina State Poole College of Management, https://erm.ncsu.edu/az/erm/i/chan/library/2019_Current_Report_on_State_of_ Risk_Oversight.pdf, last accessed 2019/11/28.

USA - House of Representatives of the United States of America in Congress. **Sarbanes-Oxley Act of 2002**. Corporate responsibility. Disponível em: <http://www.gpo. gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW- - 107publ204.pdf>. Acesso em: novembro, 2019.

VAN LAMSWEERDE, A. (2001). **Goal-oriented requirements engineering: A guided tour.** In Requirements Engineering, 2001. Proceedings. Fifth IEEE International Symposium on (pp. 249-262). IEEE.

VAN LAMSWEERDE, A. **Requirements engineering in the year 00: a research perspective**. (2000). In: The Proceedings of the 22nd International Conference on Software Engineering, Limerick, June 2000, ACM press, New York.

YU, E. **Modelling Strategic Relationships for Process Reengineering.** (1995) Ph.D. thesis, also Tech. Report DKBS-TR-94-6, Dept. of Computer Science, University of Toronto, 1995.

YU, E.; MYLOPOULOS, J. **Why goal-oriented requirements engineering**. (1998). In Proceedings of the Fourth International Workshop on Requirements Engineering: Foundations of Software Quality, Pisa, Italy, Presses Universitaires de Namur, Paris, June 1998, pp. 15–22.

YU, E.S.K., GIORGINI, P., MAIDEN, N., MYLOPOULOS, J.: **Social Modeling for Requirements Engineering**. MIT Press (2011).

YU, Y., MYLOPOULOS, J., LEITE, J.C.S.P., LIU, L., D'HOLLANDER, E.H.: **Software refactoring guided by multiple soft-goals**. Presented at the 1st workshop on Refactoring: Achievements, Challenges, and Effects (REFACE'03) , Victoria, Canada (2003).

PUC-Rio - Certificação Digital Nº 1721463/CA

Apêndice

Apêndice I. Avaliação aplicada

Analisar a estratégia de modelagem de gestão de risco com uso de linguagem intencional para atender à necessidade de representar a complexidade de informações as quais os ambientes de negocio estão exposotos. Os objetivos para a estratégia de modelagem são:

a) Separar as responsabilidades entre a área de compliance, as áreas de tecnologia da informação, a área de negócios e a alta administração empresarial;

b) Certificar-se que as decisões estratégicas sejam tomadas com base na transparência organização.

Motivação:

Organizações de qualquer tipo ou tamanho estão expostas a fatores internos e externos que tornam incerto o atingimento de seus objetivos. Em função disso, é necessário que essas entidades tomem uma série de medidas com a finalidade de responder da melhor maneira às possíveis incertezas que se apresentam e que colocam em risco a continuidade do negócio.

Dados de caraterização

Questionário 1 para colher o perfil dos respondentes da pesquisa de avaliação da modelagem e Questionário 2 para que o respondente avalie a modelagem sugerida:

PUC-Rio - Certificação Digital Nº 1721463/CA

Questionário 1: Perfil do participante

Nome:
Escolaridade: ( ) graduação ( ) mestrado ( ) doutorado
Status: ( ) cursando ( ) completo
Profissão:
01 – Há quanto tempo você atua em área relacionada a Engenharia/Tecnologia da Informação?
( ) Menos de 1 ano
( ) Entre 1 e 3 anos
( ) Entre 3 e 10 anos
( ) Acima de 10 anos
02 – Qual sua área de atuação de maior especialidade?
( ) Engenharia de Requisitos
( ) Arquiteto de Tecnologia da Informação
( ) Gestão de Riscos
03 – Qual a receita anual da empresa de maior relevância que você já trabalhou (no mínimo 2 anos)?
( ) Menos de $10 milhões
( ) Entre $10 milhões e $100 milhões
( ) Entre $100 milhões e $1 bilhão
( ) Mais de $1 bilhão
04 – Qual método de modelagem de processos você possui maior especialidade?
( ) BPMN
( ) UML
( ) iStar
( ) Outro (Qual:_____)

