UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

PROPOSTA DE TRATAMENTO DE FATORES DE RISCOS EM DESENVOLVIMENTO DE SOFTWARE PARA UMA ORGANIZAÇÃO DO SETOR PÚBLICO

MESTRANDA: SYLVIA CAMPOS DA LUZ E SILVA (SCLS@CIN.UFPE.BR)

ORIENTADOR: HERMANO PERRELLI DE MOURA (HERMANO@CIN.UFPE.BR)
CO-ORIENTADORA: CRISTINE MARTINS GOMES DE GUSMÃO
(CMGG@CIN.UFPE.BR)

Recife, fevereiro | 2011

UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE INFORMÁTICA

SYLVIA CAMPOS DA LUZ E SILVA

PROPOSTA DE TRATAMENTO DE FATORES DE RISCOS EM DESENVOLVIMENTO DE SOFTWARE PARA UMA ORGANIZAÇÃO DO SETOR PÚBLICO

TRABALHO APRESENTADO AO PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO DO CENTRO DE INFORMÁTICA DA UNIVERSIDADE FEDERAL DE PERNAMBUCO COMO REQUISITO PARCIAL PARA OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIA DA COMPUTAÇÃO

ORIENTADOR: PROF. DR. HERMANO PERRELLI DE MOURA

CO-ORIENTADORA: PROF. DRA. CRISTINE MARTINS GOMES DE GUSMÃO

RECIFE

28 DE FEVEREIRO DE 2011

Catalogação na fonte
Bibliotecária Jane Souto Maior, CRB4-571

Luz e Silva, Sylvia Campos da
Proposta de tratamento de fatores de riscos em desenvolvimento de software para organização do setor público / Sylvia Campos da Luz e Silva - Recife: O Autor, 2011.
xiv, 161 folhas : il., fig., tab.

Orientador: Hermano Perrelli de Moura.
Dissertação (mestrado) Universidade Federal de Pernambuco. CIn. Ciência da Computação, 2011.

Inclui bibliografia e anexo.

1. Engenharia de software. 2. Gerenciamento de projetos. 3. Gerência de riscos. I. Moura, Hermano Perrelli de (orientador). II. Título.

005.1 CDD (22. ed.) MEI2011 – 055

Dissertação de Mestrado apresentada por **Sylvia Campos da Luz Silva** à Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco, sob o título "**Proposta de Tratamento de Fatores de Riscos em Desenvolvimento de Software no Âmbito da Secretaria da Fazenda do Estado de São Paulo**", orientada pelo **Prof. Hermano Perrelli de Moura** e co-orientada pela **Profa. Cristine Martins Gomes de Gusmão** e aprovada pela Banca Examinadora formada pelos professores:

Prof. Sergio Castelo Branco Soares
Centro de Informática / UFPE

Profa. Caroline Maria de Miranda Mota
Departamento de Engenharia de Produção / UFPE

Profa. Cristine Martins Gomes de Gusmão
Núcleo de Telesaúde / UFPE

Visto e permitida a impressão.
Recife, 28 de fevereiro de 2011

Prof. Nelson Souto Rosa
Coordenador da Pós-Graduação em Ciência da Computação do
Centro de Informática da Universidade Federal de Pernambuco.

“É PERDOÁVEL SER DERROTADO, MAS NUNCA SURPREENDIDO”.

FREDERICO, O GRANDE.

Agradecimentos

Primeiramente, a Deus pela possibilidade de começar e concluir mais um trabalho na minha vida.

À minha família, obrigada pelo amor irrestrito e pelos cuidados e atenção prestada durante esses anos.

Van, pelo carinho e colaboração. Pelas várias horas dedicadas, sonos perdidos e muitos cafezinhos me ajudando. O impulso final para conclusão deste trabalho foi graças a você.

Leni, pelos conselhos, orientação e amizade. Por ser meu porto seguro durante esses longos meses que valeram por anos de experiência e amadurecimento.

Jeane, pela amizade invejável que temos, pelo apoio e companheirismo durante o colégio, faculdade, trabalho e principalmente na vida.

A todos os meus amigos, em especial a Shirley, Pedro, Patrícia, Marília e Renata pelo carinho e apoio nos momentos mais difíceis e por compartilharem comigo as alegrias alcançadas.

Aos meus orientadores, professores Hermano Perrelli e Cristine Gusmão pelo excepcional trabalho e pelo incentivo a buscar sempre a excelência durante todos esses anos.

