



Universidade Federal de Campina Grande  
Centro de Engenharia Elétrica e Informática  
Coordenação de Pós-Graduação em Ciência da Computação

Emanuel Dantas Filho

Uma Abordagem para Gerenciamento de Riscos em  
Projetos de Software baseada em Redes Bayesianas

Campina Grande - PB  
2021

Universidade Federal de Campina Grande  
Centro de Engenharia Elétrica e Informática  
Coordenação de Pós-Graduação em Ciência da Computação

# Uma Abordagem para Gerenciamento de Riscos em Projetos de Software baseada em Redes Bayesianas

Emanuel Dantas Filho

Tese submetida à Coordenação do Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Campina Grande como parte dos requisitos necessários para obtenção do grau de Doutor em Ciência da Computação.

Área de Concentração: Ciência da Computação

Linha de Pesquisa: Engenharia de Software

Hyggo Oliveira de Almeida

(Orientador)

Campina Grande, Paraíba, Brasil

©Emanuel Dantas Filho, Agosto, 2021

D192a Dantas Filho, Emanuel.  
Uma abordagem para gerenciamento de riscos em projetos de software baseada em redes bayesianas / Emanuel Dantas Filho. – Campina Grande, 2021.  
138 f. : il. color.

Tese (Doutorado em Ciência da Computação) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática, 2021.  
"Orientação: Prof. Dr. Hyggo Oliveira de Almeida".  
Referências.

1. Redes Bayesianas. 2. Riscos. 3. Projetos de Software. I. Almeida, Hyggo Oliveira de. II. Título.

CDU 519.226(043)



MINISTÉRIO DA EDUCAÇÃO  
**UNIVERSIDADE FEDERAL DE CAMPINA GRANDE**  
POS-GRADUACAO CIENCIAS DA COMPUTACAO  
Rua Aprigio Veloso, 882, - Bairro Universitario, Campina Grande/PB, CEP 58429-900

## FOLHA DE ASSINATURA PARA TESES E DISSERTAÇÕES

**EMANUEL DANTAS FILHO**

UMA ABORDAGEM PARA GERENCIAMENTO DE RISCOS EM PROJETOS DE SOFTWARE BASEADA EM REDES BAYESIANAS

Tese apresentada ao Programa de Pós-Graduação em Ciência da Computação como pré-requisito para obtenção do título de Doutor em Ciência da Computação.

Aprovada em: 06/08/2021

Prof. Dr. HYGGO OLIVEIRA DE ALMEIDA, Orientador, UFCG

Prof. Dr. DANILO FREIRE DE SOUZA SANTOS, Examinador Interno, UFCG

Prof. Dr. EVANDRO DE BARROS COSTA, Examinador Interno, UFAL

Prof. Dr. EVERTON TAVARES GUIMARÃES, Examinador Externo, PENN STATE

Prof. Dr. ANDRÉ CAVALCANTE HORA, Examinador Externo, UFMG



Documento assinado eletronicamente por **HYGGO OLIVEIRA DE ALMEIDA, PROFESSOR(A) DO MAGISTERIO SUPERIOR**, em 30/08/2021, às 11:43, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da [Portaria SEI nº 002, de 25 de outubro de 2018](#).



Documento assinado eletronicamente por **Everton Tavares Guimaraes, Usuário Externo**, em 31/08/2021, às 10:32, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da [Portaria SEI nº 002, de 25 de outubro de 2018](#).



Documento assinado eletronicamente por **Evandro de Barros Costa, Usuário Externo**, em 31/08/2021, às 10:52, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da [Portaria SEI nº 002, de 25 de outubro de 2018](#).

---



Documento assinado eletronicamente por **DANILO FREIRE DE SOUZA SANTOS, PROFESSOR(A) DO MAGISTERIO SUPERIOR**, em 31/08/2021, às 11:02, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da [Portaria SEI nº 002, de 25 de outubro de 2018](#).

---



Documento assinado eletronicamente por **Andre Cavalcante Hora, Usuário Externo**, em 08/09/2021, às 13:54, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da [Portaria SEI nº 002, de 25 de outubro de 2018](#).

---



A autenticidade deste documento pode ser conferida no site <https://sei.ufcg.edu.br/autenticidade>, informando o código verificador **1737867** e o código CRC **0D3A06C6**.

---

## Resumo

Processos para gerenciamento de riscos estão presentes nas metodologias tradicionais e ágeis. Riscos são eventos abstratos e subjetivos, o que torna o gerenciamento uma atividade complexa. Várias técnicas são utilizadas para reduzir a subjetividade e auxiliar no gerenciamento de riscos em projetos de software. As técnicas abordam a subjetividade de maneira direta ou indireta. Dentre as mais comuns estão a matriz de probabilidade e impacto, listas de verificação, *brainstorming* e métodos baseados em Inteligência Artificial. O estado da arte em gerenciamento de riscos para projetos de software envolvendo aspectos de inovação tecnológica apresentou lacunas no tratamento das abordagens investigadas. Particularmente, o entendimento dos riscos em projetos de software, sua identificação e tratamento adequados devem levar em consideração as características tecnológicas de um projeto, principalmente quando aspectos de inovação estão associados. Esse é um dos desafios enfrentados pela comunidade de pesquisa e consiste em um fator crítico de sucesso em qualquer metodologia de projeto e desenvolvimento de software. Dada essa lacuna, neste trabalho propõe-se uma abordagem para gerenciamento de riscos em projetos de software baseada em Redes Bayesianas, com foco na identificação e monitoramento de riscos. O objetivo da abordagem é reduzir a subjetividade em atividades do gerenciamento de riscos utilizando fatores relacionados às características tecnológicas dos projetos. Foi realizado um estudo qualitativo com 25 profissionais de dez empresas de desenvolvimento para elicitare fatores de riscos relacionados às características tecnológicas de projetos de software. Em seguida, uma Rede Bayesiana foi construída por meio de um processo de Engenharia de Conhecimento de Redes Bayesianas. A validação teve foco em projetos de inovação. Inicialmente foi realizada uma validação estática por meio de cenários de simulação que representam casos reais de projetos de software. Em cada cenário, as ações recomendadas pela abordagem foram avaliadas por oito profissionais de uma organização de inovação tecnológica. Por fim, uma validação dinâmica foi realizada por meio de um experimento. Evidências correspondentes a dados reais de seis projetos da organização são inseridas na Rede Bayesiana e uma avaliação é realizada comparando as previsões da rede e o entendimento de profissionais dos projetos. Com base nos resultados coletados, observa-se que a abordagem proposta é capaz de auxiliar na tomada de decisão nas atividades de identificação e monitoramento de riscos.

## **Abstract**

Risk management processes are present in traditional and agile methodologies. Risks are abstract and subjective events, which makes management a complex activity. Several techniques are applied to reduce subjectivity and help manage risk in software projects. These techniques address subjectivity directly or indirectly, and among the most commons are the probability and impact matrix, checklists, brainstorming, and Artificial Intelligence-based methods. State of the art in risk management for software projects involving technological innovation presented gaps in the treatment of the investigated approaches. In particular, understanding risks in software projects, their identification, and proper treatment must consider the technological characteristics of a project, significantly when aspects of innovation are associated. This is one of the challenges faced by the research community and is a critical success factor in any software design and development methodology. Given this gap, this study proposes an approach to risk management in software projects based on Bayesian Networks, focusing on identifying and monitoring risks. The objective of the approach is to reduce subjectivity in risk management activities using factors related to the projects' technological characteristics. A qualitative study was carried out with 25 professionals from ten development companies to elicit risk factors associated with the technological characteristics of software projects. Then, through a Knowledge Engineering process, a Bayesian Network was built. The validation focused on innovation projects. Initially, through simulation scenarios that represent real cases of software projects, a static validation was performed. In each scenario, eight professionals from a technological innovation organization evaluated the actions recommended by the approach. Finally, through an experiment, a dynamic validation was performed. Evidence corresponding to real-world data from six of the organization's projects was used as input to the Bayesian Network to assess the network's predictions and the understanding of the project professionals. Based on the results, the proposed approach can assist in decision-making in identifying and monitoring risks.

## **Agradecimentos**

Agradeço a Deus por me dar saúde e paz para conseguir vencer os desafios que surgem em meu caminho.

A minha família por estarem sempre ao meu lado fornecendo todo o apoio e incentivo necessários.

Ao meu orientador, Hyggo Oliveira de Almeida, que foi de fundamental importância para a concretização desse trabalho e de vários outros ao longo dos últimos anos.

Aos amigos do grupo de pesquisa que estiverem sempre dispostos a auxiliar durante a jornada da pós-graduação.

Ao Instituto Federal da Paraíba pela licença autorizada das minhas atividades docentes, o que me proporcionou tranquilidade para realização dessa pós-graduação.

A todos que contribuíram direta ou indiretamente para a conclusão deste trabalho.



# Conteúdo

<b>1</b>	<b>Introdução</b>	<b>1</b>
1.1	Problemática . . . . .	3
1.2	Objetivos . . . . .	6
1.3	Metodologia . . . . .	7
1.4	Relevância . . . . .	11
1.5	Sumário das contribuições . . . . .	12
1.6	Estrutura do Documento . . . . .	12
<b>2</b>	<b>Fundamentação Teórica</b>	<b>14</b>
2.1	Gerenciamento de Riscos . . . . .	14
2.2	Redes Bayesianas . . . . .	17
<b>3</b>	<b>Trabalhos Relacionados</b>	<b>21</b>
3.1	Abordagens para Gerenciamento de Riscos . . . . .	21
3.2	Redes Bayesianas para Gerenciamento de Riscos . . . . .	24
3.3	Considerações Finais do Capítulo . . . . .	26
<b>4</b>	<b>Estudo Qualitativo</b>	<b>29</b>
4.1	Coleta dos Dados . . . . .	29
4.1.1	Seleção dos Participantes . . . . .	30
4.1.2	Evolução das Entrevistas . . . . .	31
4.2	Análise dos Dados . . . . .	32
4.2.1	Codificação Aberta . . . . .	33
4.2.2	Codificação Axial . . . . .	34
4.2.3	Codificação Seletiva . . . . .	35

4.2.4	Teoria . . . . .	36
4.2.5	Ameaças à Validade . . . . .	38
<b>5</b>	<b>Abordagem Proposta</b>	<b>39</b>
5.1	Motivações para escolha de Redes Bayesianas . . . . .	39
5.2	Estrutura da Rede Bayesiana . . . . .	40
5.3	Processo Proposto . . . . .	47
5.4	Ferramenta Risk Control . . . . .	49
5.5	Considerações Finais do Capítulo . . . . .	55
<b>6</b>	<b>Validação da abordagem</b>	<b>57</b>
6.1	Modelagem da Rede Bayesiana . . . . .	57
6.1.1	Execução do Processo . . . . .	58
6.1.2	Ameaças à Validade . . . . .	60
6.2	Validação Estática . . . . .	61
6.2.1	Descrição dos Cenários . . . . .	61
6.2.2	Avaliação da abordagem . . . . .	69
6.2.3	Ameaças à Validade . . . . .	73
6.3	Validação Dinâmica . . . . .	73
6.3.1	Overview do Experimento . . . . .	74
6.3.2	Avaliação da abordagem . . . . .	75
6.3.3	Ameaças à validade . . . . .	82
<b>7</b>	<b>Considerações Finais</b>	<b>84</b>
7.1	Contribuições . . . . .	85
7.2	Trabalhos Futuros . . . . .	87
<b>A</b>	<b>Roteiro da Entrevista - Grounded Theory</b>	<b>103</b>
<b>B</b>	<b>Lista dos Códigos - Grounded Theory</b>	<b>105</b>
<b>C</b>	<b>Descrição dos Nós - Fragmento Núcleo</b>	<b>107</b>
<b>D</b>	<b>Listagem - Tecnologias</b>	<b>109</b>

<b>E</b>	<b>Listagem - Riscos</b>	<b>111</b>
<b>F</b>	<b>Listagem - Estratégias</b>	<b>113</b>
<b>G</b>	<b>Rede Bayesiana</b>	<b>115</b>
<b>H</b>	<b>Validação - Lista de riscos RB</b>	<b>119</b>
<b>I</b>	<b>Validação - Lista de Estratégias RB</b>	<b>120</b>
<b>J</b>	<b>Manual do Usuário - Risk Control</b>	<b>121</b>
J.1	Visão Geral do Sistema . . . . .	121
J.2	Perfil Administrador . . . . .	121
J.2.1	Login . . . . .	121
J.2.2	Criação de Domínios e Tecnologias . . . . .	122
J.2.3	Editar e remover Tecnologias . . . . .	123
J.2.4	Listagem de Riscos . . . . .	123
J.2.5	Cadastro de Riscos . . . . .	123
J.2.6	Associar Tecnologias aos Riscos . . . . .	124
J.2.7	Ponderar as Tecnologias . . . . .	125
J.2.8	Cadastrar Estratégias . . . . .	126
J.3	Perfil Usuário Comum . . . . .	127
J.3.1	Listagem Projetos . . . . .	127
J.3.2	Cadastrar Projetos . . . . .	127
J.3.3	Cadastrar Tecnologias . . . . .	128
J.3.4	Visualizar Riscos e Dashboard . . . . .	129
<b>K</b>	<b>Manual do Desenvolvedor - Risk Control</b>	<b>130</b>
K.1	Frontend . . . . .	130
K.1.1	Visão geral . . . . .	130
K.1.2	Estrutura . . . . .	130
K.1.3	Dependências . . . . .	131
K.1.4	Services . . . . .	132
K.1.5	Módulo Shared . . . . .	134

---

K.1.6	Módulo Funcionalidades . . . . .	135
K.2	Backend . . . . .	135
K.2.1	Visão Geral . . . . .	135
K.2.2	Dependências . . . . .	135
K.2.3	Estrutura . . . . .	136
K.2.4	Módulo RiskControl-Api . . . . .	137
K.2.5	Modelo de Dados . . . . .	138

# Lista de Símbolos

API - *Application Programming Interface*

CIO - *Chief Information Officer*

DAS - *Desenvolvimento Ágil de Software*

DAO - *Data Access Object*

DDD - *Domain Driven Design*

DTO - *Data Transfer Object*

GAD - *Grafo Acíclico Direcionado*

GT - *Grounded Theory*

GUI - *Graphical User Interface*

IDE - *Ambiente de Desenvolvimento Integrado*

IE - *Instituição de Ensino*

IOT - *Internet Of Things*

ISE - *Intelligent Software Engineering*

JSON - *JavaScript Object Notation*

KEBN - *Engenharia de Conhecimento de Rede Bayesiana*

KLOC - *Kilo Lines of Code*

NPD - *Desenvolvimento de Novos Produtos*

P&D - *Projetos de Pesquisa e Desenvolvimento*

PMBOK - *Project Management Body of Knowledge*

PO - *Product Owner*

RN - *Rede Neural*

RB - *Rede Bayesiana*

SWOT - *Strengths, Weaknesses, Opportunities and Threats*

SOA - *Service-Oriented Architecture*

TAM - *Modelo de Aceitação de Tecnologia*

TPN - *Tabela de Probabilidade dos Nós*

UFCG - *Universidade Federal de Campina Grande*

VIRTUS - *Núcleo de Pesquisa, Desenvolvimento e Inovação em Tecnologia da Informação, Comunicação e Automação*

# Lista de Figuras

1.1	Etapas da pesquisa . . . . .	8
2.1	Processos de Gerenciamento de Riscos segundo PMBOK 6ª Edição [89] . .	15
2.2	Diagrama do processo de gestão de riscos da norma ISO 31000 [90] . . . .	16
2.3	Tipos de raciocínio em Redes Bayesianas [66] . . . . .	18
2.4	Exemplo de Rede Bayesiana . . . . .	19
4.1	Transcrição das entrevistas . . . . .	33
4.2	Primeiros códigos identificados . . . . .	34
4.3	Codificação Seletiva para categoria “Produto”. . . . .	36
4.4	Teoria sobre fatores de riscos em projetos de software. . . . .	37
5.1	Fragmento Núcleo da RB . . . . .	41
5.2	Conexão dos fragmentos da Rede Bayesiana . . . . .	42
5.3	Exemplo de nó risco sensível ao contexto conectado ao fragmento Núcleo .	44
5.4	Exemplo de nós tecnologias conectadas a um risco sensível ao contexto . .	44
5.5	Exemplo de nó estratégia conectado a um risco sensível ao contexto . . . .	45
5.6	Exemplo de nó risco sensível ao contexto conectado ao fragmento Núcleo .	45
5.7	Exemplo de nós tecnologias conectadas a um risco sensível ao contexto . .	46
5.8	Exemplo de nó estratégia conectado a um risco sensível ao contexto . . . .	46
5.9	Processo para adaptação e modelagem da Rede Bayesiana. . . . .	47
5.10	Arquitetura da ferramenta Risk Control. . . . .	50
5.11	Modelo de Dados da ferramenta Risk Control. . . . .	51
5.12	Criação de Domínios e Tecnologias. . . . .	52
5.13	Cadastro de Riscos. . . . .	53

---

5.14	Definição de probabilidades para as tecnologias. . . . .	53
5.15	Cadastrar Projetos. . . . .	54
5.16	Associar tecnologias ao projeto . . . . .	54
5.17	Visualização de Riscos . . . . .	55
6.1	Perspectiva da Rede Bayesiana - Cenário 01 . . . . .	63
6.2	Perspectiva da Rede Bayesiana - Cenário 02 . . . . .	64
6.3	Perspectiva da Rede Bayesiana - Cenário 03 . . . . .	65
6.4	Perspectiva da Rede Bayesiana - Cenário 04 . . . . .	67
6.5	Perspectiva da Rede Bayesiana - Cenário 05 . . . . .	68
6.6	Perspectiva da Rede Bayesiana - Cenário 06 . . . . .	69
6.7	Valores de precisão calculados por perfil profissional . . . . .	78
G.1	Sub-rede Integração . . . . .	115
G.2	Sub-rede Ambiente . . . . .	116
G.3	Sub-rede Método . . . . .	117
G.4	Sub-rede Arquitetura . . . . .	118
J.1	Login da ferramenta Risk Control. . . . .	122
J.2	Criação de Domínios e Tecnologias. . . . .	122
J.3	Editar e remover Tecnologias. . . . .	123
J.4	Listagem de Riscos. . . . .	124
J.5	Cadastro de Riscos. . . . .	124
J.6	Associar Tecnologias aos Riscos. . . . .	125
J.7	Ponderar as tecnologias. . . . .	125
J.8	Risco a ser inserido no sistema. . . . .	126
J.9	Cadastrar Estratégias. . . . .	126
J.10	Listagem Projetos. . . . .	127
J.11	Cadastrar Projetos. . . . .	128
J.12	Cadastrar Tecnologias. . . . .	128
J.13	Lista de Riscos e Dashboard. . . . .	129
K.1	Estrutura Frontend . . . . .	131



---

K.2	Módulo Shared . . . . .	134
K.3	Módulo Funcionalidades . . . . .	135
K.4	Estrutura . . . . .	136
K.5	RiskControl-Api . . . . .	137
K.6	Modelo de Dados . . . . .	138

# Lista de Tabelas

3.1	Abordagens para Gerenciamento de Riscos . . . . .	22
3.2	Características das abordagens . . . . .	23
3.3	Redes Bayesianas para Gerenciamento de Riscos . . . . .	24
3.4	Fatores de Risco . . . . .	25
4.1	Informações dos participantes no estudo GT. . . . .	30
4.2	Artefatos de projetos analisados na Fase Preliminar . . . . .	31
4.3	Códigos relacionado ao Axioma Integração . . . . .	34
4.4	Códigos relacionado à Categoria Inovação de Produto . . . . .	35
5.1	Descrições dos nós folha do Fragmento Núcleo. . . . .	43
5.2	Atividade 01 - Elicitação de Conhecimento . . . . .	48
5.3	Atividade 02 - Mapeamento de Nós . . . . .	48
5.4	Atividade 03 - Simulações de Casos Reais . . . . .	49
6.1	Variáveis para avaliação da abordagem proposta . . . . .	70
6.2	Resultados do questionário . . . . .	71
6.3	Respostas do questionário sobre as tecnologias dos projetos . . . . .	76
6.4	Resultado da análise estatística - Identificação de riscos . . . . .	77
6.5	Resultado da análise estatística - Mensuração de riscos . . . . .	79
6.6	Resultado da análise estatística - Monitoramento de riscos . . . . .	81
H.1	Riscos de maior probabilidade calculados pela Rede Bayesiana . . . . .	119
I.1	Estratégias recomendadas pela Rede Bayesiana . . . . .	120

# Capítulo 1

## Introdução

Na indústria de software, os processos para gerenciamento de riscos estão presentes em projetos que utilizam tanto metodologias tradicionais quanto ágeis [85]. Um risco é um evento ou uma condição incerta que, se ocorrer, tem efeito em pelo menos um objetivo do projeto [10]. O efeito pode ser positivo (oportunidade) ou negativo (ameaça) [89].

O guia PMBOK (*Project Management Body of Knowledge*) define sete processos para o gerenciamento de riscos [89], com atividades do planejamento ao monitoramento dos riscos. Por outro lado, a norma ISO 31000 apresenta princípios e recomendações em cinco atividades que abordam riscos [54]. Neste trabalho seguimos o entendimento de Kerzner [61], tratando o gerenciamento de riscos em três atividades principais: identificar, mensurar e monitorar os riscos.

O objetivo do processo de identificação é detectar os eventos que podem afetar o projeto [12]. Com os riscos identificados, deve-se criar uma lista com o registro desses eventos [3] contendo uma descrição de suas características e um plano de respostas para cada risco identificado [89].

A mensuração de riscos consiste em avaliar e medir [46] os eventos previamente identificados [102]. Inicialmente uma análise qualitativa é realizada, considerando a probabilidade de ocorrência dos riscos e seus impactos nos objetivos do projeto [43]. Em seguida, busca-se quantificar numericamente os eventos para uma avaliação com maior precisão [64]. A saída do processo de mensuração consiste em uma lista com riscos priorizados de acordo com sua severidade [89].

Na etapa de monitoramento, os riscos são inspecionados periodicamente para avaliar

---

indicações de que o risco ocorreu ou está prestes a ocorrer [61]. É uma fase de controle, onde são implementadas estratégias de mitigação desses eventos [68]. O objetivo é evitar ou reduzir o impacto e assim melhorar o controle das atividades do projeto [27]. Nesta etapa também é realizada a identificação de novos riscos e avaliação da eficácia do processo durante todo o ciclo de vida do projeto [89].

Com relação às técnicas para identificação de riscos, *brainstorming* e entrevistas são as mais utilizadas na indústria [89], sendo também comum o uso de métodos gráficos. Russell e Taylor [95] modelaram diagramas de causa e efeito para detectar riscos em contextos específicos de projetos. De maneira equivalente, Sasankar *et al.* [96] definiram um modelo de processo onde riscos são identificados através de uma matriz SWOT (*Strengths, Weaknesses, Opportunities and Threats*).

Para mensuração de riscos, as principais técnicas existentes são baseadas em listas de verificação e análise da matriz de probabilidade e impacto [124]. Além disso, métodos baseados em Inteligência Artificial são encontrados na literatura em abordagens promissoras. Fenton *et al.* [33] utilizaram Redes Bayesianas para mensurar fatores de riscos e inferir densidade de defeitos do sistema. Essa também foi a linha do trabalho de Kumar *et al.* [67]. Redes Neurais foram utilizadas por Han [45] para reconhecer padrões e mensurar riscos em projetos de software.

Por fim, as principais técnicas para monitoramento de riscos são baseadas em auditorias e avaliações de qualidade inseridas periodicamente no cronograma do projeto [89]. Como trata-se de uma etapa de reavaliação, todas as técnicas de identificação descritas anteriormente também podem ser utilizadas nessa fase do processo.

Apesar de existirem técnicas amplamente conhecidas na indústria e academia, gerenciar riscos ainda é considerada uma tarefa complexa e crítica [4]. Riscos são eventos abstratos caracterizados pela subjetividade [55], pois as decisões no gerenciamento de riscos são tomadas de acordo com o ponto de vista dos profissionais [76, 77, 115]. Definir se um evento é ou não um risco, mensurar esses eventos com baixa ou alta probabilidade e avaliar se uma estratégia de mitigação precisa ser implementada são exemplos de decisões subjetivas tomadas pelos profissionais [76, 77]. De forma geral, as técnicas utilizadas na indústria e as abordagens investigadas no estado da arte buscam tornar o gerenciamento de risco mais objetivo e sistemático diminuindo a subjetividade na tomada de decisão [76].

Em um contexto específico, a subjetividade é ainda maior. Projetos de inovação possuem alto desafio tecnológico, pois comumente usam novas linguagens, *frameworks*, API's e bibliotecas para resolver problemas de negócio [11, 83, 100]. As características tecnológicas presentes em projetos de inovação aumentam a subjetividade no gerenciamento de riscos devido à falta de similaridade com produtos já desenvolvidos, à complexidade da solução e às indefinições de ambiente [15, 36, 97]. As características tecnológicas estão relacionadas, por exemplo, ao uso de novas tecnologias do projeto, integração com plataformas de desenvolvimento e restrições arquiteturais do software. Este é um cenário desafiador dada a dificuldade em prever impactos e incapacidade de antever consequências de decisões [100, 119].

É neste contexto de gerenciamento de riscos em projetos de software que se insere o presente trabalho. Mais especificamente, utilizam-se informações das características tecnológicas dos projetos para reduzir a subjetividade no processo de gerenciamento de riscos. A abordagem proposta neste trabalho pode ser aplicada a qualquer projeto de software, mas será validado em projetos de inovação onde as características tecnológicas são mais presentes.

## 1.1 Problemática

Abordar a subjetividade no gerenciamento de riscos não é algo novo. Em um trabalho pioneiro no assunto, Boehm [10] mencionou a dificuldade em tratar os riscos por ser algo relativo ao entendimento do indivíduo ou do grupo. Fairley [28] questiona que a materialização do risco é algo subjetivo e depende do entendimento dos envolvidos. Wohlin [122] afirma que é relativamente fácil coletar medidas dos atributos do projeto subjetivamente, porém é difícil identificar como esses fatores influenciam no sucesso do projeto. A subjetividade dos riscos também foi tratada nos trabalhos de Charette [13], Barki [6] e Muriana [79]. Os trabalhos descrevem abordagens com objetivo de reduzir a subjetividade criando mecanismos ou modelos para representar com maior clareza os fatores de riscos dos projetos, tornando os processos de gerenciamento de riscos mais sistemáticos [77].

Várias técnicas no gerenciamento de riscos abordam a subjetividade de forma direta ou indireta. A matriz de risco é uma técnica baseada no conhecimento de especialistas para fazer suposições dos valores de probabilidade e impacto [124]. Ao definir os dois parâmetros, a

matriz auxilia os times na mensuração dos riscos evitando que esta atividade seja puramente subjetiva. Seguindo a mesma linha, listas de verificação (*checklists*) também são utilizadas para avaliar os riscos do projeto [108]. Para diminuir a subjetividade ao avaliar riscos, os *checklists* possuem diversas questões a serem respondidas pelo time para definir e mensurar um risco. Entretanto, a matriz de riscos e os *checklists* são abordagens estáticas e de difícil manutenção [123, 125].

Existem técnicas baseadas em Redes Neurais [45, 109] que tratam o problema da subjetividade. As abordagens usam uma base de dados para encontrar correlações de variáveis e fazer previsões de indicadores do projeto. Estes indicadores são usados pelos gestores para auxiliar na tomada de decisão diminuindo a subjetividade do processo [45]. Porém, usar Redes Neurais demanda grande quantidade de dados para análise [98], uma premissa que não é viável para cenários onde os dados históricos são escassos [51, 66, 116]. Lógica Fuzzy também pode ser útil para diminuir a subjetividade de decisões do projeto na definição de indicadores de riscos [9, 77]. Porém, Fuzzy não é a melhor opção para tratar incerteza com dados incompletos [63, 116] e quando a incerteza pode ser quantificável nos dados de entrada das abordagens [5].

Muitos trabalhos no estado da arte utilizam Redes Bayesianas (RB) para apoiar o gerenciamento de riscos [33, 51, 67]. As Redes Bayesianas são modelos gráficos capazes de representar as relações de causalidade entre variáveis [29]. RB se apresentam como uma abordagem promissora para lidar com a subjetividade no gerenciamento de riscos tratando os efeitos colaterais das outras abordagens. Com Redes Bayesianas, dados históricos e opiniões de especialistas podem ser utilizados nas abordagens para quantificar indicadores de risco [87], reduzindo a necessidade massiva de dados e reduzindo o custo. Tais abordagens apresentam ao usuário uma estrutura do domínio que diminui a subjetividade no entendimento do problema [75]. Redes Bayesianas são estruturas que modelam incertezas e possuem características dinâmicas [8]. Além disso, permitem análises com respostas rápidas [113] e são uma opção de fácil manutenção. Em Redes Bayesianas não é necessário ter todas as informações das variáveis de entrada [29]. Após informar uma quantidade de informações sobre o domínio do problema, o cálculo é realizado de forma automática [8]. Por fim, uma vez construído o modelo probabilístico, a utilização das Redes Bayesianas é considerada uma prática simples [56].

Algumas abordagens usam Redes Bayesianas no gerenciamento de riscos para apoio à tomada de decisão em propósitos específicos: definição de cronograma [82]; definição do orçamento [62]; avaliação de qualidade [3]; e previsão de defeitos [67]. A pesquisa mais completa sobre o assunto é realizada por Fenton *et al.* [30, 31, 33, 34]. Em um trabalho pioneiro [30], os autores criaram uma Rede Bayesiana para gerenciamento de riscos que apoia a tomada de decisões em diversas atividades do projeto de software.

Porém, as abordagens existentes na literatura foram definidas utilizando fatores de riscos que incluem características dos requisitos, recursos humanos e processos de desenvolvimento. Tais fatores de riscos são comuns em projetos com características mais controladas, normalmente desenvolvidos em fábricas de software [18, 20, 42]. Ao tentar aplicar os modelos existentes, incluindo o de Fenton *et al.* [30], para modelar as características tecnológicas dos projetos, os modelos se mostraram muito genéricos no gerenciamento de riscos e pouco aplicáveis para modelar projetos onde as características tecnológicas são mais latentes. Por exemplo, para representar o uso de novas tecnologias de desenvolvimento, no modelo de Fenton [30], as variáveis mais próximas para traduzir esse fator de risco seriam “Linguagem” e “KLOC entregues”. Entretanto, uma nova tecnologia não necessariamente exigirá uma quantidade elevada de linhas de código. Por outro lado, um risco comum em projetos de software é a complexidade arquitetural do software. No modelo de Fenton [30] são avaliados fatores de riscos relacionados à complexidade de requisitos e precisão da especificação, mas não são avaliados riscos de requisitos em nível de restrições arquiteturais.

Como ponto de partida do trabalho aqui apresentado, foram realizadas entrevistas com profissionais participantes de projetos reais de software, mais especificamente, dentro de núcleos de inovação tecnológica. Nestes projetos, algumas características tecnológicas são comuns: uso de novos *frameworks* de desenvolvimento; integrações com plataformas emergentes; uso de técnicas inteligentes, como algoritmos de Inteligência Artificial, modelos de Aprendizagem de Máquina ou Blockchain, ainda em validação industrial. O gerenciamento de riscos nestes cenários é um desafio, pois a subjetividade de tratar estes eventos é maior. A frase de um dos entrevistados exalta bem isso: “*Existe um conjunto de riscos comum a qualquer projeto de software, que envolve principalmente mudanças de escopo, habilidades dos recursos e comunicação entre equipe e cliente. Porém, em nossos projetos temos riscos tecnológicos que são de difícil gestão, pois tratam-se de algo nunca antes desenvolvido na*

*organização, quiçá em outras empresas de desenvolvimento de software.”* (Participante 02 - Extraído do estudo qualitativo detalhado no Capítulo 4).

As características tecnológicas acima são muito comuns em projetos de inovação, projetos de Pesquisa e Desenvolvimento (P&D) e projetos para desenvolvimento de novos produtos (NPD). Na literatura, as pesquisas que investigam os riscos nestes projetos tratam principalmente de fatores relacionados ao mercado, ao ciclo de vida ou da similaridade do produto [15, 92, 97]. Algumas pesquisas vão além, investigando fatores de risco relacionados às características tecnológicas, mas simplificam a análise definindo apenas um fator de risco para tratar toda complexidade do projeto relacionado às tecnologias [11, 44, 59, 83]. Mesmo investigando diferentes fatores, a literatura se mostra escassa à apresentação dos diversos fatores de riscos relacionados às características tecnológicas dos projetos de software.

Diante do exposto, enuncia-se o problema de negócio abordado neste trabalho: *como auxiliar gestores no gerenciamento de riscos considerando as características tecnológicas dos projetos de software, reduzindo a subjetividade inerente ao processo?*

Dado o problema de negócio, enuncia-se o problema técnico específico abordado neste trabalho: *como utilizar fatores de riscos relacionados às características tecnológicas em uma Rede Bayesiana de forma a suportar a redução da subjetividade no gerenciamento de riscos em projetos de software?*

## 1.2 Objetivos

O objetivo nesta pesquisa é propor uma abordagem baseada em Redes Bayesianas para auxiliar no gerenciamento dos riscos em projetos de software, com foco na identificação e monitoramento de riscos. A abordagem se baseia em informações das características tecnológicas dos projetos para identificar e monitorar potenciais riscos, suas probabilidades e estratégias de mitigação, auxiliando na redução da subjetividade no gerenciamento dos riscos.

Além da definição da abordagem, tem-se como objetivo definir um processo sistemático com apoio ferramental para o gerenciamento de riscos. Desta forma, espera-se que seja viável aplicar a abordagem em projetos reais de software.

A validação da abordagem foi realizada em duas etapas (estática e dinâmica) com profissionais e projetos do Núcleo de Pesquisa, Desenvolvimento e Inovação em Tecnologia da



Informação, Comunicação e Automação (VIRTUS<sup>1</sup>) da Universidade Federal de Campina Grande (UFCG). O VIRTUS é um dos maiores centros de Pesquisa, Desenvolvimento e Inovação do país, com centenas de projetos de cooperação com a indústria, a maioria na área de software.

Com base no objetivo principal, os seguintes objetivos específicos foram definidos para este trabalho:

- Realizar estudo qualitativo sobre fatores de riscos relacionados às características tecnológicas em projetos de software reais com viés de inovação;
- Construir uma abordagem baseada em Redes Bayesianas para suporte ao gerenciamento de riscos, incluindo processo sistemático e apoio ferramental;
- Validar a abordagem em projetos de software reais com viés de inovação.

### 1.3 Metodologia

De acordo com o objetivo desta pesquisa, a mesma classifica-se como de proposta de solução, validação e avaliação [120]. Seguindo o ciclo de engenharia proposto em Wieringa [121], depois de entender o problema em questão, a solução proposta deve ser desenvolvida. Inicialmente, a mesma é validada internamente (i.e., simulação). Caso tenha obtido sucesso na etapa de validação, a mesma deve ser transferida para o contexto real e ter a sua interação com o mesmo avaliada (e.g, experimento).

O primeiro passo foi a definição das questões de pesquisa, as quais são descritas a seguir:

- **RQ1:** Quais são os fatores de riscos tecnológicos relevantes na construção de uma Rede Bayesiana na modelagem para auxiliar o gerenciamento de riscos em um projeto de software?
- **RQ2:** Qual a utilidade prática da Rede Bayesiana para o gerenciamento de riscos em projetos de software?
- **RQ3:** Qual a precisão das predições da Rede Bayesiana para identificação de riscos?

---

<sup>1</sup>VIRTUS: <http://virtus.ufcg.edu.br/>

- **RQ4:** A abordagem proposta consegue dar suporte à tomada de decisão, no sentido de auxiliar na definição de probabilidades para auxiliar a mensuração de riscos?
- **RQ5:** A abordagem proposta consegue dar suporte à tomada de decisão, no sentido de auxiliar os times na escolha de estratégias de mitigação para auxiliar o monitoramento de riscos?

Com base nas questões de pesquisa, a principal hipótese deste trabalho é a seguinte:

**H1.** É possível usar uma Rede Bayesiana para diminuir a subjetividade do gerenciamento de riscos utilizando fatores de riscos relacionados às características tecnológicas dos projetos de software.

Para responder às questões de pesquisa e validar a hipótese principal, as atividades para o desenvolvimento desta pesquisa são ilustradas na Figura 1.1 e detalhadas a seguir.

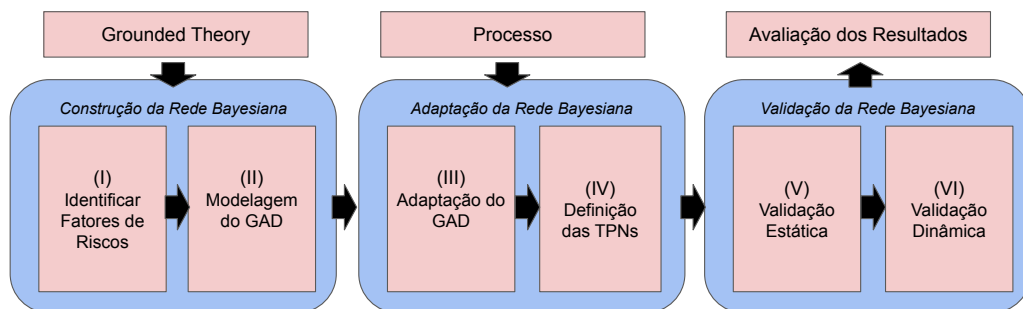


Figura 1.1: Etapas da pesquisa

Os relacionamentos das atividades ilustradas na Figura 1.1 com as questões de pesquisa são apresentadas a seguir:

- I. Identificar os principais fatores de risco relacionados às características tecnológicas de projetos de software (**RQ1**);
- II. Utilizar os fatores de risco identificados para modelar o Grafo Acíclico Dirigido (GAD) da Rede Bayesiana (**RQ1**);

- III. Adaptar o Grafo Acíclico Dirigido para o contexto de projeto alvo do estudo (**RQ1**);
- IV. Consultar especialistas para definir as Tabelas de Probabilidade dos Nós (TPN) da Rede bayesiana (**RQ1**);
- V. Realizar uma validação estática da Rede Bayesiana por meio de cenários de simulação com profissionais da área (**RQ2**);
- VI. Realizar uma validação dinâmica da Rede Bayesiana por meio de um experimento na indústria (**RQ3, RQ4 e RQ5**);

Na atividade I, para identificar os fatores de riscos foi utilizado como base o resultado de um estudo qualitativo. Este estudo foi conduzido com o método de pesquisa *Grounded Theory* (GT) [106], abordagem que tem sido muito utilizada na Engenharia de Software [48, 72, 104]. Aplicamos o GT com base em entrevistas com 25 profissionais de dez organizações que executam projetos de software. Os profissionais selecionados no estudo participam de projetos de parceria entre empresas e centros de pesquisa (ou universidades), privados ou públicos. Os projetos destas organizações fazem uso de novas tecnologias para resolver problemas de negócios. Com o estudo, foi possível identificar fatores de riscos já conhecidos em outros trabalhos da literatura [30, 51, 67] (e.g., mudança de escopo, falta de habilidades do time, falhas na execução do processo), e em especial, fatores de riscos relacionados às características tecnológicas (e.g., configuração de servidor, integração de plataformas, implementação de técnicas inteligentes, restrições arquiteturais).