PUC-Rio - Certificação Digital Nº 1721463/CA

Questionário 2: Avaliação da modelagem

1.	De modo geral, é possível visualizar os riscos de TI por meio da modelagem apresentada...	Discordo (1) (2) (3) (4) (5) Concordo
2.	A modelagem facilita a visualização da separação as responsabilidades entre a área de conformidade, gerentes de TI e executivos...	Discordo (1) (2) (3) (4) (5) Concordo
3.	A modelagem facilita a visualização da transparecia das informações para tomada de decisões...	Discordo (1) (2) (3) (4) (5) Concordo
4.	A modelagem pode ajudar no trabalho rotineiro de engenheiros de requisitos, arquitetos de TI e gestores de riscos...	Discordo (1) (2) (3) (4) (5) Concordo
5.	Considerando um determinado risco, a modelagem possibilita uma melhor percepção dos fatores associados a este risco?	Discordo (1) (2) (3) (4) (5) Concordo
6.	Indique fatores positivos que encontrou na modelagem.	
7.	Indique fatores negativos que encontrou na modelagem.	
8.	Indique a prática de seu conhecimento/uso e compare-a com o que foi apresentado?	

PUC-Rio - Certificação Digital Nº 1721463/CA

Apêndice II. Contextualização do método para modelagem

O presente documento contempla a contextualização sobre a da linguagem i-estrela, o processo de construção da modelagem e por fim a analise dos riscos a partir da modelagem.

QUESTIONARIO SOBRE A MODELAGEM INTENCIONAL DE TI PARA COMPREENSÃO DE RISCOS

1. INTRODUÇÃO 57

2. CONCEITOS PARA MODELAGEM 57

3. MODELAGEM 61

4. ABORDAGEM DO QUESTIONÁRIO 64

PUC-Rio - Certificação Digital Nº 1721463/CA

1. Introdução

Este documento tem por objetivo: a) explicar os conceitos referentes a modelagem dos processos organizacionais para identificação de riscos no contexto da tecnologia da informação; b) exibir as modelagens (SD e NFR) para entendimento dos riscos mencionados e posterior respostas ao questionário quantitativo.

2. Conceitos para Modelagem

Abordagem orientada a meta

As abordagens de engenharia de requisitos orientadas a meta têm aumentado nos últimos anos. Sua modelagem teve origem de forma mais bem-conceituada no fim da década de 90.

A abordagem orientada a meta captura o motivo e as funções dos dados estarem presentes no software, e se são suficientes para atingir os objetivos de alto nível que surgem naturalmente no processo de engenharia de requisitos (propósito mais preciso, justificar os requisitos de software).

A modelagem baseada na análise mais tradicional foca em quais características (ex. atividades e entidades) um sistema irá suportar.

Modelagem i*

A motivação de utilizar o framework i* (i-estrela) para modelagem de requisitos (Yu, 1995) deve-se em função de sua aderência em modelagens orientadas a meta.

O framework i-estrela contém algumas modelagens que permitem um melhor entendimento das informações mapeadas:

Modelo SD: modelo de representação que possui um conjunto de nós (atores) dependentes entre si. Essas dependências são criadas para que uma determinada meta seja satisfeita, um recurso seja concedido, uma tarefa seja realizada ou uma meta-flexível seja satisfeita a contento. Há quatro possíveis tipos de dependências entre atores. Essas dependências podem ser por:

– Meta: quando um ator depende de outro para que determinado objetivo seja alcançado.
– Tarefa: quando um ator depende de outro para que este outro execute uma tarefa.
– Recurso: quando um ator depende de outro para que um objeto seja concedido.
– Meta-flexível: quando um ator depende de outro para que este desempenhe alguma tarefa. Esta ligação servirá de base para que uma meta flexível seja satisfeita de forma adimissível, considerando as partes interessadas no modelo elaborado.

Catálogo de processos, atores e dependências

O Catalogo base para a estrutura de processos de uma área de TI seguiu os frameworks Cobit 5, Itil 4 e Pmbok 6, essencialmente o primeiro.