Ao Departamento de Tecnologia pela confiança e colaboração durante toda a pesquisa.

Muito obrigada.

Resumo

Os projetos de Tecnologia de Informação possuem características marcantes, que os diferencia dos demais - são projetos onde o controle sobre as incertezas e as indefinições é um forte fator de determinação do sucesso ou do fracasso do empreendimento

A Gerência de Riscos é, possivelmente, a forma escolhida por muitos gestores e executivos para prevenir-se dos aspectos críticos associados aos seus negócios. Executar corretamente os processos envolvidos na identificação, análise e tratamento dos riscos do projeto promove a maximização dos resultados das ocorrências positivas e minimização das consequências negativas.

Sendo recentemente introduzida no setor público brasileiro, a Gestão de Riscos possui diferenças fundamentais, neste âmbito, que devem ser consideradas. Além das particularidades inerentes a cada empresa ou organização, sabe-se que órgãos públicos possuem características diversas ao âmbito privado que potencializam o aparecimento de fatores de riscos que não são encontrados ou possuem impactos diferenciados no setor privado. Podemos citar como exemplo os fatores políticos, sociais e legais.

A identificação dos riscos e de seus fatores significa a compreensão das origens de cada perigo. Deve-se buscar responder por que o perigo existe no ambiente, quais são as condições que potencializam a concretização do evento estudado.

O escopo deste trabalho é mapear e analisar os principais Fatores de Riscos existentes no ambiente de Desenvolvimento de Software de uma Organização do Setor Público e desenvolver seus planos de ações utilizando como metodologia de pesquisa a Teoria Fundamentada em Dados e o Método Brasiliano de Análise de Riscos.

PALAVRAS-CHAVES:
Desenvolvimento de Software, Gerenciamento de Riscos, Fatores de Riscos, Riscos em Organizações Públicas, Teoria Fundamentada em Dados, Método Brasiliano de Análise de Risco.

Abstract

Information Technology projects possess marking characteristics, which differentiate them from others – they are projects where control over uncertainties and indefinitions are a strong determining factor of success or failure of the enterprise.

Risk management is, possibly, the chosen form for preventing critical aspects in the business by managers and executives. The correct execution of the processes involved in the identification, analysis and treatment of project risks promotes the maximization of results from positive occurrences and the minimization of negative consequences.

Recently introduced in the Brazilian public sector, Risk Management possesses fundamental differences, in this environment, that must be taken into consideration. Besides the inherent particularities of each company or organization, it is known that public government agencies have different characteristics from the private sector that increase the appearance of risk factors that are not encountered or have few differentiated impacts in the private sector. We can cite as an example the political, social and legal factors.

The identification of risks and their factors encompass the comprehension of the origins of each danger. An answer must be sought regarding why the danger exists and which conditions increase the chances of realization of the event studied.

The scope of this work is to map and analyze the main existing Risk Factors in the Software Development environment of a Public Sector Organization and develop its action plans using Grounded Theory and the Brasiliano Method for Risk Analysis as research methodology.

KEY-WORDS:

Software Development, Risk Management, Risks Factors, Public Sector Risks, Grounded Theory, Brasiliano Method for Risk Analysis.

Índice de Tabelas

Tabela 1: Diferenças na abordagem de risco do Setor Privado para o Setor Público.....3

Tabela 2: Metodologia de Trabalho.....14

Tabela 3: Matriz de Impactos Cruzados – Grau de Impacto.....52

Tabela 4: Nível do Fator de Risco.....56

Tabela 5: Escala do Critério da Exposição.....57

Tabela 6: Classificação do Nível de Probabilidade.....58

Tabela 7: Escala do Fator Impacto "Imagem".....59

Tabela 8: Escala do Fator Impacto "Financeiro".....60

Tabela 9: Escala do Fator Impacto "Legislação".....60

Tabela 10: Escala do Fator Impacto "Operacional".....60

Tabela 11: Escala de Classificação do Nível de Impacto.....61

Tabela 12: Métodos Quantitativos versus Métodos Qualitativos: Quadro Comparativo.....72

Tabela 13: Exemplos de categorias de "Achado de Risco" identificadas na codificação axial 102

Tabela 14: Exemplos de categorias de "Plano de Ação" identificadas na codificação axial..102

Tabela 15: Passos da codificação *versus* Tipo de categorias identificadas.....104