Para a modelagem, validação e avaliação da Rede Bayesiana (atividades II, III, IV, V e VI), foram adotados princípios da Engenharia de Conhecimento de Rede Bayesiana (KEBN) apresentados em Mendes [74]. De acordo com o KEBN, o primeiro passo é construir o GAD, para isso é necessário identificar as variáveis, seus estados e o relacionamento entre as mesmas. Neste trabalho, o GAD da Rede Bayesiana é dividido em fragmentos. Na atividade II, os fatores de risco relacionados às características tecnológicas identificados no GT foram utilizados como variáveis para modelar o fragmento núcleo da Rede Bayesiana. O fragmento núcleo é a estrutura central e foi modelado para ser independente de contexto (i.e., uma estrutura base com os principais fatores de riscos relacionados às características tecnológicas de projetos de software).

Na atividade III, o fragmento núcleo é complementado com informações do contexto de projeto que a abordagem será aplicada. Além do fragmento núcleo, a abordagem proposta possui mais três fragmentos: tecnologias, estratégias e riscos sensíveis ao contexto. Essas informações precisam ser adicionadas ao fragmento núcleo para que a abordagem reflita a realidade de contextos específicos. O contexto pode estar relacionado ao domínio do projeto (e.g., mobile, Web e IoT); finalidade de execução (e.g., protótipo e produto); ou de aspectos organizacionais. Neste trabalho, a abordagem foi modelada para o contexto de projetos de desenvolvimento para dispositivos móveis.

Na atividade IV, especialistas da organização onde está sendo implantada a abordagem devem ser consultados para definição das tabelas de probabilidades. Neste trabalho, dois especialistas do VIRTUS com mais de cinco anos de experiência em projetos de desenvolvimento para dispositivos móveis foram consultados. Para guiar as atividades III e IV um processo foi definido para auxiliar na elicitação de informações com especialistas de cada organização. Os detalhes da Rede Bayesiana modelada estão no Capítulo 5, apresentando a resposta para questão **RQ1** desta pesquisa.

Na atividade V uma validação estática [41] com seis cenários de simulação foi executada. Os cenários representam casos reais de projetos de software. Cada cenário descreve um projeto de software, com suas tecnologias, riscos e estratégias de mitigação. Em seguida é descrito como a Rede Bayesiana pode ser utilizada para auxiliar na tomada de decisão na identificação, mensuração ou monitoramento de riscos. As ações recomendadas pela abordagem foram avaliadas por oito profissionais do VIRTUS através de um *Focus Group* [65]. Para avaliação dos resultados discutiu-se a utilidade prática da abordagem à luz do Modelo de Aceitação de Tecnologia (TAM) [22]. Os resultados serviram para identificar os benefícios da abordagem proposta. Os detalhes da avaliação dos resultados estão no Capítulo 6, apresentando a resposta à questão **RQ2** desta pesquisa.

Por fim, na atividades VI a validação dinâmica da abordagem é realizada por meio de um experimento [99]. Evidências correspondentes a dados reais de seis projetos são inseridas na Rede Bayesiana e uma avaliação é realizada comparando as previsões da RB e o entendimento de profissionais do projeto. Para identificação de riscos, foram calculados o *precision*, *recall* e *f-measure* dos riscos previstos por diferentes profissionais do projeto com os riscos recomendados pela Rede Bayesiana. Para mensuração, um *ranking* dos riscos de maior

probabilidade calculados pela RB foram apresentados aos profissionais. Em seguida, eles responderam uma pergunta na escala Likert [58] com cinco respostas possíveis avaliando a capacidade da abordagem em auxiliar a mensuração de riscos. O processo se repetiu para o monitoramento de riscos, neste caso os profissionais avaliaram as estratégias recomendadas pela abordagem para mitigar os riscos previamente identificados. Com base nos resultados coletados, observa-se que a abordagem proposta é capaz de auxiliar na tomada de decisão nas atividades de identificação e monitoramento de riscos. A avaliação não foi conclusiva em relação ao suporte à mensuração de riscos e, por este motivo, desconsiderou-se a mensuração como contribuição deste trabalho. Os detalhes da avaliação dos resultados estão no Capítulo 6, apresentando as respostas às questões **RQ3, RQ4 e RQ5**.

## 1.4 Relevância

A área de riscos é uma das mais importantes do gerenciamento de projetos, pois norteia decisões estratégicas relacionados ao escopo, tempo, custo e qualidade [89]. Ao gerenciar riscos é possível maximizar os eventos positivos em oportunidades e minimizar os efeitos que possam impactar negativamente os objetivos dos projetos. Assim, um bom gerenciamento de riscos contribui diretamente para elevar as taxas de sucesso dos projetos de software [119].

Após a conclusão do presente trabalho, espera-se que a solução proposta possa contribuir com o avanço no estado da arte. Abordagens para gerenciamento de riscos têm sido alvo de pesquisas nos mais diversos contextos e para diferentes propósitos [33, 62, 67, 82]. Espera-se que o resultado deste trabalho possibilite insumos nas futuras pesquisas que investiguem abordagens para auxiliar o gerenciamento de riscos em projetos de software.

Acredita-se também que o sistema proposto irá beneficiar equipes na indústria, especialmente em *startups* e times vinculados a núcleos de inovação tecnológica. Com melhor entendimento dos eventos, espera-se uma menor subjetividade do processo de gerenciamento de riscos. Com isso, espera-se proporcionar maior confiabilidade na decisão final dos gestores em relação às diversas decisões realizadas durante o planejamento e execução dos projetos.

Por fim, este trabalho tem relevância para o avanço nas pesquisas do grupo ISE <sup>2</sup> da UFCG, que investiga a aplicação de técnicas inteligentes para a melhoria da produtividade

---

<sup>2</sup>ISE: <http://www.virtus.ufcg.edu.br/ise-group/>

na prática de Engenharia de Software. Além disso, espera-se contribuir para a melhoria prática dos processos do VIRTUS, que também é parte da UFCG.

## 1.5 Sumário das contribuições

As principais contribuições desta tese são apresentadas a seguir:

- Estudo qualitativo realizado em núcleos de inovação tecnológica sobre os principais fatores de riscos em projetos de software. Este estudo complementa o estado da arte listando os fatores de riscos relacionados às características tecnológicas de projetos de software;
- Rede Bayesiana para prognóstico dos riscos tecnológicos em função de informações das tecnologias dos projetos de software. A Rede também realiza prognósticos dos riscos em função das estratégias de mitigação;
- Processo sistemático para adaptação da Rede Bayesiana em projetos de diferentes contextos nas organizações de desenvolvimento de software, com suporte de ferramenta de software;
- Ferramenta para dar suporte a identificação, mensuração e monitoramento de riscos, abstraindo dos usuários detalhes da Rede Bayesiana construída.

## 1.6 Estrutura do Documento

Os Capítulos restantes que compõem este documento estão estruturados da seguinte forma:

**Capítulo 2: Fundamentação Teórica.** Apresenta definições gerais dos temas abordados neste documento, que servem para dar embasamento teórico aos leitores.

**Capítulo 3: Trabalhos Relacionados.** Discute os trabalhos relacionados na área de gerenciamento de riscos com foco em abordagens com Redes Bayesianas.

**Capítulo 4: Grounded Theory.** Apresenta detalhes sobre estudo qualitativo realizado que serviu de base para construção da Rede Bayesiana.

**Capítulo 5: Abordagem Proposta.** Apresenta detalhes sobre a Rede Bayesiana construída, incluindo o processo para utilização da abordagem proposta em organizações de desenvolvimento de software.

**Capítulo 6: Validação.** Apresenta os resultados da validação estática e dinâmica da abordagem de acordo com a utilidade prática e a previsão das predições da Rede Bayesiana.

**Capítulo 7: Conclusões.** Apresenta as considerações finais, sendo discutidos as limitações do trabalho, os resultados e sugestões para trabalhos futuros.

# Capítulo 2

## Fundamentação Teórica

Neste Capítulo são apresentados conceitos necessários ao entendimento desta tese. Nas próximas Seções são apresentadas considerações acerca de Gerenciamento de Riscos e Redes Bayesianas.

### 2.1 Gerenciamento de Riscos

Um risco de projeto é um evento ou condição incerta que, se realizado, afeta pelo menos um de seus objetivos [10]. Seu efeito pode ser positivo (i.e., oportunidade) ou negativo (i.e., ameaça) [89] e é o resultado de uma série de fatores internos ou externos [94]. Os riscos podem levar a perdas nas organizações, que podem estar relacionadas à diminuição da qualidade do produto, aumento dos custos de produção e não cumprimento dos prazos dos projetos [6, 91].

Processos para gerenciamento de riscos estão presentes em diversas metodologias e normas [54, 89, 107]. De forma geral, riscos gerenciados corretamente colaboram para que recursos sejam direcionados de forma assertiva [108] e ações coordenadas possam aumentar efetivamente as taxas de sucesso dos projetos [71]. Segundo Kerzner [61], o gerenciamento de riscos deve começar no início de um projeto, e as estratégias de mitigação destes eventos devem ser avaliadas ao longo do de todo ciclo de vida do projeto.

De acordo com o PMI (*Project Management Institute*) [89], é necessário desenvolver uma abordagem aos riscos que seja apropriada para cada projeto. O primeiro passo consiste em desenvolver o plano de gerenciamento dos riscos. O plano é vital para obtenção de apoio



das partes interessadas para garantir que o processo seja apoiado e executado de maneira efetiva [89]. Após planejar o gerenciamento dos riscos, os próximos processos consistem em: identificar os riscos, realizar a análise qualitativa dos riscos, realizar a análise quantitativa dos riscos, planejar respostas aos riscos, implementar respostas aos riscos e monitorar os riscos. Os processos estão distribuídos nas fases de planejamento, execução e monitoramento dos projetos conforme apresentado na Figura 2.1.

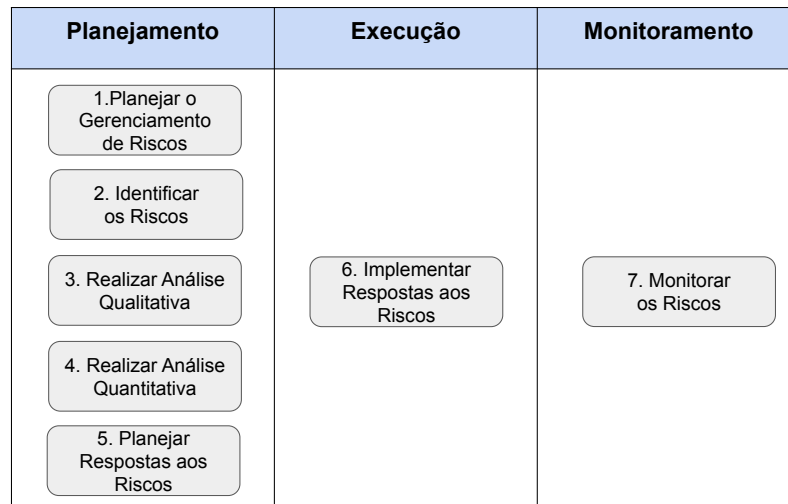


Figura 2.1: Processos de Gerenciamento de Riscos segundo PMBOK 6ª Edição [89]

Princípios para o gerenciamento de riscos podem ser encontrados também na norma ISO 31000 [54]. É definido um conjunto de diretrizes para gerenciar qualquer forma de risco de uma maneira sistemática, transparente e confiável, dentro de qualquer escopo e contexto. A norma ISO 31000 estabelece princípios que incluem proteger o valor do negócio, auxiliar a tomada de decisões e apoiar o tratamento de incertezas. Segundo a norma, o sucesso do gerenciamento de riscos irá depender do engajamento da organização em todos os níveis [69]. Na norma ISO 31000, os processos de gestão de riscos são representados pelo diagrama apresentado na Figura 2.2. Os processos de gestão de riscos estão localizados entre as etapas de Comunicação e Consultas com Monitoramento e Análise Crítica. São etapas que tratam da comunicação das partes interessadas internas e externas e da melhoria contínua do processo, respectivamente. Como entrada dos processos de riscos, o contexto com os fatores internos e externos que influenciam os objetivos da organização devem estar documentados com as responsabilidades de cada setor da organização. Em seguida, os processos de riscos são exe-

cutados em sequencia: Identificação do risco, análise do risco e avaliação do risco. Por fim, o tratamento do risco refere-se ao processo onde os controles existentes são aperfeiçoados ou novos controles são desenvolvidos e implementados [90].

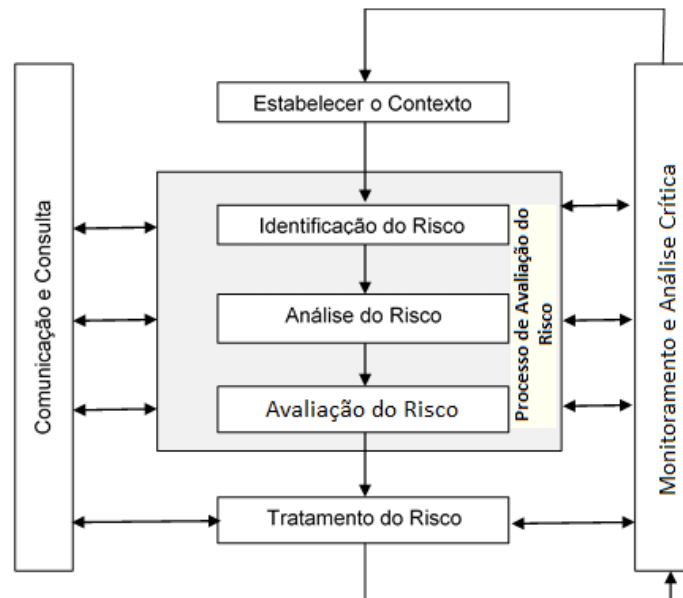


Figura 2.2: Diagrama do processo de gestão de riscos da norma ISO 31000 [90]

Modelos de maturidade de processos como o CMMI [17] e MPS.Br [103] fornecem um *framework* para a implantação e melhoria do processo de software das organizações. A gestão de riscos é conduzida pelo estabelecimento e manutenção de uma estratégia para identificar, analisar e mitigar riscos. Normalmente, isto é documentado em um plano de gestão de riscos. A estratégia refere-se às ações específicas e à abordagem utilizada para aplicar e controlar o gerenciamento do risco, composto pela identificação das fontes do risco, categorização dos riscos e os parâmetros usados para avaliar, limitar e controlar riscos para uma manipulação eficaz [23].

As metodologias de desenvolvimento ágil não contêm técnicas explícitas de gerenciamento de riscos [110], pois acredita-se que ciclos curtos de desenvolvimento iterativo minimizarão qualquer impacto imprevisível relacionado ao desenvolvimento de produtos [24, 85]. No entanto, em projetos maiores ou durante o desenvolvimento de produtos complexos, existe a necessidade de um gerenciamento de risco adequado [112]. Na literatura existem abordagens para auxiliar o gerenciamento de riscos sem trazer *overhead* ao processo ágil. Por exemplo, Hossain *et al.* [49] definiram um *framework* para auxiliar o ge-

renciamento de riscos em projetos com metodologia Scrum com múltiplos *stakeholders*. Seguindo a mesma linha, princípios SOA (*Service-Oriented Architecture*) foram usados por Lee *et al.* [21] para criar uma estrutura para gerenciamento de riscos para projetos ágeis de software.

Com relação as técnicas, a Matriz de Probabilidade e Impacto [89] ou simplesmente Matriz de Riscos [124] é a principal técnica utilizada na indústria para gerenciamento de riscos. Outros métodos utilizados para auxiliar atividades do gerenciamento de riscos são: matriz SWOT [96]; diagramas de causa e efeito [95]; listas de verificação [50]; e *brainstorming* [89]. Além disso, existem técnicas promissoras baseadas em Inteligência Artificial e Aprendizado de Máquina sendo investigadas no estado da arte para dar suporte ao gerenciamento de riscos. Mais detalhes sobre as técnicas e abordagens para auxiliar o gerenciamento de riscos são descritas no Capítulo 3.

## 2.2 Redes Bayesianas

As Redes Bayesianas são modelos gráficos capazes de representar as relações de causalidade entre variáveis [29]. Pertencem à família de modelos probabilísticos usados para representar incertezas de um domínio [8]. Segundo Neapolitan *et al.* [81], a técnica surgiu para representar contextos em que há um grande número de variáveis, e o objetivo de verificar a influência probabilística que uma ou mais variáveis exercem sobre outras.

Uma Rede Bayesiana pode ser dividida em termos qualitativos e quantitativos [114]. A parte qualitativa, o chamado aprendizado estrutural, é a representação gráfica das variáveis em forma de um Grafo Acíclico Dirigido. A parte quantitativa, chamada de aprendizado de parâmetros, define relações de dependência como funções de probabilidade condicional entre variáveis, usando relações de causa e consequência [62]. Uma função de probabilidade é representada com uma Tabela de Probabilidade dos Nós [86].

O conhecimento de uma Rede Bayesiana é extraído da probabilidade condicional de um conjunto de variáveis de consulta, de acordo com as variáveis de evidência. [8]. Esta probabilidade é calculada utilizando o Teorema de *Bayes*, onde a probabilidade de um evento é definido dado que outro evento ocorreu [81].

Com o grafo estruturado e as tabelas de probabilidades definidas, o raciocínio para uso

das Redes Bayesianas pode ser realizado de quatro maneiras distintas [84] conforme ilustrado na Figura 2.3. O raciocínio de diagnóstico está dirigido em sentido oposto das arestas da rede, implicando: se existe um efeito, a causa pode ser estimada. O raciocínio preditivo ou prognóstico calcula efeitos futuros segundo às causas apresentadas. A direção desse raciocínio coincide com a direção das arestas. O raciocínio inter-causal relaciona as causas correspondentes a um efeito comum. Finalmente, o raciocínio combinado é o mais complexo, implicando o uso dos raciocínios de diagnóstico e preditivo [66].

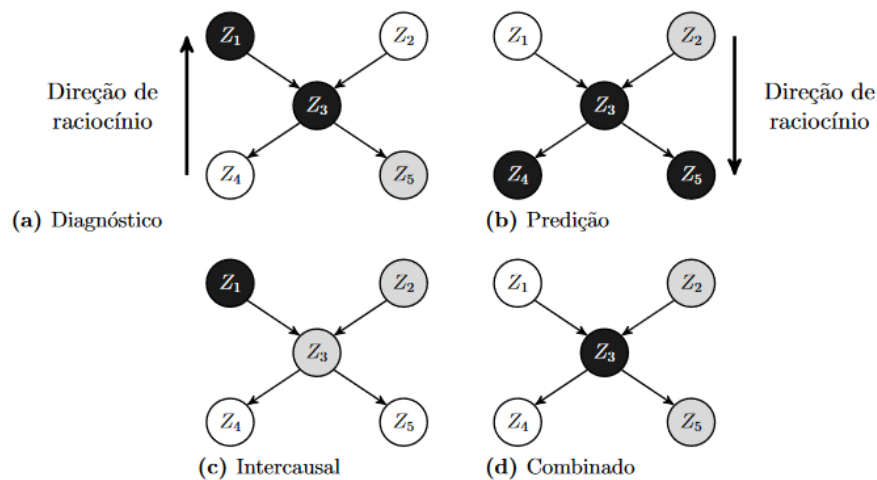


Figura 2.3: Tipos de raciocínio em Redes Bayesianas [66]

A relação de causalidade entre as variáveis é definida de acordo com o domínio do problema modelado na Rede Bayesiana. Por exemplo, quando se realiza um diagnóstico deseja-se saber o porquê de um fenômeno, na predição a consequência de evento(s) é analisada para um determinado objetivo [86]. Na Figura 2.4 ilustra-se um exemplo de Rede Bayesiana. Os nós representam as variáveis probabilísticas e os arcos os relacionamentos causais entre essas variáveis [32].

Neste caso, deseja-se calcular a probabilidade de um projeto ter sucesso dado o histórico das organizações em relação a maturidade de processos e da qualidade dos requisitos. As TPNs dos nós pai representam o conhecimento a priori com relação a essas variáveis. Por exemplo, para  $X_1$ , assume-se que 20% das organizações tem alto nível de maturidade de processos; para  $X_2$ , que 60% dos requisitos de projetos tem qualidade aceitável. Os valores de  $X_1$  e  $X_2$  podem ser atualizados com evidências do ambiente onde a RB for usada, caso não exista histórico ou evidência pode-se assumir distribuições uniformes de probabilidades.

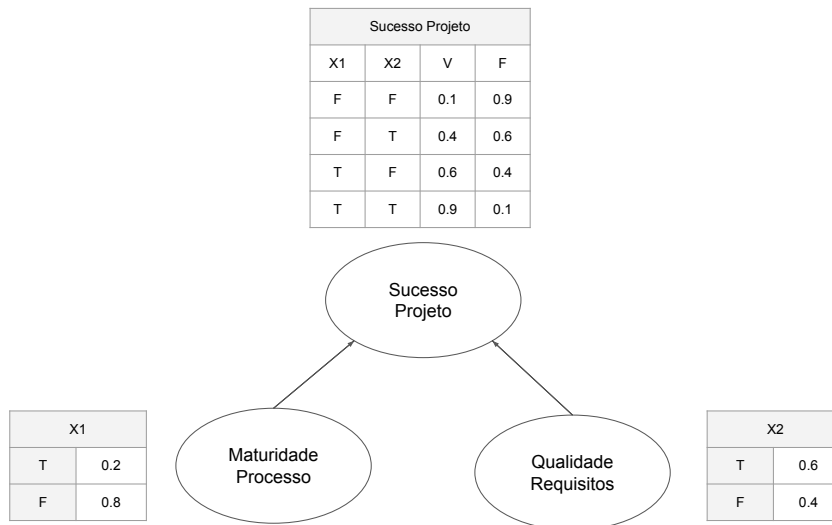


Figura 2.4: Exemplo de Rede Bayesiana

A TPN do nó filho representa as probabilidades de um projeto ter sucesso dada cada combinação possível de valores dos nós pai. Por exemplo, para situação em que a organização tem maturidade de processo e requisitos de qualidade, a RB infere que o projeto tem 90% de sucesso. Os valores das TPN podem ser definidos de acordo com dados históricos de projetos ou conhecimento de especialistas.

Formalmente, uma Rede Bayesiana  $B$  é um grafo acíclico direcionado que representa a distribuição conjunta de probabilidade sobre o conjunto de variáveis aleatórias  $V$  [37]. A rede é definida pelo par  $B = \{G, \Theta\}$ .  $G$  é o grafo acíclico direcionado cujos nós  $X_1, \dots, X_n$  representam variáveis aleatórias, e os arcos representam dependências diretas entre essas variáveis. O grafo  $G$  codifica suposições de independência, nas quais cada variável  $X_i$  é independente dos seus *não-dependentes* dados seus *pais* em  $G$ .  $\Theta$  representa o conjunto de parâmetros da rede. Esse conjunto contém o parâmetro  $\theta_{x_i|\pi_i} = P_B(x_i|\pi_i)$  para cada  $x_i$  em  $X_i$  condicionado por  $\pi_i$ , o conjunto de parâmetros de  $X_i$  em  $G$ . Equação 2.1 apresenta a distribuição conjunta definida por  $B$  sobre  $V$ .

$$P_B(X_1, \dots, X_n) = \prod_{i=1}^n P_B(x_i|\pi_i) = \prod_{i=1}^n \theta_{x_i|\pi_i} \quad (2.1)$$

Existem duas formas de coletar dados e definir as probabilidades: dados históricos e especialistas [88]. Para executar os cálculos, é necessário definir os estados e probabilidades para cada nó. Contudo, não é fácil encontrar uma base de dados adequada para um cenário

específico de um problema prático. Por outro lado, a definição das TPN com a ajuda de especialistas requer bastante esforço [35].

Há vários métodos que têm como objetivo diminuir a complexidade e codificar a experiência de especialistas em grandes TPN. Noisy-OR [52] é um modelo útil para nós *booleanos* quando não existem informações suficientes para preenchimento da rede, o modelo possibilita uma aproximação da previsão. Perkusich *et al.* [88], por sua vez, para otimizar o processo de construção de TPN, propõem um algoritmo cujo objetivo é ordenar os nós pais com base em sua relevância para o nó filho. Por fim, Fenton *et al.* [34] propõem uma abordagem para Nós Ranqueados baseada numa distribuição normal duplamente truncada (TNormal) que usa como média um tipo de função ponderada em função dos valores dos nós pais.

# Capítulo 3

## Trabalhos Relacionados

Neste Capítulo são apresentados os trabalhos relacionados a esta proposta de tese. Inicialmente são listadas abordagens para auxiliar atividades do gerenciamento de riscos em projetos de software. Em seguida é dado um foco específico em abordagens baseadas em Redes Bayesianas.

### 3.1 Abordagens para Gerenciamento de Riscos

Várias técnicas são encontradas na literatura para auxiliar o gerenciamento de riscos em projetos de software. Seja na identificação, mensuração ou monitoramento de riscos, as técnicas auxiliam os profissionais estruturando o conhecimento ou fornecendo indicadores para diminuir a subjetividade ao tratar os riscos do projeto [10, 80].

Foi observado que existe uma variedade de formas para apresentar os indicadores de riscos. O mais comum é uma avaliação binária se o projeto é de risco ou não [78, 108]. Mas também são encontrados trabalhos que utilizam escala de avaliação em três níveis (alto, médio ou baixo risco) [16, 53, 111], ou simplesmente apresentam o resultado em escala ordinal [9].

As técnicas mais comuns são entrevistas e *brainstorming*, que são usadas separadamente ou em conjunto com outros métodos durante todo ciclo do projeto [89]. Alguns exemplos de abordagens mais elaboradas, encontradas no estado da arte, estão listados na Tabela 3.1.

Métodos gráficos, como matriz SWOT [96] e diagramas de causa e efeito [95], auxiliam equipes no gerenciamento dos riscos para diminuir a subjetividade na identificação dos ris-

Tabela 3.1: Abordagens para Gerenciamento de Riscos

<b>Autores</b>	<b>Técnica</b>	<b>Propósito</b>
Russell e Taylor [95]	Diagramas de Causa e Efeito	Identificação de Riscos
Sasankar <i>et al.</i> [96]	Matriz SWOT	
Xiaosong <i>et al.</i> [123]	Matriz de Riscos	Mensuração de Riscos
Takagi <i>et al.</i> [108]	Checklist	Identificação e Mensuração de Riscos
Min <i>et al.</i> [77]	Lógica Fuzzy	Identificação e Mensuração de Riscos
Han <i>et al.</i> [45]	Redes Neurais	Identificação e Mensuração de Riscos
Fenton <i>et al.</i> [33]	Redes Bayesianas	Identificação e Mensuração de Riscos

cos. São técnicas usadas em conjunto com *brainstorming* principalmente nas fases iniciais dos projetos. O objetivo é detectar as principais ameaças e as causas que possam materializar os riscos do projeto. Embora sejam métodos eficientes para identificação dos eventos, não oferecem mecanismos para mensuração ou avaliação dos riscos [96].

Para mensuração de riscos, a matriz de probabilidade e impacto é a técnica mais usada na indústria [89]. Os profissionais definem para cada risco valores de probabilidade e impacto. A subjetividade diminui quando os profissionais cruzam as informações nesses dois eixos com valores categóricos pré-definidos [124]. O impacto de um risco é a capacidade do evento em trazer consequências no projeto. A probabilidade é a chance de um evento de risco ocorrer [89]. Entretanto, a escolha destes valores continua sendo definido sob o ponto de vista dos especialistas [60].

Uma técnica que oferece mecanismos de identificação e mensuração de riscos são as listas de verificação (*checklists*). As listas são preenchidas para o gestor e demais membros da equipe terem conhecimento dos principais riscos e da complexidade destes eventos. É uma abordagem que diminui a subjetividade tornando o processo mais sistemático [50]. Porém, os *checklists* são estáticos [125], o que torna difícil sua manutenção em cenários onde as restrições e premissas dos projetos mudam constantemente. Outra limitação é que os *checklists* não são eficazes quando as informações do projeto são incompletas, um cenário comum em projetos com alto nível de incerteza.

Técnicas inteligentes [87], que fazem uso de Inteligência Artificial e Aprendizado de Máquina, são utilizadas em muitos trabalhos na literatura para gerenciamento de riscos. A



Lógica Fuzzy pode ser útil para diminuir a subjetividade de informações do projeto para definição de indicadores de riscos. Porém, de acordo com Verbert *et al.* [116] é uma técnica útil para tratar incerteza em cenários com imprecisão dos dados, não sendo a melhor escolha para tratar incerteza com dados incompletos [63]. Abordagens baseadas em Redes Neurais [45, 109] também são eficientes para calcular indicadores que diminuem a subjetividade do processo. Entretanto, são abordagens que demandam grande quantidade de dados para análise, o que torna o uso inviável em cenários onde não é possível criar uma base histórica [66, 98].

Por fim, Rede Bayesiana é uma técnica utilizada em muitos trabalhos para auxiliar o gerenciamento de riscos em projetos de software [33, 51, 67]. As Redes Bayesianas fazem uso de informações históricas dos projetos e apoio de especialistas para definir a estrutura e tabelas de probabilidades [8]. As abordagens propõem modelos causais para representar o domínio do problema e calcular indicadores de risco [114].

Na Tabela 3.2 é apresentado um resumo das principais técnicas citadas e suas características. Nesta análise não consideramos os métodos gráficos (SWOT e Diagrama de Causa e Efeito) por serem técnicas que tratam exclusivamente do processo de identificação de riscos.

Tabela 3.2: Características das abordagens

<b>Técnica</b>	<b>Estrutura de raciocínio</b>	<b>Base de Dados Massiva</b>	<b>Resposta a novos dados</b>	<b>Tratar dados incompletos</b>
Matriz de Riscos	N/A	Não	Estática	Não
Checklist	N/A	Não	Estática	Não
Lógica Fuzzy	Não	Não	Dinâmica	Não
Redes Neurais	Não	Sim	Dinâmica	Sim
Redes Bayesianas	Sim	Não	Dinâmica	Sim

Além de apresentar indicadores de risco, as abordagens com Redes Bayesianas fornecem a estrutura de raciocínio (modelo causal) para auxiliar a tomada de decisão. Todas as técnicas utilizam dados históricos para definição de variáveis ou melhor entendimento de contexto, mas apenas Redes Neurais necessitam de uma base massiva na abordagem. Algumas abordagens são estáticas, por isso, demandam muito esforço para tratar novos dados de forma intermitente. As técnicas dinâmicas ao receber uma informação nova recalculam os indicadores de risco de forma automática. Por fim, apenas as abordagens com Redes Neurais e Redes Bayesianas possibilitam tratar cenários com dados incompletos, ou seja, realizam o cálculo dos indicadores de risco mesmo quando não são disponibilizadas todas as

informações de entrada.

Após análise das abordagens da Tabela 3.2, Rede Bayesiana foi considerada a técnica mais promissora para esta pesquisa. Na próxima Seção são apresentados os principais trabalhos do estado da arte que utilizam redes Bayesianas para o gerenciamento de riscos em projetos de software.

## 3.2 Redes Bayesianas para Gerenciamento de Riscos

No estado da arte, abordagens com Redes Bayesianas para o gerenciamento de riscos em projetos de software apresentam propósitos diversos. As abordagens calculam indicadores de risco para apoio à decisão em diferentes áreas do projeto, como: tempo, custo e qualidade. Na Tabela 3.3 são listados alguns trabalhos encontrados no estado da arte.

Tabela 3.3: Redes Bayesianas para Gerenciamento de Riscos

<b>Título</b>	<b>Autores</b>	<b>Propósito</b>
A Bayesian Critical Path Method for Managing Common Risks in Software Project Scheduling	Nguyen <i>et al.</i> (2018)	Cronograma
Project cost risk analysis: A Bayesian networks approach for modeling dependencies between cost items	Khodakarami <i>et al.</i> (2014)	Custos
On the effectiveness of early life cycle defect prediction with Bayesian Nets	Fenton <i>et al.</i> (2008)	Qualidade
Software Delivery Risk Management: Application of Bayesian Networks in Agile Software Development	Ancveire <i>et al.</i> (2015)	Qualidade
Software defects estimation using metrics of early phases of software development life cycle	Kumar <i>et al.</i> (2017)	Qualidade
Assessing new product development project risk by Bayesian network with a systematic probability generation methodology	Chin <i>et al.</i> (2009)	Risco de Produção
Developing a Bayesian belief network model for prediction of R&D project success	Sharma e Chanda (2017)	Custo, Qualidade e Tempo

O trabalho de Nguyen *et al.* [82] propõe uma Rede Bayesiana para mensurar os riscos com intuito de auxiliar a definição do cronograma do projeto. Os autores utilizam a RB para avaliar a incerteza de cada tarefa. Com essas informações o método auxilia o processo de *scheduling* na definição do caminho crítico do projeto. No trabalho de Khodakarami *et al.* [62] é apresentada uma Rede Bayesiana para quantificar a incerteza dos itens de custo, sendo proposta uma solução para auxiliar na definição do orçamento.

É comum encontrar abordagens que usem Redes Bayesianas no gerenciamento de riscos para auxiliar atividades de qualidade. Fenton *et al.* [33] propõem um modelo formado com fatores quantitativos e qualitativos relacionados ao processo de desenvolvimento. Os autores

utilizam uma RB para prever a densidade de defeitos do software. Também relacionado a previsão de defeitos, Kumar *et al.* [67] propõem uma Rede Bayesiana a ser usada nas fases iniciais do projeto. Ancveire *et al.* [3] utilizam uma RB para avaliar a saúde do projeto e auxiliar times para garantir entregas bem sucedidas do software.

O trabalho de Chin *et al.* [15] avalia em um projeto de P&D duas alternativas para desenvolvimento de um novo produto. Uma Rede Bayesiana é usada para mensurar qual das soluções possui maior risco. No contexto de projetos de inovação, Sharma and Chanda [97] propõem uma Rede Bayesiana para prever a exposição de riscos do projeto em relação ao custo, qualidade e tempo.

Independentemente do propósito, os trabalhos citados na Tabela 3.3 utilizam diferentes fatores de riscos. Para escolha dos fatores, os autores se basearam na literatura (e.g., Nguyen *et al.* [82]) ou na opinião de especialistas (e.g., Fenton *et al.* [33]). Os fatores são representados na Rede Bayesiana por Nós. No que se refere às conexões dos fatores, especialistas são responsáveis por identificar as relações de causalidade.

Os fatores de risco são definidos de acordo com o contexto de cada pesquisa, porém, mesmo em cenários semelhantes, a forma de calculá-los pode mudar. No trabalho de Fenton *et al.* [33], o fator complexidade do software foi calculado de acordo com a quantidade de componentes de arquitetura, enquanto Khodakarami *et al.* [62] para representar este fator considerou a complexidade ciclomática do sistema. Dentre os trabalhos listados na Tabela 3.3, os principais fatores de risco das abordagens foram listados na Tabela 3.4.

Tabela 3.4: Fatores de Risco

Artigo	Fatores
Nguyen et al. (2018)	Treinamento insuficiente, Excessivo Planejamento, Falta de Ferramentas, Tecnologia Apropriada
Khodakarami et al. (2014)	Mudança Escopo, Inflação, Complexidade Fornecedores, Preço Materiais
Fenton et al. (2008)	Complexidade, Documentação, Stakeholders, Expertise do time
Ancveire et al. (2015)	Informações da Documentação, Habilidades do Time, PO, Código, Testes, Deliveries
Kumar et al. (2017)	Experiência do time, Complexidade do software, Qualidade Especificação
Chin et al. (2009)	Complexidade da solução, Similaridade com legado, Fornecedores, Capacidade
Sharma and Chanda (2017)	Tecnologia, Concorrência de mercado, Gestão, Fatores Ambientais

Os fatores de riscos mais comuns identificados nos trabalhos estão relacionados ao time

(i.e., experiência, *expertise*, habilidades dos recursos), requisitos (i.e., mudanças de escopo, qualidade e informações da documentação) e ao processo (i.e., relação com o PO, treinamentos e planejamento). De forma geral, as abordagens concentram-se na definição de fatores de riscos e na descoberta de correlações entre os fatores e algum objetivo do projeto [25, 57]. Uma lacuna observada é a falta de modelagem dos diversos fatores de riscos relacionados as características tecnológicas dos projetos de software. Algumas das abordagens analisadas modelam essas características, mas limitam-se em definir um fator específico para este propósito. Por exemplo: Chin [15] modelou o fator *Complexidade do Produto*, Sharma [97] chamou o fator de *Tecnologia*, khodakarami [62] de *Complexidade* e Kumar [67] de *Complexidade do software*.

Desafios tecnológicos estão presentes em qualquer projeto de software [42]. Entretanto, existem projetos onde as características tecnológicas estão mais presentes. Essas características aumentam a subjetividade no gerenciamento de riscos devido a falta de similaridade com produtos já desenvolvidos, à complexidade da solução e as indefinições de ambiente [15, 36, 97]. Esse cenário é comum em projetos de inovação, projetos de Pesquisa e Desenvolvimento e projetos para desenvolvimento de novos produtos. Em projetos com essas características é comum o uso de novos *frameworks* de desenvolvimento; integrações com plataformas emergentes; uso de técnicas inteligentes, como algoritmos de Inteligência Artificial, modelos de Aprendizado de Máquina ou Blockchain, ainda em validação industrial. Dos trabalhos analisados, apenas as abordagens de Chin [15] e Sharma [97] se aprofundam em investigar as características tecnológicas dos projetos de software. Porém, estes trabalhos tem foco em riscos relacionados ao mercado e similaridade do produto.