A partir da literatura, em particular a partir do COBIT5, ITIL4 e PMBOK6. A partir dos conhecimentos utilizados para a elicitação de requisitos, será proposto o diagrama SD ilustrando as dependências neste contexto.

PUC-Rio - Certificação Digital Nº 1721463/CA

Macroprocessos para gestão de TI

1 – Alinhar a TI ao negócio
1.1 - Gerenciar a estratégia e o plenejamento de TI
Desenvolver estratégias de TI
Desenvolver planejamento de TI
1.2 - Gerenciar o desempenho da TI
Monitorar o desempenho financeiro
Gerenciar o desempenho dos processos de TI
Gerenciar o desempenho operacional de TI
1.3 - Alinhar arquitetura de TI ao negócio
Desenvolver arquitetura de TI
Prospectar novas tecnologias de TI
Padronizar tecnologias existentes
1.4 - Gerenciar a prestação de serviços aos clientes
Gerir os recursos de ambientes informatizados
Gerenciar o catálogo de serviços de TI
Gerenciar o portfólio de serviços de TI
5 - Fornecer inovação através de processos e tecnologia

- Gerenciar o relacionamento com as áreas de clientes
1 - Avaliar novas soluções de TI
Estruturar o planejamento das ideias de TI
Identificar benefícios e requisitos de TI das ideias
Identificar necessidade das soluções de TI
Consolidar soluções propostas
2 – Gerenciar o portfólio de TI
Identificar projetos de TI
Priorizar os projetos de TI
Controlar os projetos de TI
2.3 – Monitorar os serviços de TI
Desenvolver relatórios e indicadores de serviços
Controlar os serviço de TI
Realizar reuniões de acompanhamento com clientes
Avaliar mudanças em projetos
Avaliar pós implantação dos projetos
2.4 - Executar consultoria de serviços de TI
Aprofundar as relações com os clientes
Prospectar soluções de clientes
Executar consultoria a serviços solicitados
2.5 - Gerenciar modelo de informação de TI

3 – Implementar as soluções de TI
3.1 - Desenvolver protótipo de projetos
Desenvolver estrutura de soluções de TI

4 – Sustentar os serviços de TI
4.1 – Controlar solicitações de ativos e incidentes
Tratar eventos e solicitações de TI
Tratar incidentes
Controlar ativos de TI
4.2 - Gerenciar a qualidade na passagem para a produção
Documentação mudança de infra-estrutura
Controlar documentação de requisitos de sistemas
Gerir integridade e disponibilidade dos sistemas
Manter catálogo de aplicações
4.3 – Controlar ambientes e produtos de TI
Controlar a disponibilidade de ambientes de TI
Gerenciar mudanças nas configurações de TI e infra-estrutura
Gerenciar a continuidade dos serviços de TI
Executar serviços de TI
4.4 - Manter sistemas e ambientes de TI
Prover correção e manutenção de aplicações
Garantir a manutenção preventiva de ambientes de produção
Executar gestão de ambientes em produção
Preparar documento de manutenção para novos sistemas

5 - Apoiar a organização de TI
5.1 - Gerenciar a segurança, risco e conformidade
Gerenciar as políticas, normas e padrões de segurança da informação
Gerenciar arquitetura tecnológica de segurança da informação
Gerenciar os riscos de TI
Gerenciar conformidades de TI
Gerenciar perfis de acesso e identidade em TI
5.2 - Gerenciar fornecedores e contratos de TI
Gerenciar contratações e aquisições
Gerenciar relacionamentos com fornecedores
Realizar pequenas contratações
5.3 - Gerenciar a administração e orçamento de TI
Gerenciar a administração de TI
Gerir o orçamento de TI
Verificar pagamentos e contratos de TI
Gerir os recursos humanos e conhecimento de TI
Gerenciar satisfaçãos de empregados em TI
Gerir e desenvolver funcionários de TI
Gerenciar conhecimento de TI
5.4 – Suportar comunicação de TI
Gerir a mudança em ambientes de TI
Gerir a comunicação interna e externa