Tabela 16: Matriz SWOT – Cálculo da Motricidade.....110

Tabela 17: Critério da Exposição adaptado.....119

Tabela 18: Escala do Fator "Imagem" adaptada.....121

Tabela 19: TFD - Categorias de "Plano de Ação".....144

Tabela 20: TFD – Categorias de "Achados de Risco".....148

Tabela 21: TFD – Categorias de "Fator de Risco".....150

Tabela 22: TFD – Categorias de "Perigo".....152

Índice de Figuras

Figura 1: Cronologia da Gerência de Riscos [Gusmão 2007] 19

Figura 2: Perigo versus Riscos versus Fatores de Risco 22

Figura 3: Técnicas para Identificação de Riscos [Gusmão 2007].....30

Figura 4: ISO 3100 – Estrutura.....40

Figura 5: ISO 31000 – Processo de Gerenciamento de Riscos.....43

Figura 6: Diagrama de Causa e Efeito.....48

Figura 7: Matriz SWOT.....50

Figura 8: Matriz de Impactos Cruzados – Exemplo de uso 52

Figura 9: Gráfico - Motricidade x Dependência.....53

Figura 10: Fatores de Impacto 59

Figura 11: Matriz de Vulnerabilidade 62

Figura 12: Plano de Ação - Técnica 5W-2H.....65

Figura 13: 1ª Fase: Estrutura Geral - Teoria Fundamentada em Dados.....85

Figura 14: Organizacional do Departamento de Tecnologia da Informação 98

Figura 15: Esquema gráfico com as associações relacionadas ao Perigo [P04] Fuga da Informação.....105

Figura 16: Esquema gráfico com as associações relacionadas ao Perigo [P11] Estimativas de tempo e prazo irreais. 105

Figura 17: Esquema gráfico com as associações relacionadas ao Perigo [P12] Requisitos mal entendidos e/ou definidos. 106

Figura 18: Esquema gráfico com as associações relacionadas ao Perigo [P14] Indisponibilidade de sistemas durante a implantação.....106

Figura 19: Esquema gráfico com as associações relacionadas ao Perigo [P10] Perda da motivação da equipe. 107

Figura 20: Matriz de Impactos Cruzados - Resultado 113

Figura 21: Matriz Motricidade x Dependência - Resultado 114

Figura 22: Perigo “Requisitos mal entendidos e/ou definidos” - Diagrama de Causa e Efeito. 118