### 3.3 Considerações Finais do Capítulo

Neste capítulo foram apresentadas várias abordagens para o gerenciamento de riscos em projetos de software, com mais destaque aos trabalhos alinhados com o proposto nesta tese, que utiliza Redes Bayesianas como base. Apesar das inúmeras abordagens presentes no estado da arte, replicar as Redes Bayesianas discutidas nesse capítulo para representar as características tecnológicas dos projetos de software torna-se inviável. Como descrito na Seção 3.2, alguns trabalhos [15, 62, 67, 98] limitam-se em definir um fator específico para

representar o risco associado a todas as características tecnológicas do projeto. Uma opção seria adaptar uma Rede Bayesiana mais genérica, como o modelo descrito no trabalho de Fenton [30]. Porém, ao tentar representar as diversas características tecnológicas de projetos de software, o modelo se mostrou muito genérico e pouco útil para auxiliar o gerenciamento de riscos. Por exemplo:

- Para representar o risco do uso de novas tecnologias, no modelo de Fenton [30], a variável mais próxima para traduzir esse fator de risco seria uma combinação dos fatores “Linguagem” e “KLOC entregues”. Entretanto, o risco em usar novas tecnologias não necessariamente está relacionado à quantidade de linhas de código.
- Nessa linha, para representar o risco da complexidade da solução, no modelo de Fenton [30], a variável mais próxima para traduzir esse fator de risco seria uma combinação dos fatores “Número de Inputs e Outputs” e “Número de telas GUI”. Entretanto, o risco de complexidade da solução não necessariamente está relacionado à quantidade de telas e de dados de entrada e saída.
- Um risco comum em projetos de software é a integração do sistema com outras plataformas. Esse risco tem relação com a instabilidade de serviços e problemas de conexões externas. No modelo de Fenton [30] são avaliados fatores de riscos relacionados à comunicação externa, mas em nível de processo entre o time de desenvolvimento e *Stakeholders*. Não são avaliados riscos de comunicação em nível de tecnologias e ferramentas.
- Outro risco comum em projetos de software é a complexidade arquitetural do software. Esse risco tem relação principalmente com restrições em nível de segurança dos dados e desempenho em requisições. No modelo de Fenton [30] são avaliados fatores de riscos relacionados à complexidade de requisitos, mas em relação ao nível de envolvimento de *Stakeholders* e precisão da especificação. Não são avaliados riscos de requisitos em nível de restrições arquiteturais.

As dificuldades de utilização e adaptação das abordagens citadas motivaram a modelagem de uma nova Rede Bayesiana para gerenciamento de riscos para projetos de software

com foco nas características tecnológicas. De forma geral, as pesquisas citadas neste capítulo foram utilizadas como *benchmark* para definição da abordagem proposta desse trabalho. No Capítulo 4 é apresentado o estudo qualitativo que serviu de base para construção da abordagem.

# Capítulo 4

## Estudo Qualitativo

A metodologia escolhida nesta pesquisa para o estudo qualitativo foi o *Grounded Theory* [38]. O foco do GT é definir uma teoria detalhando características para um determinado fenômeno. O processo é realizado por meio de interações com coleta e análise de dados de forma simultânea [40]. Ao final do estudo, a teoria é definida por um conjunto sistemático de conceitos que ajudam a explicar o fenômeno em análise [19].

Nesta pesquisa, o fenômeno analisado é o gerenciamento de riscos em projetos de software, na qual foram realizadas entrevistas com profissionais de diferentes organizações. Ao final do estudo, os conceitos gerados refletem as premissas dos projetos, principais desafios, boas práticas e fatores de risco. Para esta tese, será apresentada apenas a estrutura da teoria referente aos fatores de risco em projetos de software. Os detalhes da coleta e análise dos dados desta pesquisa são apresentados nas Seções 4.1 e 4.2, respectivamente.

### 4.1 Coleta dos Dados

Uma das principais características do *Grounded Theory* está na capacidade de tratar dados não numéricos e não estruturados (e.g., transcrições de entrevistas, notas de reuniões) [40]; e a possibilidade da teoria ser criada a partir de casos práticos [118]. Nesta pesquisa, aplicamos o GT com a transcrição de entrevistas com vinte e cinco profissionais de dez diferentes organizações. Também coletamos dados em documentos de projetos fornecidos pelos participantes do estudo.

### 4.1.1 Seleção dos Participantes

Para selecionar os participantes do estudo, buscamos profissionais que falassem português, língua nativa do autor desta tese, e que possuíssem experiência na gestão de projetos de software. A busca por profissionais aconteceu via LinkedIn <sup>1</sup> ou por indicações de colaboradores do grupo ISE <sup>2</sup>. Foram enviados quarenta e oito convites via e-mail, nos quais, vinte e cinco se disponibilizaram a colaborar com o estudo.

Com o aceite, a entrevista foi agendada e realizada *in loco* ou por video conferência tendo o áudio gravado para posterior transcrição. Os profissionais participam de projetos de parceria entre empresas e centros de pesquisa (ou universidades), privados ou públicos. Os projetos destas organizações fazem uso de novas tecnologias (i.e., *frameworks*, linguagens, arquiteturas) para resolver problemas de negócios. Na Tabela 4.1 é apresentada uma visão geral dos participantes do estudo.

Tabela 4.1: Informações dos participantes no estudo GT.

Participante	Experiência	Empresa	País	Sector Atuação	Fase
P1	5 anos	E1	Brasil	Engenharia	Preliminar
P2	7 anos	E1	Brasil	Telecomunicações	Preliminar
P3	12 anos	E1	Brasil	Engenharia	Preliminar
P4	10 anos	E1	Brasil	Engenharia	Preliminar
P5	9 anos	E1	Brasil	Engenharia	Preliminar
P6	5 anos	E1	Brasil	Telecomunicações	Fase 01
P7	5 anos	E1	Brasil	Telecomunicações	Fase 01
P8	6 anos	E1	Brasil	Engenharia	Fase 01
P9	6 anos	E2	Brasil	Engenharia	Fase 01
P10	6 anos	E3	Canadá	Mercado Financeiro	Fase 01
P11	4 anos	E4	Brasil	Telecomunicações	Fase 01
P12	6 anos	E5	Brasil	Administrativo	Fase 01
P13	5 anos	E6	Brasil	Elétrico	Fase 01
P14	6 anos	E7	Brasil	Segurança Pública	Fase 01
P15	8 anos	E7	Brasil	Engenharia	Fase 01
P16	4 anos	E8	Brasil	Segurança Pública	Fase 02
P17	7 anos	E8	Brasil	Segurança Pública	Fase 02
P18	5 anos	E3	Canadá	Mercado Financeiro	Fase 02
P19	7 anos	E3	Canadá	Mercado Financeiro	Fase 02
P20	5 anos	E2	Brasil	Engenharia	Fase 02
P21	6 anos	E2	Brasil	Telecomunicações	Fase 02
P22	2 anos	E2	Brasil	Telecomunicações	Fase 02
P23	4 anos	E9	Brasil	Engenharia	Fase 02
P24	7 anos	E10	Canadá	Sistemas Médicos	Fase 02
P25	5 anos	E10	Canadá	Engenharia	Fase 02

<sup>1</sup>LinkedIn: <https://www.linkedin.com/>

<sup>2</sup>ISE: <http://www.virtus.ufcg.edu.br/ise-group/>



Os profissionais listados na Tabela 4.1 trabalham como gerentes de projeto, líderes técnicos ou Scrum Master. Os participantes de empresas canadenses são brasileiros que já trabalham no país há alguns anos. A maioria dos participantes são formados em cursos de Tecnologia da Informação (84%), já os demais (16%) são profissionais com outras formações mas desempenham um perfil de liderança nos projetos. A maioria dos profissionais são homens (76%), e a faixa etária com mais de 30 anos é preponderante entre os participantes (88%). Os profissionais trabalham em organizações com foco na inovação, usando o conhecimento recém-adquirido em novas tecnologias [59] para o desenvolvimento de novos produtos ou serviços [2]. Essas organizações são centros de desenvolvimento colaborativo entre universidades e indústria (64%) ou laboratórios que realizam projetos de pesquisa e desenvolvimento (36%).

#### 4.1.2 Evolução das Entrevistas

Conforme observado na Tabela 4.1, as entrevistas foram realizadas em três fases. Na fase preliminar foram realizadas cinco entrevistas, e nas fases 01 e 02, dez entrevistas em cada etapa. Na fase preliminar foram entrevistados profissionais de uma organização (E1). As perguntas utilizadas eram genéricas para um entendimento geral do contexto. Os entrevistados foram questionados sobre os principais riscos dos projetos que gerenciam na empresa. Somado a isto, na fase preliminar também foram analisados documentos de projetos com diferentes domínios e tecnologias fornecidos por estes profissionais (Tabela 4.2).

Tabela 4.2: Artefatos de projetos analisados na Fase Preliminar

Projeto	Setor Atuação	Domínio	Tecnologias
PJ-1	Engenharia	Web	Express, Angular
PJ-2	Engenharia	Mobile	Android, iOS, Unity, .net
PJ-3	Telecomunicações	Web/ Mobile	Express, Angular, MongoDB
PJ-4	Telecomunicações	Web/ Analytics	Django, Python
PJ-5	Engenharia	Web/ Analytics	Django, Python
PJ-6	Engenharia	Web	Android, iOS, Unity, .net
PJ-7	Engenharia	Web	Python, SQL
PJ-8	Engenharia	Web	Python, SQL

As entrevistas realizadas eram semiestruturadas [70] e o roteiro foi sendo adaptado com o passar das fases do estudo, uma vez que esse refinamento constante é uma característica do *Grounded Theory* [38]. Com um melhor entendimento do contexto, nas fases seguintes as perguntas tornaram-se mais objetivas no foco da pesquisa.

Na fase 01 foram realizadas mais dez entrevistas (participantes P6 - P15) com profissionais de sete diferentes organizações. O roteiro foi adaptado dando ênfase a questões de tecnologia e arquitetura dos projetos, assuntos esses que tiveram destaque nas entrevistas da fase preliminar.

Finalmente, na fase 02 foram realizadas as últimas dez entrevistas (participantes P16 - P25) com profissionais de cinco empresas. Nessa fase o foco esteve nas questões consideradas mais desafiadoras citadas pelos entrevistados nas fases anteriores como: ambiente de desenvolvimento e homologação, integrações do sistema com plataformas externas e técnicas de Inteligência Artificial.

Por fim, dado o melhor entendimento do fenômeno analisado durante as entrevistas da fase 02, foi necessário contactar participantes das fases anteriores para retirarem dúvidas pontuais. Essa revisão de entrevistas passadas é algo comum em trabalhos que utilizam *Grounded Theory* [38]. Para mais detalhes, no Apêndice A é apresentado o roteiro utilizado nas entrevistas durante a última fase do estudo.

## 4.2 Análise dos Dados

Ao final de cada fase do estudo, as entrevistas foram transcritas e analisadas com apoio do software AtlasTI<sup>3</sup>. Esta ferramenta permite ao pesquisador acompanhar as transcrições, gerenciar uma lista de códigos, gerar conjuntos de códigos relacionados e criar suporte gráfico destes códigos. Na Figura 4.1 é apresentado um exemplo de transcrição de entrevista.

De acordo com a metodologia *Grounded Theory*, a análise dos dados deve acontecer de forma incremental, pois em cada interação a análise deve ser realizada por meio de diferentes etapas de codificação. Desta forma, em cada fase das entrevistas (fase preliminar, fase 01 e fase 02) foram executados os procedimentos de codificação aberta, axial e seletiva [105]. Ao final da vigésima segunda entrevista, foi alcançado o nível de saturação, quando não existem mais conceitos a serem adicionados [1]. Com isso, a teoria emergente é definida com as categorias, axiomas e códigos relacionados ao fenômeno analisado [105].

O processo de codificação foi conduzido por três pesquisadores, que inclui o autor desta tese com auxílio de dois colaboradores do grupo ISE. O autor da tese foi o responsável por

---

<sup>3</sup>AtlasTI: <https://software.com.br/p/atlas-ti>

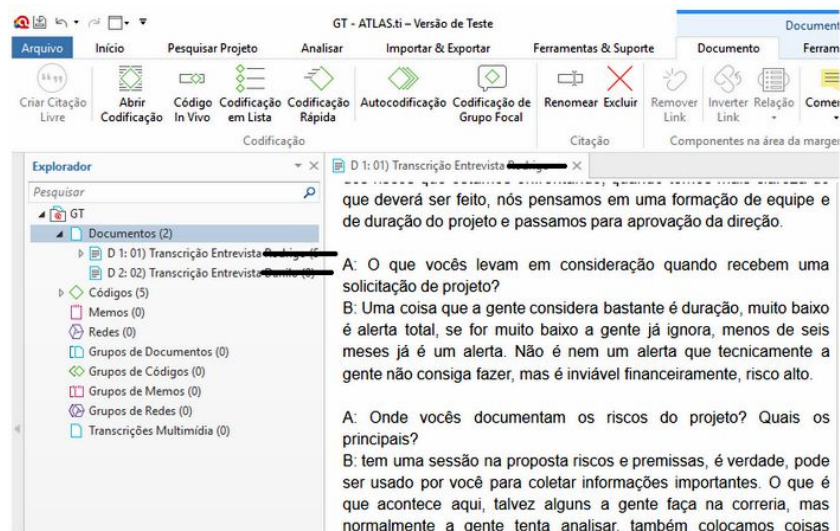


Figura 4.1: Transcrição das entrevistas

extrair os códigos, agrupá-los em axiomas e definir as categorias. Um segundo pesquisador realizou a checagem e ao final de cada uma das fases das entrevistas, os dois pesquisadores reuniram-se para avaliar os códigos extraídos, axiomas e categorias criadas. No caso de discordância, um terceiro pesquisador foi consultado para juntos tomarem uma decisão. As principais divergências aconteceram nas nomenclaturas de categorias e subcategorias, uma vez que o entendimento final foi escolher nomes que aproximem a teoria com normativas de gerenciamento de riscos existentes [54, 89].

### 4.2.1 Codificação Aberta

A primeira etapa do processo de análise consiste na codificação aberta que tem como objetivo encontrar códigos que sirvam para definição da teoria investigada [39], pois as entrevistas transcritas foram analisadas linha por linha. Nessa pesquisa usou-se o critério das palavras mais citadas no texto e as que os participantes deram maior ênfase na entrevista.

A codificação aberta realizada na fase preliminar serviu para identificação dos primeiros códigos. Na Figura 4.2 podem ser observados alguns códigos registrados após a análise das primeiras entrevistas. À medida que as entrevistas foram sendo transcritas e analisadas, a lista de códigos foi atualizada com as novas informações coletadas.

Durante o processo, novos códigos foram identificados, com a realidade dos entrevistados

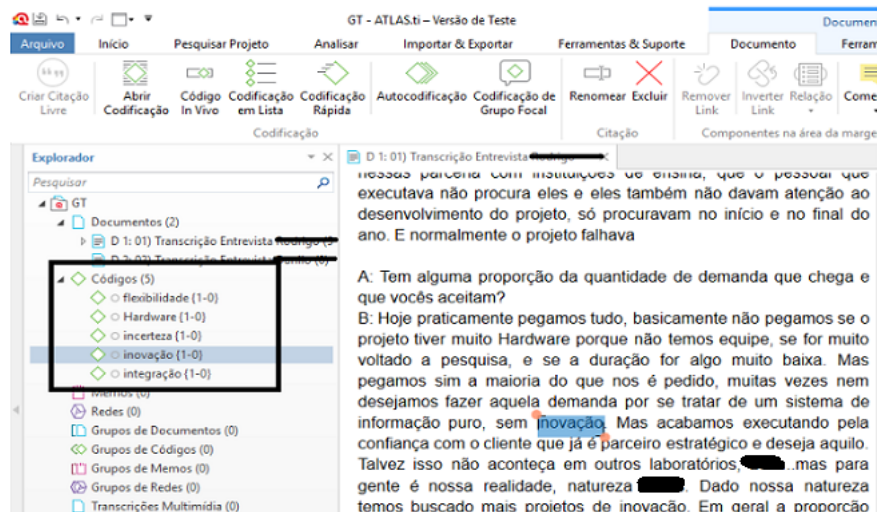


Figura 4.2: Primeiros códigos identificados

e outros eram atualizados ou excluídos, por serem considerados informações pontuais de um determinado projeto. Ao final das entrevistas nas três fases, uma lista definitiva com 90 códigos foi gerada como base da teoria definida nessa pesquisa. A lista completa de códigos gerados pode ser consultada no Apêndice B.

### 4.2.2 Codificação Axial

Com os códigos identificados, o próximo passo na análise consistiu em agrupar os itens que se relacionam e formam os axiomas [106]. Esse processo é iterativo, em que os primeiros axiomas foram identificados na fase 01 da pesquisa e refinados até o final das entrevistas. Por exemplo, foi identificado que muitos códigos transcritos nas entrevistas relacionavam-se à integração do sistema alvo com plataformas de terceiros. Com isso, o axioma “Integração” foi criado conforme apresentado na Tabela 4.3.

Tabela 4.3: Códigos relacionado ao Axioma Integração

Axioma	Código
Integração	API
	SGBD
	Linguagem
	Plataforma
	Fatores Externos
	Nova Versão
	Legado
	Suporte

Os axiomas que compartilham de mesmo contexto formam as categorias da teoria in-

vestigada [106]. Durante os ciclos de análises, as categorias vão sendo definidas agrupando códigos de conjuntos de axiomas. Como exemplo, o axioma “Integração” apresentado na Tabela 4.3 foi agrupado com outras informações tecnológicas para formar a categoria “Produto”. Os códigos desta categoria estão descritos na Tabela 4.4, de modo que estes códigos estão relacionados a aspectos tecnológicos do desenvolvimento de um produto de software, que vai desde o banco de dados à usabilidade da aplicação.

Tabela 4.4: Códigos relacionado à Categoria Inovação de Produto

<b>Categoria</b>	<b>Código</b>
Produto	Tecnologia
	SGBD
	Linguagem
	Arquitetura
	Dados
	Incerteza
	Método
	Plataforma
	Cliente
	Interface
	Ambiente
	Integração
	Fatores Externos
	Nova Versão
	Usabilidade
Legado	

Os axiomas e categorias são definidos de acordo com o entendimento dos pesquisadores em relação aos dados coletados, posto que essas estruturas refletem a visão dos pesquisadores sobre o fenômeno analisado. Desta forma, as entrevistas vão sendo realizadas e em cada fase novas estruturas vão sendo criadas, atualizadas ou excluídas.

### 4.2.3 Codificação Seletiva

O processo de codificação seletiva assemelha-se à criação de uma rede. Os códigos de cada categoria são analisados em busca de relacionamentos conforme o contexto. Por exemplo, dos códigos listados na seção anterior da categoria “Produto”, alguns relacionamentos criados incluem: usabilidade com interface, cliente com incerteza, tecnologia com linguagem. Os relacionamentos são criados até que ao redor da categoria apenas os códigos mais representativos estejam presentes, representando de forma sumarizada os demais conceitos. Na Figura 4.3 é apresentado como a codificação seletiva foi realizada para os códigos da ca-

tegoria “Produto”. Ao final, apenas quatro códigos (i.e., Integração, Ambiente, Método e Arquitetura) foram considerados relevantes para representar a categoria em questão.

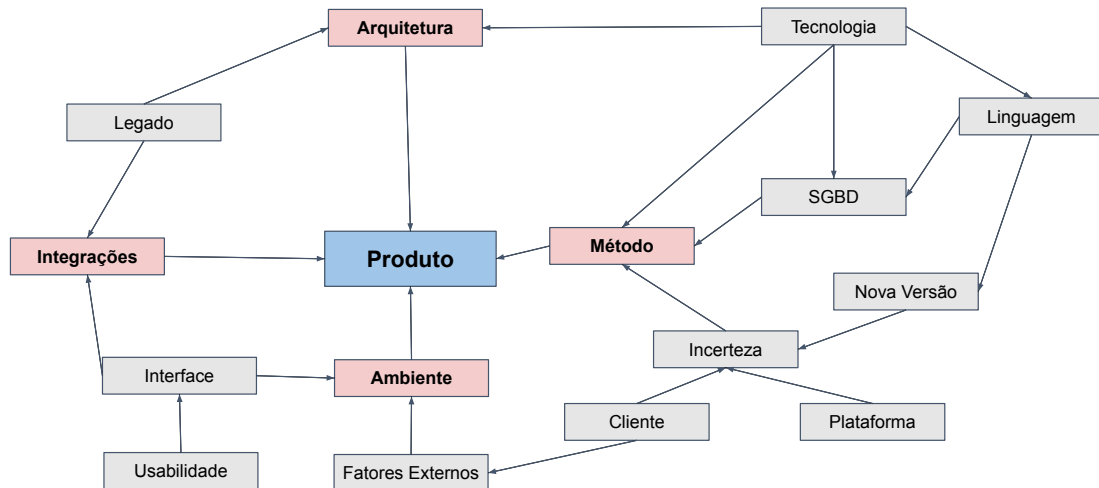


Figura 4.3: Codificação Seletiva para categoria “Produto”.

A codificação seletiva foi realizada em todas as categorias identificadas no estudo. Ao final deste processo, uma listagem dos principais códigos para cada categoria foi registrado. Os códigos restantes não são descartados, eles ficam arquivados e servem de consulta para explanar com mais detalhes cada categoria criada. O processo se encerra realizando a integração das categorias para definição da teoria emergente.

#### 4.2.4 Teoria

Na Figura 4.4 é apresentada a teoria criada após a análise das entrevistas nos diversos ciclos de codificação. O diagrama que representa a teoria criada serve de visão geral das principais características do fenômeno analisado, uma vez que é possível identificar as relações entre as categorias e os códigos. Após a análise realizada, os fatores de riscos em projetos de software foram divididos em três categorias: “Negócio”, “Execução” e “Técnica”.

A categoria “Negócio” tem duas subcategorias: “Cliente” e “Requisitos”. A subcategoria “Cliente” envolve os fatores de risco relacionados à parceria com o cliente do projeto. Portanto, exemplos de fatores de riscos desta subcategoria são: falta de suporte, atraso de

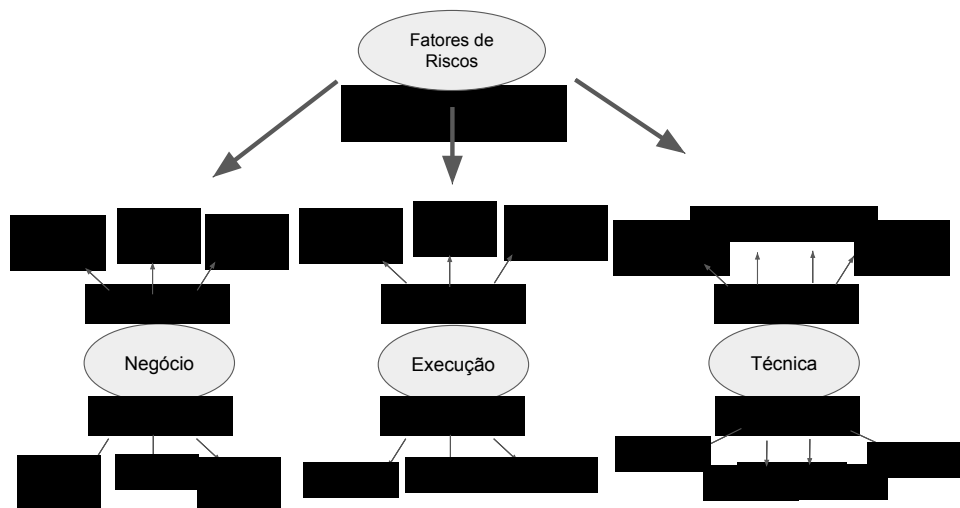


Figura 4.4: Teoria sobre fatores de riscos em projetos de software.

*feedback* e conflito de interesses nos múltiplos *stakeholders*. Sobre a subcategoria “Requisitos”, os fatores de risco identificados são: requisitos incertos, mudanças excessivas e falta de critérios de aceitação.

A categoria “Execução” é composta por fatores de risco relacionados à “Equipe” e ao “Ferramental”. Os principais fatores de riscos de “Equipe” são: falta de experiência, rotatividade e motivação. Por outro lado, os fatores de risco do “Ferramental” estão relacionados à capacidade em dar suporte aos processos da organização, pois para esta subcategoria, foram identificados os fatores: baixa usabilidade, dificuldade de acesso às informações históricas e poucas opções para apresentarem indicadores.

Finalmente, a categoria “Técnica” representa os fatores relacionados às subcategorias “Pesquisa” e “Produto”. Em “Pesquisa”, são analisados riscos das atividades de pesquisa do projeto. Os fatores de risco desta subcategoria são: solução proposta, aplicabilidade da solução, motivação científica e aspectos de validação. E na subcategoria “Produto”, estão fatores de risco relacionados às características tecnológicas para desenvolvimento do produto. São fatores de risco: a integração de sistemas, restrições arquiteturais, método implementado e o ambiente de desenvolvimento.

Os resultados do GT sugerem que profissionais de diferentes empresas compartilham um entendimento semelhante dos fatores de risco dos projetos de software. Ao analisar a teoria, percebe-se que os fatores de riscos relacionados às categorias “Negócio” e “Execução”

possuem semelhanças com fatores de risco apresentados nos trabalhos relacionados analisados no Capítulo 3. Porém, a teoria amplia a literatura existente, apresentando os fatores de riscos da categoria “Técnica”. Na Figura 4.4 apresentam-se apenas as informações centrais. Para cada fator de risco ilustrado, um conjunto de outros fatores correlacionados podem ser rastreados como resultado do estudo qualitativo realizado. Em especial, a subcategoria “Produto” contém os fatores de risco relacionados às características tecnológicas de projetos de software. Estes fatores de riscos foram filtrados e analisados para construção da Rede Bayesiana descrita no Capítulo 5.

### 4.2.5 Ameaças à Validade

O estudo qualitativo GT apresentado neste Capítulo possui ameaças à validade do tipo interna e externa. Com relação à ameaça interna, destaca-se o problema da elicitação dos conceitos ser realizada por um único profissional. Apesar de ser um especialista com vasta experiência na área, não há como garantir que outros especialistas, ao realizar os procedimentos de codificação, criassem a mesma estrutura para representar a teoria. Para minimizar esta ameaça, durante as etapas de codificação outros dois especialistas foram consultados para validar os códigos, axiomas e categorias.

A ameaça externa se deve à falta de resultados empíricos comprovando a completude dos fatores de riscos apresentados na teoria. Os fatores das categorias “Negócio” e “Execução” estão presentes nos trabalhos relacionados. Por outro lado, os fatores de risco da categoria “Técnica” são informações novas resultado da análise desta pesquisa. Porém, não se pode garantir que estes fatores representam a realidade dos riscos de todos os projetos de software. Para minimizar esta ameaça, no estudo GT os especialistas consultados foram encorajados a recordar de fatores de riscos de projetos passados em outras organizações onde já atuaram. Portanto, buscou-se uma amostra mais significativa dos fatores de riscos elicitados no estudo.



# Capítulo 5

## Abordagem Proposta

A abordagem proposta é baseada na utilização de Redes Bayesianas para dar suporte ao prognóstico de riscos tecnológicos em função das tecnologias dos projetos de software. A rede também realiza prognósticos dos riscos em função das estratégias de mitigação. O objetivo é diminuir a subjetividade do gerenciamento de riscos modelando fatores de risco relacionados às características tecnológicas com viés para projetos de inovação.

Na Seção 5.1 são descritas as motivações para a escolha de Redes Bayesianas como técnica deste trabalho. A estrutura da Rede Bayesiana proposta está descrita na Seção 5.2, com detalhes para os fragmentos que compõem o Grafo Acíclico Dirigido. Na Seção 5.3 é apresentado um processo para modelagem e adaptação da Rede Bayesiana para diferentes contextos de projetos. Na Seção 5.4 é apresentada uma ferramenta que implementa a abordagem proposta, facilitando o uso da RB no dia a dia das organizações. Por fim, na Seção 5.5 são apresentadas conclusões do capítulo.

### 5.1 Motivações para escolha de Redes Bayesianas

As motivações para a escolha de Redes Bayesianas são descritas a seguir:

- **Ausência de Dados Históricos** - As características tecnológicas utilizadas na modelagem da abordagem tem alta volatilidade, ou seja, as variáveis mudam com frequência. Isso dificulta a criação de uma base histórica para usarmos técnicas conhecidas de análise de dados. Com Redes Bayesianas podemos fazer uso de especialistas para modelagem da solução e não depender exclusivamente de dados históricos [76, 127].

- **Estrutura de Raciocínio** - No gerenciamento de riscos, indicadores são importantes para diminuir a subjetividade na identificação e mensuração dos eventos. As Redes Bayesianas, além de apresentar indicadores, possuem também uma interface gráfica que facilita a comunicação e análise das variáveis possibilitando um aprendizado estrutural [30, 127].
- **Resposta a Novos Dados** - Mudanças de tecnologias são comuns em projetos de software. Os profissionais precisam ser ágeis para tomada de decisão com relação aos riscos conhecidos e para identificar novos riscos do projeto. A Rede Bayesiana é uma técnica eficaz para este cenário porque tem grande flexibilidade para aceitar entradas e fornecer novos resultados [47, 113].
- **Suporte a Dados Incompletos** - Nas primeiras fases dos projetos de software as informações podem ser escassas, um cenário que contribui para uso de Rede Bayesiana. RB é uma técnica com bons resultados ao tratar cenários com dados incompletos, pois as tabelas de probabilidades podem ser configuradas para estes casos [14]. Assim, as decisões podem ser amadurecidas a partir do momento em que novas evidências são determinadas [7].

## 5.2 Estrutura da Rede Bayesiana

A Rede Bayesiana é formada por quatro fragmentos: Núcleo, Tecnologia, Estratégia e Risco Sensível ao Contexto. O fragmento Núcleo é independente de contexto (i.e., contém a estrutura central com fatores de riscos para qualquer projeto de software), os demais fragmentos devem ser adicionados para cada contexto de projeto que deseja modelar-se a abordagem.

A construção do fragmento Núcleo foi conduzida pelo autor desta tese. As informações geradas pelo estudo qualitativo descrito no Capítulo 4 serviram de base para criação do fragmento. Mais especificamente, os fatores de risco presentes na subcategoria “Produto” da teoria emergente foram utilizados na modelagem, pois estes fatores representam os riscos tecnológicos de projetos de software. A Figura 5.1 apresenta o fragmento Núcleo.

Como pode ser observado na Figura 5.1, a modelagem do fragmento Núcleo seguiu uma hierarquia. O nó raiz corresponde ao risco tecnológico do projeto, enquanto que os nós

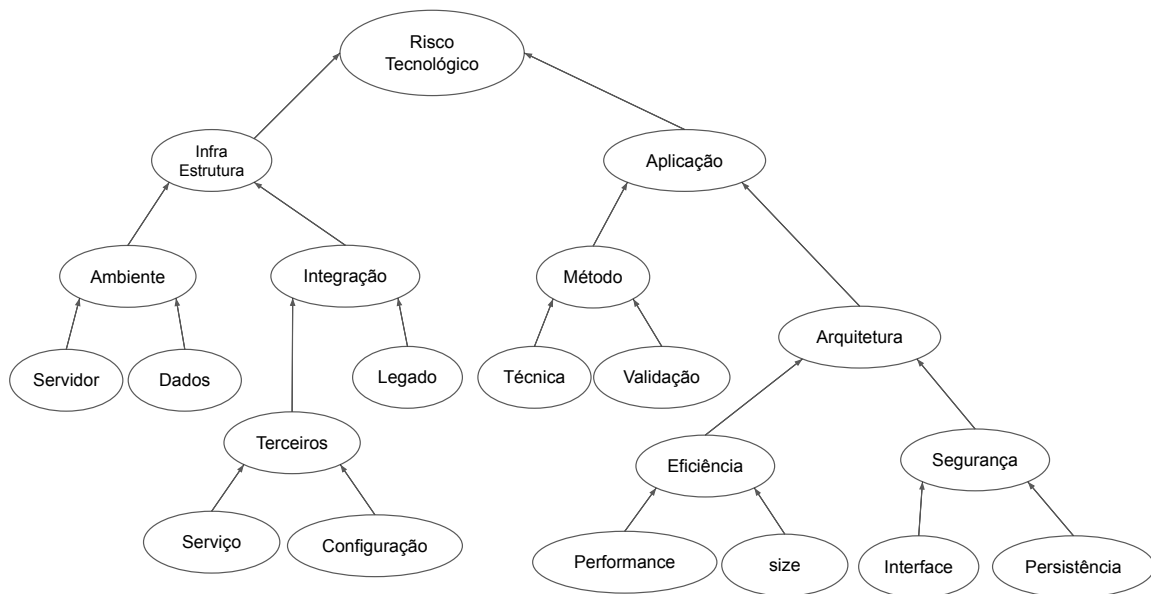


Figura 5.1: Fragmento Núcleo da RB

intermediários são fatores de riscos em diferentes níveis. Os fatores de riscos mais abstratos foram modelados próximos à raiz da rede, enquanto que os nós folhas são representações mais objetivas de riscos. Todos os nós do fragmento Núcleo representam fatores de risco, enquanto que cada nó pai é resultado dos riscos representados pelos nós filhos.

O nó raiz “Risco Tecnológico” é resultado dos nós filhos “Infraestrutura” e “Aplicação”. O primeiro representa o risco de todo arcabouço de ambiente e sistemas que dão suporte ao projeto. Enquanto que o segundo representa o risco de implementação da aplicação. Seguindo a rede, abaixo do nó “Infraestrutura” estão os riscos de “Ambiente” e “Integração”; enquanto que os nós filhos de “Aplicação” são os nós “Arquitetura” e “Método”.

O nó “Ambiente” refere-se ao risco com o ambiente de desenvolvimento, tendo como filhos os nós de “Servidor” e “Dados”. Estes representam, respectivamente, os riscos de conexão e execução de tarefas no servidor, e o risco com o uso de dados e artefatos do cliente para subir a aplicação. Por outro lado, o nó “Integração” representa o risco de integração com sistemas externos, pois este nó tem como filhos os nós “Legado” e “Terceiros” que representam, respectivamente, os riscos de integração com sistemas legados do cliente e de integração com plataformas externas de terceiros. Por fim, como resultado do risco de “Terceiros”, temos os riscos de “Serviço” e “Configuração”, que representam, respectiva-

mente, o risco de consumir serviços de plataformas externas e o risco de compatibilidade no versionamento com a plataforma.

O nó “Arquitetura” refere-se ao risco arquitetural para desenvolvimento da aplicação. Este tem como filhos nós que representam restrições em nível de “Segurança” e “Eficiência”. Para o nó “Segurança”, os nós filhos são “Interface” e “Persistência” que representam, respectivamente, riscos de confiabilidade e integridade dos dados. Para o nó “Eficiência”, os nós filhos são “Size” e “Performance” que representam riscos relacionados ao tamanho de recursos necessários (e.g, memória, disco) e restrições de desempenho (e.g, quantidade de usuários, simultaneidade de operações), respectivamente. Como filhos do nó “Método”, temos os riscos de “Técnica” e “Validação”, que representam o risco com a técnica implementada (e.g, implementar um algoritmo de IA, codificar uma rede Blockchain) e o risco relacionado a validação no uso de ferramentas de *delivery* e *deploys* do sistema. Para mais detalhes, no Apêndice C é apresentado um catálogo onde são descritos todos os nós do fragmento Núcleo.

Os nós folhas deste fragmento (i.e., Servidor, Dados, Serviço, Configuração, Legado, Técnica, Validação, *Size*, Performance, Interface e Persistência) são os pontos de conexão dessa estrutura com os demais fragmentos da abordagem. Na Tabela 5.1 é apresentado uma descrição destes nós folhas do fragmento Núcleo. Enquanto que na Figura 5.2 é apresentada uma perspectiva de como estes nós devem ser conectados com os nós dos demais fragmentos da Rede Bayesiana.

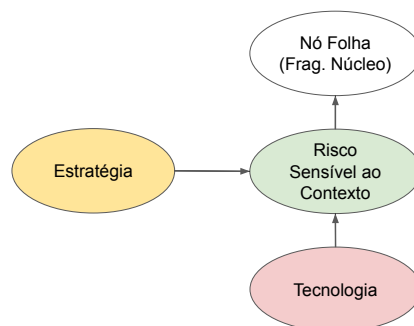


Figura 5.2: Conexão dos fragmentos da Rede Bayesiana

Na Figura 5.2, o nó folha do fragmento núcleo (branco) está conectado ao nó de risco sensível ao contexto (verde), uma vez que este possui conexão com nós de tecnologia (ver-

Tabela 5.1: Descrições dos nós folha do Fragmento Núcleo.

Nó	Descrição
Servidor	este nó representa o risco com o servidor de aplicação do projeto - a conexão, a execução de tarefas e configuração do servidor.
Dados	este nó representa o risco com os dados do projeto - a integridade, disponibilidade e durabilidade dos dados.
Serviço	Este nó representa o risco em usar serviços de terceiros - instabilidade de tecnologias, erro de comunicação.
Configuração	Este nó representa o risco com a configuração do sistema com plataformas externas - falha de compatibilidade, integração e versionamento.
Legado	Representa o risco de integração do sistema com sistemas legado do cliente - acesso a funcionalidades, método de comunicação e de troca de dados.
Técnica	Este nó representa o risco com a técnica implementada - treinar um modelo preditivo de ML, codificar uma rede Blockchain.
Validação	Este nó representa o risco com a validação da aplicação - ferramentas de deliveries, publicação do sistema, necessidade de dados.
Performance	Representa o risco relacionado ao número de usuários que acessarão o sistema, simultaneidade de operações, desempenho na realização de operações.
Size	Este nó representa o risco relacionado ao tamanho das tabelas, uso de memória, necessidade de cache.
Interface	Este nó representa o risco de segurança em nível de interface - autenticação dos usuários, disponibilidade dos dados.
Persistência	Este nó representa o risco de segurança em nível de banco - integridade dos dados.

melho) e estratégia (amarelo). Este relacionamento está alinhado com o processo de modelagem de causa-consequência descrito por Fenton e Neil [31]. As tecnologias são gatilhos para os riscos modelados, e as estratégias são eventos de mitigação objetivando diminuir a probabilidade de ocorrência dos riscos.

Os nós de tecnologia, estratégia e risco sensível ao contexto devem ser adicionados de acordo com um contexto de projeto de software. Sendo assim, a definição do contexto é importante porque existem restrições técnicas específicas que precisam ser modeladas para cada realidade do projeto. O contexto pode estar relacionado, por exemplo, ao domínio do projeto (e.g., Mobile, Web, IoT), sistema operacional (e.g., Android, IOS) ou finalidade de execução (e.g., protótipo, produto).

Os riscos sensíveis ao contexto são eventos específicos e recorrentes para realidade de um contexto de projeto de software. As tecnologias são os *frameworks*, APIs, bibliotecas, serviços e linguagens que dão suporte ao desenvolvimento do projeto. E as estratégias são recomendações, boas práticas ou procedimentos técnicos que podem ser adotados para diminuir a probabilidade de ocorrência dos riscos. A modelagem é aberta, um nó de tecnologia pode ser conectado a vários riscos sensíveis ao contexto, e o risco pode ter várias estraté-

gias de mitigação associadas. Para ilustrar os fragmentos que compõem a Rede Bayesiana será apresentado a seguir uma possível modelagem a partir do nó folha “Persistência” do fragmento Núcleo. Inicialmente o exemplo será no contexto de projetos para dispositivos móveis. Neste cenário, o risco sensível ao contexto “Falha na persistência offline” é comum devido a limitações de recursos computacionais dos dispositivos. A Figura 5.3 ilustra a modelagem para este exemplo.