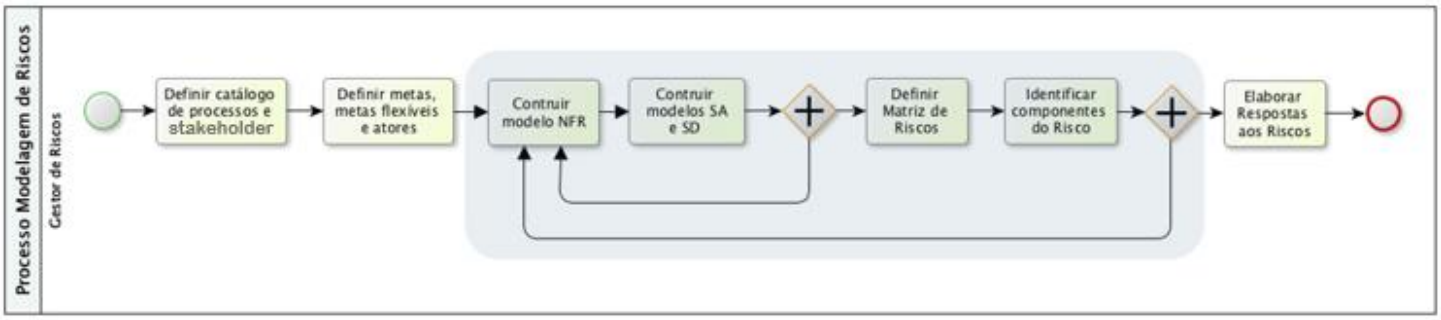
PUC-Rio - Certificação Digital Nº 1721463/CA

Reunir informações, processos e requisitos
Prototipar sistemas de informação
3.2 - Implementar soluções de software
Realizar análise e projeto de soluções de software
Desenvolver soluções de software
Testar e aprovar aplicações de TI
Prospectar ferramentas pre-existentes de software
3.3 - Implementar soluções de infraestrutura
Realizar análise e projeto de soluções de infra
Desenvolver soluções de infra
Testar e aprovar sokuções de infra
3.4 - Gerenciar métodos e documentação
Gerenciar documentação padrãode ambiente
Gerenciar recursos e ferramentas
Gerenciar métodos para desenvolvimento e manutenção

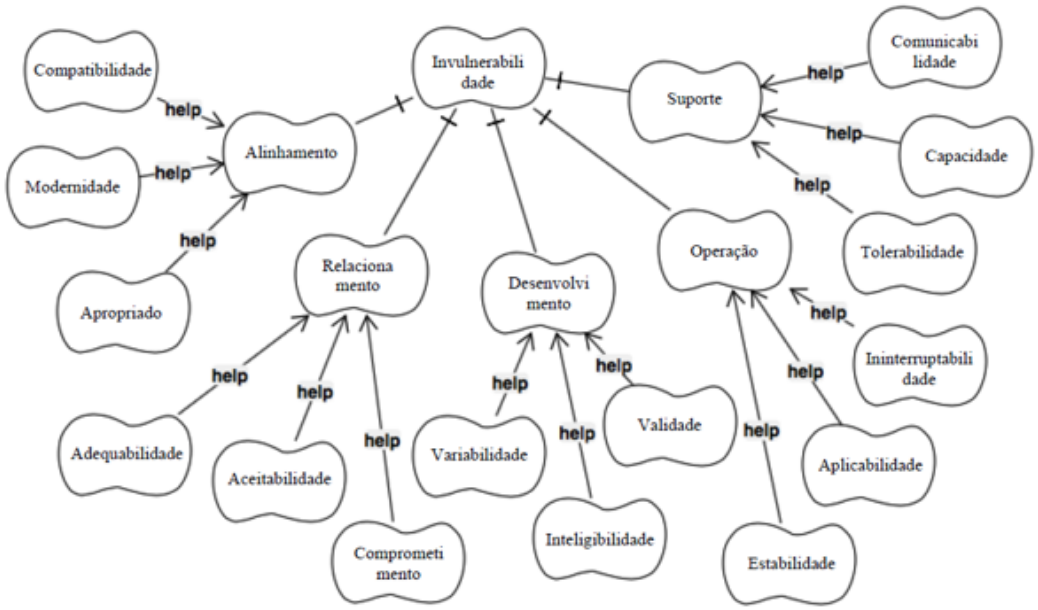
PUC-Rio - Certificação Digital Nº 1721463/CA