Figura 23: Análise dos Riscos - Probabilidade.....120

Figura 24: Análise dos Riscos - Impacto.....122

Figura 25: Matriz de Riscos - Resultado.....123

Figura 26: Plano de Ação Proposto 126

Figura 27: P01 – Diagrama de Causa e Efeito 153

Figura 28: P02 – Diagrama de Causa e Efeito 153

Figura 29: P03 – Diagrama de Causa e Efeito 154

Figura 30: P04 – Diagrama de Causa e Efeito 154

Figura 31: P05 – Diagrama de Causa e Efeito 155

Figura 32: P06 – Diagrama de Causa e Efeito 155

Figura 33: P07 – Diagrama de Causa e Efeito 156

Figura 34: P08 – Diagrama de Causa e Efeito 156

Figura 35: P09 – Diagrama de Causa e Efeito 157

Figura 36: P10 – Diagrama de Causa e Efeito 157

Figura 37: P11 – Diagrama de Causa e Efeito 158

Figura 38: P12 - Diagrama de Causa e Efeito.....158

Figura 39: P13 – Diagrama de Causa e Efeito 159

Figura 40: P14 – Diagrama de Causa e Efeito 159

Figura 42: P15 – Diagrama de Causa e Efeito 160

Figura 43: P16 – Diagrama de Causa e Efeito 160

Figura 44: P17 – Diagrama de Causa e Efeito 161

Índice de Equações

Equação 1: Cálculo dos pontos médios de motricidade e de dependência 53

Equação 2: Cálculo do Críterio do Fator de Risco 57

Equação 3: Cálculo do Grau de Probabilidade 58

Equação 4: Cálculo do Nível de Impacto 61

Equação 5: Cálculo do Critério “Fator de Risco”. 119

Sumário

1. Introdução 1

1.1. Engenharia de Software 4

1.2. Gerenciamento de Riscos 8

1.3. Teoria Fundamentada em Dados 9

1.4. Problema Tratado 12

1.5. Objetivos e Contribuições 13

1.6. Metodologia de trabalho 14

1.7. Organização da Dissertação 15

2. Referencial Teórico 17

2.1. Gerenciamento de Riscos 17

2.1.1. História e Origens 17

2.1.2. Perigo *versus* Risco *versus* Fatores de Risco 20

2.1.3. Riscos em Engenharia de Software 22

2.1.4. Gerência de Riscos e Tomada de Decisão 24

2.1.5. Gerenciamento de Projetos *versus* Gerenciamento de Riscos 25

2.1.6. Atividades da Gerência de Riscos: Visão de Metodologias 27

2.1.7. Métodos de Identificação de Riscos 29

2.1.8. Técnicas de Análise e Avaliação de Riscos 34

2.2. Método Brasiliano de Análise de Riscos 37

2.2.1. ISO 31000:2009 – Gestão de Riscos 38

2.2.1.1. Objetivos 38

2.2.1.2. Estrutura Geral da Norma 39

2.2.1.3. Processos 43

2.2.2. Método Brasiliano 45

2.2.2.1. Comunicação e Consulta 46

2.2.2.2. Contextos Estratégicos 46
2.2.2.3. Processo de Avaliação de Riscos 46
2.2.2.3.1. Identificação dos Perigos e Fatores de Riscos 47
2.2.2.3.2. Análise dos Riscos 54
2.2.2.3.3. Avaliação dos Riscos – Nível de Risco 61
2.2.2.4. Resposta aos Riscos – Plano de Ação 63
2.2.2.5. Monitoração e Análise Crítica 67
2.3. Teoria Fundamentada em Dados 68
2.3.1. Métodos Qualitativos *versus* Métodos Quantitativos 68
2.3.2. Métodos Qualitativos 70
2.3.3. Métodos Quantitativos 71
2.3.4. A Teoria Fundamentada em Dados 74
2.3.4.1. Linhas de Pesquisa 74
2.3.4.2. Princípio da Emergência 75
2.3.4.3. Comparação Constante 76
2.3.4.4. Amostragem Teórica 77
2.3.4.5. Procedimentos de Codificação 78
2.3.4.6. Aplicação da Teoria Fundamentada em Dados na Área de Software 80
2.4. Resumo do Capítulo 82
3. Metodologia de Pesquisa 83
3.1. Estratégias e Ações 83
3.2. 1ª Fase - Descrição dos Passos 85
3.2.1. 1º Passo – Definir o contexto e escopo do estudo 86
3.2.2. 2º Passo – Definir e aplicar mecanismos de coleta de dados 87
3.2.3. 3º Passo – Realizar codificação aberta dos dados 89
3.2.4. 4º Passo – Realizar codificação axial dos dados 90

3.2.5. 5º Passo – Realizar codificação seletiva dos dados 91
3.2.6. 6º Passo – Auditar o estudo 92
3.3. 2ª Fase - Descrição dos Passos 93
3.3.1. 1º Passo – Identificar os Fatores de Riscos 93
3.3.2. 2º Passo – Identificar a Motricidade dos Fatores de Riscos 93
3.3.3. 3º Passo – Cálculo do Grau de Probabilidade 94
3.3.3.1. Critério do Fator de Risco (FR) 94
3.3.3.2. Critério da Exposição (E) 94
3.3.4. 4º Passo – Definição da Relevância do Impacto 95
3.3.5. 5º Passo – Determinação do Nível de Impacto 95
3.3.6. 6º Passo – Construção da Matriz de Riscos 95
3.3.7. 7º Passo – Elaboração do Plano de Ação 95
3.4. Resumo do Capítulo 96
4. Mapeamento dos Fatores de Riscos e Plano de Respostas 97
4.1. Resultados da 1ª Fase – Teoria Fundamentada em Dados 97
4.1.1. Contexto Organizacional 97
4.1.1.1. Departamento de Tecnologia da Informação 98
4.1.1.2. Centro de Desenvolvimento de Sistemas 99
4.1.2. Mecanismo de coleta de dados 100
4.1.3. Codificação dos dados 101
4.2. Resultados da 2ª Fase – Método Brasiliano de Análise de Riscos 109
4.2.1. Identificação dos Perigos e Fatores de Riscos 109
4.2.2. Identificação da Motricidade dos Fatores de Riscos 110
4.2.3. Análise dos Riscos 116
4.2.3.1. Cálculo do Grau de Probabilidade 117
4.2.3.1.1. Cálculo do Critério “Fator de Risco” 117