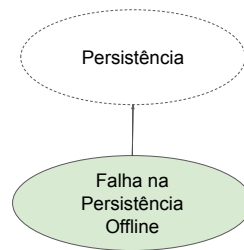


Figura 5.3: Exemplo de nó risco sensível ao contexto conectado ao fragmento Núcleo

Para complementar o exemplo ilustrado na Figura 5.3, sabe-se que o risco supracitado é comum quando: usam-se bibliotecas que abstraem o SGBD principal ao realizar persistência de quantidades não triviais de dados estruturados (e.g, com uso da biblioteca Room); e existem notificações em múltiplas plataformas (e.g, com uso do Firebase do Google). A Figura 5.4 complementa o exemplo mostrado na Figura 5.3 conectando os nós tecnologias “Room” e “Firebase” ao nó do risco sensível ao contexto “Falha na persistência offline”.

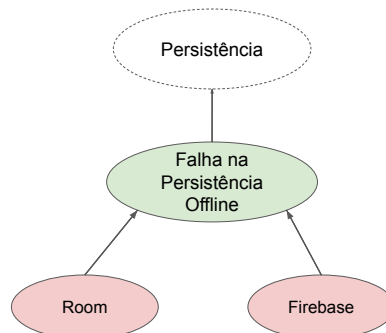


Figura 5.4: Exemplo de nós tecnologias conectadas a um risco sensível ao contexto

Para finalizar o exemplo de modelagem apresentado na Figura 5.4, sabe-se que para uma estratégia mitigar o risco supracitado é necessário ativar a persistência em disco. Desta

forma, mesmo que o sistema operacional seja reiniciado os dados não serão perdidos. A Figura 5.5 complementa o exemplo mostrado na Figura 5.4 conectando o nó estratégia “Ativar persistência em disco” ao nó do risco sensível ao contexto “Falha na persistência offline”.

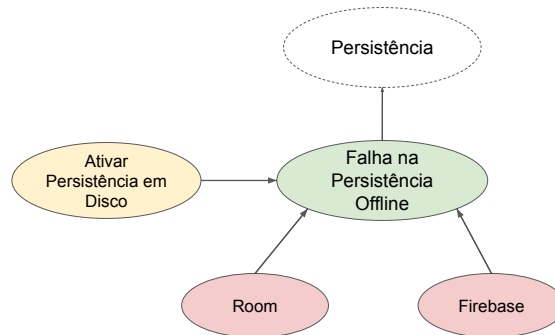


Figura 5.5: Exemplo de nó estratégia conectado a um risco sensível ao contexto

As Figuras 5.3, 5.4 e 5.5 ilustram um exemplo de modelagem para o contexto de projetos móveis a partir do nó “Persistência” do fragmento Núcleo. A seguir, será apresentado um exemplo similar, mas para o contexto de projetos Web. Neste cenário, o risco sensível ao contexto “Falha no mapeamento de objetos” é comum em projetos Web que utilizam diferentes tecnologias de armazenamento de dados. A Figura 5.6 ilustra a modelagem para este exemplo.



Figura 5.6: Exemplo de nó risco sensível ao contexto conectado ao fragmento Núcleo

Para complementar o exemplo ilustrado na Figura 5.6, sabe-se que o risco supracitado é comum quando: usa-se dados semiestruturados em bancos NoSQL; utiliza-se um padrão para mapeamento objeto-relacional com especificação JPA (e.g., com uso de Hibernate); e faz-se uso de Spring para unificar o acesso ao banco. A Figura 5.7 complementa o exemplo

mostrado na Figura 5.6 conectando os nós tecnologias “NoSQL”, “Hibernate” e “Spring” ao nó do fragmento risco sensível ao contexto “Falha no mapeamento de objetos”.

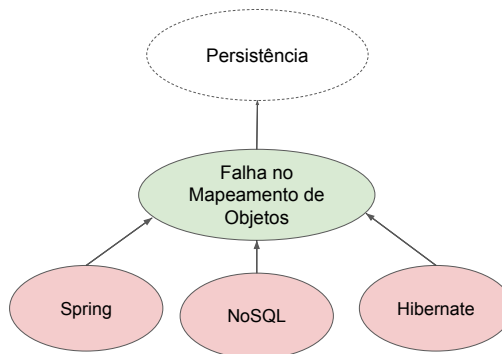


Figura 5.7: Exemplo de nós tecnologias conectadas a um risco sensível ao contexto

Para finalizar o exemplo de modelagem apresentado na Figura 5.7, sabe-se que uma estratégia para mitigar o risco supracitado é escrever as consultas ao banco em anotações nos métodos DAO (*Data Access Objects*). Desta forma, as consultas são compiladas assim que o contexto da aplicação é criado e não apenas na primeira vez que a consulta é utilizada. A Figura 5.8 complementa o exemplo mostrado na Figura 5.7 conectando o nó estratégia “Consultas nas anotações DAO” ao nó do fragmento risco sensível ao contexto “Falha no mapeamento de objetos”.

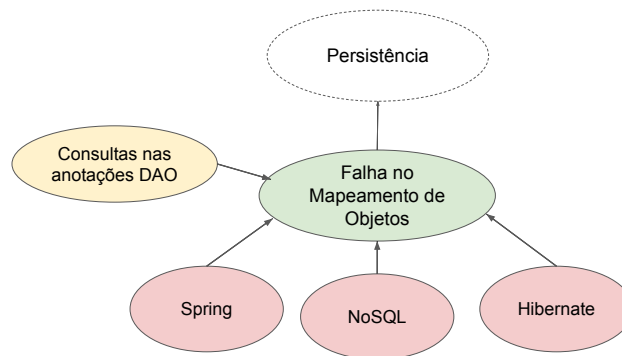


Figura 5.8: Exemplo de nó estratégia conectado a um risco sensível ao contexto

Os exemplos apresentados nesta Seção ilustram a modelagem de nós da abordagem para diferentes contextos de projetos de software. Sendo assim, para utilização da abordagem é necessária a modelagem de tecnologias, estratégias e riscos sensíveis ao contexto. Para que a abordagem seja útil no dia a dia das organizações, o maior número de nós devem ser



definidos a partir dos nós folha do fragmento Núcleo. Para isso, um processo foi criado para ser executado nas organizações com apoio de especialistas e dados históricos.

### 5.3 Processo Proposto

O processo é composto por três atividades: elicitación de conhecimento, mapeamento de nós e simulação de casos reais. Conforme apresentado na Figura 5.9, o processo é cíclico e as atividades devem ser executadas até que a Rede Bayesiana esteja calibrada. Ou seja, este resultado torna-se perceptível quando a abordagem estiver modelada com informações suficientes para representar os riscos de um contexto; e quando a abordagem estiver realizando previsões que façam sentido para os especialistas da organização.

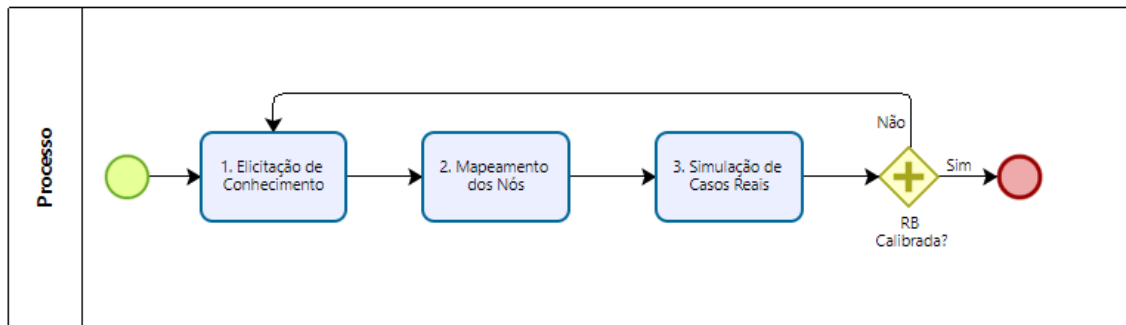


Figura 5.9: Processo para adaptação e modelagem da Rede Bayesiana.

Para executar o processo dois papéis são necessários. O **Consultor Externo** tem a incumbência de garantir que o processo seja entendido, como também é responsável por validar as previsões da abordagem. Enquanto que o **Especialista Interno** é responsável por fornecer as informações técnicas para modelagem da Rede Bayesiana, qualquer profissional da organização pode assumir os papéis. Porém, recomenda-se para Consultor Externo os profissionais de escritórios de projetos (PMO) ou escritórios de qualidade da empresa. Já para o papel de Especialista Interno deve ser encabeçado primordialmente por profissionais com larga experiência técnica (e.g., arquiteto de software, líder técnico ou desenvolvedor sênior).

Na atividade 01 acontece a elicitación de conhecimento para o contexto de projeto previamente definido. O Especialista Interno deve listar os riscos sensíveis ao contexto, tecnologias e estratégias de mitigação. Para elicitar as tecnologias, o Especialista Interno deve listar não apenas as tecnologias com que já trabalhou, mas todas de seu conhecimento para

o desenvolvimento de aplicações para o contexto. É recomendado que seja realizado um *Brainstorming* com times de desenvolvimento para alcançar uma listagem de tecnologias mais completa. Por fim, para elicitar os riscos sensíveis ao contexto e estratégias de mitigação, o Especialista Interno deve realizar consultas a artefatos de projetos encerrados (e.g, planilhas de riscos, declaração de escopo, atas de reuniões) e registros em ferramentas de gestão e desenvolvimento (e.g., notas de entrega, lições aprendidas e *dashboards*). A Tabela 5.2 apresenta um resumo da atividade 01 do processo.

Tabela 5.2: Atividade 01 - Elicitação de Conhecimento

<b>Entrada</b>	Artefatos dos Projetos da Organização
	Registros de Ferramentas de Gestão
	Registros de Ferramentas de Desenvolvimento
<b>Responsável</b>	Especialista Interno
<b>Saída</b>	Lista de Tecnologias
	Lista de Estratégias de Mitigação
	Lista de Riscos Sensíveis ao Contexto

A próxima atividade é fazer o mapeamento dos nós. Inicialmente, o Especialista Interno deve mapear os riscos sensíveis ao contexto com os nós folhas do fragmento Núcleo. Em um segundo momento, ocorre o mapeamento das tecnologias e estratégias com os riscos sensíveis ao contexto. Para executar essa atividade o Especialista Interno deve receber um treinamento preliminar do Consultor Externo sobre a estrutura da Rede Bayesiana descrita na Seção 5.2. Após a modelagem dos nós, o Especialista Interno deve inferir a probabilidade para cada risco sensível ao contexto de acordo com as tecnologias previamente associadas a este risco. Por fim, reavaliar a probabilidade do risco de acordo com as estratégias de mitigação. A Tabela 5.3 apresenta um resumo da atividade 02 do processo.

Tabela 5.3: Atividade 02 - Mapeamento de Nós

<b>Entrada</b>	Lista de Tecnologias
	Lista de Estratégias de Mitigação
	Lista de Riscos Sensíveis ao Contexto
<b>Responsável</b>	Especialista Interno
<b>Saída</b>	Grafo Acíclico Dirigido modelado
	Tabelas de Probabilidades preenchidas
	-

A última atividade da etapa 3 consiste em realizar simulações de casos reais. Esse procedimento deve ser realizado pelo Consultor Externo. As simulações devem ser realizadas avaliando projetos reais da organização. Deve-se comparar os riscos registrados nos projetos com os riscos potenciais identificados pela abordagem. Também devem ser avaliadas as estratégias de mitigação previamente modeladas para estes riscos. O objetivo dessa atividade é avaliar as previsões da Rede Bayesiana. A Tabela 5.4 apresenta um resumo da atividade 03 do processo.

Tabela 5.4: Atividade 03 - Simulações de Casos Reais

<b>Entrada</b>	Grafo Acíclico Dirigido modelado
	Tabelas de Probabilidades preenchidas
	-
<b>Responsável</b>	Consultor Externo
<b>Saída</b>	Riscos identificados pela Rede Bayesiana
	Probabilidades dos riscos identificados
	Estratégias de mitigação para os riscos identificados

Desta forma, caso a abordagem não esteja calibrada, o processo deve ser reiniciado para realização de ajustes, assim as probabilidades podem ser reavaliadas e nós podem ser criados ou excluídos. Com a Rede Bayesiana calibrada, a abordagem está pronta para ser usada na organização. Analisando como uma caixa preta, a abordagem realiza prognósticos ao receber informações das tecnologias usadas nos projetos, e como saída apresenta ao usuário riscos potenciais e suas probabilidades. De forma complementar, também é possível realizar prognósticos selecionando estratégias de mitigação para reavaliar as probabilidades dos riscos.

## 5.4 Ferramenta Risk Control

A principal função da ferramenta na perspectiva desta pesquisa é implementar um software que dê suporte à abordagem proposta. A ferramenta denominada *Risk Control* possibilita a operacionalização da Rede Bayesiana nesta pesquisa, facilitando o processo de transferência de tecnologia para a indústria. A ferramenta tem como propósito auxiliar a identificação, mensuração e monitoramento de riscos. O usuário deverá cadastrar projetos informando suas tecnologias, em seguida a ferramenta irá identificar riscos, informar suas probabilidades

e recomendar estratégias de mitigação.

A arquitetura da ferramenta é apresentada na Figura 5.10. Como pode ser observado, *Risk Control* recebe informações de ferramentas de gestão e desenvolvimento. São dados históricos de riscos, tecnologias e estratégias que também podem ser coletados de acordo com a experiência dos especialistas da organização. Na versão atual, essas informações são repassadas de forma manual. Em um momento posterior, pretende-se desenvolver mecanismos para importar dados via JSON (*JavaScript Object Notation*) e assim facilitar a conexão automática com outras ferramentas. Essas informações devem ser coletadas para realizar a modelagem das Redes Bayesianas para cada contexto de projeto na organização.

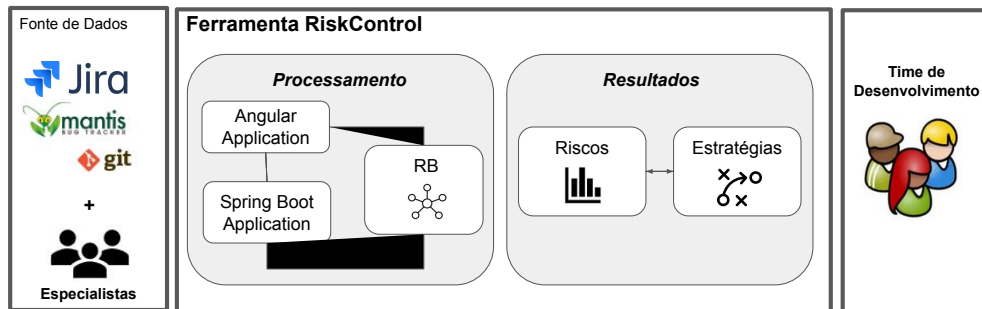


Figura 5.10: Arquitetura da ferramenta Risk Control.

Na Figura 5.10 podemos observar a relação de tecnologias utilizadas no processamento interno da ferramenta. O *backend* da aplicação foi implementada com Spring Boot<sup>1</sup>, nesta camada acontece a integração com a engine SMILE<sup>2</sup> para realização das inferências Bayesianas. A ferramenta é composta também por uma camada de *frontend* desenvolvida em Angular<sup>3</sup>. Através do *frontend* os usuários podem cadastrar projetos informando as tecnologias que serão utilizadas no desenvolvimento. Como resultado do processamento interno com as Redes Bayesianas, a ferramenta apresenta ao time de desenvolvimento os riscos e

<sup>1</sup><https://spring.io/projects/spring-boot>

<sup>2</sup><https://www.bayesfusion.com/smile/>

<sup>3</sup><https://angular.io/>

estratégias de mitigação para o projeto em questão.

Com relação ao modelo de dados, uma versão simplificada é apresentada na Figura 5.11. Um registro na tabela “Projeto” está associado a um item na tabela “Domínio” (i.e., contexto de projeto) e a um conjunto de itens na tabela “Tecnologias-Projeto”. Ou seja, ao cadastrar um projeto na ferramenta *Risk Control*, obrigatoriamente o usuário deve associar o projeto a um domínio e informar as tecnologias a serem utilizadas no projeto. No *backend* da aplicação as tecnologias são utilizadas para instanciar a Rede Bayesiana. Como resultado do processamento, registros são inseridos nas tabelas “Riscos-Projeto” e “Estratégias-Projeto” para futura visualização aos usuários dos riscos e estratégias do projeto em questão.

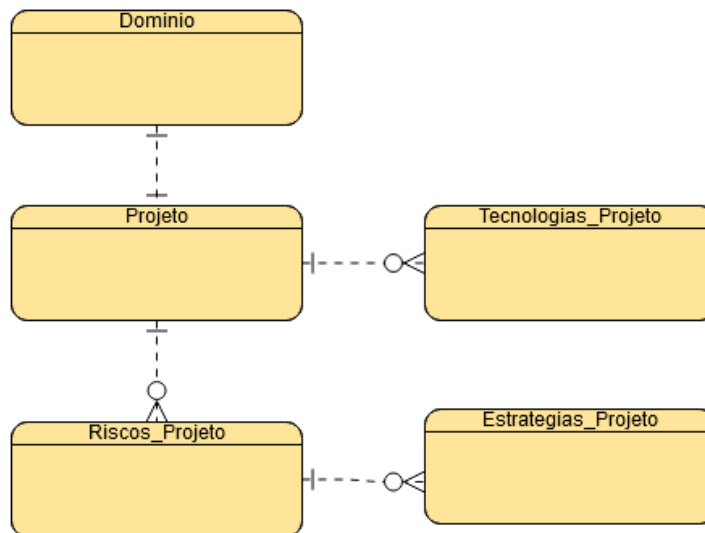


Figura 5.11: Modelo de Dados da ferramenta Risk Control.

Mais detalhes com relação à arquitetura do *Risk Control* (i.e., informações das tecnologias utilizadas e suas dependências, diagrama com os principais componentes, banco de dados) estão no manual do desenvolvedor descrito no Apêndice K. A ferramenta encontra-se na versão beta, atualmente estão sendo implementados mecanismos para facilitar a definição de probabilidades dos riscos. O código do *Risk Control* está disponível publicamente em repositório hospedado no Gitlab <sup>4</sup>.

As funcionalidades da ferramenta estão separadas em dois perfis de usuários: administrador e usuário comum. Para o perfil de administrador, estão disponíveis as operações para

<sup>4</sup>RISK CONTROL: <https://gitlab.virtus.ufcg.edu.br/virtus-softex/>

dar suporte à modelagem da abordagem proposta. Para isso, o administrador tem a opção de realizar os cadastros de tecnologias, riscos e estratégias. Este perfil também é o responsável por realizar o mapeamento destas informações e configurar as probabilidades dos relacionamentos.

Na Figura 5.12 é apresentado uma tela na visão do administrador para cadastro de domínios e tecnologias. Para cada domínio cadastrado, a ferramenta apresenta uma listagem de tecnologias associadas para que o administrador possa adicionar, editar ou remover itens. Na Figura 5.12 é possível visualizar três domínios cadastrados (i.e., Web, Mobile e IoT) e exemplos de tecnologias para o domínio web.

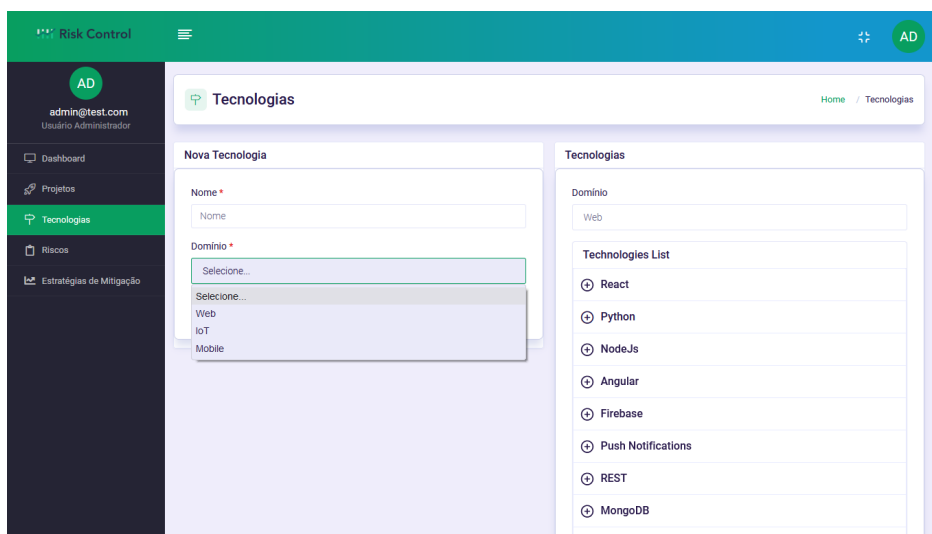


Figura 5.12: Criação de Domínios e Tecnologias.

Com as tecnologias cadastradas para cada domínio, o próximo passo é realizar o cadastro dos riscos. Na Figura 5.13 é apresentado a visão do administrador na ferramenta para esta operação. Para criação de um risco, o administrador informa um “Nome” e uma “Descrição”, além disso deve ser informado um “Tipo” (i.e., a relação do risco com nós do fragmento Núcleo da Rede Bayesiana), e um “Domínio”. Por fim, o administrador deve selecionar as tecnologias que estão associadas a este risco.

Para complementar o cadastro de risco ilustrado na Figura 5.13, o administrador deve informar as probabilidades da relação de tecnologias com o risco cadastrado. A Figura 5.14 apresenta o resultado de um cadastro de risco para o domínio *Mobile*. Na Figura 5.14 pode ser observado as definições de probabilidades para as tecnologias “Ionic” e “Kotlin Corouti-

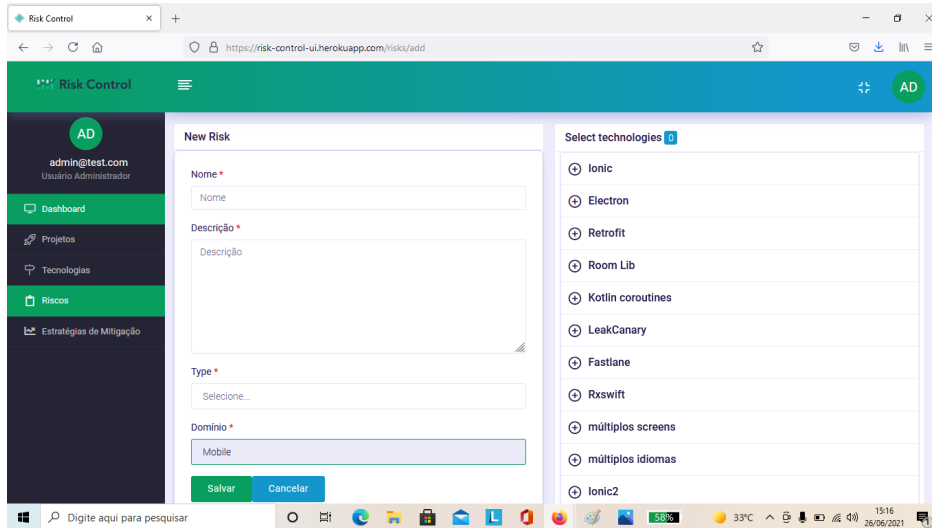


Figura 5.13: Cadastro de Riscos.

nes”. O somatório de valores de probabilidades das tecnologias para cada risco deve ser igual a 100%. No qual essas informações são utilizadas para configuração da Rede Bayesiana.

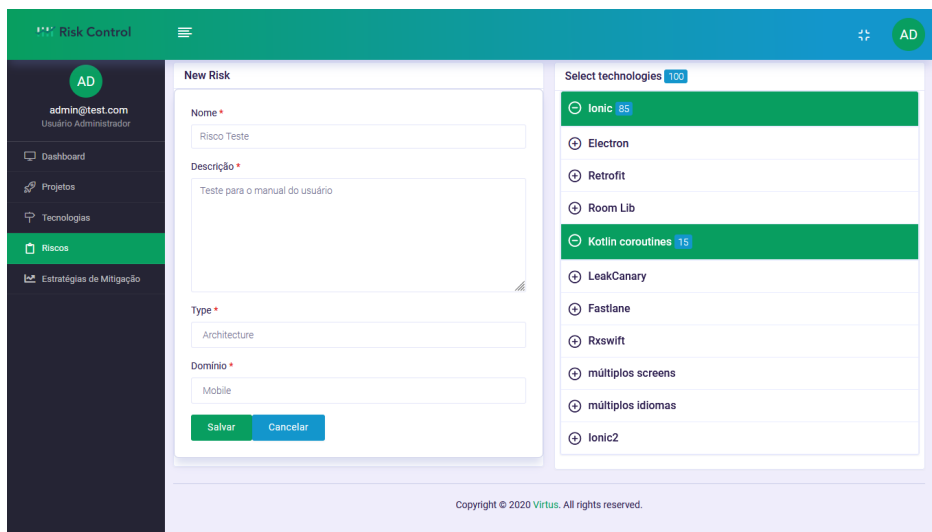


Figura 5.14: Definição de probabilidades para as tecnologias.

Com a Rede Bayesiana modelada, a ferramenta *Risk Control* proporciona ao usuário final o cadastro de projetos. Na Figura 5.15 é possível visualizar o cadastro de um projeto, com os campos “Nome”, “Descrição”, “Domínio”, “Data Inicial” e “Data Final”.

Ao realizar o cadastro, o usuário deve informar as tecnologias a serem utilizadas no desenvolvimento. Na Figura 5.16 é possível visualizar o cadastro de tecnologias para um

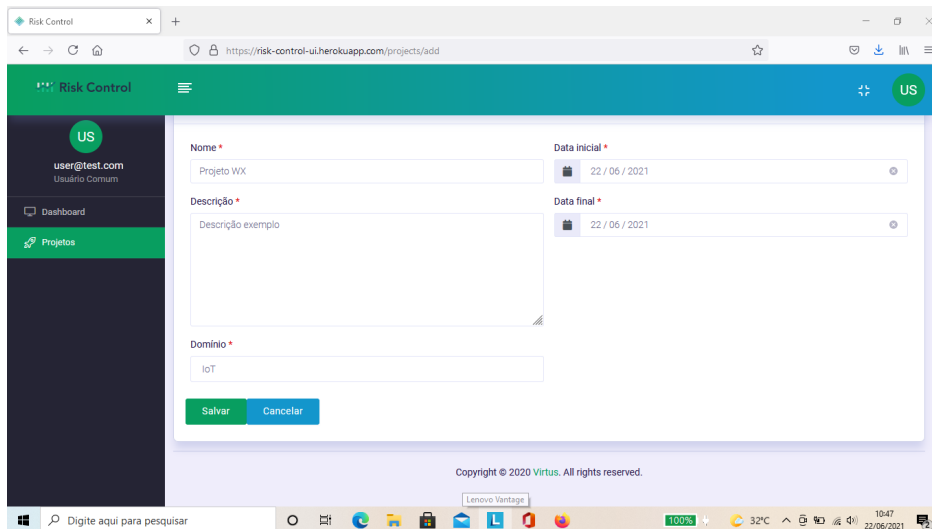


Figura 5.15: Cadastrar Projetos.

projeto de domínio Mobile. Com essas informações, a Rede Bayesiana é instanciada e executada em um processamento interno. Com isso, os riscos do projeto são definidos de acordo com as tecnologias informadas pelo usuário.

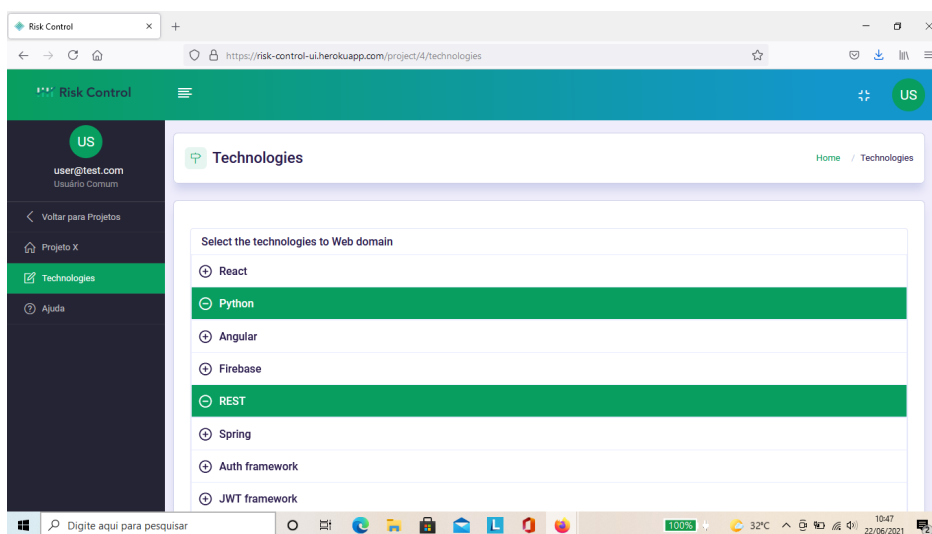


Figura 5.16: Associar tecnologias ao projeto

Por fim, a Figura 5.17 ilustra um exemplo dos riscos recomendados pela ferramenta para um projeto. Nesta Figura também é possível visualizar um *dashboard* com o quantitativo de riscos para os principais eixos da Rede Bayesiana.

Uma descrição completa das funcionalidades da ferramenta *Risk Control* estão no manual



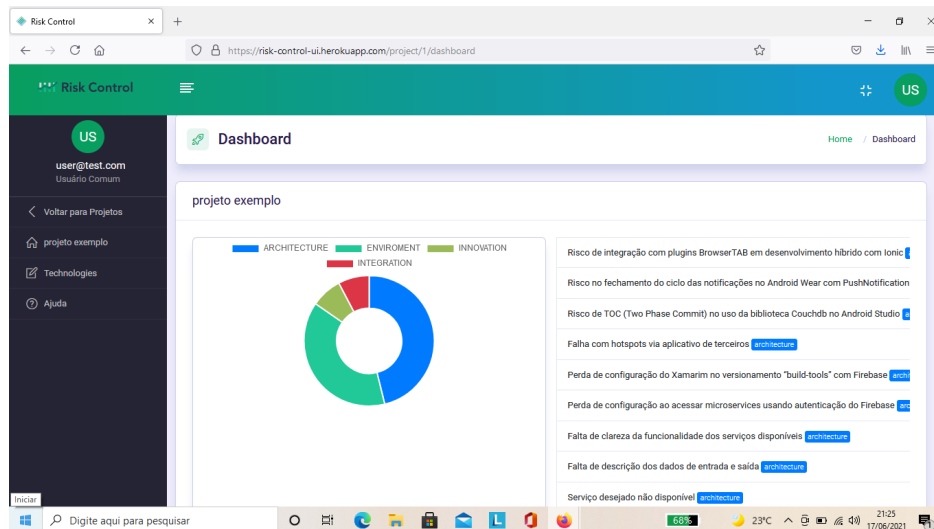


Figura 5.17: Visualização de Riscos

do usuário (Apêndice J). As funcionalidades estão divididas por operações relacionadas à modelagem da Rede Bayesiana (perfil administrador) e operações para uso da ferramenta no dia a dia de empresas de desenvolvimento de software (perfil usuário comum).

## 5.5 Considerações Finais do Capítulo

Neste capítulo, foi descrita a abordagem proposta que visa dar suporte a times de desenvolvimento de software na identificação, mensuração e monitoramento de riscos. A abordagem proposta tem como objetivo diminuir a subjetividade dos processos de gerenciamento de riscos. Para isso, foi construída uma Rede Bayesiana com foco nos riscos tecnológicos de projetos de software. Diferente dos trabalhos do estado da arte, a abordagem proposta neste trabalho modela uma granularidade maior dos fatores de riscos relacionados às características tecnológicas dos projetos.

A Rede Bayesiana é composta por quatro fragmentos: Núcleo, Tecnologias, Estratégias e Riscos Sensíveis ao Contexto. O primeiro é um fragmento independente de contexto com os principais fatores de riscos dos projetos de software. Para os demais, foi proposto um processo para auxiliar a modelagem e adaptação da abordagem em diferentes contextos de projetos.

Por fim, para viabilizar a operacionalização da Rede Bayesiana, como parte do trabalho

foi desenvolvida uma ferramenta para implementação da abordagem proposta, chamada de *Risk Control*. Através da ferramenta é possível modelar as tecnologias para um determinado contexto de projeto, visualizar os riscos e realizar intervenções no modelo. A abordagem proposta neste trabalho pode ser aplicada a qualquer projeto de software, mas será validada em projetos de inovação nos quais as características tecnológicas são mais presentes.

# Capítulo 6

## Validação da abordagem

Na Seção 6.1 são apresentados detalhes da modelagem da Rede Bayesiana em uma organização. O contexto escolhido foi de projetos de desenvolvimento para dispositivos móveis. Em seguida foi realizada uma validação estática [41] com seis cenários de simulação. Os cenários representam casos reais de projetos deste contexto. Em cada cenário, os riscos e estratégias recomendados pela abordagem foram avaliadas por oito profissionais da organização através de um *Focus Group* [65]. Por fim, a validação dinâmica da abordagem é realizada por meio de um experimento, no qual evidências correspondentes a dados de seis projetos reais da organização são inseridas na RB e uma avaliação é realizada comparando as predições da rede e o entendimento de profissionais dos projetos. Os detalhes da validação estática e dinâmica estão nas seções 6.2 e 6.3, respectivamente.

### 6.1 Modelagem da Rede Bayesiana

A organização escolhida para aplicação do processo foi o Núcleo de Pesquisa, Desenvolvimento e Inovação em Tecnologia da Informação, Comunicação e Automação (VIRTUS<sup>1</sup>) da Universidade Federal de Campina Grande (UFCG). O contexto utilizado para modelagem da abordagem foram projetos de desenvolvimento para dispositivos móveis. A motivação para escolha está na experiência dos profissionais que colaboraram na pesquisa e na quantidade de projetos desse contexto em execução na organização.

O processo descrito no Capítulo 5 foi executado pelo autor desta tese com apoio de três

---

<sup>1</sup>VIRTUS: <http://virtus.ufcg.edu.br/>

profissionais do VIRTUS. Para o papel de Especialista Interno, um arquiteto foi escolhido. O profissional possui mais de dez anos de experiência no desenvolvimento de projetos de software, sendo metade em projetos para dispositivos móveis. Para executar as atividades do processo, o Especialista Interno contou com apoio de outros dois profissionais, sendo um arquiteto e um desenvolvedor sênior. Para Consultor Externo, o autor desta tese assumiu o papel na execução do processo. O autor possui oito anos de experiência em fábricas de software, sendo três anos como gerente de projetos. Mais detalhes sobre a execução do processo estão na Subseção 6.1.1. Por fim, ameaças à validade da modelagem da Rede Bayesiana são apresentadas na Subseção 6.1.2.

### 6.1.1 Execução do Processo

Para a atividade 01 do processo (i.e., elicitação do conhecimento), o primeiro passo foi listar as tecnologias de projetos para dispositivos móveis. Para tal, o Especialista Interno realizou um *Brainstorming* com os outros dois profissionais da organização que colaboraram com essa etapa da pesquisa. Ao final, trinta e uma tecnologias foram listadas, entre *frameworks*, bibliotecas e APIs (Apêndice D). Em seguida, o Especialista Interno rastreou os riscos sensíveis ao contexto para projetos desse contexto. Para isso foram avaliados artefatos e registros de ferramentas de sete projetos encerrados da organização. Ao todo, vinte e dois riscos foram listados (Apêndice E). Por fim, foram definidas estratégias para mitigação dos riscos previamente listados (Apêndice F). A maioria das informações elicidadas foram com o consenso do Especialista Interno com os demais profissionais que colaboraram com a pesquisa. Para os casos em que existiu divergência, optou-se por manter todas as variáveis possíveis e avaliá-las durante a validação da abordagem.

As listas de tecnologias, riscos e estratégias são entradas para a atividade 02 do processo (i.e, mapeamento de nós). Inicialmente o Consultor Externo apresentou ao Especialista Interno a descrição dos nós do fragmento Núcleo conforme catálogo descrito no Apêndice C. Em seguida, para cada nó folha do fragmento Núcleo os riscos sensíveis ao contexto foram mapeados e o próximo passo foi mapear as tecnologias com os riscos sensíveis ao contexto. Para essa atividade foi utilizado o entendimento de Fenton e Neil [31]: as tecnologias foram avaliadas como gatilhos para os riscos previamente modelados. Por fim, as estratégias de mitigação previamente listadas foram conectadas aos riscos sensíveis ao contexto.

Com o Grafo Acíclico Dirigido modelado, o próximo passo consiste em preencher as tabelas de probabilidades. Para evitar complexidade no processo de coleta de dados, optou-se por utilizar nós *booleanos* para representar todos os estados dos nós da rede. Com relação à escala, a classificação de Renooij [93] foi adotada, na qual escala permite que os especialistas verbalizem sua opinião em sete opções de respostas. Dada a disponibilidade do Especialista Interno e dos dois outros profissionais, optou-se por preencher as tabelas manualmente sem auxílio de algoritmos de otimização [34, 52, 88]. Perguntas eram realizadas aos especialistas para elicitarem as probabilidades de todos os nós intermediários da rede. Para cada nó, os especialistas informavam a probabilidade dos nós serem TRUE dadas as evidências dos nós filhos. A maioria das variáveis elicitadas foram consenso do Especialista Interno com os demais profissionais que colaboraram com a pesquisa. Para os casos em que existiu divergência, optou-se por manter o valor mais alto de probabilidade e avaliá-la durante a validação da abordagem.

Para a última atividade do processo (i.e., simulação de casos reais) foram consultados artefatos de cinco projetos do mesmo contexto que a abordagem foi modelada. O Consultor Externo instanciou a Rede Bayesiana com as tecnologias de cada um dos projetos. Em seguida, com apoio do Especialista Interno, os riscos calculados pela rede foram comparados com os registros de riscos desses projetos. Com isso, uma calibração nas tabelas foi realizada para que a abordagem represente de forma precisa os riscos de projetos desse contexto na organização. Por fim, foi definido o limiar de 50% para representar os riscos potenciais aos projetos segundo a Rede Bayesiana (i.e., de acordo com a abordagem, sempre que um nó intermediário possuir uma probabilidade maior ou igual que 50% em ser TRUE, o risco correspondente deve ser avaliado pela equipe).