3. Modelagem

Como demonstração de seu uso será proposto um diagrama SD e um catalogo de metas não funcionais. O objetivo do modelo é representar as dependências da organização de suas tarefas, recursos, metas e objetivos (metas de qualidade, NFRs). Refletindo uma abstração de alto nível das dependências.



Para entender melhor o papel das qualidades (NFRs) no gerenciamento de riscos, usamos a estrutura NFR para ajudar a modelar o conhecimento obtido na literatura para a qualidade Invulnerability [Risk Management]. A Figura abaixo mostra também um catálogo NFR parcial para Invulnerability.

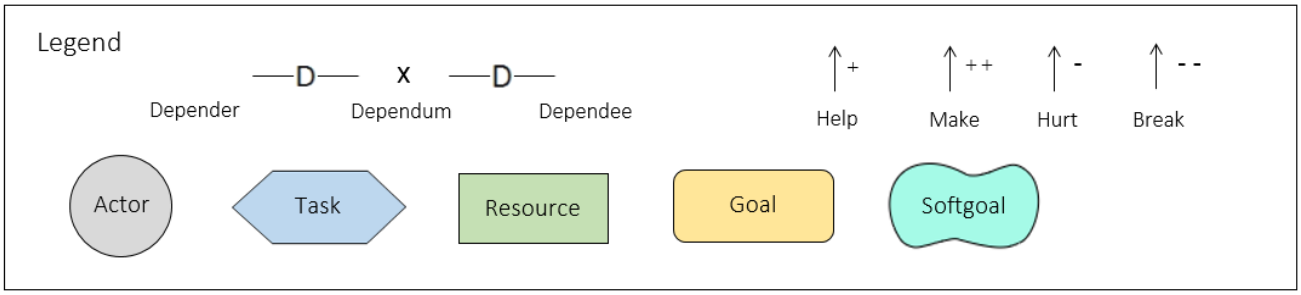


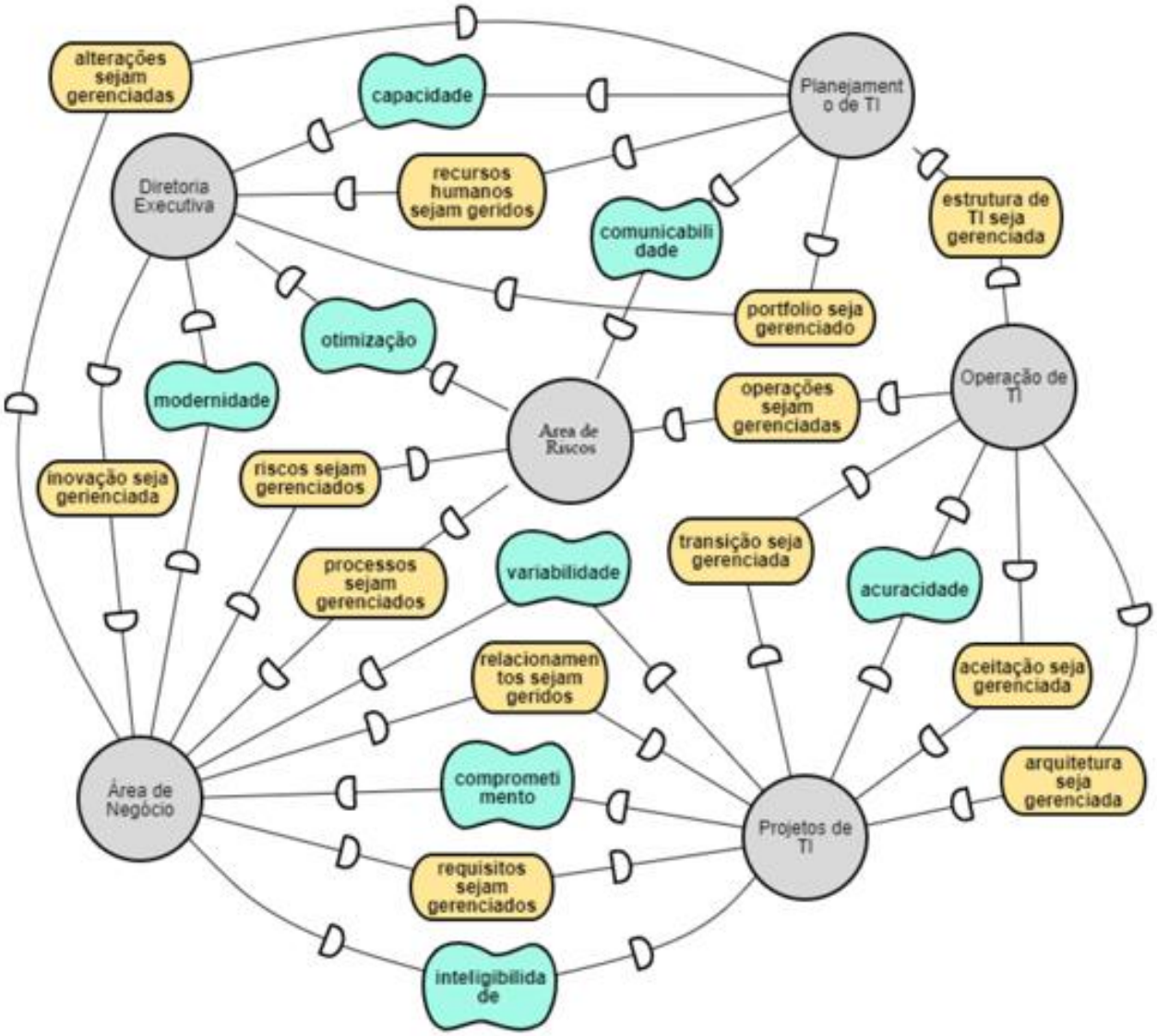
Catálogo NFR - Invulnerability

Esse modelo permite uma melhor compreensão das qualidades relacionadas ao gerenciamento de riscos, modelando os riscos e suas

PUC-Rio - Certificação Digital Nº 1721463/CA

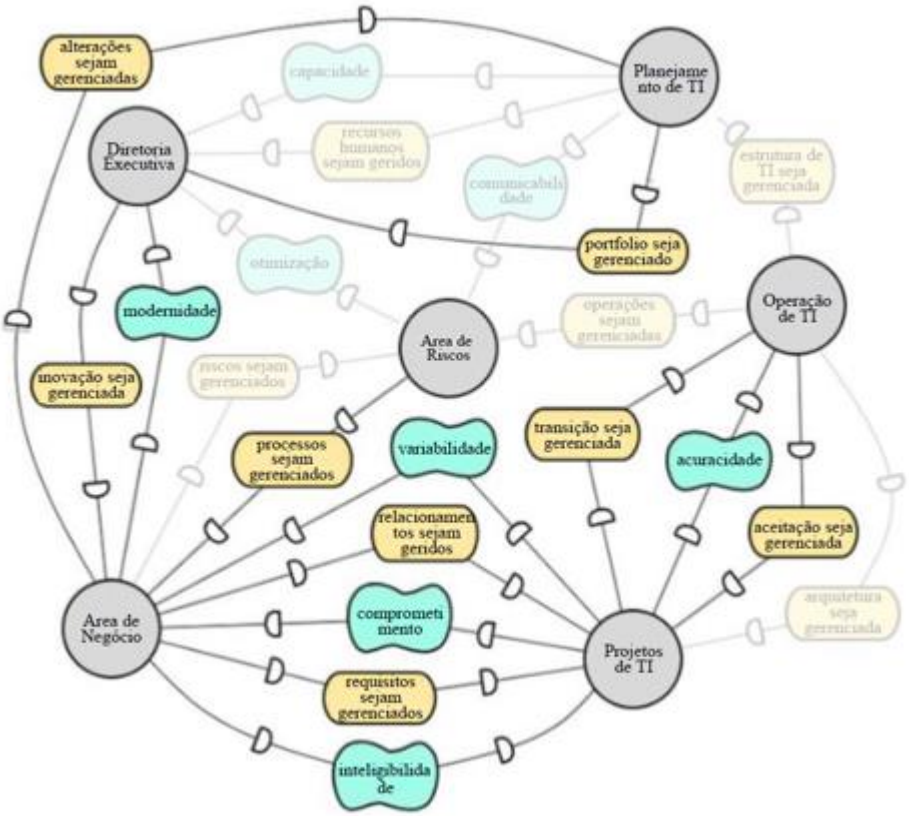
interdependências. Geralmente, as diretrizes de gerenciamento de riscos não se concentram na interação de qualidades. Dessa forma, os softgols permitem descrever como essas qualidades se afetam, bem como as tarefas (procedimentos) e os recursos da organização.