4.2.3.1.2. Cálculo do Critério da Exposição 119
4.2.3.2. Definição da Relevância do Impacto 120
4.2.3.3. Determinação do Nível de Impacto 121
4.2.4. Avaliação de Riscos 122
4.2.4.1. Construção da Matriz de Riscos 122
4.2.5. Resposta aos Riscos: Plano de Ação 124
4.2.5.1. Elaboração do Plano de Ação 124
4.3. Resumo do Capítulo 127
5. Conclusões e Trabalhos Futuros 128
5.1. Resultados 128
5.2. Limitações 129
5.3. Conclusões 130
5.4. Trabalhos Futuros 131
5.5. Trabalhos Relacionados 131
Referências 134
Anexo I 144

1. Introdução

Para ser bem-sucedida, a organização deve estar comprometida com uma abordagem de riscos proativa consistente durante todo o projeto [PMBOK 2004]. Com esta citação o Guia PMBOK – *Project Management Body of Knowledge* [PMI 2009] demonstra a crescente preocupação da comunidade de Engenharia de Software com a gestão de riscos como parte fundamental da gerência de projetos.

Relatório recém-lançado do *Standish Group*, o *Chaos Report* 2009 [Standish Group 2009] mostra uma queda no percentual dos projetos com sucesso, atingindo apenas 32% dos projetos entregues no prazo, no orçamento com recursos e funções planejados, 44% dos projetos estão atrasados, com o orçamento estourado e poucas funcionalidades requeridas inicialmente, e 24% dos projetos foram cancelados antes de sua conclusão ou entregues e nunca foram usados pelas empresas. “Esses números representam uma decepção nas taxas de sucesso de do estudo anterior, bem como um aumento significativo no número de falhas”, diz Jim Crear, *Standish Group* CIO. “Eles são ponto mais baixo nos últimos cinco períodos de estudo. Este ano, os resultados representam a maior taxa de falha em mais de uma década.”

Estes dados mostram que, mesmo décadas após a crise do software, muito ainda deve ser feito. Neste período, a sistematização e aplicação de boas práticas e metodologias mudaram significativamente a realidade, porém, se este avanço tem sido lento devido as dificuldade das pequenas organizações em implantar processos, a situação ainda é mais agravante em organizações dos setores públicos, que ainda estão dando os primeiros passos na incorporação da gestão de projetos em sua cultura organizacional.

Os projetos de Tecnologia de Informação possuem características marcantes, que os diferencia dos demais – são projetos onde o controle sobre as incertezas e as indefinições é um forte fator de determinação do sucesso ou do fracasso do empreendimento. Os projetos de TI iniciam-se com vagas ideias do que se deseja, pouco conhecimento do processo e quase nenhuma visão dos resultados. Este é um cenário normalmente encontrado, que requer grande esforço da equipe de TI e, principalmente, muita atenção

do Gerente do Projeto para transformar desejos dos usuários em um ferramental que torne os seus clientes mais competitivos para o mercado. Gerenciar este ambiente desconhecido é o propósito que as novas técnicas de gestão buscam resolver, entre elas está o Gerenciamento de Risco.

A indústria de Tecnologia de Informação (TI) está evoluindo e desenvolvendo metodologias, técnicas e instrumentos para que os projetos de TI sejam mais previsíveis e que alcancem seus resultados no prazo, dentro do orçamento e com a qualidade previamente especificada. O Gerenciamento de Risco é uma técnica recente e ainda é muito pouco empregada, mas representa um grande instrumento para o Gerente do Projeto [Rovai 2005].

Greg Shipler, diretor de tecnologia na Neohapsis também colaborador da *InformationWeek* EUA [Greg Shipler 2010], depois de analisar sucessos e fracassos e de conversar com líderes da indústria, notou que uma tendência se destaca: Quando se trata de iniciativas de desenvolvimento de software, o mantra "Seja pró-ativo, não reativo!" já vem sendo disseminado há algum tempo. Infelizmente, se percebe que muitas organizações continuam a definir suas prioridades com base nos incidentes que já ocorreram.

A Gerência de Riscos procura identificar os riscos associados às suas probabilidades de manifestação, estimar os prejuízos, orientar quanto aos procedimentos a serem adotados e monitorar o processo de desenvolvimento do software. Ao disponibilizar visões de suporte e favorecer o compartilhamento das informações geradas, o processo de Gerência de Riscos permite a tomada de decisão melhor fundamentada, minimizando assim os problemas supracitados.