Neste trabalho, o processo foi executado apenas uma vez, mas para o uso no dia a dia das organizações a abordagem deve ser atualizada com frequência para melhores resultados. No Apêndice G é apresentada a versão final da Rede Bayesiana modelada com todos os nós: riscos do fragmento núcleo (cor branca), riscos sensíveis ao contexto (cor verde), tecnologias (cor rosa) e estratégias (cor amarela). Por questões de espaço, as imagens foram divididas em quatro partes, de acordo com os principais eixos da rede (i.e., integração, arquitetura, ambiente e método).

*RQ1: Quais são os fatores de riscos tecnológicos relevantes na construção de uma Rede Bayesiana na modelagem para auxiliar o gerenciamento de riscos em um projeto de software?.* No Capítulo 5 foi apresentado o fragmento núcleo da RB com os fatores de riscos centrais relacionados às características tecnológicas de um projeto de software. Nesta seção a Rede Bayesiana foi modelada com informações de tecnologias, estratégias e riscos sensíveis ao contexto de projetos de desenvolvimento para dispositivos móveis. A abordagem realiza prognósticos dos riscos e suas probabilidades de acordo com as tecnologias usadas nos projetos. De forma complementar, também é possível realizar prognósticos selecionando estratégias de mitigação para reavaliar as probabilidades dos riscos. Desta forma, as características tecnológicas utilizadas na modelagem reduzem as subjetividades nas atividades de identificação, mensuração e monitoramento de riscos.

### 6.1.2 Ameaças à Validade

Com relação à construção da Rede Bayesiana, há quatro tipos de ameaça à validade: interna, externa, conclusão e de confiabilidade. A ameaça de conclusão se deve à falta de resultados empíricos comprovando a causalidade entre os fatores de riscos modelados na Rede Bayesiana. Desta forma, não se pode garantir que as entidades são mensuradas corretamente pelo modelo. Para minimizar esta ameaça, os especialistas consultados para modelagem da abordagem possuem vasta experiência em projetos de software no contexto escolhido para construção da Rede Bayesiana. Com relação à ameaça interna, destaca-se o problema de modelagem da abordagem para realidade da organização. Apesar da consulta com especialistas com vasta experiência, não há como garantir que outros especialistas, ao construir um modelo para o mesmo contexto, selecionasse as mesmas variáveis e preenchesse de forma idêntica as TPNs.

Para a ameaça externa, não existem garantias de que o modelo definido para uma organização possa ser reaproveitado por outras organizações que desenvolvem software do mesmo contexto. Desta forma, para minimizar a ameaça, a abordagem foi construída a partir de um fragmento núcleo para auxiliar o reaproveitamento de informações. Por fim, para minimizarmos as ameaças à confiabilidade garantimos que os dados coletados fossem revisados pelos participantes do estudo. Os especialistas foram consultados inicialmente de forma

separada para definição dos nós e preenchimento das tabelas de probabilidade. Em um segundo momento foram realizadas reuniões nos quais juntos definiram a versão final da Rede Bayesiana.

## 6.2 Validação Estática

Nesta Seção será apresentada a validação estática da abordagem proposta. De acordo com Gorscheck e Wohlin [41], realizar uma validação estática é vital para identificar os benefícios da solução proposta e obter a adesão dos profissionais. Para este propósito, seguindo uma diretriz da engenharia do conhecimento de Redes Bayesianas [73], desenvolvemos seis cenários simulados em colaboração com dois especialistas do grupo de pesquisa ISE<sup>2</sup>. Posteriormente, realizamos um *focus group* [65] com oito profissionais do VIRTUS para avaliar a utilidade prática da Rede Bayesiana proposta sob a ótica do Modelo de Aceitação de Tecnologia (TAM) [22]. A seguir, nas Subseções 6.2.1 e 6.2.2 são apresentadas as descrições dos cenários e a avaliação da abordagem com o *Focus Group*. Por fim, ameaças à validade da validação estática são apresentadas na Subseção 6.2.3.

### 6.2.1 Descrição dos Cenários

De acordo com as diretrizes da Engenharia do Conhecimento em Redes Bayesianas [74], definir cenários simulados é essencial porque antes de adotar a RB em projetos reais, é necessário obter uma avaliação de quão bem os especialistas “sentem” que o modelo calcula o que deve estimar pelo valor de face [26]. Os cenários simulados são cenários do tipo “e se” representando situações para uso do modelo, estabelecendo um conjunto de entradas e saídas esperadas e comparando-as com as saídas calculadas da Rede Bayesiana.

Dois colaboradores do grupo ISE foram convidados para criar os cenários. O primeiro colaborador tem mais de dez anos de experiência com projetos de software e três anos de experiência com desenvolvimento de aplicativos móveis. O segundo tem mais de cinco anos de experiência com projetos de software e dois anos de experiência com desenvolvimento de aplicativos móveis.

---

<sup>2</sup>ISE: <https://www.virtus.ufcg.edu.br/ise-group/>

Os seis cenários de simulação foram criados no contexto de projetos de desenvolvimento para dispositivos móveis. Cada cenário descreve um projeto de software com exemplos de decisões tecnológicas a serem tomadas por uma equipe de desenvolvimento. Para definir cada cenário, primeiro, foram criados os requisitos de um produto e em seguida, foram discutidas as possíveis tecnologias que poderiam ser adotadas para cumprir os requisitos e os riscos que eles poderiam causar ao projeto. Quando necessário, as probabilidades dos riscos foram discutidas e estratégias foram criadas para mitigar estes riscos. Desta forma, os cenários refletem situações envolvendo a identificação, mensuração e monitoramento de riscos.

### Cenário 01

**Descrição:** *Uma equipe de desenvolvimento de software está na sprint zero de um projeto mobile. O projeto tem as seguintes restrições técnicas definidas pelo cliente: os dados dos usuários devem ser criptografados no cadastro, as requisições durante as operações não podem demorar mais que 500 ms, o aplicativo deve funcionar no IOS e Android, e por fim, a aplicação deve se conectar com plataformas de crédito em tempo real. O líder técnico discute com o time as tecnologias a serem usadas e marca com TRUE os nós folhas correspondentes na Rede Bayesiana: Keystore, Firebase, Ionic, Webservices, Room e Mongoose. Ao finalizar a análise, o líder técnico executa a rede e visualiza as probabilidades calculadas para cada nó intermediário. Alguns nós apresentaram alta probabilidade, o que representa na semântica da rede que são riscos em potencial. Um exemplo é o risco “falha de segurança na persistência offline”. Com os riscos identificados, alternativas são analisadas para garantir o sucesso do projeto. O líder técnico apresenta a possibilidade de não utilizar a biblioteca “Room” para persistência dos dados. Após marcar esse nó como FALSE na Rede Bayesiana, a probabilidade do risco “falha de segurança na persistência offline” diminuiu drasticamente. A equipe irá avaliar a possibilidade de não usar a tecnologia na execução do projeto.*

A Figura 6.1 mostra uma perspectiva da Rede Bayesiana para o cenário 01. O risco sensível ao contexto “falha de segurança na persistência offline” identificado com alta probabilidade tem relacionamento com as tecnologias *Firebase*, *Mongoose* e *Room*. Este risco está conectado ao fragmento núcleo através do nó “Segurança”. O cenário ilustra a retirada



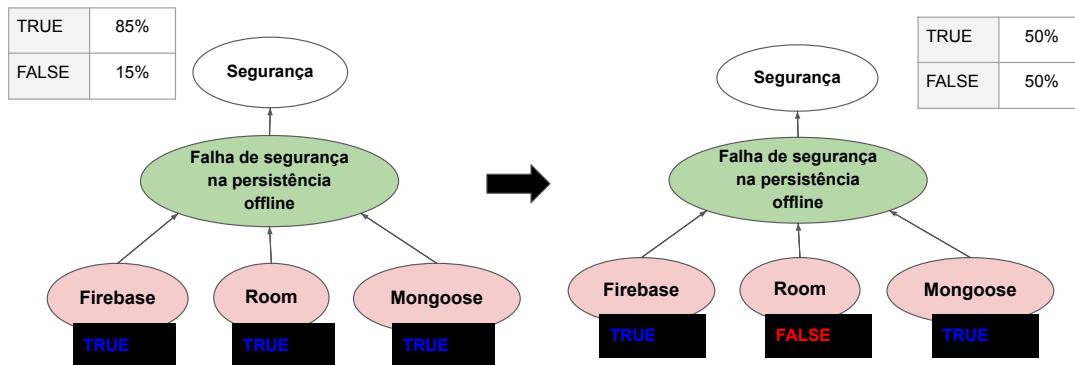


Figura 6.1: Perspectiva da Rede Bayesiana - Cenário 01

da tecnologia *Room* do projeto, uma situação que diminuiria a probabilidade do risco “falha de segurança na persistência offline”. Este cenário mostrou o potencial da Rede Bayesiana em identificar riscos de acordo com as tecnologias adotadas no projeto. A abordagem tem como objetivo auxiliar a tomada de decisão. Desta forma, fica a critério do time analisar a escolha das tecnologias e se o risco é realmente inerente ao projeto.

## Cenário 02

**Descrição:** *Uma equipe de desenvolvimento de software está desenvolvendo um projeto mobile. O projeto tem as seguintes restrições técnicas definidas pelo cliente: a aplicação deve dar suporte ao processamento de alta carga de mídias dos usuários, o usuário poderá aplicar filtros às imagens e visualizar o processamento em menos de 1 segundo, deve existir também um chat para interação de grupos de usuários, por fim, o aplicativo deve funcionar no IOS e Android. O líder técnico está avaliando as tecnologias a serem usadas no projeto para atingir os objetivos com o menor risco possível. O líder técnico discute as tecnologias a serem usadas com a equipe, e marca com TRUE os nós folhas correspondentes dessas tecnologias na Rede Bayesiana: Ionic, Glide, biblioteca Room e Couchdb. Ao finalizar a análise, o líder técnico executa a rede e visualiza as probabilidades calculadas para cada nó inter-*

mediário. Alguns nós apresentaram alta probabilidade, o que representa na semântica da rede que são riscos em potencial. Um exemplo é o risco “falha de conexão para visualizar mídias”. Com essas informações, a equipe avaliou a escolha das tecnologias, marcando novas tecnologias na rede e substituindo algumas das escolhidas inicialmente. Uma possibilidade analisada é trocar a tecnologia *Glide* por *Picasso*, após essa alteração na rede, a probabilidade do nó que representa este risco diminuiu significativamente. O líder técnico junto com a equipe irá avaliar a mudança dessa tecnologia para execução do projeto.

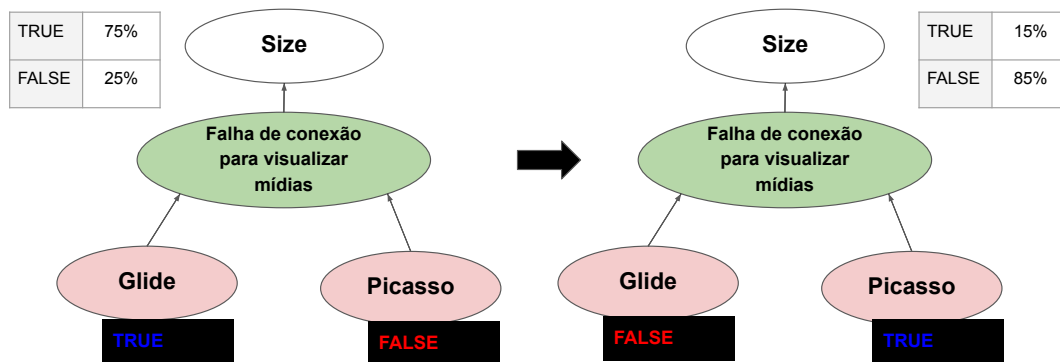


Figura 6.2: Perspectiva da Rede Bayesiana - Cenário 02

A Figura 6.2 mostra uma perspectiva da Rede Bayesiana para o cenário 02. O risco sensível ao contexto “falha de conexão para visualizar mídias” identificado com alta probabilidade tem relacionamento com a tecnologia *Glide*. Este risco está conectado ao fragmento núcleo através do nó *Size*. O cenário ilustra a alteração das tecnologias *Glide* por *Picasso*, uma situação que diminuiria a probabilidade do risco “falha de conexão para visualizar mídias”. Este é mais um cenário onde a Rede Bayesiana pode ser utilizada para identificar riscos de acordo com as tecnologias adotadas no projeto. Assim como no cenário anterior, fica a critério do time analisar a escolha das tecnologias e se o risco é realmente inerente ao projeto.

### Cenário 03

**Descrição:** Um projeto na plataforma mobile está em desenvolvimento por um time que utiliza a metodologia Scrum. Atualmente, a equipe informou que o projeto encontra-se com um risco tecnológico: baixo desempenho das builds. Essa informação corresponde a um nó intermediário da rede. Sabe-se também que as principais tecnologias utilizadas no desenvolvimento são: NodeJs com uso do Firebase, Flavors, JetPack Navigation e LeakCanary. Essas informações foram marcadas como TRUE na Rede Bayesiana e em seguida a rede foi executada e as probabilidades dos nós calculadas. O líder técnico observou a probabilidade do nó correspondente ao risco e avaliou opções na rede marcando como TRUE alguns nós que representam estratégias de mitigação. Em especial ao escolher o nó: colocar depurador no primeiro plano, o risco supracitado diminuiu de probabilidade significativamente. A equipe irá avaliar a recomendação para definir as estratégias de mitigação dos riscos do projeto.

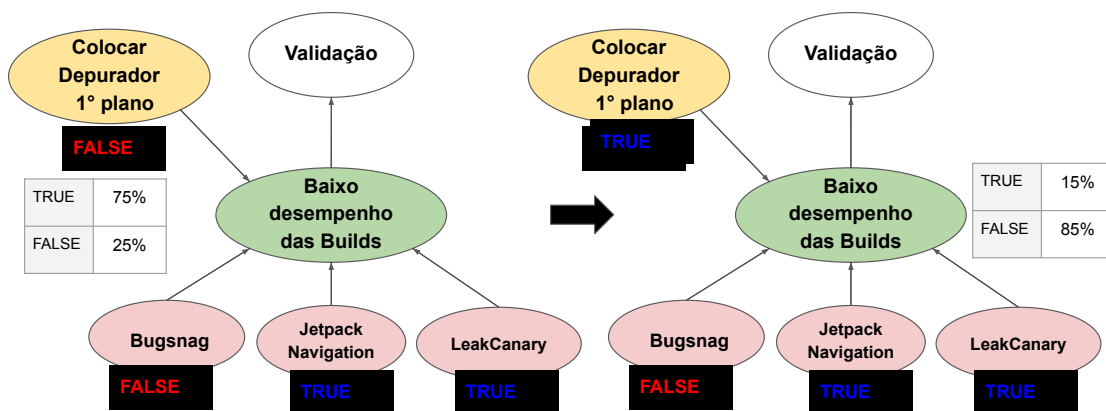


Figura 6.3: Perspectiva da Rede Bayesiana - Cenário 03

A Figura 6.3 mostra uma perspectiva da Rede Bayesiana para o cenário 03. O risco sensível ao contexto “baixo desempenho das builds” está conectado ao nó “Validação” do fragmento núcleo. Neste cenário, as tecnologias associadas ao risco não foram excluídas ou alteradas. Porém, foi avaliada a implementação da estratégia de mitigação “colocar de-

purador no primeiro plano” que reduziu a probabilidade do risco supracitado. Este cenário mostrou o potencial da Rede Bayesiana em recomendar estratégias de mitigação de acordo com riscos identificados pelo time de desenvolvimento, ficando a critério do time analisar se a estratégia precisa ser implementada.

#### **Cenário 04**

**Descrição:** *Um projeto na plataforma mobile está em desenvolvimento por um time que utiliza a metodologia Scrum. Atualmente, a equipe informou que o projeto encontra-se com um risco tecnológico: baixo desempenho na comunicação com microserviços. Essa informação corresponde a um nó intermediário da rede. Sabe-se também que as principais tecnologias utilizadas no desenvolvimento são: webservices e REST na comunicação com legado, Firebase e Ionic. Essas informações foram marcadas como TRUE na Rede Bayesiana e em seguida a rede foi executada e as probabilidades dos nós calculadas. O líder técnico observou a probabilidade do nó correspondente ao risco e avaliou opções na rede marcando como TRUE alguns nós que representam estratégias de mitigação. Em especial ao escolher o nó: Interagir Containers com Kubernetes, o risco supracitado diminuiu de probabilidade significativamente. A equipe irá avaliar a recomendação para definir as estratégias de mitigação dos riscos do projeto.*

A Figura 6.4 mostra uma perspectiva da Rede Bayesiana para o cenário 04. O risco sensível ao contexto “baixo desempenho na comunicação com microserviços” está conectado ao nó “Legado” do fragmento núcleo. Assim como no cenário anterior, as tecnologias associadas ao risco não foram excluídas ou alteradas. Foi avaliada a implementação de uma estratégia de mitigação. Para este cenário a estratégia “Interagir Containers com Kubernetes” reduziu a probabilidade do risco supracitado. Este cenário mostrou o potencial da Rede Bayesiana em recomendar estratégias de mitigação de acordo com riscos identificados pelo time de desenvolvimento, ficando a critério do time analisar se a estratégia precisa ser implementada.

#### **Cenário 05**

**Descrição:** *Uma equipe de desenvolvimento irá participar de um projeto mobile. O principal desafio tecnológico do projeto está no processamento de uma grande base de dados*

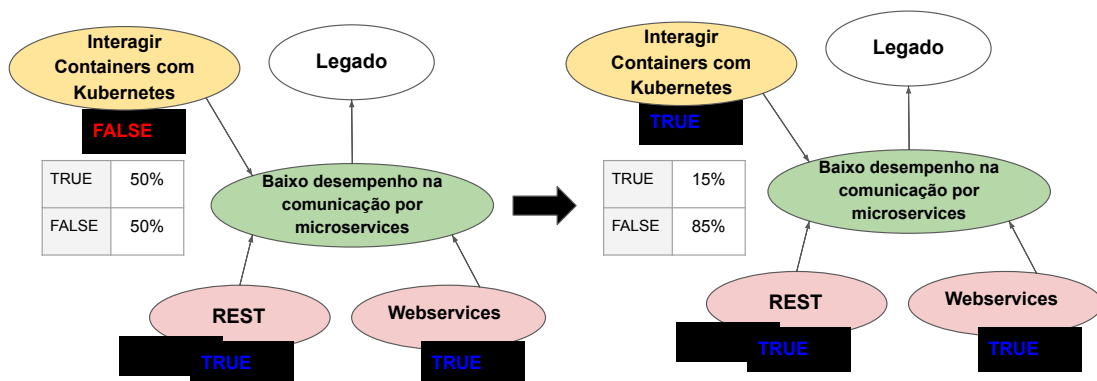


Figura 6.4: Perspectiva da Rede Bayesiana - Cenário 04

em um servidor remoto. O aplicativo deverá apresentar ao usuário informações com alta performance de acordo com a geolocalização do usuário. O líder técnico discute as tecnologias a serem usadas com a equipe, e marca com TRUE os nós folhas correspondentes dessas tecnologias na Rede Bayesiana: Redis, Apache Cassandra, Pandas, Numpy e Flavors. Ao finalizar a análise, o líder técnico executa a rede e visualiza as probabilidades calculadas para cada nó intermediário. Alguns nós apresentaram alta probabilidade, o que representa na semântica da rede que são riscos em potencial. O líder técnico deseja priorizar os riscos para tratar inicialmente os riscos de maior probabilidade. De acordo com a rede, os riscos em ordem do maior para o de menor probabilidade são: “lentidão em operações com vetores alinhados”, “falha na escalabilidade de dados” e “baixo desempenho no uso de sockets”. Com essas informações, a equipe avaliou os riscos e escolheu tratar na sprint zero o risco de maior probabilidade, ou seja, a “lentidão em operações com vetores alinhados”. Estratégias de mitigação serão investigadas para tratar o risco supracitado.

A Figura 6.5 mostra uma perspectiva da Rede Bayesiana para o cenário 05. Os riscos sensíveis ao contexto “lentidão em operações com vetores alinhados”, “falha na escalabilidade de dados” e “baixo desempenho no uso de sockets” identificados tem relacionamento com nós “Size” e “Performance” do fragmento núcleo. O cenário ilustra as probabilidades

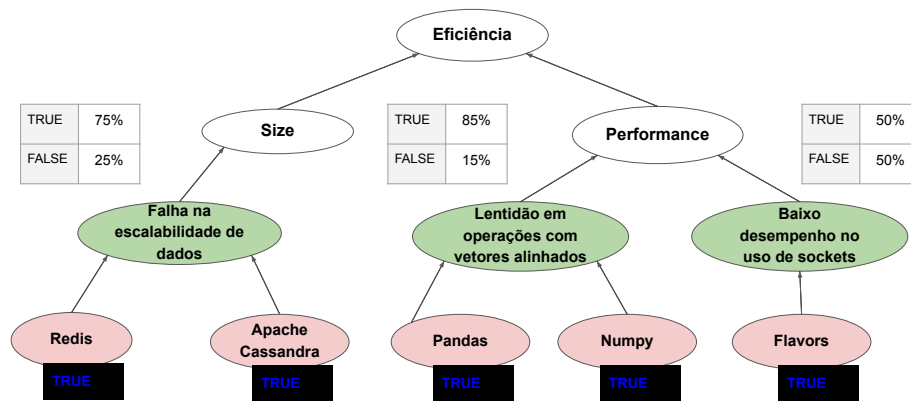


Figura 6.5: Perspectiva da Rede Bayesiana - Cenário 05

dos riscos sensíveis ao contexto de acordo com as tecnologias utilizadas no projeto. Após executar a Rede Bayesiana é possível visualizar os valores de probabilidades dos riscos identificados. Este cenário mostrou o potencial da Rede Bayesiana em identificar e mensurar riscos de acordo com as tecnologias adotadas no projeto. A abordagem tem como objetivo auxiliar a tomada de decisão, de modo que fica a critério do time analisar se os riscos são realmente inerentes ao projeto e como desejam priorizá-los.

### Cenário 06

**Descrição:** *Uma equipe de desenvolvimento irá participar de um projeto mobile. O projeto é de uma pequena rede social local para uma Universidade. O maior desafio tecnológico do projeto está na integração de informações do usuário em redes sociais já existentes com dados acadêmicos. O sistema deve garantir interoperabilidade e segurança. O líder técnico discute as tecnologias a serem usadas com a equipe, e marca com TRUE os nós folhas correspondentes dessas tecnologias na Rede Bayesiana: Push Notifications do Google, Firebase, Apollo e Retrofit. Ao finalizar a análise, o líder técnico executa a rede e visualiza as probabilidades calculadas para cada nó intermediário. Alguns nós apresentaram alta probabilidade, o que representa na semântica da rede que são riscos em potencial. O líder técnico deseja priorizar os riscos para tratar inicialmente os riscos de maior probabilidade. De acordo com a rede, os riscos em ordem do maior para o de menor probabilidade são:*

“perda de configuração no versionamento” e “falha na integração com plugins”. Com essas informações, a equipe avaliou os riscos e escolheu tratar na sprint zero o risco de maior probabilidade, ou seja, a “perda de configuração no versionamento”. Estratégias de mitigação serão investigadas para tratar o risco supracitado.

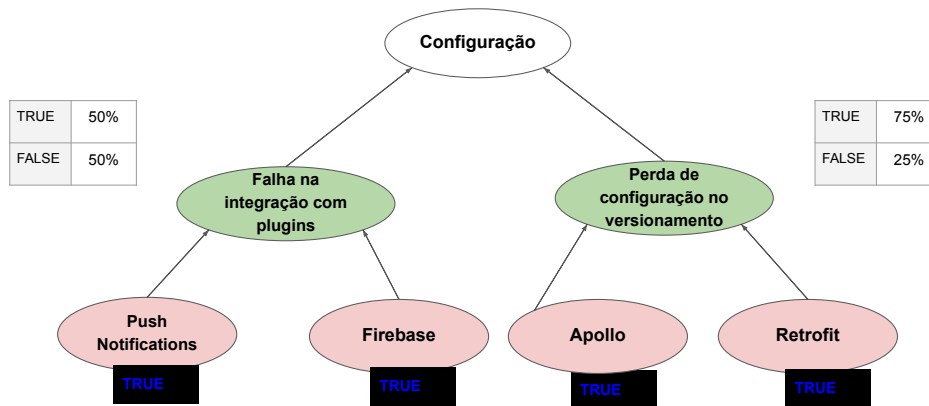


Figura 6.6: Perspectiva da Rede Bayesiana - Cenário 06

A Figura 6.6 mostra uma perspectiva da Rede Bayesiana para o cenário 06. Os riscos sensíveis ao contexto “perda de configuração no versionamento” e “falha na integração com plugins” identificados tem relacionamento com o nó “Configuração” do fragmento núcleo. O cenário ilustra as probabilidades dos riscos sensíveis ao contexto de acordo com as tecnologias utilizadas no projeto. Após executar a Rede Bayesiana é possível visualizar os valores de probabilidades dos riscos identificados. Este cenário mostrou o potencial da Rede Bayesiana em identificar e mensurar riscos de acordo com as tecnologias adotadas no projeto. A abordagem tem como objetivo auxiliar a tomada de decisão. Fica a critério do time analisar se os riscos são realmente inerentes ao projeto e como desejam priorizá-los.

### 6.2.2 Avaliação da abordagem

Para avaliar a abordagem foi realizado um *Focus Group* [99] com oito profissionais do VIR-TUS. A maioria dos participantes eram desenvolvedores (75%), e os demais líderes técnicos (25%). Todos os participantes possuem pelo menos dois anos de experiência com proje-

tos para dispositivos móveis. Para evitar viés, os profissionais convidados para adaptação e modelagem da abordagem (Seção 6.1) não participaram desta etapa da pesquisa.

A sessão do *Focus Group* durou 2 horas e 30 minutos. Depois de ler cada uma das descrições dos seis cenários, foram instanciados os nós da Rede Bayesiana e foi apresentado como a abordagem pode auxiliar a identificação, mensuração e monitoramento dos riscos. Depois de discutir cada cenário, aplicamos um questionário baseado no Modelo de Aceitação de Tecnologia (TAM) [22] para avaliar a impressão dos profissionais com a abordagem proposta. As respostas seguiram uma escala Likert [58] com cinco respostas possíveis, variando entre discordo totalmente (mapeado para o número 1) e concordo totalmente (mapeado para o número 5).

De acordo com a TAM, duas variáveis impactam a adoção de uma nova abordagem tecnológica: utilidade percebida e facilidade de uso [101]. A utilidade percebida refere-se ao grau em que um indivíduo acredita que o uso de uma determinada abordagem melhoraria seu desempenho no trabalho. A facilidade de uso refere-se ao grau em que um indivíduo acredita que o uso da abordagem não tem esforço excessivo [117]. A Tabela 6.1 apresenta as variáveis (i.e., questões realizadas aos profissionais) definidas para este estudo.

Tabela 6.1: Variáveis para avaliação da abordagem proposta

Variável	Tipo
V1: Usar a abordagem é útil para identificar riscos	Utilidade Percebida (PU)
V2: Usar a abordagem é útil para mensurar riscos	Utilidade Percebida (PU)
V3: Usar a abordagem é útil para monitorar riscos	Utilidade Percebida (PU)
V4: Aprender como a abordagem funciona foi fácil pra mim	Facilidade de Uso (FU)
V5: Frequentemente me confundo em usar a abordagem	Facilidade de Uso (FU)
V6: Entender o objetivo da abordagem é simples	Facilidade de Uso (FU)

A avaliação tem como objetivo responder a segunda questão de pesquisa desse trabalho: **RQ2: Qual a utilidade prática da Rede Bayesiana para o gerenciamento de riscos em projetos de software?.** Para isso, foram calculados a média, mediana e desvio padrão (SD) das respostas ao questionário aplicado aos oito participantes do *Focus Group*. A Tabela 6.2 apresenta os valores calculados. Para complementar a análise também foram registradas sugestões e críticas dos participantes durante a apresentação dos cenários.

Como pode ser observado na Tabela 6.2, os valores médios das três primeiras variáveis foram superiores a 4,0 (i.e., Utilidade Percebida). Esse resultado indica que os participantes tiveram atitudes positivas em relação à abordagem. Em particular, os participantes relataram



Tabela 6.2: Resultados do questionário

Variável	Definição	Média	Mediana	SD
V1	Usar a abordagem é útil para identificar riscos	4.71	5	0.745
V2	Usar a abordagem é útil para mensurar riscos	4.12	4	0.783
V3	Usar a abordagem é útil para monitorar riscos	4.56	5	0.755
V4	Aprender como a abordagem funciona foi fácil pra mim	4.35	4	0.715
V5	Frequentemente me confundo em usar a abordagem	3.82	3	0.852
V6	Entender o objetivo da abordagem é simples	4.12	4	0.841

que a abordagem é benéfica para a identificação e monitoramento de riscos (V1 e V3 com mediana igual a 5). Em relação às variáveis sobre a Facilidade de Uso, a avaliação da abordagem também foi positiva. Apenas a variável V5 apresentou valor médio inferior a 4. O resultado deve ser motivado porque alguns participantes não possuíam familiaridade prévia com Redes Bayesianas. Durante o *Focus Group*, os participantes mencionaram sugestões e críticas à abordagem proposta. Por exemplo, alguns participantes comentaram sobre o momento em que a abordagem seria mais útil na prática:

*“Achei a abordagem interessante para fazer análise de risco. Imagino que seria mais útil na indústria na definição da arquitetura do projeto. Ou seja, no momento da criação da proposta ou durante o sprint zero.”.* (E02, Desenvolvedor)

*“Sugiro rodar a Rede Bayesiana no final do projeto para analisar se as decisões tomadas pela equipe durante o desenvolvimento foram as mais corretas. ”.* (E03, Líder Técnico)

Conforme esses relatos, os participantes veem utilidade da abordagem no início dos projetos para fazer avaliação de riscos arquiteturais, como também no final dos projetos para auxiliar nas reuniões de lições aprendidas do projeto. Outro ponto importante está na atividade do gerenciamento de riscos que a abordagem pode ser útil. Alguns comentários foram nesse sentido:

*“Vejo que a abordagem possa estar integrada as ferramentas de gestão da empresa. Sempre que a equipe for cadastrando atividades, a Rede Bayesiana*

*poderia processar informações implícitas e explícitas das atividades para recomendar riscos potenciais ao projeto.”. (E02, Desenvolvedor)*

*“ Minha sugestão é que a abordagem seja sempre atualizada com as principais estratégias de mitigação. Uma espécie de fórum para ser consultado por novos times nas retrospectivas, que sendo usado com uma Rede Bayesiana por baixo traria maior facilidade de uso para as equipes. ”. (E05, Líder Técnico)*

Estes relatos estão em consonância do resultado estatístico apresentado na Tabela 6.2. Os participantes visualizaram utilidade prática da abordagem para identificação de riscos de acordo com características do projeto. Também vislumbram usar a abordagem para auxiliar na definição de estratégias de mitigação no monitoramento de riscos. Por fim, algumas críticas a abordagem foram relatadas e precisam ser avaliadas para uso da abordagem na prática:

*“ Achei o suporte à decisão das estratégias de mitigação fantástico, mas a escolha das tecnologias é mais complicada. É muito subjetivo dizer que ao usar a tecnologia X ou Y teremos um risco. O que pode acontecer em um projeto não é regra para outro. ”. (E05, Líder Técnico)*

*“ Acredito que a abordagem não teria uma vida longa na prática. Os riscos são eventos subjetivos. Apesar de compartilharem características comuns, os projetos têm suas particularidades. E é nessas coisas mais específicas que residem os riscos mais significativos. ”. (E08, Desenvolvedor)*

Os relatos acima vão de encontro com o objetivo da abordagem em reduzir a subjetividade no gerenciamento de riscos. Entretanto, os riscos nunca deixarão de ser subjetivos e abstratos. O objetivo da abordagem é reduzir a subjetividade propiciando a equipe informações para auxiliar nos processos do gerenciamento de riscos. Também é importante frisar que a Rede Bayesiana deve ser atualizada de forma contínua nas organizações para maior utilidade da abordagem na prática.

**RQ2:** *Qual a utilidade prática da Rede Bayesiana para gerenciamento de riscos em projetos de software?*. Para responder essa pergunta, neste trabalho foi realizada uma validação estática da Rede Bayesiana com cenários de simulação. Os cenários representaram casos reais de projetos de software. Os cenários ilustraram situações nas quais a abordagem poderia ser utilizada para apoiar a identificação, mensuração e monitoramento dos riscos. Ao final, um questionário baseado no TAM [22] foi aplicado com oito profissionais que concluíram que a abordagem é de fácil aplicação e útil principalmente para as atividades de identificação e monitoramento de riscos.

### 6.2.3 Ameaças à Validade

Em relação à validação estática com cenários simulados, classificamos as ameaças à validade como conclusão, internas, externas e de construção. Com relação às ameaças de construção, os cenários de simulação utilizados para validar a Rede Bayesiana podem não ser suficientes para garantir que as previsões do modelo são corretas. Para minimizar essa ameaça, foram construídos seis cenários com diferentes situações em que a abordagem pode auxiliar o gerenciamento de riscos. Na mesma linha, os cenários podem não refletir corretamente decisões reais em projetos de software, pois os especialistas consultados podem ter esquecido detalhes e terem criado cenários de baixa qualidade. Pensando nisso, para minimizar essa ameaça interna, na criação dos cenários os especialistas foram questionados sobre situações já vividas em projetos passados.

Por fim, validamos a abordagem com apenas oito profissionais da área, um pequeno subconjunto de especialistas. Assim, para minimizar ameaças de conclusão, os dados estatísticos calculados com as respostas do questionário foram somados às perguntas abertas para melhor análise dos resultados. Em relação às ameaças externas, validamos a abordagem com profissionais de apenas uma organização. Portanto, os resultados do estudo não podem ser generalizados.

## 6.3 Validação Dinâmica

Nesta seção será apresentada a validação dinâmica da abordagem proposta. Um experimento foi realizado com projetos reais de uma organização de desenvolvimento de software. Se-

guindo as diretrizes da engenharia do conhecimento de Redes Bayesianas [73], comparamos as impressões dos profissionais da organização com as predições da abordagem proposta. Na Subseção 6.3.1 são apresentados detalhes do experimento, enquanto que a Subseção 6.3.2 apresenta a avaliação da abordagem. Por fim, ameaças a validade são discutidas na Subseção 6.3.3.

### 6.3.1 Overview do Experimento

Para avaliar a predição da Rede Bayesiana, dados foram coletados de projetos do Núcleo de Pesquisa, Desenvolvimento e Inovação em Tecnologia da Informação, Comunicação e Automação (VIRTUS). A coleta de dados aconteceu em seis projetos de desenvolvimento de aplicações para dispositivos móveis. Cada projeto é composto por uma equipe de desenvolvimento distinta. As equipes têm entre três e seis desenvolvedores, com perfis variados de alunos recém formados em cursos de TI a profissionais com mais de dez anos de experiência em projetos de software. Para completar as equipes, em todos projetos um líder técnico é responsável por acompanhar o desenvolvimento e resolver conflitos internos. Por fim, um gerente de projetos tem atribuições relacionadas à divisão de atividades, negociação com o cliente e monitoramento dos indicadores do projeto.

Para evitar viés, os profissionais da organização que participaram da modelagem da abordagem (Seção 6.1) e da validação estática (Seção 6.2) não participaram da validação dinâmica. Nesta etapa, as predições da Rede Bayesiana foram comparadas com a realidade dos seis projetos sob a ótica dos diferentes perfis profissionais. A validação foi realizada em três etapas, uma para cada processo de gerenciamento de riscos: identificação, mensuração e monitoramento dos riscos.

Como ponto de partida do experimento, os times responderam um questionário sobre as tecnologias dos projetos que trabalham (Apêndice D). As perguntas correspondem aos nós folha da Rede Bayesiana relacionados ao fragmento de tecnologias. Essas informações foram utilizadas para instanciar a Rede Bayesiana com a realidade de cada projeto. Em seguida, os profissionais responderam um segundo questionário (Apêndice E), onde estão listados os riscos de projetos para dispositivos móveis. Cada profissional selecionou os riscos do projeto de acordo com seu ponto de vista. As perguntas do questionário correspondem aos nós da Rede Bayesiana que representam o fragmento de riscos sensíveis ao contexto.

Durante o experimento, as últimas questões de pesquisa deste trabalho foram respondidas. Inicialmente, para responder a questão **RQ3**: *Qual a precisão das predições da Rede Bayesiana para identificação de riscos?* foram calculados o *precision*, *recall* e *f-measure*. Para isso, foram comparados os riscos selecionados por cada perfil profissional nos seis projetos com os riscos de maior probabilidade calculados pela Rede Bayesiana.

Posteriormente, foram respondidas as questões de pesquisa **RQ4**: *A abordagem proposta consegue dar suporte à tomada de decisão, no sentido de auxiliar na definição de probabilidades para auxiliar a mensuração de riscos?* e **RQ5**: *A abordagem proposta consegue dar suporte à tomada de decisão, no sentido de auxiliar os times na escolha de estratégias de mitigação para auxiliar o monitoramento de riscos?*. Para responder **RQ4**, em cada projeto os riscos de maior probabilidade da Rede Bayesiana foram ordenados em um *ranking*. Por outro lado, para responder a **RQ5**, uma lista foi criada com estratégias recomendadas pela RB para mitigar os riscos previamente identificados. Nos dois casos, os profissionais dos projetos foram consultados para avaliar os riscos, probabilidades e estratégias sugeridas pela abordagem. As respostas seguiram uma escala Likert [58] com cinco respostas possíveis variando de discordo totalmente (mapeado para o número 1) a concordo totalmente (mapeado para o número 5). Em seguida foram calculadas média, mediana e desvio padrão com os valores das respostas para os profissionais dos seis projetos.

Ao final do experimento, os profissionais foram apresentados aos resultados e o autor desta tese coletou sugestões e críticas da abordagem para análise.

### 6.3.2 Avaliação da abordagem

Na Tabela 6.3 são apresentadas as tecnologias para cada um dos seis projetos. As tecnologias são os *frameworks*, APIs, bibliotecas, serviços e linguagens que dão suporte ao desenvolvimento do projeto. Para listar essas informações, o gerente de cada projeto preencheu o questionário (Apêndice D) de forma conjunta com os demais membros do time.