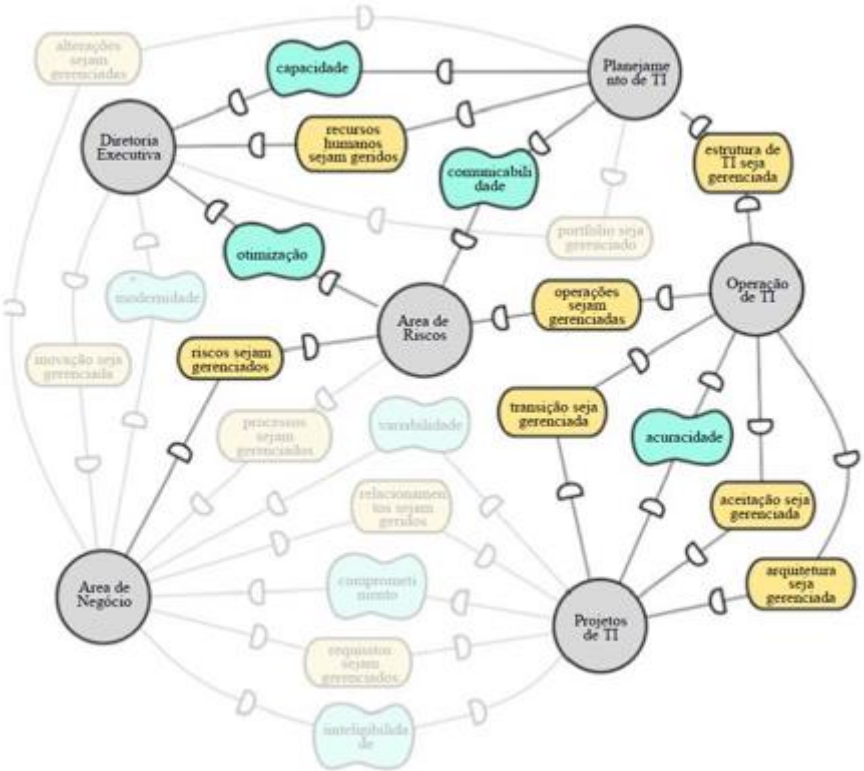




PUC-Rio - Certificação Digital Nº 1721463/CA

Risco 3 e 4, conform figuras a seguir





PUC-Rio - Certificação Digital Nº 1721463/CA

4. Etapa de respostas ao questionário

Após entendimento da modelagem por meio desta documentação, o avaliador irá responder aos questionários 1 e 2 em relação ao seu perfil e a percepção sobre a compreensão dos modelos criados pelo autor.

PUC-Rio - Certificação Digital Nº 1721463/CA