No Guia PMBOK, podemos encontrar metodologias e práticas para abordar, planejar e executar atividades de gerenciamento de riscos. Dentre os processos da gerência de riscos estão: identificação de riscos, análise qualitativa de riscos, análise quantitativa de riscos, planejamento de resposta a riscos, monitoramento e controle dos riscos. Dentre esses processos, a identificação de riscos é crucial para que os mesmos possam ser gerenciados de forma efetiva; sem a identificação dos riscos é impraticável a elaboração de ações para reduzir as ameaças aos objetivos do projeto.

Para apoiar a implementação da gestão de riscos, diversos programas têm sido conduzidos com o propósito de desenvolver e aprimorar frameworks de melhores práticas de gerenciamento de riscos. Alguns exemplos são: ISO 31000:2009 para Gestão de Riscos [ISO 3100 2009], PMI – *Project Management Institute* através do RMMM - *Risk Management Maturity Model* ou Modelo de Maturidade em Gerenciamento de Riscos e pelo PMBOK® *Guide* [PMI 2009]. O SEI - *Software Engineering Iinstitute* através dos modelos do CMMI (Capability Maturity Model Integration) define o processo de Gerência de Riscos [SEI 2001] e *The Risk Management Society* (RIMS) apresenta também um modelo para maturidade em Gerenciamento de Riscos (Risk Model Maturity) [RIMS 2008].

Recentemente, com a Gestão de Riscos sendo introduzida no setor público brasileiro, a primeira questão enfrentada é a seguinte: a abordagem de risco do setor privado pode ser empregada no setor público?

É fato que alguns riscos que são importantes para o setor privado também afetam o setor público, como por exemplo: riscos de processos judiciais, riscos de falhas na tecnologia da informação, riscos financeiros advindo da globalização. Entretanto, há diferenças fundamentais que devem ser levadas em consideração, como as sintetizadas no quadro abaixo [Freitas 2002]:

Tabela 1: Diferenças na abordagem de risco do Setor Privado para o Setor Público

Setor Privado	Setor Público	Diferença
Foco principal nos negócios	Foco nos órgãos e programas (orçamento)	No setor público o risco é sistêmico, ou seja, depende de várias organizações
Objetiva o lucro	Objetiva a continuidade dos serviços	Valor Público ao invés de valor para o cliente
Decisões sobre risco confidenciais	Decisões sobre risco públicas e transparentes	Exigência de *accountability* no setor público

Na literatura encontramos algumas referências sobre estudos de implantação da gestão de riscos no ambiente de desenvolvimento de software. Mas a maioria é dedicada ao âmbito corporativo do setor privado [Fontoura, 2004, Leopoldino 2004, Coelho 2004, Machado 2002, Mielke 2003, Neves 2010, Pinto 2002, Souza 2006] e poucas são aplicadas com eficiência em uma organização pública devido a significativas diferenças na abordagem de risco, como visto anteriormente, e diferenças organizacionais, culturais, políticas e etc.

A identificação dos riscos e de seus fatores significa a compreensão das origens de cada perigo. Deve-se buscar responder por que o perigo existe no ambiente e quais são as condições que potencializam a concretização do evento estudado.

A compreensão da origem do perigo é imperiosa para a eficácia no tratamento e na priorização que a organização vai poder dedicar para mitigar aquela situação. Somente após o entendimento do porquê da existência de cada perigo, é que se poderá sugerir medidas eficazes para controlá-lo ou no caso de riscos positivos – que representam oportunidades -, potencializá-lo. Como veremos nos capítulos seguintes em detalhes, a palavra risco quer dizer apenas a potencialidade de um evento ocorrer. Este evento pode ser positivo ou negativo – por isso encontramos na literatura [PMBOK 2009] referências sobre riscos negativos e riscos positivos, também conhecidos como ameaças e oportunidades, respectivamente.

Na área de Gerenciamento de Riscos de TI no setor público foram encontradas poucas referências, e essas são relacionados às áreas como Gestão Estratégica [Silva 2004], Terceirização [Pratico 2010, Alencar e Viera 2003, Ferreira 2010, Oliveira e Santos 2006] e Segurança da Informação [TCU 2010]. Não foram encontradas referências sobre fatores de riscos existentes em ambientes de desenvolvimento de software de organizações públicas bem como o tratamento adequado a esses riscos.