A Rede Bayesiana foi instanciada para cada projeto com informações das tecnologias apresentadas na Tabela 6.3. Em seguida a Rede Bayesiana foi executada e as probabilidades dos nós intermediários foram calculadas. De acordo com a modelagem da abordagem descrita na Seção 6.1, os riscos potenciais ao projeto são os nós intermediários com probabilidade igual ou superior a 50%. Para validação, os riscos sensíveis ao contexto com

Tabela 6.3: Respostas do questionário sobre as tecnologias dos projetos

Projeto I	Projeto II	Projeto III	Projeto IV	Projeto V	Projeto VI
Glide	REST	REST	Ionic	REST	Kotlin Coroutines
Jetpack	Retrofit	Background Services	REST	Auth	REST
REST	Integração CI/CD	Apollo	JWT	JWT	Apollo
Retrofit	GRPC	Couchdb	Background Services	Integração CI/CD	Firebase
Flavors	Kotlin Coroutines	JWT	Room	Keystore	Push Notifications
Background Services		Retrofit	Webservices	Webservices	
Integração CI/CD					
Push Notifications					
Webservices					

essas probabilidades foram registrados. No Apêndice H estão listados os riscos de maior probabilidade de acordo com a Rede Bayesiana para cada um dos seis projetos.

Para responder a questão de pesquisa **RQ3**, a análise aconteceu de forma distinta para cada perfil de profissional da equipe (i.e., desenvolvedor júnior, desenvolvedor pleno, desenvolvedor sênior, líder técnico e gerente de projeto). Cada profissional respondeu um questionário (Apêndice E) de forma individual listando os riscos tecnológicos de acordo com seu entendimento. Na Tabela 6.4 encontram-se os resultados da análise estatística realizada ao comparar os riscos recomendados pela RB (Apêndice H) e os riscos identificados pelos profissionais em cada projeto.

Em alguns projetos existem mais de um desenvolvedor por perfil, e nestes casos o resultado apresentado na Tabela 6.4 corresponde a média aritmética dos valores de *Precision*, *Recall* e *F-Measure* calculados para cada perfil nos projeto. Como observado, os valores de *F-Measure* para os desenvolvedores tiveram valores crescentes de acordo com o nível de experiência do profissional. Para os gerentes de projetos, mesmo sendo profissionais com alto nível de experiência os valores de *F-Measure* oscilaram e em alguns projetos foram menores que dos desenvolvedores. Na Figura 6.7 uma visão sumarizada é apresentada dos valores de precisão calculados para cada perfil profissional.

Como observado na Figura 6.7 a abordagem teve uma precisão maior quando comparada

Tabela 6.4: Resultado da análise estatística - Identificação de riscos

	<b>Perfil</b>	<b>Precision</b>	<b>Recall</b>	<b>F-Measure</b>
<b>Projeto 01</b>	Dev. Junior	28.57%	40.00%	22.85%
	Dev. Pleno	28.57%	40.00%	22.85%
	Dev. Senior	42.85%	60.00%	49.99%
	Líder Técnico	71.42%	83.33%	76.98%
	Gerente	42.85%	60.00%	49.99%
<b>Projeto 02</b>	Dev. Junior	0%	0%	0%
	Dev. Pleno	20.00%	25.00%	22.22%
	Dev. Senior	20.00%	25.00%	22.22%
	Líder Técnico	60.00%	75.00%	66.67%
	Gerente	40.00%	50.00%	44.44%
<b>Projeto 03</b>	Dev. Junior	16.66%	14.28%	15.37%
	Dev. Pleno	33.33%	28.57%	31.40%
	Dev. Senior	33.33%	28.57%	31.40%
	Líder Técnico	50.00%	42.85%	46.14%
	Gerente	33.33%	40.00%	36.01%
<b>Projeto 04</b>	Dev. Junior	40.00%	28.57%	33.34%
	Dev. Pleno	40.00%	33.33%	36.34%
	Dev. Senior	60.00%	33.33%	42.85%
	Líder Técnico	80.00%	40.00%	48.00%
	Gerente	60.00%	33.33%	42.85%
<b>Projeto 05</b>	Dev. Junior	14.28%	20.00%	16.62%
	Dev. Pleno	14.28%	20.00%	16.62%
	Dev. Senior	50.00%	42.85%	46.14%
	Líder Técnico	60.00%	50.00%	54.54%
	Gerente	40.00%	50.00%	44.44%
<b>Projeto 06</b>	Dev. Junior	20.00%	14.28%	16.66%
	Dev. Pleno	20.00%	16.66%	18.18%
	Dev. Senior	40.00%	33.33%	36.36%
	Líder Técnico	50.00%	42.85%	46.15
	Gerente	40.00%	40.00%	40.00%

com os riscos identificados pelo líder técnico. Em todos os projetos analisados, foi esse o perfil em que os valores de *Precision* e *F-Measure* foram mais altos. Portanto, a abordagem pode ser utilizada por este profissional para auxiliar a identificação de riscos ou como suporte dos demais profissionais do projeto.

Após informarem os riscos de acordo com seus pontos de vista, os profissionais tiveram acesso aos riscos recomendados pela abordagem. Neste momento, os participantes foram convidados a deixar sugestões e críticas. Com relação a identificação de riscos alguns comentários são apresentados a seguir:

*“Entendo que a abordagem ajude a diminuir a subjetividade para identificar os riscos. Primeiro porque padroniza os principais riscos tecnológicos dos projetos. Segundo porque cria mecanismos para identificar os gatilhos dos riscos. Muitos dos riscos listados pela abordagem podem acontecer, realmente, mas*

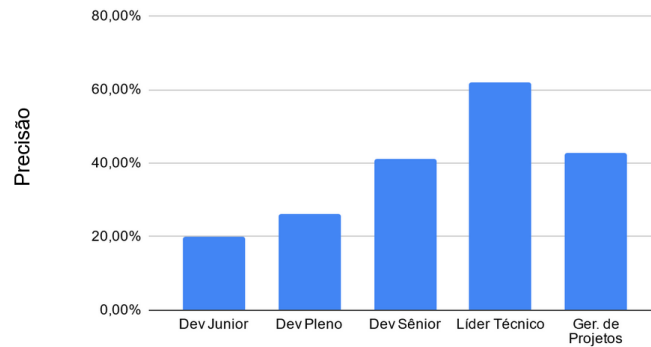


Figura 6.7: Valores de precisão calculados por perfil profissional

*não foram minhas escolhas iniciais por acreditar que o time já tenha expertise com isso. ”. (Líder Técnico - Projeto 03)*

*“Os riscos tecnológicos são comuns em todos os projetos. Mas normalmente negligenciados porque o time acredita que é algo implícito do projeto. Para fazer essa análise eu procurei listar os riscos que já atrasaram entregas do nosso time. Porém, alguns dos riscos identificados pela abordagem que eu não pensei inicialmente também fazem sentido para o projeto.”. (Líder Técnico - Projeto 04)*

Os dois líderes explanaram que alguns riscos identificados pela abordagem não estiveram na listagem inicialmente prevista, mas consideraram que são riscos potenciais para os projetos que fazem parte. Essas impressões somadas aos resultados apresentados na Tabela 6.4 corroboram que a abordagem é promissora para identificação dos riscos. Portanto, para responder a questão de pesquisa **RQ3**, conclui-se que a abordagem tem boa precisão na identificação dos riscos sob a ótica dos líderes técnicos.

Por fim, um gerente de projeto justifica seu entendimento sobre os riscos tecnológicos modelados na abordagem:

*“Estes riscos são muito específicos do desenvolvimento. Normalmente essas decisões eu delego para o time. Os riscos que estão na minha responsabilidade são os riscos mais gerais do projeto, principalmente relacionados as negociações com o cliente. ”. (Gerente - Projeto 01)*



O relato acima corrobora com os baixos valores de *precision* para esse perfil descritos na Tabela 6.4. Apesar de possuírem formação na área de tecnologia de informação, nos projetos de software estes profissionais não são responsáveis por gerenciar os riscos tecnológicos.

**RQ3:** *Qual a precisão das predições da Rede Bayesiana para identificação de riscos?*. Para responder a esta pergunta, neste trabalho foi realizada uma validação dinâmica da abordagem em um experimento com seis projetos reais do VIRTUS. Para cada projeto, foi realizada a instanciação da Rede Bayesiana com as tecnologias do projeto. Em seguida, foi avaliada a precisão nos riscos recomendados pela abordagem com os riscos de acordo com os diferentes profissionais dos projetos. Para avaliar os resultados, foram calculados *precision*, *recall* e *f-measure*. Como resultado, verificou-se que a precisão foi maior com os perfis de mais experiência, em especial com o líder técnico. Somado aos dados estatísticos, relatos dos profissionais corroboraram para a capacidade da abordagem em auxiliar a identificação de riscos. Assim, a abordagem pode ser utilizada por esse profissional para auxiliar na identificação de riscos ou pelo restante do time para diminuir a dependência do líder técnico.

Para responder a questão **RQ4**, os riscos previamente recomendados pela RB foram ordenados em forma de *ranking* (para mais detalhes, o Apêndice H lista os riscos em ordem de maior para o de menor probabilidade). Para esta etapa de validação, não houve distinção de perfil, e os profissionais de cada projeto responderam uma questão simples de acordo com o ranking apresentado (i.e., priorização dos riscos). As respostas seguiram uma escala Likert [58] de cinco níveis. Os resultados são apresentados na Tabela 6.5.

Tabela 6.5: Resultado da análise estatística - Mensuração de riscos

	<b>Média</b>	<b>Mediana</b>	<b>SD</b>
Projeto 01	3.83	3	0,784
Projeto 02	3.64	3	0,456
Projeto 03	4.08	3	0,584
Projeto 04	3.86	3	0,486
Projeto 05	3.74	3	0,545
Projeto 06	4.27	4	0,746

De acordo com os resultados apresentados na Tabela 6.5, apenas o Projeto 06 teve mediana igual a quatro (i.e., concorda com a recomendação), o restante teve um valor mediano de três (i.e., nem concordo nem discordo). Os valores médios também apontaram para uma avaliação apenas razoável da abordagem para auxiliar a mensuração de riscos. Para complementar a análise, foi solicitado aos participantes sugestões e críticas sobre essa etapa da validação. Alguns pontos importantes são apresentados a seguir:

*“É complicado priorizar riscos tecnológicos, porque eles são mais subjetivos que os riscos normais. Achei a rede interessante para identificar os riscos, mas para priorizar não faz sentido. No meu entendimento os riscos listados tem a mesma probabilidade.”. (Líder Técnico - Projeto 02)*

*“ O ranking me ajuda a fazer a priorização dos riscos. Mas se tratando de riscos tecnológicos acredito que estes devem ser mitigados já no início do projeto na definição de arquitetura e ferramentas. A abordagem nesse ponto só faz sentido pra mim se for usada aqui e todos os riscos mitigados de forma conjunta.”. (Líder Técnico - Projeto 04)*

Os profissionais ressaltaram a importância da abordagem para identificação de riscos, mas fazem ressalvas para parte de mensuração. Portanto, para responder a questão de pesquisa **RQ4**, conclui-se que a abordagem atualmente não auxilia a mensuração de riscos em projetos de software. Entretanto, a seguir é apresentado um último relato com uma sugestão que pode mudar esse cenário em uma versão futura da abordagem:

*“ Priorizar riscos é uma atividade importante porque na prática não iremos ter tempo de tratar todos os riscos do projeto, então escolhemos alguns para gerenciar e torcemos para que os demais não se concretizem. Acredito que a abordagem tenha mais valor se ao apresentar a listagem de riscos priorizados, apresentasse um quantitativo das vezes que esses riscos aconteceram no passado na organização. Junto poderia ter algum link para tasks encerrados para avaliarmos qual o impacto destes riscos no passado.”. (Desenvolvedor Sênior - Projeto 03)*

O relato acima indica um fato importante para continuação dessa pesquisa em um momento posterior. Uma vez que a Rede Bayesiana seja utilizada na prática, as equipes irão aderir a padronização de riscos utilizadas na abordagem. Assim, será possível fazer a rastreabilidade dos riscos em projetos encerrados. Com isso, mais informações estarão disponíveis para modelagem da abordagem para realidade dos projetos da organização.

Por fim, a última questão de pesquisa a ser analisada neste estudo é a **RQ5**. Para isso, o autor desta tese instanciou as diversas estratégias de mitigação da Rede Bayesiana e verificou

quais destas estratégias reduziam os riscos previamente identificados (para mais detalhes, o Apêndice I apresenta as estratégias recomendadas para cada projeto). Para esta etapa de validação não houve distinção de perfil, os profissionais de cada projeto responderam uma questão se estavam de acordo com a lista de estratégias apresentada. As respostas seguiram uma escala Likert [58] e os resultados são apresentados na Tabela 6.6.

Tabela 6.6: Resultado da análise estatística - Monitoramento de riscos

	<b>Média</b>	<b>Mediana</b>	<b>SD</b>
Projeto 01	4.45	5	0,634
Projeto 02	4.64	5	0,658
Projeto 03	4.21	4	0,804
Projeto 04	4.06	4	0,621
Projeto 05	4.34	5	0,645
Projeto 06	4.36	4	0,664

De acordo com os resultado apresentados na Tabela 6.6, todos os projetos tiveram valores médios acima de 4.0. Com relação a mediana, metade apontaram para uma satisfação em nível quatro (i.e., concordo) e outra metade em nível cinco (i.e., concordo plenamente). Assim como nas etapas anteriores, para complementar a análise, foi solicitado aos participantes sugestões e críticas. Alguns pontos importantes são apresentados a seguir:

*“Imagino esta parte funcionando na prática como um repositório de lições aprendidas. Para ser interessante o ideal era ser alimentado de forma coletiva, a abordagem poderia ter uma técnica inteligente por baixo que selecionasse apenas estratégias com um certo número de recomendações dos times. ”.*

(Líder Técnico do Projeto 01)

*“ Todas as estratégias listadas fazem sentido para mim. Podem ser utilizadas para mitigar os riscos citados, como outros riscos tecnológicos. Eu vejo essa lista como um guia de boas práticas de programação. ”.* (Desenvolvedor Pleno

- Projeto 04)

Os profissionais ressaltaram que as estratégias listadas fazem sentido para mitigar os riscos previamente identificados. Para responder a **RQ5** foram analisados os relatos dos profissionais e as respostas apresentadas na Tabela 6.6. Assim, foi concluído que a abordagem pode ser usada para auxiliar o monitoramento de riscos na atividade de seleção de estratégias

de mitigação. Por fim, um dos participantes fez uma ressalva relevante sobre essa etapa da validação:

*“Como meu projeto já se encontra nas últimas sprints foi mais fácil para mim avaliar tanto os riscos quanto as estratégias pertinentes ao meu projeto. Acredito que se estivessem no início, seria mais complicado fazer as previsões. ”.*

(Desenvolvedor Sênior - Projeto 01)

Para a validação dinâmica descrita nesta Seção, não foi considerado o estágio em que os projetos se encontravam. Como descrito no relato acima, as impressões dos profissionais é mais confiável caso os projetos se encontrem na fase final. Dessa forma, é encorajado uma validação a posteriori com projetos sendo avaliados desde a concepção até as etapas finais.

**RQ4:** *A abordagem proposta consegue dar suporte à tomada de decisão, no sentido de auxiliar na definição de probabilidades para auxiliar a mensuração de riscos?* e a **RQ5:** *A abordagem proposta consegue dar suporte à tomada de decisão, no sentido de auxiliar os times na escolha de estratégias de mitigação para auxiliar o monitoramento de riscos?.* Para responder essas perguntas, foram apresentados aos profissionais de cada projeto uma lista dos riscos ranqueados e uma lista de estratégias de mitigação para os riscos previamente identificados. Os profissionais deveriam avaliar e responder seguindo uma escala Likert [58] de cinco níveis, e ao final foram calculadas média, mediana e desvio padrão. Os resultados apontaram para utilidade da abordagem no monitoramento de riscos. Porém, os profissionais fizeram ressalvas sobre a aplicabilidade com relação à mensuração de riscos.

### 6.3.3 Ameaças à validade

Com relação à validação dinâmica, há três tipos de ameaça à validade: interna, externa e de conclusão. A ameaça de conclusão é resultado da falta de padronização aos riscos dos projetos da organização, posto que os riscos são registrados e gerenciados de formas distintas pelos times. Desta forma, não se pode garantir a precisão dos riscos recomendados pela abordagem em relação aos riscos reais do projeto. Para minimizar esta ameaça, os profissionais foram encorajados a consultar artefatos dos projetos e ferramentas de gestão. Com essas informações e de acordo com seus pontos de vista foram identificados os riscos dos projetos que fazem parte.

Uma ameaça à validade interna está nos profissionais que participaram da validação da Rede Bayesiana. Estes representam um pequeno grupo de profissionais da área. Para minimizar essa ameaça, a validação aconteceu com profissionais de diferentes perfis. Portanto, os resultados deste estudo devem ser considerados como indicadores e avaliações adicionais com outros profissionais devem ser realizadas. Para evitar viés, os profissionais envolvidos no experimento na validação dinâmica não participaram da validação estática com cenários de simulação.

Com relação à ameaça externa, assim como na validação estática descrita na Seção anterior, o experimento foi executado em apenas uma organização. Portanto, os resultados desta pesquisa não podem ser generalizados. Para minimizar essa ameaça, os seis projetos escolhidos na análise são de diferentes clientes.

# Capítulo 7

## Considerações Finais

Nesta pesquisa, foi apresentada uma abordagem para auxiliar no gerenciamento de riscos em projetos de software. O objetivo é tornar o gerenciamento de risco mais objetivo e sistemático diminuindo a subjetividade na tomada de decisão em atividades relacionadas à identificação, mensuração e monitoramento de riscos. Rede Bayesiana foi a técnica escolhida, motivada pela capacidade de tratar dados incompletos; rápida resposta a novos dados; estrutura de raciocínio; e possibilidade de usar especialistas na modelagem da solução. A abordagem proposta neste trabalho foi planejada para ser utilizada em empresas de desenvolvimento de software que utilizam tanto metodologias tradicionais quanto ágeis. Não é propósito da abordagem proposta substituir técnicas e ferramentas já utilizadas pelos profissionais nas organizações, como também não é propósito da abordagem avaliar riscos relacionados ao tempo, custo ou dos recursos humanos do projeto.

As Redes Bayesianas descritas na literatura utilizam diferentes fatores de riscos para modelar as variáveis que influenciam os riscos dos projetos. Os fatores de riscos mais utilizados estão relacionados aos requisitos do projeto, equipe e processo de desenvolvimento [3, 25, 82]. Porém, a literatura se mostra escassa para apresentar os fatores de riscos relacionados às características tecnológicas dos projetos. Essas características estão presentes em qualquer projeto de software, mas estão em evidência principalmente em projetos de inovação, P&D ou NPD. Algumas pesquisas modelam aspectos tecnológicos, porém estes trabalhos limitam-se a definir um fator específico para representar o risco associado a todas as características tecnológicas do projeto [15, 62, 67, 98]. Dada a dificuldade de reprodução ou a pouca utilidade dos modelos presentes no estado da arte [15, 33, 67], neste trabalho

foi criado um modelo próprio para o gerenciamento de riscos. O foco da abordagem está em modelar os fatores de riscos relacionados às características tecnológicas dos projetos de software.

A Rede Bayesiana foi construída por meio da elicitaco do conhecimento de especialistas seguindo o processo de Engenharia de Conhecimento de Redes Bayesianas [73]. Uma estrutura central (i.e., fragmento ncleo) da abordagem foi modelada como resultado de um estudo qualitativo com vinte e cinco profissionais de dez diferentes organizaes. Para ser til em diferentes contextos de projetos de software, um processo sistemtico foi definido para adaptao da abordagem para diferentes contextos. O processo descrito na Seo 5.3 guia o incremento da abordagem com informaes de tecnologias, estratgias de mitigao e riscos sensveis ao contexto. Neste trabalho a abordagem foi modelada para projetos de desenvolvimento de aplicaes para dispositivos mveis. Para isso, o autor desta tese teve apoio de trs especialistas do Ncleo de Pesquisa, Desenvolvimento e Inovao em Tecnologia da Informao, Comunicao e Automao (VIRTUS) da Universidade Federal de Campina Grande.

## 7.1 Contribuies

Neste trabalho foram definidas cinco questes de pesquisa. A primeira  **RQ1**: *Quais so os fatores de riscos tecnolgicos relevantes na construo de uma Rede Bayesiana na modelagem para auxiliar o gerenciamento de riscos em um projeto de software?*. Para isso, foi realizado um estudo qualitativo em que foram identificadas informaes tecnolgicas que serviram de base para construo da Rede Bayesiana. Cada n intermedirio representa um risco relacionado a caractersticas tecnolgicas (e.g., segurana de dados, eficincia de requisies, configurao do servidor de aplicao, integrao com plataformas de terceiros, implementao de tcnica inteligentes). Os ns folha representam informaes de tecnologias (e.g., linguagens, APIs, bibliotecas, *frameworks*) e estratgias de mitigao de riscos (e.g., configurar servidor, reiniciar servios, adotar algum padro de projeto). De forma geral, a Rede Bayesiana recebe de entrada informaes das tecnologias do projeto, realiza um processamento e calcula a probabilidade dos riscos. Tambm  possvel instanciar estratgias para reavaliar as probabilidades dos riscos.

A segunda questão de pesquisa é **RQ2**: *Qual a utilidade prática da Rede Bayesiana para gerenciamento de riscos em projetos de software?*. Para isso, foi realizada uma validação estática da Rede Bayesiana com cenários de simulação. Os cenários representaram casos reais de projetos de software. Os cenários ilustraram situações nas quais a abordagem poderia ser utilizada para apoiar a identificação, mensuração e monitoramento dos riscos. Ao final, um questionário baseado no TAM [22] foi aplicado com oito profissionais que concluíram que a abordagem é de fácil aplicação e útil principalmente para as atividades de identificação e monitoramento de riscos.

A terceira questão de pesquisa é a **RQ3**: *Qual a precisão das predições da Rede Bayesiana para identificação de riscos?*. Para isso, foi realizada uma validação dinâmica da abordagem em um experimento com seis projetos reais do VIRTUS. Para cada projeto, foi realizada a instanciação da Rede Bayesiana com as tecnologias do projeto. Em seguida, foi avaliada a precisão nos riscos recomendados pela abordagem com os riscos de acordo com os diferentes profissionais dos projetos. Para avaliar os resultados, foram calculados *precision*, *recall* e *f-measure*. Como resultado, verificou-se que a precisão foi maior com os perfis de mais experiência, em especial com o líder técnico. Somado aos dados estatísticos, relatos dos profissionais corroboraram para a capacidade da abordagem em auxiliar a identificação de riscos. Assim, a abordagem pode ser utilizada por esse profissional para auxiliar na identificação de riscos ou pelo restante do time para diminuir a dependência do líder técnico.

As últimas questões de pesquisa são a **RQ4**: *A abordagem proposta consegue dar suporte à tomada de decisão, no sentido de auxiliar na definição de probabilidades para auxiliar a mensuração de riscos?* e a **RQ5**: *A abordagem proposta consegue dar suporte à tomada de decisão, no sentido de auxiliar os times na escolha de estratégias de mitigação para auxiliar o monitoramento de riscos?*. Para responder essas perguntas, foram apresentados aos profissionais de cada projeto uma lista dos riscos ranqueados e uma lista de estratégias de mitigação para os riscos previamente identificados. Os profissionais deveriam avaliar e responder seguindo uma escala Likert [58] de cinco níveis, e ao final foram calculadas média, mediana e desvio padrão. Os resultados apontaram para utilidade da abordagem no monitoramento de riscos. Porém, os profissionais fizeram ressalvas sobre a aplicabilidade com relação à mensuração de riscos.

As seguintes contribuições foram alcançadas com este trabalho:



Estudo qualitativo realizado em núcleos de inovação tecnológica sobre os principais fatores de riscos em projetos de software. Para isso, foram entrevistados 25 profissionais de dez organizações. Com o estudo, foi possível identificar fatores de riscos já conhecidos em outros trabalhos da literatura, e em especial, fatores de riscos relacionados às características tecnológicas. Desta forma, este estudo complementa o estado da arte listando os fatores de riscos relacionados às características tecnológicas de projetos de software;

Rede Bayesiana para prognóstico dos riscos tecnológicos em função de informações das tecnologias dos projetos e das estratégias de mitigação. Para isso, foi construído uma Rede Bayesiana com fatores de risco relacionados às características tecnológicas de projetos de software com viés para projetos de inovação. Desta forma, a Rede Bayesiana auxilia à tomada de decisão diminuindo a subjetividade em atividades do gerenciamento de riscos em projetos de software;

Processo sistemático para adaptação da Rede Bayesiana em projetos de diferentes contextos nas organizações de desenvolvimento de software, com suporte ferramental. Para isso, foi implementado uma ferramenta para facilitar o uso da abordagem, onde os próprios usuários alvo possam modelar tecnologias do projeto, visualizar os riscos e fazer as intervenções do modelo. Desta forma, a abordagem proposta pode ser utilizada por profissionais em projetos reais de software de diferentes contextos.

Ferramenta *Risk Control* implementada para dar suporte a identificação, mensuração e monitoramento de riscos. A ferramenta realiza o processamento ao modelar a abordagem proposta, de forma a abstrair dos usuários detalhes da Rede Bayesiana construída.

## 7.2 Trabalhos Futuros

Para construção da Rede Bayesiana utilizou-se um processo dirigido à elicitación de conhecimento por especialistas [73]. A partir do momento em que o modelo é aplicado em uma empresa, dados com relação às variáveis de interesse podem ser coletados. Dessa forma, pode-se atualizar o processo sistemático para adequação contínua da Rede Bayesiana de acordo com os dados coletados na organização. Além disso, pode-se definir um processo para, a partir do momento que um modelo é calibrado para um contexto com os dados de uma empresa, transferir o conhecimento para realidade de outra empresa e assim minimizar

o custo de implantação do mesmo, explorando conceitos apresentados em Zhou *et al.* [126].

Outra perspectiva futura é a aplicação do processo sistemático e conseqüentemente a modelagem de Redes Bayesianas para outros contextos de projetos de desenvolvimento de software. Nesta pesquisa o fragmento núcleo foi incrementado com informações de projetos para dispositivos móveis. Outros contextos na mesma organização foram identificados e podem ser explorados em pesquisas futuras, são exemplos: aplicações Web, sistemas IoT ou aplicações para *Business Intelligence*.

A validação dinâmica descrita na Seção 6.3 ilustrou o uso da Rede Bayesiana para fazer prognósticos de riscos associados as tecnologias adotadas no projeto. Também foram realizados prognósticos dos riscos a partir de estratégias de mitigação que poderiam ser implementadas no projeto. Por outro lado, a Rede Bayesiana também pode ser utilizada para realizar diagnóstico. Algumas situações foram ilustradas na validação estática da Seção 6.2. Experimentos futuros na indústria podem explorar a capacidade da abordagem em realizar diagnósticos dos riscos.

Com o uso da abordagem nas organizações espera-se uma padronização na definição dos riscos relacionados as características tecnológicas dos projetos de software. Com isso, catálogos de riscos podem ser criados para diferentes contextos de projeto. Com catálogos, dados históricos seriam registrados com maior clareza e serviriam de apoio na tomada de decisão em projetos futuros da organização. Como descrito na validação, os profissionais envolvidos na validação desta pesquisa apontam para criação de uma base de conhecimento de riscos e estratégias. Esta base de conhecimento deve ser colaborativa, contando com apoio de todos profissionais da organização.

Finalmente, é necessário coletar dados em outros projetos e também em outras organizações. Com uso da abordagem em diferentes cenários pode-se ter mais confiança estatística que o modelo pode ser generalizado para diferentes situações em empresas de desenvolvimento de software. O uso da abordagem nas organizações também deve ser alvo de novos estudos científicos para avaliar limitações da validação apresentada nesta pesquisa (e.g., avaliar o uso da abordagem com times de diferentes níveis de experiência e com projetos em fases distintas).

# Bibliografia

- [1] Steve Adolph, Wendy Hall, and Philippe Kruchten. Using grounded theory to study the experience of software development. Empirical Software Engineering, 16(4):487–513, 2011.
- [2] Allan Afuah. Innovation management-strategies, implementation, and profits. Oxford University Press, USA, 2a edition, 2020. ISBN 978-0195142303.
- [3] Ieva Ancveire, Ilze Gailite, Made Gailite, and Janis Grabis. Software delivery risk management: Application of bayesian networks in agile software development. Information Technology and Management Science, 18(1):62–69, 2015.
- [4] Chamundeswari Arumugam, Sriraghav Kameswaran, and Baskaran Kaliamourthy. Global software development: A design framework to measure the risk of the global practitioners. In Proceedings of the 7th International Conference on Computer and Communication Technology, ICCCT-2017, page 1–8, New York, NY, USA, 2017. Association for Computing Machinery.
- [5] Piero Baraldi, Luca Podofillini, Lusine Mkrtchyan, Enrico Zio, and Vinh N. Dang. Comparing the treatment of uncertainty in Bayesian networks and fuzzy expert systems used for a human reliability analysis application. Reliability Engineering and System Safety, 2015.
- [6] Henri Barki, Suzanne Rivard, and Jean Talbot. Toward an assessment of software development risk. J. Manage. Inf. Syst., 10(2):203–225, September 1993.
- [7] Dense Bastos, Paulo e Oliveira. Redes Bayesianas: Aplicações em Confiabilidade e no Diagnóstico de Perdas não Técnicas. Editora Appris, 1a edition, 2017. ISBN 978-8547303778.

- 
- [8] Irad Ben-Gal. Bayesian networks. Encyclopedia of statistics in quality and reliability, 1(2), 2008.
- [9] Nitin Bhatia and Namarta Kapoor. Fuzzy cognitive map based approach for software quality risk analysis. SIGSOFT Softw. Eng. Notes, 36(6):1–9, November 2011.
- [10] Barry Boehm. Software risk management. In C. Ghezzi and J. A. McDermid, editors, ESEC '89, pages 1–19, Berlin, Heidelberg, 1989. Springer Berlin Heidelberg.
- [11] John Bowers and Alireza Khorakian. Integrating risk management in the innovation project. European Journal of innovation management, 17(1):25–40, 2014.
- [12] Saad Yasser Chadli and Ali Idri. Identifying and mitigating risks of software project management in global software development. In Proceedings of the 27th International Workshop on Software Measurement and 12th International Conference on Software Process and Product Measurement, IWSM Mensura '17, page 12–22, New York, NY, USA, 2017. Association for Computing Machinery.
- [13] Robert Charette. Software engineering risk analysis and management. McGraw-Hill, USA, 1a edition, 1989. ISBN 978-0070106611.
- [14] Jie Cheng, Russell Greiner, Jonathan Kelly, David Bell, and Weiru Liu. Learning bayesian networks from data: An information-theory based approach. Artificial Intelligence, 137(1):43–90, 2002.
- [15] Kwai-Sang Chin, Da-Wei Tang, Jian-Bo Yang, Shui Yee Wong, and Hongwei Wang. Assessing new product development project risk by bayesian network with a systematic probability generation methodology. Expert Systems with Applications, 36(6):9879–9890, 2009.
- [16] David C. Chou. Risk identification in green it practice. Computer Standards Interfaces, 35(2):231–237, 2013.
- [17] Mary Beth Chrissis, Mike Konrad, and Sandra Shrum. CMMI for development: guidelines for process integration and product improvement. Pearson Education, 2a edition, 2011. ISBN 978-0321279675.

- 
- [18] Paul Clements and Linda Northrop. Software product lines: Patterns and practice. Addison-Wesley: Reading, MA, 1a edition, 2001. ISBN 978-0201703320.
- [19] Juliet Corbin and Anselm Strauss. Basics of qualitative research: Techniques and procedures for developing grounded theory. Sage publications, 4a edition, 2014. ISBN 978-1412906449.
- [20] Michael A Cusumano. The software factory: a historical interpretation. IEEE Software, 6(2):23–30, 1989.
- [21] One-Ki Daniel Lee and DV Baby. Managing dynamic risks in global it projects: Agile risk-management using the principles of service-oriented architecture. International Journal of Information Technology & Decision Making, 12(06):1121–1150, 2013.
- [22] Fred D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q., 13(3):319–340, September 1989.
- [23] Cristine Martins Gomes de Gusmão and Hermano Perrelli de Moura. Iso, cmmi and pmbok risk management: a comparative analysis. The International Journal of Applied Management and Technology, 1(1):65–75, 2003.
- [24] Rick Dove and Ralph LaBarge. Fundamentals of agile systems engineering–part 1. In International Council on Systems Engineering, volume 30, pages 121–150. Las Vegas, US-NV, 2014.
- [25] J Drew Procaccino, June M Verner, Scott P Overmyer, and Marvin E Darter. Case study: factors for early prediction of software development success. Information and Software Technology, 44(1):53–62, 2002.
- [26] Ellen Drost. Validity and reliability in social science research. International Perspectives on Higher Education Research, 38(1):105–124, 2011.
- [27] Khaled El Emam and A. Günes Koru. A replicated survey of it software project failures. IEEE Software, 25(5):84–90, 2008.
- [28] Richard Fairley. Risk management for software projects. IEEE Softw., 11(3):57–67, May 1994.

- [29] Chin-Feng Fan and Yuan-Chang Yu. Bbn-based software project risk management. Journal of Systems and Software, 73(2):193–203, 2004. Applications of statistics in software engineering.
- [30] N. Fenton, W. Marsh, M. Neil, P. Cates, S. Forey, and M. Tailor. Making resource decisions for software projects. In Proceedings. 26th International Conference on Software Engineering, pages 397–406, 2004.
- [31] Norman Fenton and Martin Neil. Risk assessment and decision analysis with Bayesian networks. Crc Press, 2a edition, 2012. ISBN 978-1138035119.
- [32] Norman Fenton, Martin Neil, and David A Lagnado. A general structure for legal arguments about evidence using bayesian networks. Cognitive science, 37(1):61–102, 2013.
- [33] Norman Fenton, Martin Neil, William Marsh, Peter Hearty, undefin dukasz Radliński, and Paul Krause. On the effectiveness of early life cycle defect prediction with bayesian nets. Empirical Softw. Engg., 13(5):499–537, October 2008.
- [34] Norman E Fenton, Martin Neil, and Jose Galan Caballero. Using ranked nodes to model qualitative judgments in bayesian networks. IEEE Transactions on Knowledge and Data Engineering, 19(10):1420–1432, 2007.
- [35] Arthur Freire, Mirko Perkusich, Renata Saraiva, Hyggo Almeida, and Angelo Perkusich. A bayesian networks-based approach to assess and improve the teamwork quality of agile teams. Information and Software Technology, 100:119–132, 2018.
- [36] Vitor Freitas, Emilia Mendes, and Burak Turhan. Providing tool-support for value-based decision-making: A usability assessment. In 2016 42th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), pages 34–41, 2016.
- [37] Nir Friedman, Dan Geiger, and Moisés Goldszmidt. Bayesian network classifiers. Machine Learning, 29(2-3):131–163, 1997.
- [38] Anselm L. Glaser, Barney G. Strauss. The Discovery of Grounded Theory: Strategies for Qualitative Research, volume 81. London: Wiedenfeld and Nicholson, 1999. ISBN: 978-0202302607.

- [39] Barney G. Glaser. Theoretical Sensitivity: Advances in the Methodology of Grounded Theory. Sociology Press, 1978. ISBN: 978-1884156014.
- [40] Barney G Glaser. Basics of grounded theory analysis: Emergence vs forcing, volume 03. Sociology press, 1a edition, 1992. ISBN 978-1884156007.
- [41] Tony Gorschek, Per Garre, Stig Larsson, and Claes Wohlin. A model for technology transfer in practice. IEEE Software, 23(6):88–95, 2006.
- [42] Catarina Gralha, Daniela Damian, Anthony Wasserman, Miguel Goulão, and João Araújo. The evolution of requirements practices in software startups. In 2018 IEEE/ACM 40th International Conference on Software Engineering (ICSE), pages 823–833, 2018.
- [43] Daya Gupta and Mohd Sadiq. Software risk assessment and estimation model. In 2008 International Conference on Computer Science and Information Technology, pages 963–967, 2008.
- [44] Johannes IM Halman and JIMME A Keizer. Diagnosing risks in product-innovation projects. International Journal of Project Management, 12(2):75–80, 1994.
- [45] Wen-Ming Han. Discriminating risky software project using neural networks. Comput. Stand. Interfaces, 40(C):15–22, June 2015.
- [46] Peter Hearty, Norman Fenton, Martin Neil, and Patrick Cates. Automated population of causal models for improved software risk assessment. In Proceedings of the 20th IEEE/ACM International Conference on Automated Software Engineering, ASE '05, page 433–434, New York, NY, USA, 2005. Association for Computing Machinery.
- [47] David Heckerman. Bayesian networks for data mining. Data mining and knowledge discovery, 1(1):79–119, 1997.
- [48] Rashina Hoda, James Noble, and Stuart Marshall. The impact of inadequate customer collaboration on self-organizing agile teams. Inf. Softw. Technol., 53(5):521–534, May 2011.

- [49] Emam Hossain, Muhammad Ali Babar, Hye-young Paik, and June Verner. Risk identification and mitigation processes for using scrum in global software development: A conceptual framework. In 2009 16th Asia-Pacific Software Engineering Conference, pages 457–464, 2009.
- [50] Martin Host and Per Runeson. Checklists for software engineering case study research. In First International Symposium on Empirical Software Engineering and Measurement (ESEM 2007), pages 479–481, 2007.
- [51] Yong Hu, Xizhu Mo, Xiangzhou Zhang, Yuran Zeng, Jianfeng Du, and Kang Xie. Intelligent analysis model for outsourced software project risk using constraint-based bayesian network. Journal of Software, 7(2):342 – 348, 2012.
- [52] Kurt Huang and Max Henrion. Efficient search-based inference for noisy-or belief networks: Topepsilon. Proceedings of the Twelfth International Conference on Uncertainty in Artificial Intelligence, pages 325–331, 2013.
- [53] Sun-Jen Huang and Wen-Ming Han. Exploring the relationship between software project duration and risk exposure: A cluster analysis. Information Management, 45(3):175–182, 2008.
- [54] International Standards Organisation. Iso 31000: Risk management—principles and guidelines. Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso:31000:en>. Acesso em: 15 abril 2021, 2018.
- [55] Shareeful Islam. Software development risk management model: a goal driven approach. In Proceedings of the doctoral symposium for ESEC/FSE on Doctoral symposium, pages 5–8, 2009.
- [56] Kawal Jeet, Nitin Bhatia, and Rajinder Singh Minhas. A model for estimating the impact of low productivity on the schedule of a software development project. SIGSOFT Softw. Eng. Notes, 36(4):1–6, August 2011.
- [57] James Jiang and Gary Klein. Software development risks to project effectiveness. Journal of Systems and Software, 52(1):3–10, 2000.



- [58] Ankur Joshi, Saket Kale, Satish Chandel, and D Kumar Pal. Likert scale: Explored and explained. Current Journal of Applied Science and Technology, pages 396–403, 2015.
- [59] Jimme A Keizer and Johannes IM Halman. Risks in major innovation projects, a multiple case study within a world’s leading company in the fast moving consumer goods. Intl. Journal of Technology Management, 48(4):499–517, 2009.
- [60] Jimme A Keizer, Jan-Peter Vos, and Johannes IM Halman. Risks in new product development: devising a reference tool. R&D Management, 35(3):297–309, 2005.
- [61] Harold Kerzner. Project management: a systems approach to planning, scheduling, and controlling. John Wiley & Sons, 11a edition, 2017. ISBN 978-1118022276.
- [62] Vahid Khodakarami and Abdollah Abdi. Project cost risk analysis: A bayesian networks approach for modeling dependencies between cost items. International Journal of Project Management, 32(7):1233–1245, 2014.
- [63] George Klir and Bo Yuan. Fuzzy sets and fuzzy logic, volume 4. Prentice hall New Jersey, 1a edition, 1995. ISBN 978-0131011717.
- [64] Tsutomu Kojima, Toru Hasegawa, Munechika Misumi, and Tsuyoshi Nakamura. Risk analysis of software process measurements. Software Quality Journal, 16(3):361–376, 2008.
- [65] Jyrki Kontio, Johanna Bragge, and Laura Lehtola. The Focus Group Method as an Empirical Tool in Software Engineering, pages 93–116. Springer London, London, 2008.
- [66] Kevin B Korb and Ann E Nicholson. Bayesian artificial intelligence, volume 3. CRC press, 2010.
- [67] Chandan Kumar and Dilip Kumar Yadav. Software defects estimation using metrics of early phases of software development life cycle. International Journal of System Assurance Engineering and Management, 8(4):2109–2117, 2017.

- [68] Rohit Kumar, Anjali Tayal, and Sargam Kapil. Analyzing the Role of Risk Mitigation and Monitoring in Software Development. IGI Global, 1a edition, 2018. ISBN 978-1522560296.
- [69] Matthew Leitch. Iso 31000: The new international standard on risk management. Risk Analysis: An International Journal, 30(6):887–892, 2010.
- [70] Robyn Longhurst. Semi-structured interviews and focus groups. Key methods in geography, 3(2):143–156, 2003.
- [71] Cristina López and Jose L Salmeron. Modeling maintenance projects risk effects on erp performance. Computer Standards & Interfaces, 36(3):545–553, 2014.
- [72] Jorge Melegati, Alfredo Goldman, Fabio Kon, and Xiaofeng Wang. A model of requirements engineering in software startups. Information and Software Technology, 109:92–107, 2019.
- [73] Emilia Mendes. Expert-Based Knowledge Engineering of Bayesian Networks, pages 73–105. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.
- [74] Emilia Mendes. Practitioner’s Knowledge Representation: a pathway to improvesoftware effort estimation. Springer, 4a edition, 2014. ISBN 978-3642541568.
- [75] Emilia Mendes, Vitor Freitas, Mirko Perkusich, João Nunes, Felipe Ramos, Alexandre Costa, Renata Saraiva, and Arthur Freire. Using bayesian network to estimate the value of decisions within the context of value-based software engineering: A multiple case study. International Journal of Software Engineering and Knowledge Engineering, 29(11):1629–1671, 2019.
- [76] Emilia Mendes, Pilar Rodriguez, Vitor Freitas, Simon Baker, and Mohamed Amine Atoui. Towards improving decision making and estimating the value of decisions in value-based software engineering: The value framework. Software Quality Journal, 26(2):607–656, June 2018.

- [77] Wang Min, Zhang Jun, and Zhang Wei. The application of fuzzy comprehensive evaluation method in the software project risk assessment. In Proceedings of the 2017 International Conference on Management Engineering, Software Engineering and Service Sciences, ICMSS '17, page 76–79, New York, NY, USA, 2017. Association for Computing Machinery.
- [78] Osamu Mizuno, Takanari Hamasaki, Yasunari Takagi, and Tohru Kikuno. An empirical evaluation of predicting runaway software projects using bayesian classification. In Frank Bomarius and Hajimu Iida, editors, Product Focused Software Process Improvement, pages 263–273, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.
- [79] Cinzia Muriana and Giovanni Vizzini. Project risk management: A deterministic quantitative technique for assessment and mitigation. International Journal of Project Management, 35(3):320–340, 2017.
- [80] Kwan-Sik Na, James T. Simpson, Xiaotong Li, Tushar Singh, and Ki-Yoon Kim. Software development risk and project performance measurement: Evidence in korea. Journal of Systems and Software, 80(4):596–605, 2007. Software Performance.
- [81] Richard E Neapolitan et al. Learning bayesian networks, volume 38. Pearson Prentice Hall Upper Saddle River, NJ, 2004.
- [82] Ngoc-Tuan Nguyen, Quyet-Thang Huynh, and Thi-Huong-Giang Vu. A bayesian critical path method for managing common risks in software project scheduling. In Proceedings of the Ninth International Symposium on Information and Communication Technology, SoICT 2018, page 382–388, New York, NY, USA, 2018. Association for Computing Machinery.
- [83] Liudmila V Nikolova, Juriy Ju Kuporov, and Dmitriy G Rodionov. Risk management of innovation projects in the context of globalization. International Journal of Economics and Financial Issues, 5(3S), 2015.
- [84] P Russel Norvig. Artificial Intelligence - A modern approach. Prentice Hall, 3a edition, 2009. ISBN 978-0136042594.

- [85] Edzreena Edza Odzaly and Darryl Stewart Des Greer. Lightweight risk management in agile projects. 26th Software Engineering and Knowledge Engineering (SEKE), pages 321–326, 2014.
- [86] Judea Pearl. Bayesianism and Causality, or, Why I am Only a Half-Bayesian, pages 19–36. Springer Netherlands, Dordrecht, 2001.
- [87] Mirko Perkusich, Lenardo Chaves e Silva, Alexandre Costa, Felipe Ramos, Renata Saraiva, Arthur Freire, Ednaldo Dilorenzo, Emanuel Dantas, Danilo Santos, Kyller Gorgônio, Hyggo Almeida, and Angelo Perkusich. Intelligent software engineering in the context of agile software development: A systematic literature review. Information and Software Technology, 119:106241, 2020.
- [88] Mirko Perkusich, Angelo Perkusich, and Hyggo Oliveira de Almeida. Using survey and weighted functions to generate node probability tables for bayesian networks. In 2013 BRICS Congress on Computational Intelligence and 11th Brazilian Congress on Computational Intelligence, pages 183–188, 2013.
- [89] Project Management Institute (PMI). A Guide to the Project Management Body of Knowledge (PMBOK Guide), volume 6. EUA, 2019.
- [90] Grant Purdy. Iso 31000: 2009—setting a new standard for risk management. Risk Analysis: An International Journal, 30(6):881–886, 2010.
- [91] Md. Forhad Rabbi and Khan Olid Bin Mannan. A review of software risk management for selection of best tools and techniques. In 2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pages 773–778, 2008.
- [92] Eric Reis. The lean startup. New York: Crown Business, 3a edition, 2018. ISBN 978-0307887894.
- [93] Silja Renooij and Cilia Witteman. Talking probabilities: communicating probabilistic information with words and numbers. International Journal of Approximate Reasoning, 22(3):169–194, 1999.

- [94] Philipp Rosenberger and József Tick. Suitability of pmbok 6th edition for agile-developed it projects. In 2018 IEEE 18th International Symposium on Computational Intelligence and Informatics (CINTI), pages 000241–000246, 2018.
- [95] Robert S Russell and Bernard W Taylor-Iii. Operations management along the supply chain. John Wiley & Sons, 1a edition, 2008. ISBN 978-0470233795.
- [96] Ashish B Sasankar and Vinay Chavan. Swot analysis of software development process models. International Journal of Computer Science Issues (IJCSI), 8(5):390, 2011.
- [97] Satyendra Kumar Sharma and Udayan Chanda. Developing a bayesian belief network model for prediction of r&d project success. Journal of Management Analytics, 4(3):321–344, 2017.
- [98] Vidushi Sharma, Sachin Rai, and Anurag Dev. A comprehensive study of artificial neural networks. International Journal of Advanced research in computer science and software engineering, 2(10), 2012.
- [99] Forrest Shull, Janice Singer, and Dag IK Sjøberg. Guide to advanced empirical software engineering. Springer, 2007.
- [100] Hélène Sicotte and Mario Bourgault. Dimensions of uncertainty and their moderating effect on new product development project performance. R&d Management, 38(5):468–479, 2008.
- [101] Jislane Silva, Danilo Siqueira Ramos, and M. S. Soares. On criteria to choose a content management system: A technology acceptance model approach. In 28th Software Engineering and Knowledge Engineering (SEKE), 2016.
- [102] Preston G Smith and Guy M Merritt. Proactive risk management: Controlling uncertainty in product development. Productivity Press, 1a edition, 2002. ISBN 978-1563272653.
- [103] SOFTEX. Mps - melhoria de processo do software brasileiro. Disponível em: <https://softex.br/mpsbr/guias/>. Acesso em: 04 abril 2021, 2021.

- [104] Klaas-Jan Stol, Paul Ralph, and Brian Fitzgerald. Grounded theory in software engineering research: A critical review and guidelines. In Proceedings of the 38th International Conference on Software Engineering, ICSE '16, page 120–131, New York, NY, USA, 2016. Association for Computing Machinery.
- [105] Klaas-Jan Stol, Paul Ralph, and Brian Fitzgerald. Grounded theory in software engineering research: a critical review and guidelines. In Proceedings of the 38th International Conference on Software Engineering, pages 120–131, 2016.
- [106] Anselm Strauss and Juliet M Corbin. Grounded theory in practice. Sage, 1a edition, 1997. ISBN 978-0761907480.
- [107] Jeff Sutherland and Ken Schwaber. The scrum guide. Disponível em: <http://www.scrumguides.org/docs/scrumguide/v1/Scrum-Guide-US.pdf>, 2021. Acessado em: 01-05-2021.
- [108] Yasunari Takagi, Osamu Mizuno, and Tohru Kikuno. An empirical approach to characterizing risky software projects based on logistic regression analysis. Empirical Software Engineering, 10(4):495–515, 2005.
- [109] Madjid Tavana, Amir-Reza Abtahi, Debora Di Caprio, and Maryam Poortarigh. An artificial neural network and bayesian network model for liquidity risk assessment in banking. Neurocomputing, 275:2525–2554, 2018.
- [110] Breno Gontijo Tavares, Carlos Eduardo Sanches da Silva, and Adler Diniz de Souza. Risk management analysis in scrum software projects. International Transactions in Operational Research, 26(5):1884–1905, 2019.
- [111] Amrit Tiwana and Mark Keil. The one-minute risk assessment tool. Commun. ACM, 47(11):73–77, November 2004.
- [112] Martin Tománek and J. Juricek. Project risk management model based on prince2 and scrum frameworks. The International Journal of Software Engineering Applications (IJSEA), 6(1), 2015.
- [113] Laura Uusitalo. Advantages and challenges of bayesian networks in environmental modelling. Ecological Modelling, 203(3):312–318, 2007.

- [114] L. C. van der Gaag. Bayesian Belief Networks: Odds and Ends. The Computer Journal, 39(2):97–113, 01 1996.
- [115] Roger L Van Scoy. Software development risk: opportunity, not problem. Technical report, Univ. Pittsburgh - Software Engineering Inst, 1992.
- [116] Kim Verbert, R Babuška, and Bart De Schutter. Bayesian and dempster–shafer reasoning for knowledge-based fault diagnosis—a comparative study. Engineering Applications of Artificial Intelligence, 60:136–150, 2017.
- [117] Linda G. Wallace and Steven D. Sheetz. The adoption of software measures: A technology acceptance model (tam) perspective. Information Management, 51(2):249–259, 2014.
- [118] Nicholas Walliman. Research methods: The basics. Routledge, 3a edition, 2017. ISBN 978-0415489942.
- [119] Juite Wang, Willie Lin, and Yu-Hsiang Huang. A performance-oriented risk management framework for innovative r&d projects. Technovation, 30(11-12):601–611, 2010.
- [120] Roel Wieringa, Neil Maiden, Nancy Mead, and Colette Rolland. Requirements engineering paper classification and evaluation criteria: A proposal and a discussion. Requir. Eng., 11(1):102–107, December 2005.
- [121] Roel J Wieringa. Design science methodology for information systems and software engineering. Springer, 1a edition, 2014. ISBN 978-3662438381.
- [122] Claes Wohlin and Anneliese Amschler Andrews. Prioritizing and assessing software project success factors and project characteristics using subjective data. Empirical Software Engineering, 8(3):285–308, 2003.
- [123] Li Xiaosong, Liu Shushi, Cai Wenjun, and Feng Songjiang. The application of risk matrix to software project risk management. In 2009 International Forum on Information Technology and Applications, volume 2, pages 480–483, 2009.

- 
- [124] Zhiwei Xu, Taghi M. Khoshgoftaar, and Edward B. Allen. Application of fuzzy expert systems in assessing operational risk of software. Information and Software Technology, 45(7):373–388, 2003. Software Engineering with Computational Intelligence S.I.
- [125] Lihong Zhou, Ana Vasconcelos, and Miguel Nunes. Supporting decision making in risk management through an evidence-based information systems project risk checklist. Information management & computer security, 2:480–483, 2008.
- [126] Yun Zhou, Timothy M Hospedales, and Norman Fenton. When and where to transfer for bayesian network parameter learning. Expert systems with applications, 55:361–373, 2016.
- [127] Hadar Ziv, Debra Richardson, and René Klösch. The uncertainty principle in software engineering. In 19th International Conference on Software Engineering (ICSE), pages 823–833, 1997.



# Apêndice A

## Roteiro da Entrevista - Grounded Theory

- Como os riscos são identificados na organização?
- Os riscos são medidos? Como os riscos são medidos?
- Quais os principais riscos dos projetos?
- Como os riscos são priorizados?
- Como os riscos de maior severidade são tratados?
- Riscos inesperados são frequentes de acontecer?
- Riscos considerados de pouca probabilidade costumam acontecer?
- Riscos considerados de pouco impacto costumam acontecer?
- A organização tem planos de resposta aos riscos?
- Quais os principais gatilhos dos riscos dos projetos da organização?
- Qual característica dos projetos o configuram serem de maior risco?
- Qual o nível de interesse dos clientes com os riscos do projeto?
- Qual o principais riscos tecnológicos?
- Como são tratadas as integrações do sistema?
- Você considera a equipe motivada no projeto?

- Como mitigar o risco do uso de técnicas nunca usadas?
- Os projetos têm mais de um *stakeholder*? Como gerenciar?
- Qual risco associado ao ambiente de desenvolvimento?
- Qual risco associado à arquitetura de desenvolvimento?
- Como gerenciar os riscos ao usar técnicas de Inteligência Artificial?
- Como gerenciar um risco referente a uma tecnologia nova para equipe?

# Apêndice B

## Lista dos Códigos - Grounded Theory

- Perspectiva Mercado
- Turnover
- Legado
- Suporte
- Ciclos Curtos
- Competência
- Aplicabilidade
- Prototipagem
- Aceite Entregas
- Colaboração Mútua
- Avaliação Desempenho
- Experiência
- Motivação
- Arquitetura
- Integração
- Motivação Científica
- Dados
- Interface
- Criptografia
- Workshop
- Cronograma
- Engajamento Stakeholders
- Serviço
- Gerência Configuração
- Plataforma
- Instituição de Ensino
- Servidor Híbrido
- Capacitação
- Testes Críticos
- Fatores Externos
- Tecnologia
- Nova Versão
- ROI
- Expectativas do Cliente
- Estimativas
- Validação
- Incerteza
- Usabilidade
- SGBD
- Mentoring
- API
- Conflito Interesses

- 
- Clareza Requisitos
  - Entrega Contínua
  - Expertise
  - Gestão
  - Linguagem
  - Testes Hipóteses
  - Prova de Conceito
  - Machine Learning
  - Conhecimento
  - Análise Histórico
  - Brainstorming
  - TRL
  - Impacto
  - Solução Proposta
  - Inovação
  - Adaptação Processo
  - Probabilidade
  - Multidisciplinar
  - Pesquisa
  - Recursos Humanos
  - Trabalho em Grupo
  - Cache
  - Simultaneidade
  - Ambiente
  - Validação
  - Produção
  - Documentação
  - Produto
  - Financiamento
  - Liderança
  - Inteligência Artificial
  - Migração Dados
  - Artefatos do ambiente
  - Fomento
  - Parceria
  - Prospecção
  - Processo
  - Rede Neural
  - Overfitting
  - Geolocalização
  - Problema de Pesquisa
  - Teste Aceitação
  - Critérios Aceitação
  - Blockchain
  - Tamanho tabelas
  - Criatividade
  - Restrições Organizacionais
  - Segurança

# Apêndice C

## Descrição dos Nós - Fragmento Núcleo

- **Infraestrutura** - este nó representa o risco com a infraestrutura - a rede, o ambiente, os servidores de aplicação e os bancos de dados.
  - **Ambiente** - este nó representa o risco com o ambiente de desenvolvimento.
    - \* **Servidor** - este nó representa o risco com o servidor de aplicação do projeto - a conexão, a execução de tarefas e configuração do servidor.
    - \* **Dados** - este nó representa o risco com os dados do projeto - a integridade, disponibilidade e durabilidade dos dados.
  - **Integração** - Este nó representa o risco de integração do sistema com sistemas legados do cliente e plataformas externas (terceiros).
    - \* **Legado** - Este nó representa o risco de integração do sistema com sistemas legado do cliente - acesso a funcionalidades, método de comunicação e mecanismos de troca de dados.
    - \* **Terceiros** - Este nó representa o risco de integração do sistema com terceiros (APIs, Frameworks, bibliotecas).
      - **Serviço** - Este nó representa o risco em usar serviços de terceiros - instabilidade de tecnologias, erro de comunicação.
      - **Configuração** - Este nó representa o risco com a configuração do sistema com plataformas externas - falha de compatibilidade de tecnologias, integração de ferramentas, versionamento.

- 
- **Aplicação** - este nó representa o risco com a aplicação desenvolvida - aspectos arquiteturais, sistema operacional, linguagens e técnicas implementadas.
    - **Arquitetura** - este nó representa o risco arquitetural do sistema.
      - \* **Segurança** - este nó representa o risco de segurança da aplicação - métodos de criptografia, certificado digital, tokens.
        - **Interface** - Este nó representa o risco de segurança em nível de interface - autenticação dos usuários, disponibilidade dos dados.
        - **Persistência** - Este nó representa o risco de segurança em nível de banco - integridade dos dados.
      - \* **Eficiência** - este nó representa o risco de eficiência da aplicação.
        - **Size** - este nó representa o risco relacionado ao tamanho das tabelas, uso de memória, necessidade de cache .
        - **Performance** - este nó representa o risco relacionado ao número de usuários que acessarão o sistema, simultaneidade de operações, desempenho na realização de operações e execução de processos.
    - **Método** - Este nó representa o risco com o método de desenvolvimento da aplicação - sistema operacional, linguagem, tecnologias inovadoras.
      - \* **Técnica** - Este nó representa o risco com a técnica implementada - treinar um modelo preditivo de ML, implementar algum algoritmo de IA, codificar uma rede Blockchain, validar uma nova linguagem/framework de programação.
      - \* **Validação** - Este nó representa o risco com a validação da aplicação - ferramentas de deliverys, publicação do sistema, necessidade de dados/ artefatos específicos do cliente.

# Apêndice D

## Listagem - Tecnologias

Tecnologias elicidadas para o contexto de projetos de desenvolvimento de aplicações móveis:

- Framework **Ionic** para desenvolvimento híbrido
- Framework **Electron** para desenvolvimento híbrido
- **FireBase** para autenticação multiplataforma
- Serviço de **Push Notifications** do Google
- Biblioteca **Apollo** para requests
- Serviço **Jetpack Navigation**
- Serviço de comunicação **REST**
- Biblioteca **RxJava** para programação reativa
- Biblioteca **Room** para persistência
- Biblioteca **Retrofit** para comunicação
- Serviço **Fastlane** para publicação
- **Kotlin Coroutines** para execução de tarefas
- Biblioteca **Glide** para tratar imagens
- Biblioteca **Picasso** para tratar imagens

- Bigtable com **Apache Cassandra**
- Biblioteca **Couchdb** para banco de dados
- **Redis** para banco de dados
- **Mongoose** para banco de dados
- **Background services** para execução de tarefas
- Gerência de de usuários com **Flavors**
- Framework **JWT** para segurança
- Framework **Auth** para segurança
- **Bugsnag** para monitorar exceções
- **LeakCanary** para detectar memory leaks
- Integração com **CI/CD**
- **RMI** para acesso a recursos remotos
- **Webservice** para comunicação
- **GRPC** para comunicação
- **Numpy** para armazenar dados
- **Pandas** para processamento de dados
- **Keystore** para armazenar chaves



# Apêndice E

## Listagem - Riscos

Riscos sensíveis ao contextos elicitadas para o contexto de projetos de desenvolvimento de aplicações móveis:

- Falha na integração com *plugins*
- Falha no fechamento do ciclo das notificações
- Erro de TOC (Two Phase Commit)
- Falha com *hotspots* via aplicativo de terceiros
- Perda de configuração no versionamento
- Falha de conexão para visualizar mídias
- Perda de dados armazenados em servidor híbrido
- Perda de conexão em requisição HTTP via *Postman*
- Lentidão em operações com vetores alinhados
- Falha na escalabilidade de dados
- Falha no estado de durabilidade dos dados
- Falha na execução de tarefas assíncronas
- Falha de segurança na persistência offline

- Erro no mecanismo de criptografia
- Falha de segurança na decodificação dos *tokens*
- Perda de autenticação em área restrita
- Baixo desempenho no uso de *sockets*
- Baixo desempenho na comunicação por microserviços
- Falha na atualização dos *drivers*
- Falha no tratamento de geolocalização
- Baixo desempenho das *builds*
- Indisponibilidade de recursos multimídia

# Apêndice F

## Listagem - Estratégias

Estratégias de mitigação elicitadas para o contexto de projetos de desenvolvimento de aplicações móveis:

- Colocar uma Unique Constraint no Index
- Padronizar troca de dados com JSON
- Criar um Post Type para organizar
- Usar Controllers
- Submeter pequenos patches
- Interagir containers com Kubernetes
- Usar Loaders para gerenciar ciclo de vida
- Inserir Authorization Header
- Verificar dependências build gradle
- Avaliar configurações do proxy
- Verificar status do plugin AndroidPermisscion
- Acessar funcionalidades das APIs pela WebView
- Colocar depurador no primeiro plano

- Avaliar compatibilidade dos pacotes de IDE
- Usar SDK Admin
- Verificar imports do projeto
- Ativar persistência em disco
- Especificar um provedor
- Criar arrays com links para um RecyclerView
- Verificar objetos callback
- Evitar usar loops de repetição
- Revisar Drivers do sistema operacional

# Apêndice G

## Rede Bayesiana

A Rede Bayesiana modelada neste trabalho é dividida em quatro sub-redes: integração, ambiente, método e arquitetura.

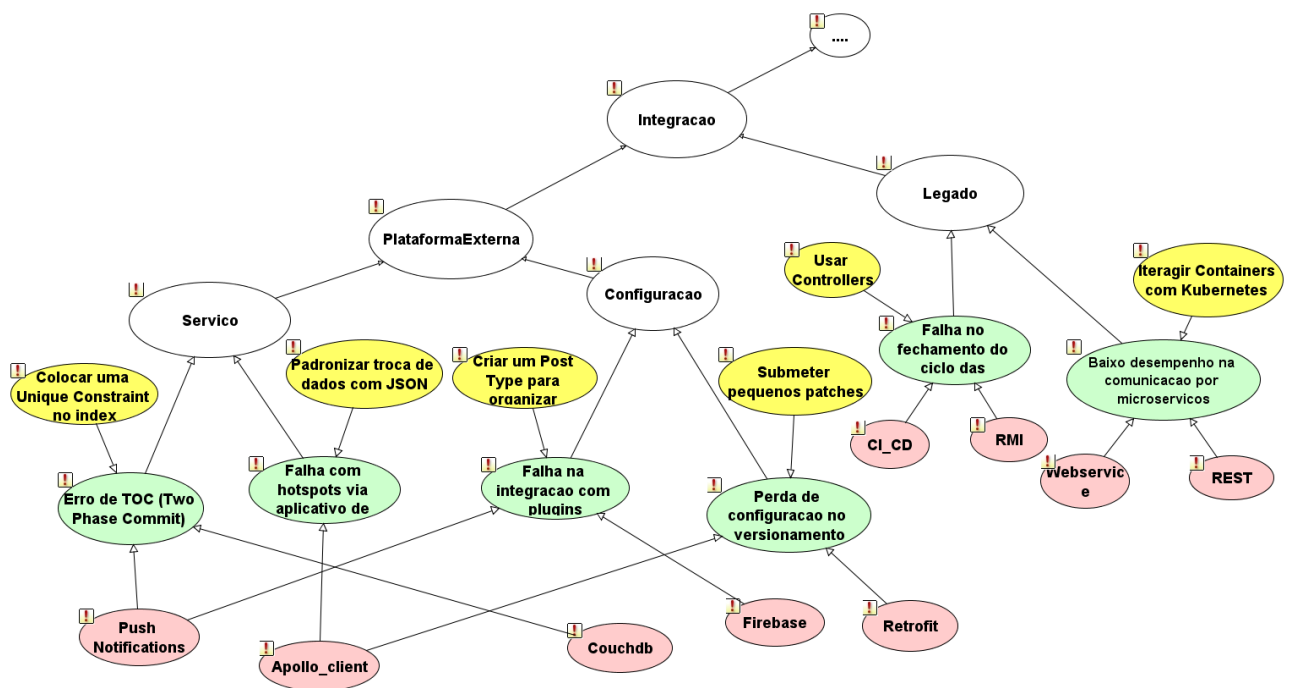


Figura G.1: Sub-rede Integração



Figura G.2: Sub-rede Ambiente

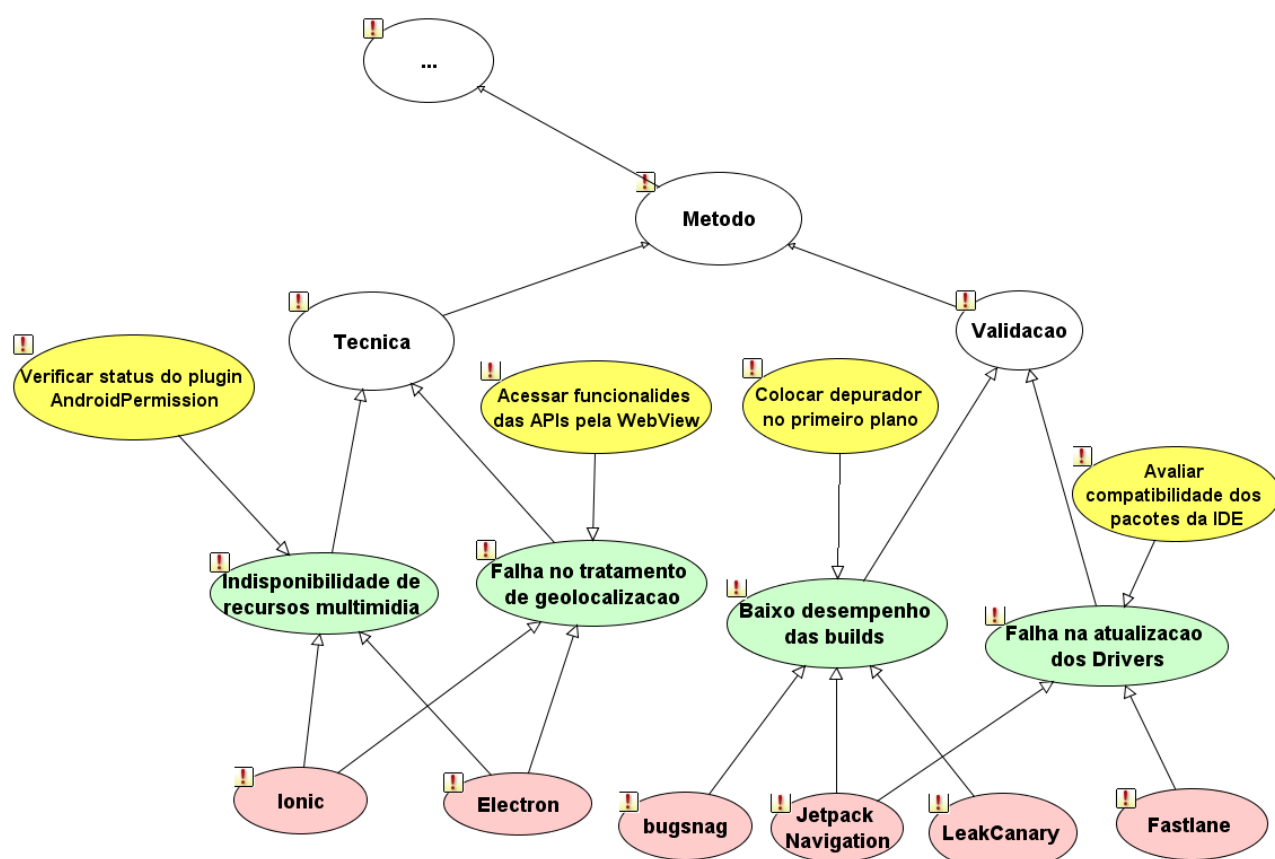


Figura G.3: Sub-rede Método

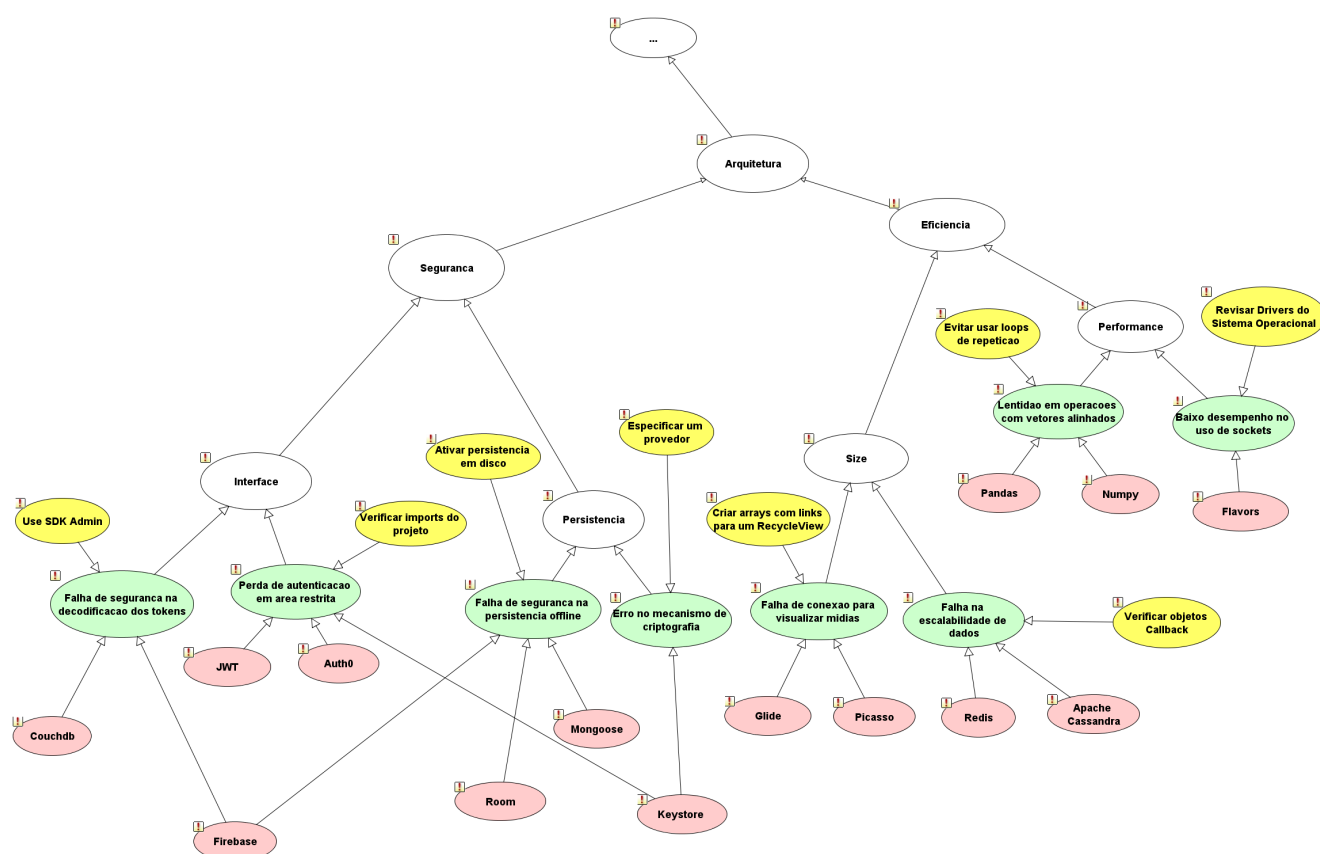


Figura G.4: Sub-rede Arquitetura



# Apêndice H

## Validação - Lista de riscos RB

Tabela H.1: Riscos de maior probabilidade calculados pela Rede Bayesiana

<b>Projeto I</b>	<b>Projeto II</b>	<b>Projeto III</b>
Baixo Desempenho Comunicação com microserviços	Falha na execução de tarefas assíncronas	Baixo Desempenho Comunicação com microserviços
Baixo desempenho nas builds	Baixo Desempenho Comunicação com microserviços	Falha no estado de durabilidade dos dados
Perda de Conexão em requisição HTTP via POSTman	Perda de configuração no versionamento	Falha de segurança na decodificação dos tokens
Perda de Configuração no versionamento	Perda de dados armazenados em servidor híbrido	Perda de autenticação em área restrita
Falta de Conexão para visualizar mídias	Falha no fechamento do ciclo das notificações	Falha com hotspots via aplicativo de terceiros
Erro de TOC (Two Phase Commit)	-	Perda de configuração no versionamento
Baixo desempenho no uso de sockets	-	-
<b>Projeto IV</b>	<b>Projeto V</b>	<b>Projeto VI</b>
Baixo Desempenho Comunicação com microserviços	Baixo Desempenho Comunicação com microserviços	Falha na integração com plugins
Perda de autenticação na área restrita	Perda de autenticação na área restrita	Baixo Desempenho Comunicação com microserviços
Falha de segurança na persistência offline	Falha no fechamento do ciclo de notificações	Falha na execução de tarefas assíncronas
Indisponibilidade de recursos multimídia	Erro no mecanismo de criptografia	Falha de segurança na persistência offline
Falha no tratamento de geolocalização		Falha com hotspots via aplicativos de terceiros
Falha na execução de tarefas assíncronas		Perda de configuração no versionamento
Falha no estado de durabilidade dos dados		

# Apêndice I

## Validação - Lista de Estratégias RB

Tabela I.1: Estratégias recomendadas pela Rede Bayesiana

<b>Projeto I</b>	<b>Projeto II</b>	<b>Projeto III</b>
Interagir Containers com Kubernetes	Usar Loaders para Gerenciar Ciclo de Vida	Interagir Containers com Kubernetes
Colocar depurador no primeiro plano	Interagir Containers com Kubernetes	Verificar Dependências BuildGradle
Inserir Authorization Header	Submeter pequenos Patches	Usar SDK Admin
Submeter pequenos Patches	Avaliar Configurações do Proxy	Verificar Imports do Projeto
Inserir Arrays com Links para um RecyclerView	Usar Controllers	Padronizar Troca de Dados com JSON
Colocar uma Unique Constraint no Index		Submeter pequenos Patches
Revisar Drivers do Sistema Operacional		
<b>Projeto IV</b>	<b>Projeto V</b>	<b>Projeto VI</b>
Interagir Containers com Kubernetes	Interagir Containers com Kubernetes	Criar um Post Type para Organizar Importações
Verificar Imports do Projeto	Verificar Imports do Projeto	Interagir Containers com Kubernetes
Ativar Persistência em Disco	Usar Controllers	Usar Loaders para Gerenciar Ciclo de Vida
Verificar status do Plugin AndroidPermission	Especificar um Provedor	Ativar Persistência em Disco
Acessar Funcionalidades das APIs pela Webview		Padronizar Troca de Dados com JSON
Usar Loaders para Gerenciar Ciclo de Vida		Submeter pequenos Patches
Verificar Dependências BuildGradle		

# Apêndice J

## Manual do Usuário - Risk Control

### J.1 Visão Geral do Sistema

O *Risk Control* é uma ferramenta para auxiliar times de desenvolvimento no gerenciamento de riscos tecnológicos dos projetos de software. Por meio de um perfil Administrador é possível criar domínios de projetos (i.e., contextos), associar tecnologias aos domínios, criar riscos tecnológicos, associar as tecnologias aos riscos, ponderar o impacto das tecnologias com os riscos, cadastrar estratégias, associar as estratégias aos riscos e ponderar o impacto das estratégias aos riscos. A ferramenta implementa uma Rede Bayesiana, e utiliza todas as informações cadastradas pelo administrador para modelagem do grafo e preenchimento das tabelas de probabilidade. Por fim, um perfil de usuário comum pode acessar o sistema tendo como funcionalidades: cadastrar projetos, cadastrar tecnologias, visualizar riscos potenciais ao projeto em listagem e *dashboard* e visualizar estratégias para os riscos previamente identificados.

### J.2 Perfil Administrador

#### J.2.1 Login

Ao acessar a URL do sistema, a primeira opção a ser visualizada é a tela de autenticação. O usuário deve informar login e senha para entrar no *Risk Control*. São dois perfis de usuário: administrador e usuário comum. Pela URL, é possível realizar o cadastro de usuários

comuns. As contas de administradores são definidas via banco de dados.

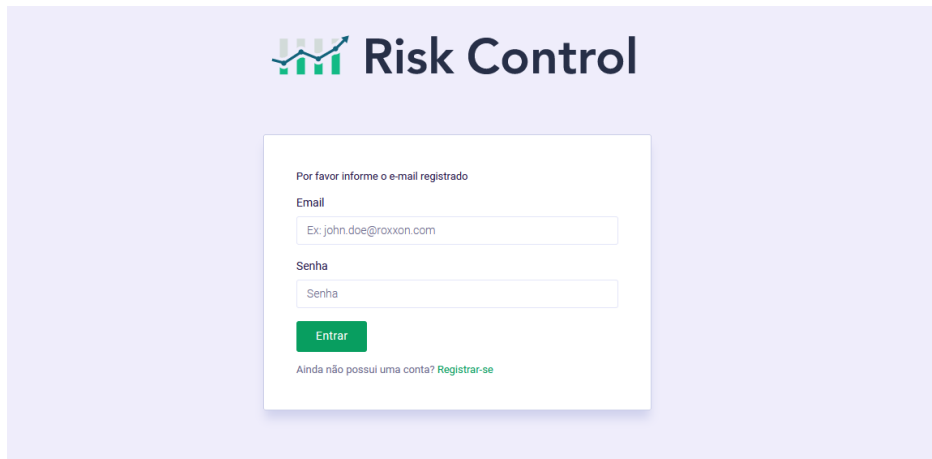


Figura J.1: Login da ferramenta Risk Control.