1.1. Engenharia de Software

Friedrich Ludwig Bauer foi o primeiro a definir a engenharia de software como sendo: "Engenharia de Software é a criação e a utilização de sólidos princípios de engenharia a fim de obter software de maneira econômica, que seja confiável e que trabalhe

eficientemente em máquinas reais" [Bauer 1969]. O próprio significado de engenharia já traz os conceitos de criação, construção, análise, desenvolvimento e manutenção.

Segundo o *Institute of Electrical and Electronics Engineers* – IEEE, a Engenharia de Software é a [IEEE 1990]: (1) aplicação de uma abordagem sistemática, disciplinada e quantificável, para o desenvolvimento, operação e manutenção do software; isto é, a aplicação da engenharia ao software. (2) O estudo das abordagens como as de (1).

Conforme Pressman [Pressman 2006], a Engenharia de Software (ES) é uma tecnologia em camadas cuja base é o foco na qualidade do software desenvolvido. Portanto, inclusive do ponto de vista didático, é interessante estudarmos a ES em suas camadas de Processo, Métodos e Ferramentas.

De acordo com o *Software Engineering Body of Knowledge* – SWEBOK (Corpo de Conhecimento da Engenharia de Software), versão 2004, as áreas de conhecimento da Engenharia de Software são:

- **Requisitos de Software**

  Aquisição, análise, especificação e gestão de requisitos de software.

- **Projeto de Software**

  Transformação de requisitos (de software), tipicamente estabelecidos em termos relevantes ao domínio do problema, em uma descrição explicando como solucionar os aspectos do problema relacionados com software.

- **Construção de Software**

  Construção de programas funcionais e coerentes através da codificação, auto-validação e teste unitário.

- **Teste de Software**

  Verificação dinâmica do comportamento do programa através do uso de um conjunto finito de casos de teste - adequadamente selecionados de um domínio de execuções usualmente infinito - contra o comportamento esperado deste.

- **Manutenção de software**

Atividades de suporte custo-efetivo a um sistema de software, que pode ocorrer antes e após a entrega do software. Após a entrega do software são feitas modificações com o objetivo de corrigir falhas, melhorar seu desempenho ou adaptá-lo a um ambiente modificado. Antes da entrega do software são feitas atividades de planejamento.

- **Gerência de Configuração de Software**

  Identifica a configuração do sistema (características documentadas do hardware e software que o compõem) em pontos discretos no tempo, de modo a controlar sistematicamente suas mudanças e manter sua integridade e rastreabilidade durante o ciclo de vida do sistema.

- **Gerência de Engenharia de Software**

  Gerencia projetos de desenvolvimento de software.

- **Processos de Engenharia de Software**

  Define, implementa, mede, gerencia, modifica e aperfeiçoa o processo de desenvolvimento de software.

- **Ferramentas e Métodos de Engenharia de Software**

  Ferramentas de software automatizam o processo de engenharia de software. Métodos impõem estrutura sobre a atividade de desenvolvimento e manutenção de software com o objetivo de torná-la sistemática e mais propensa ao sucesso.

- **Qualidade de Software**

  Conjunto de atividades relacionadas com garantia de qualidade de software, entre estas as atividades de verificação e validação.

Com base nestas definições podemos considerar que no desenvolvimento de software estão envolvidos alguns componentes importantes para garantir o sucesso destas aplicações, como disciplina e organização do ambiente em questão.

Inicialmente é preciso utilizar um processo bem definido e orientado às metas institucionais, proporcionando o acúmulo das experiências passadas e a transformação

destas em conhecimento organizacional. Outro ponto não menos importante é a identificação de critérios que subsidiam medidas do processo e do produto gerado para validar as necessidades requeridas [Barbarán 1999].

De posse destas informações se abrem possibilidades para a evolução do conjunto das atividades, seja por adaptação ou melhoria contínua, mas, sobretudo, permitindo suporte à tomada de decisão. O uso de valor quantificável permite uma avaliação mais realista da situação vivenciada, promovendo uma melhor visão das situações futuras através do reuso destas experiências.

Neste contexto a Engenharia de Software é uma área multidisciplinar, pois para a realização de um projeto de software é requerido um conhecimento vasto, como o conhecimento sobre computação, sobre o domínio da aplicação e sobre a aplicação propriamente dita [Gusmão 2007].

A aplicação dos processos da engenharia para a construção de um produto de software também pode trazer dificuldades, pois nem tudo funciona como planejado, seja por puro desconhecimento, seja por falta de ferramental de apoio. Essas dificuldades podem ser transformadas em reais problemas – riscos - ao longo do ciclo de vida de desenvolvimento de um produto.