## J.2.2 Criação de Domínios e Tecnologias

Ao selecionar a opção “Tecnologias” no menu vertical, uma tela é apresentada ao usuário para cadastro de Domínios e as respectivas Tecnologias. Na Figura abaixo é possível visualizar três domínios cadastrados (i.e., Web, Mobile e IoT) e exemplos de tecnologias para o domínio web.

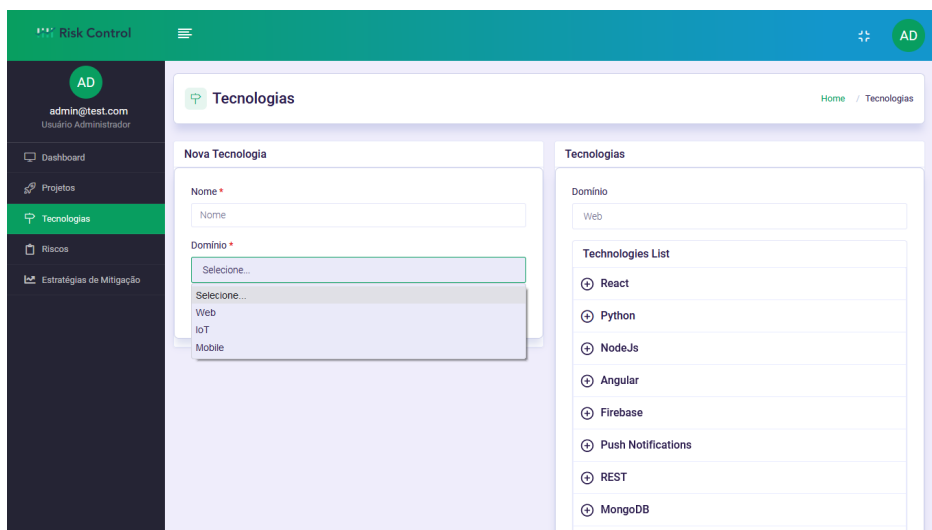


Figura J.2: Criação de Domínios e Tecnologias.

### J.2.3 Editar e remover Tecnologias

O administrador pode editar a descrição e nomenclatura das tecnologias previamente cadastradas. Também é possível removê-las, porém para garantir a integridade dos dados, apenas as tecnologias que ainda não foram associadas a riscos podem ser excluídas do sistema.

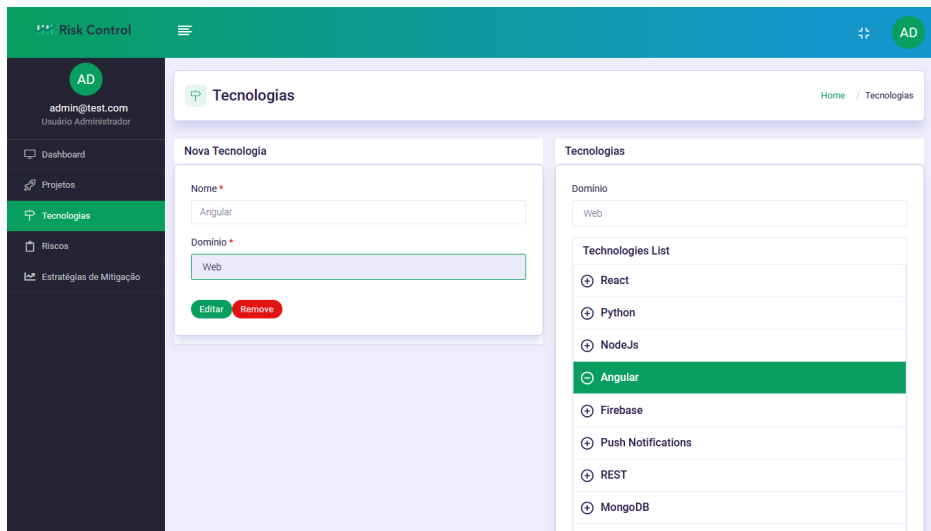


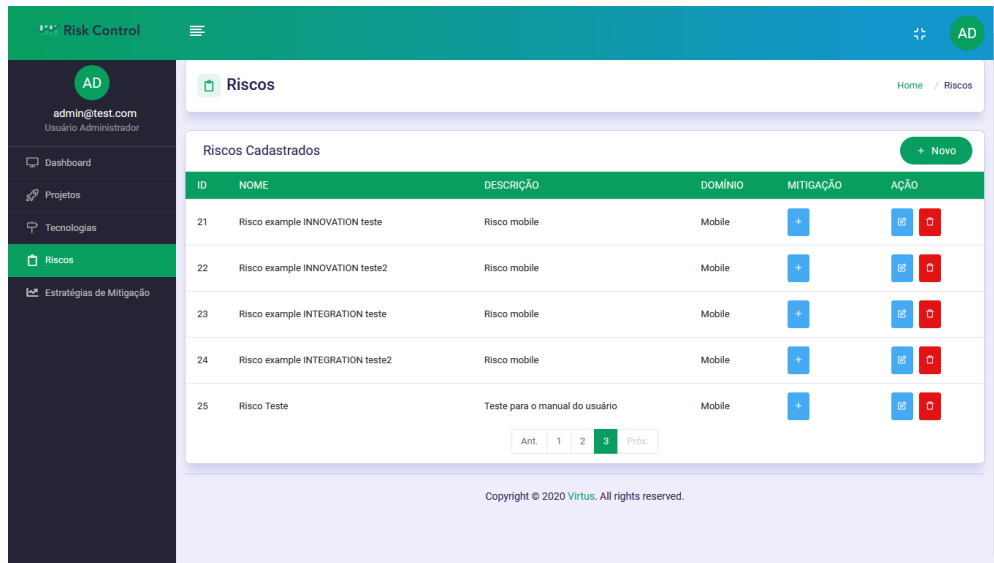
Figura J.3: Editar e remover Tecnologias.

### J.2.4 Listagem de Riscos

Ao selecionar a opção “Riscos” no menu vertical, uma tela é apresentada ao usuário com a listagem dos riscos cadastrados no sistema. Para cada risco listado, temos as seguintes opções de funcionalidades: criar um novo risco, associar estratégia de mitigação, editar ou remover o risco.

### J.2.5 Cadastro de Riscos

Ao selecionar a opção “+ Novo” sobre a listagem dos riscos, uma tela é apresentada ao usuário para cadastro de riscos. Na Figura abaixo é possível visualizar a tela de inserção, o usuário deve informar o risco, colocar uma descrição, informar seu tipo (valores pré definidos de acordo com a Rede Bayesiana) e o domínio.

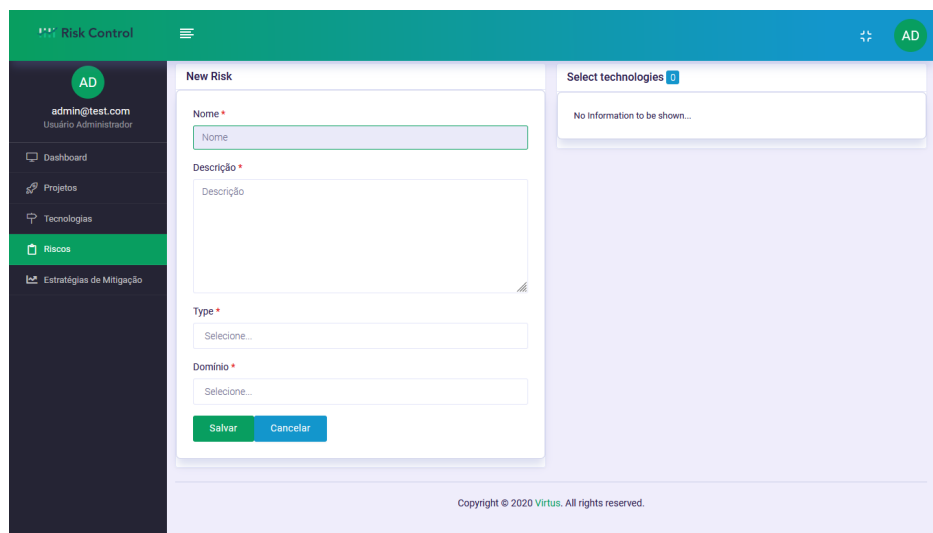


The screenshot displays the 'Riscos' (Risks) section of the Risk Control application. The interface includes a sidebar with navigation options: Dashboard, Projetos, Tecnologias, Riscos (selected), and Estratégias de Mitigação. The main content area shows a table of registered risks with the following data:

ID	NOME	DESCRIÇÃO	DOMÍNIO	MITIGAÇÃO	AÇÃO
21	Risco example INNOVATION teste	Risco mobile	Mobile	+	[Edit] [Delete]
22	Risco example INNOVATION teste2	Risco mobile	Mobile	+	[Edit] [Delete]
23	Risco example INTEGRATION teste	Risco mobile	Mobile	+	[Edit] [Delete]
24	Risco example INTEGRATION teste2	Risco mobile	Mobile	+	[Edit] [Delete]
25	Risco Teste	Teste para o manual do usuário	Mobile	+	[Edit] [Delete]

At the bottom of the table, there is a pagination control showing 'Art. 1 2 3 Próx.' with '3' highlighted. The footer of the application reads 'Copyright © 2020 Virtus. All rights reserved.'

Figura J.4: Listagem de Riscos.



The screenshot displays the 'New Risk' form in the Risk Control application. The form includes the following fields and controls:

- Nome \***: A text input field with the placeholder 'Nome'.
- Descrição \***: A text area with the placeholder 'Descrição'.
- Type \***: A dropdown menu with the placeholder 'Selecione...'.
- Domínio \***: A dropdown menu with the placeholder 'Selecione...'.
- Buttons**: 'Salvar' (Save) and 'Cancelar' (Cancel) buttons.

On the right side of the form, there is a section titled 'Select technologies' with a sub-header 'Select technologies' and a message 'No information to be shown...'. The footer of the application reads 'Copyright © 2020 Virtus. All rights reserved.'

Figura J.5: Cadastro de Riscos.

## J.2.6 Associar Tecnologias aos Riscos

Complementando o cadastro de riscos, o usuário deverá associar as tecnologias que têm relação com o risco. As tecnologias serão instanciadas no *backend* como nós folhas da Rede Bayesiana. Apenas as tecnologias previamente cadastradas são visualizadas.

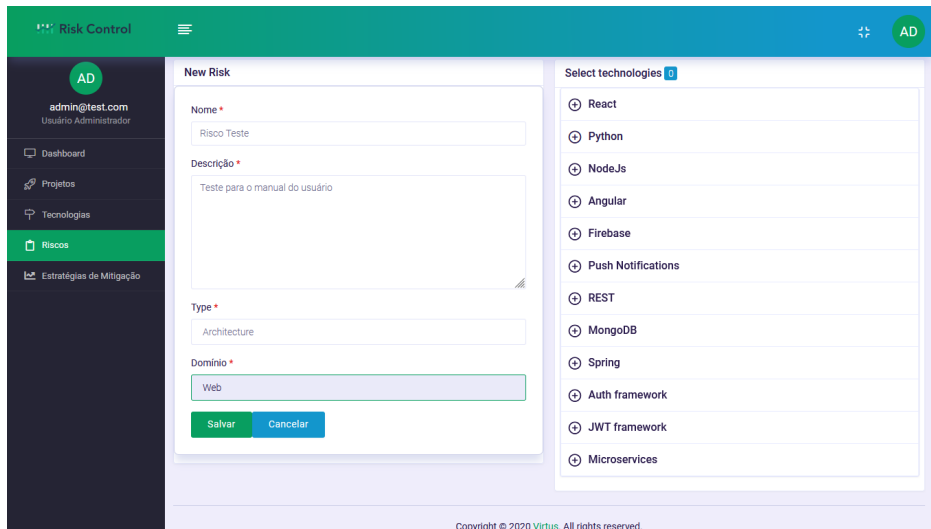


Figura J.6: Associar Tecnologias aos Riscos.

### J.2.7 Ponderar as Tecnologias

Ao associar tecnologias, o usuário deverá informar o impacto associada a esta tecnologia no risco supracitado. Essas informações servirão para preencher as tabelas de probabilidades da Rede Bayesiana.

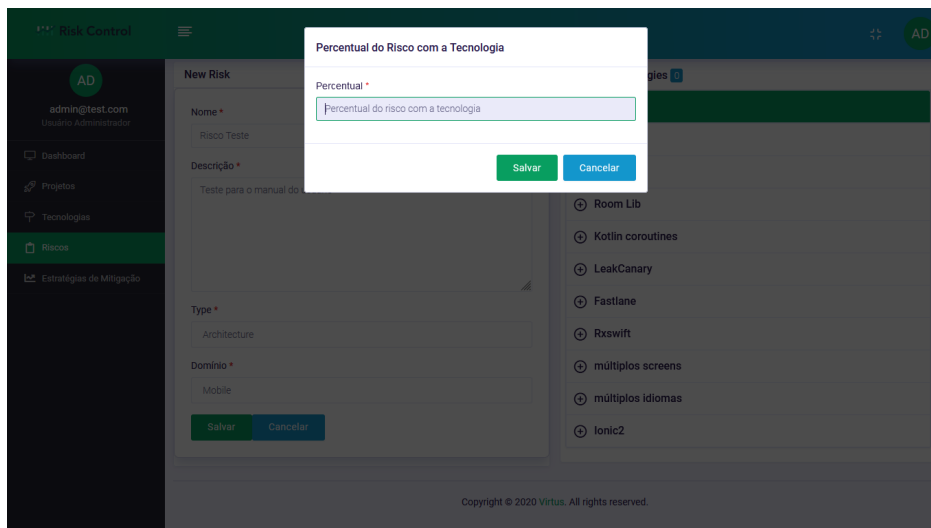


Figura J.7: Ponderar as tecnologias.

Nas figura abaixo todas informações para inserção do novo risco ao sistema estão apresentadas. Uma validação ocorre para verificar se o somatório de valores de probabilidades associadas as tecnologias é igual a 100%.

The screenshot displays the 'New Risk' form in the Risk Control application. The form contains the following fields and values:

- Nome:** Risco Teste
- Descrição:** Teste para o manual do usuário
- Type:** Architecture
- Domínio:** Mobile

On the right, the 'Select technologies' panel shows a list of technologies with their respective counts:

- Ionic: 85
- Electron
- Retrofit
- Room Lib
- Kotlin coroutines: 15
- LeakCanary
- Fastlane
- Rxswift
- múltiplos screens
- múltiplos idiomas
- Ionic2

The sidebar on the left shows the user 'admin@test.com' and navigation options: Dashboard, Projetos, Tecnologias, Riscos (highlighted), and Estratégias de Mitigação.

Figura J.8: Risco a ser inserido no sistema.

## J.2.8 Cadastrar Estratégias

É possível criar estratégias de mitigação ao selecionar a opção “Estratégias” no menu vertical, ou diretamente na listagem de riscos. As estratégias são individuais para cada risco, e são usadas para realizar a modelagem da Rede Bayesiana. As estratégias serão instanciadas no *backend* como nós folhas da Rede Bayesiana.

The screenshot displays the 'Estratégias de Mitigação' form in the Risk Control application. The form contains the following fields and values:

- Nome:** Nome
- Descrição:** Descrição

On the right, the 'Estratégias de Mitigação' panel shows a list of strategies with their respective counts:

- Estratégia teste
- Ant.: 1
- Próx.

The sidebar on the left shows the user 'admin@test.com' and navigation options: Dashboard, Projetos, Tecnologias, Riscos, and Estratégias de Mitigação (highlighted).

Figura J.9: Cadastrar Estratégias.



## J.3 Perfil Usuário Comum

### J.3.1 Listagem Projetos

Estando logado como usuário comum, a primeira tela a ser visualizada no sistema é a listagem de projetos sob coordenação do referido usuário. Na listagem existe o *link* para funcionalidades para adicionar tecnologias e edição dos dados gerais do projeto. Na parte superior o botão “Novo” é o caminho para o cadastro de novos projetos. No menu vertical do lado esquerdo é possível visualizar a opção “Dashboard” para visualização de um gráfico para cada projeto.

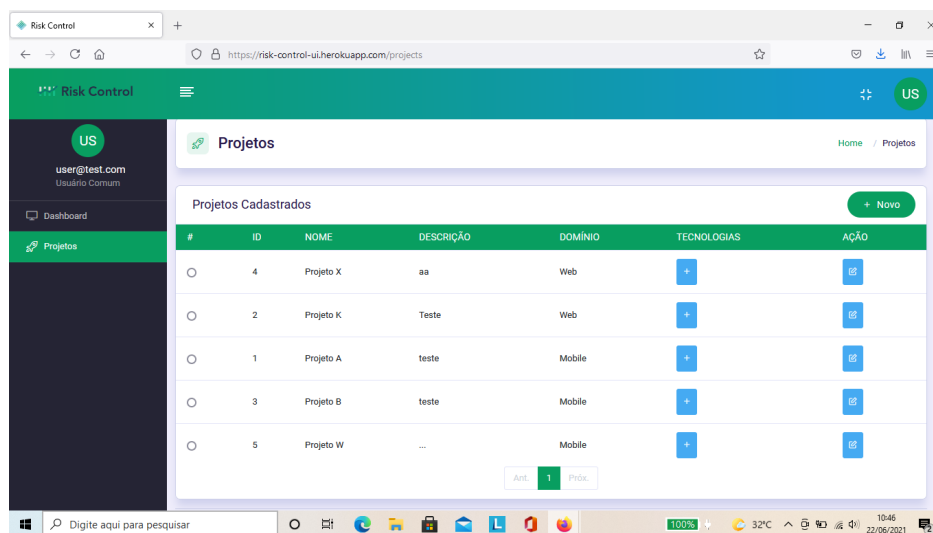


Figura J.10: Listagem Projetos.

### J.3.2 Cadastrar Projetos

Ao selecionar a opção “Novo” na listagem de projetos uma tela é apresentada ao usuário para cadastro de um novo projeto. Na Figura abaixo é possível visualizar o cadastro de um projeto, com os campos “Nome”, “Descrição”, “Domínio”, “Data de início” e “Data Final”. Ao salvar o projeto, este é inserido na listagem inicial.

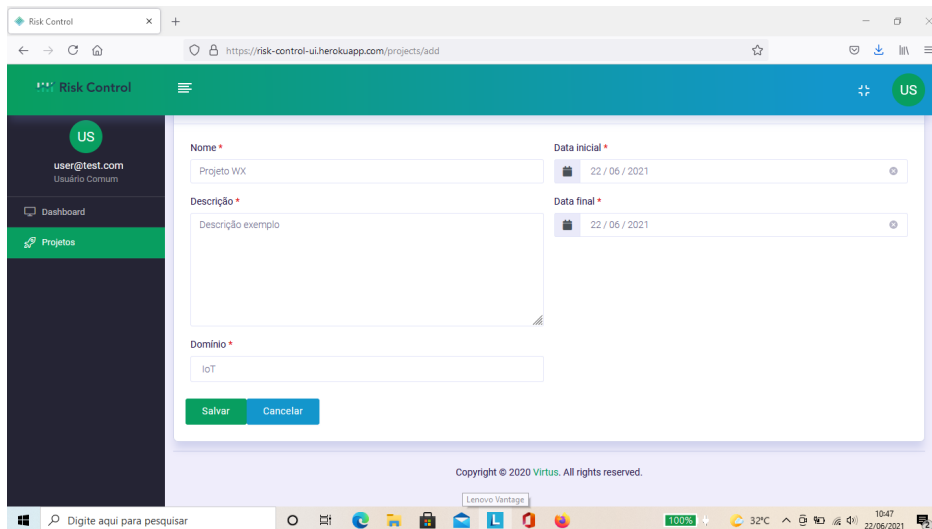


Figura J.11: Cadastrar Projetos.

### J.3.3 Cadastrar Tecnologias

Ao selecionar a opção “Tecnologias” para algum projeto na listagem uma tela é apresentada ao usuário para cadastro das tecnologias de um projeto. Na Figura abaixo é possível visualizar o cadastro de tecnologias para um projeto de domínio Mobile. As tecnologias listadas foram previamente cadastradas pelo administrador. Ao salvar o projeto, as tecnologias selecionadas são associadas ao projeto em questão.

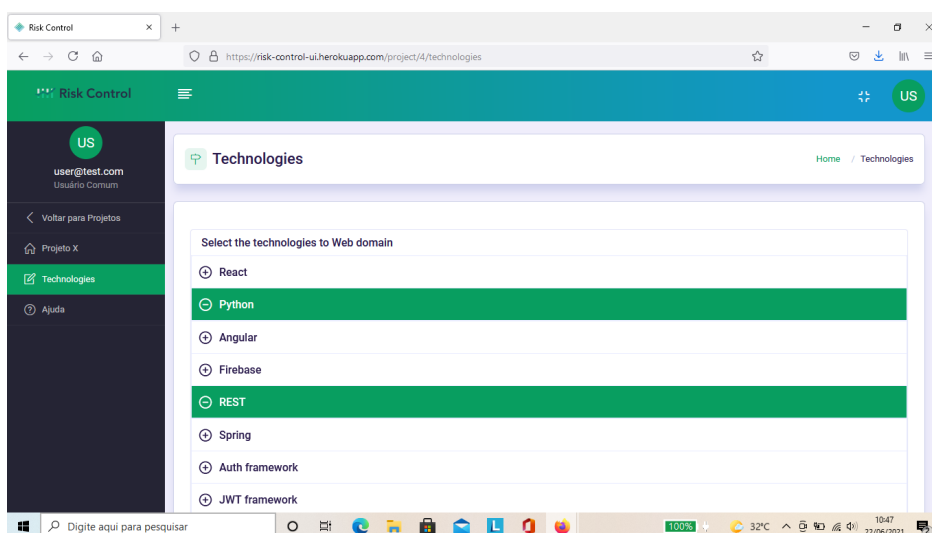


Figura J.12: Cadastrar Tecnologias.

### J.3.4 Visualizar Riscos e Dashboard

Ao selecionar um projeto e clicar na opção “Dashboard”, uma tela é apresentada ao usuário com uma visão dos riscos do projeto. Na Figura abaixo é possível visualizar a listagem de riscos para os projetos, estes são classificados por um tipo de acordo com os principais eixos da Rede Bayesiana (i.e, Ambiente, Inovação, Arquitetura e Método). Importante ressaltar que os riscos estão listados por ordem crescente de probabilidade. Também é possível observar um gráfico onde são divididos os quantitativos dos riscos de acordo com o eixos.

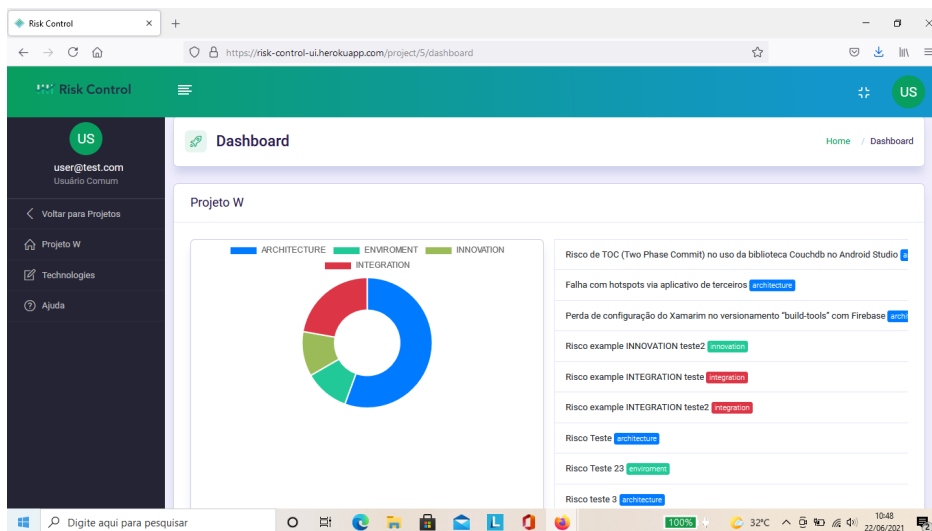


Figura J.13: Lista de Riscos e Dashboard.

# Apêndice K

## Manual do Desenvolvedor - Risk Control

### K.1 Frontend

#### K.1.1 Visão geral

De forma geral, a ferramenta *RiskControl* possui um módulo *Backend* implementado em Spring Boot, uma camada de *Frontend* desenvolvida em Angular. Para o processamento interno é utilizado uma *engine* SMILE para realizar as inferências bayesianas.

No *Frontend* encontra-se os componentes necessários para apresentação da aplicação no navegador. A principal tecnologia utilizada para o desenvolvimento desta aplicação é o *framework* Angular. Nesta seção encontram-se as dependências utilizadas no desenvolvimento do aplicativo, instruções para instalação e descrições dos componentes desenvolvidos.

#### K.1.2 Estrutura

Para organizar o *Frontend*, foi implementada uma estrutura que visa fazer uma separação em módulos e componentes. Os módulos são agrupados por nível de funcionalidade. Cada componente representa uma página (como login, por exemplo) ou algum elemento da aplicação (como o menu lateral), podendo conter *views* em HTML, *controllers*, *services*, *directives* e folhas de estilo. Os componentes e módulos são organizados da seguinte forma:

Mais detalhes dos componentes serão apresentados nas demais seções deste manual.

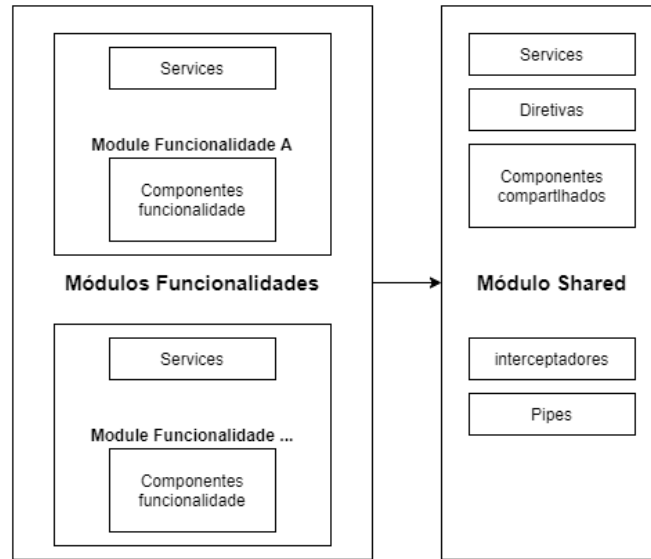


Figura K.1: Estrutura Frontend

### K.1.3 Dependências

Com relação as dependências este manual separou em dependências de desenvolvimento (i.e., as bibliotecas e ferramentas utilizadas para o ambiente de desenvolvimento do *frontend*) e as dependências da própria aplicação Web (i.e., bibliotecas e ferramentas utilizadas pela aplicação Web).

As dependências de desenvolvimento são:

@angular-devkit/build-angular	Essa dependência oferece a infraestrutura para construir e testar aplicativos Angular
@angular/cli	É uma ferramenta de interface de linha de comando para inicializar e criar scaffold e manter aplicações diretamente de um Shell
jasmine	É uma estrutura de desenvolvimento orientada a comportamento para testar o código JavaScript
karma	Test runner integrado ao Angular
protractor	Framework para criação de testes end-to-end
Typescript	Linguagem de programação nativa do Angular que é convertida para Javascript na aplicação final

As dependências da aplicação Web são:

Bootstrap e @ng-bootstrap	Biblioteca de componentes de interface integrados a aplicação
@angular/**	Dependências contendo todos os recursos do framework utilizado
8+@ng-select	Componente select utilizado na aplicação
@ngx-translate/core	Utilizado para lidar cenários de internacionalização
angular-mydatepicker	Componente de calendário
chart.js e ng2-charts	Dependências utilizadas para criar gráficos
jquery-mask-plugin	Biblioteca utilizada para tratar máscaras em formulários
moment e date-fns	Biblioteca utilizada para tratar diferentes formatos de datas
ngx-toastr	Utilizado para exibir mensagens de alerta ao usuário
rxjs	Biblioteca para programação reativa
sweetalert2	Fornece opções de diálogos de confirmação de operações.

### K.1.4 Services

Durante o desenvolvimento foi optado pela implementação de uma classe abstrata denominada **CrudService**. Esta contém detalhes genéricos para acessar recursos de APIs externas como criar, atualizar, buscar e deletar entidades utilizadas nas funcionalidades. Esta classe tem por objetivo o reaproveitamento de código e a otimização no desenvolvimento de serviços contendo recursos com operações comuns.

Por meio da classe abstrata **CrudService** é possível usufruir de operações básicas de um Crud sem necessidade de implementar novamente toda a lógica das operações. Um exemplo desse cenário é demonstrado no trecho de código a seguir.

---

```

1 import { Observable } from 'rxjs';
2 import { HttpClient, HttpParams } from '@angular/common/http';
3 import { Page } from '../model/page';
4 import { map } from 'rxjs/operators';
5
6 export abstract class CrudService<T, ID> {
7     constructor(
8         protected _http: HttpClient,
9         protected _base: string

```

```
10     ) { }
11     save(t: T): Observable<T> {
12         return this._http.post<T>(this._base, t);
13     }
14     update(id: ID, t: T): Observable<T> {
15         return this._http.put<T>(this._base + '/' + id, t, {});
16     }
17     updatePartial(id: ID, t: T): Observable<T> {
18         return this._http.patch<T>(this._base + '/' + id, t, {});
19     }
20     findOne(id: ID): Observable<T> {
21         return this._http.get<T>(this._base + '/' + id).pipe(map(
22             item => {
23                 return item;
24             }
25         ));
26     }
27     findAll(options: {params?: HttpParams}): Observable<T[]> {
28         return this._http.get<T[]>(this._base, options);
29     }
30     findAllPaginated(options: {params?: HttpParams}): Observable<Page
31         <T>> {
32         return this._http.get<Page<T>>(this._base, options);
33     }
34     delete(id: ID): Observable<T> {
35         return this._http.delete<T>(this._base + '/' + id);
36     }
37 }
```

Diante do código, é possível observar que na classe **RiskService**, todos os recursos de um crud comum ficam disponíveis usando os recursos de Herança com uso de *Generics*. Assim, torna-se necessário apenas a implementação de recursos mais específicos a um determinado serviço.

```
1 @Injectable({ providedIn: 'root' })
2 export class RiskService extends CrudService<Risk, number>{
3     constructor(protected _http: HttpClient) {
4         super(_http, 'api/risks');
5     }
6 }
```

```
6     findByDomainNameAndTechnologiesIdInPaginated(domain: Domain, options:
      { params?: HttpParams }): Observable<Page<Risk>>{
7         return this._http.get<Page<Risk>>(this._base + '/domain/' +
          domain.name, options);
8     }
9     findByDomainNameAndTechnologiesIdIn(domain: Domain, options: { params
      ?: HttpParams }): Observable<Risk[]>{
10        return this._http.get<Risk[]>(this._base + '/domain/' + domain.
          name, options);
11    }
12 }
```

---

### K.1.5 Módulo Shared

Com o objetivo de centralizar e reaproveitar componentes, foi criado o módulo Shared. O mesmo entendimento segue para serviços, pipes, interceptadores na aplicação. São exemplos *modals*, componentes de notificação, pipes para formatação de informações e interceptadores de autenticação. Na Figura K.2 é apresentado uma visão do módulo Shared.

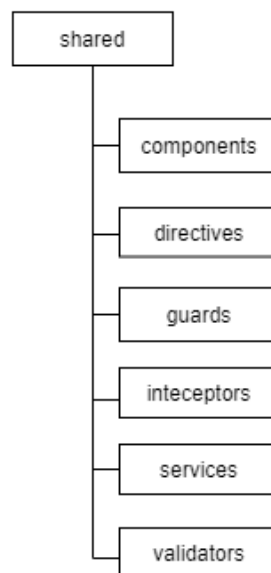


Figura K.2: Módulo Shared



## K.1.6 Módulo Funcionalidades

Cada contexto de funcionalidade foi separado em um módulo do Angular. Por exemplo, temos o módulo de risco que contém toda a lógica, serviços e componentes relacionados a um operações de risco. Diante disto, o módulo de funcionalidade a nível global organiza a distribuição e acesso a esses módulos com a configuração e carregamento de cada módulo. Na Figura K.3 é apresentado uma visão do módulo Funcionalidades.

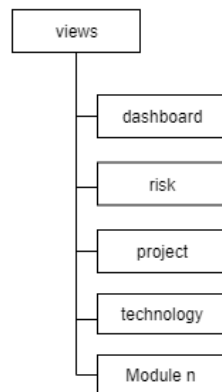


Figura K.3: Módulo Funcionalidades

## K.2 Backend

### K.2.1 Visão Geral

O *Backend* trata-se de uma API responsável pela gerência da persistência de dados e lógicas de negócios da aplicação. Sua construção foi baseada no estilo de arquitetura REST que utiliza os verbos HTTP como forma de comunicação entre serviços ou aplicação de terceiros. Nesse cenário, foi adotado com padrão de implementação o *framework* Spring Boot que fornece padrões e infraestrutura para criação e exposição de serviços.

### K.2.2 Dependências

Para o gerenciamento das dependências foi utilizado o Maven, contendo as seguintes dependências:

spring-boot-starter-web	Contém toda infraestrutura necessária para inicializar a aplicação.
spring-boot-starter-test	Contém toda infraestrutura necessária para realização de testes de unidade e de integração.
spring-boot-starter-security	Contém a infraestrutura necessária para adicionar uma camada de segurança no projeto.
postgresql	Fornecer configurações para comunicação da aplicação com o banco de dados
spring-boot-starter-data-jpa	Contém a estrutura para criar, atualizar e remover registros no banco de dados
flyway-core	Ferramenta para gerenciamento do versionamento do banco de dados
h2	Fornecer configuração para criação e comunicação de instâncias para o banco de dados em memória h2

### K.2.3 Estrutura

O projeto *Backend* foi dividido em três módulos Maven, a Figura K.4 apresenta esta separação. A opção de dispor de mais de um módulo no desenvolvimento deu-se pelo o objetivo de reaproveitar e melhor organizar o código, motivado por arquiteturas de software como *Domain Driven Design* (DDD) e *Clean Architecture*. Dado pelo incentivo de construir softwares com contextos bem delimitados, lidando com uma maior divisão entre negócio e infraestrutura. Abaixo é descrito cada um dos módulos presentes no projeto.

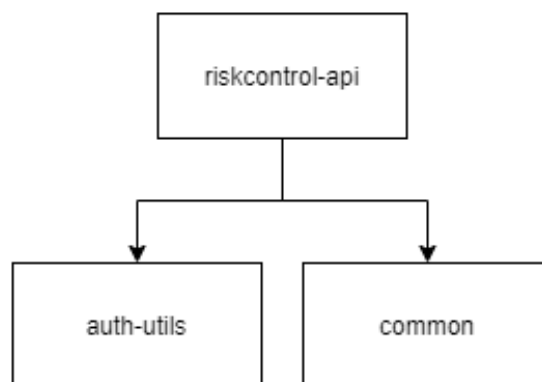


Figura K.4: Estrutura

- **Módulo auth-utils:** Agrupa um conjunto de regras, configurações para adição de uma

camada de autenticação no projeto;

- **Módulo common:** Agrupa configurações, serviços genéricos, validações e classes utilitárias genéricas para serem reutilizadas em outros módulos;
- **riskcontrol-api:** Contém a lógica de negócio, recursos e persistência da aplicação, sendo a parte principal do projeto Back-end.

#### K.2.4 Módulo RiskControl-API

O riskcontrol-api possui todos os controles, modelos e repositórios necessários para criação e execução de todas as regras do negócio do projeto.



Figura K.5: RiskControl-API

No que diz respeito aos controles, de forma semelhante à apresentada no projeto *frontend*, foi priorizado pelo o uso de uma classe abstrata genérica de controle. Com isso foi realizada a implementação de operações básicas para salvar, atualizar, remover e um determinado recurso.

Durante a implementação dos controles que fornecem todos os recursos via HTTP disponibilizados externamente, foram criados *Data Transfer Objects* (DTOs) para desvincular o modelo de negócio dos objetos a serem acessados e persistidos por terceiros. Desta forma garantindo a integridades das informações sensíveis para o negócio.

Para persistência dos dados foi adotado o padrão de projeto *Repository*. Este por sua vez, está totalmente integrado ao *framework* Spring, sendo provido interfaces e configurações que permitem as operações comuns na base de dados. Neste contexto, é abstraída a complexidade do acesso e gerenciamento de conexões com a base de dados e empregada uma linguagem mais intuitiva a orientação de objetos no que refere-se às operações com SQL.

### K.2.5 Modelo de Dados

Para a persistência, foi adotado o banco de dados relacional PostgreSQL, escrito na linguagem SQL. O modelo de dados é gerenciado pela ferramenta Flyway que integrada ao Spring cria e atualiza as tabelas. A Figura K.6 apresenta o modelo de dados da aplicação.

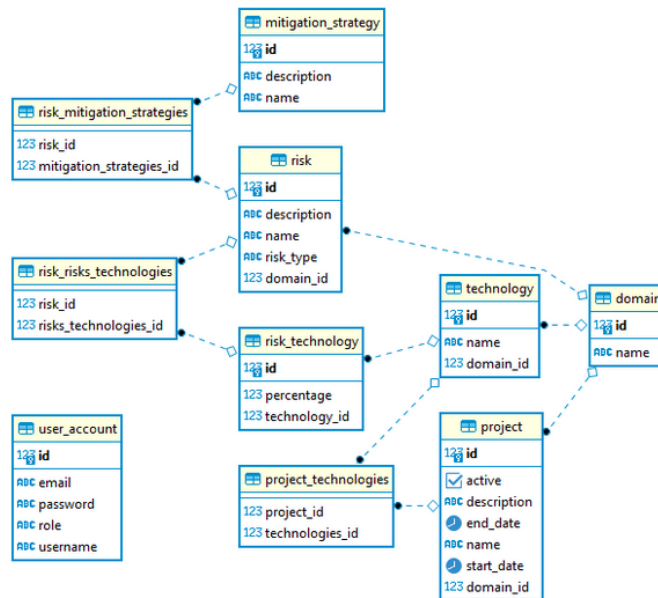


Figura K.6: Modelo de Dados