Mesmo com a preocupação de planejar cuidadosamente o projeto, muitos eventos ou situações incertas podem passar despercebidos, não sendo antecipados e tratados logo no início do projeto. Ao longo do ciclo de desenvolvimento do produto de software, situações podem precisar ser revistas, conflitos podem surgir, decisões difíceis precisam ser tomadas, significando que várias etapas intermediárias são necessárias e vitais para garantir o sucesso do projeto.

Observa-se que projetos de desenvolvimento de software apresentam atrasos em seus cronogramas, custos realizados além do planejado e funcionalidades aquém das expectativas dos clientes. Esses riscos, na sua maioria, embora considerados inerentes ao desenvolvimento de software por muitos autores [Boehm 1991, Sommerville 2003, De Marco 2003, Pressman 2006] podem ser minimizados e controlados por uma Gerência de Riscos contínua [Gusmão e Moura 2004].

Todos esses aspectos mostram que o processo de desenvolvimento de software tem uma intensa necessidade de informação associada à gestão e tomada de decisão, no qual um grupo de pessoas qualificadas trabalha cooperativamente entre si para alcançar o sucesso de um negócio específico.

1.2. Gerenciamento de Riscos

A demanda por software de qualidade tem aumentado o interesse das organizações em processos eficientes, que aumentem a produtividade e permitam o cumprimento de prazos e custos. Um bom entendimento dos riscos que ameaçam os objetivos dos projetos é fundamental para que se possa evitá-los, mitigá-los ou possivelmente transformá-los em oportunidades.

Como qualquer outra abordagem de Engenharia de Software, o desenvolvimento de sistemas, baseados no gerenciamento de riscos, também possui inúmeros problemas e desafios associados. De acordo com Robert Charette [Charette 2001] “atualmente, é uma habilidade das organizações compreenderem e gerenciarem o espectro completo do risco, que define o limite entre o sucesso e o fracasso”.

A Gerência de Riscos é, possivelmente, a forma escolhida por muitos gestores e executivos para prevenir-se dos aspectos críticos associados aos seus negócios. Executar corretamente os processos envolvidos na identificação, análise e tratamento dos riscos do projeto promove a potencialização dos resultados das ocorrências positivas e minimização das consequências negativas [PMI 2009].

Tradicionalmente, a Gerência de Riscos é vista como sendo uma parte da Gerência de Projetos. No entanto, a conceituação de Gerência de Riscos varia na literatura e nas próprias organizações, sendo ora vista como disciplina independente, ora como a própria razão da Gerência de Projetos – visto que, não havendo riscos, não haveria necessidade do gerenciamento de projetos, tornando-se esta uma atividade meramente administrativa [Grey 1995].

A Gerência de Riscos pode ser definida como o emprego de habilidades e competências, aliado ao conhecimento adquirido, através do uso de processos com a utilização de técnicas e métodos para a identificação, análise e controle dos riscos.

O Gerenciamento de Riscos é um processo onde os gerentes de projeto satisfazem as necessidades de identificação de fatores de riscos chave para os projetos em andamento, obtendo consistência e entendimento, escolhendo ou priorizando que riscos devem ser mitigados e eliminados, como também potencializando os resultados das oportunidades encontradas.

Dentre os diversos conceitos encontrados na literatura, encontramos consenso no que se diz respeito à importância do gerenciamento proativo, estruturado e consistente dos riscos, sendo fator determinante para o sucesso dos projetos de uma organização.

1.3. Teoria Fundamentada em Dados

Métodos quantitativos de pesquisa envolvem a coleta e análise de dados numéricos e são fortemente apoiados em estatística. Esses métodos podem ser aplicados eficientemente em estudos experimentais para medir a correlação entre as variáveis de um estudo. Variáveis são coisas que podem ser medidas, controladas ou manipuladas em uma pesquisa.

Métodos qualitativos de pesquisa envolvem a coleta e análise de dados como palavras (documentos, questionários de entrevistas, etc), imagens, ou objetos (por exemplo, um artefato). Métodos de pesquisa qualitativos foram desenvolvidos principalmente por pesquisadores na área de educação e outros cientistas sociais para estudar a complexidade do comportamento humano, por exemplo, motivação, comunicação e entendimento humano [Seaman 1999].

Enquanto estudos quantitativos geralmente procuram seguir com rigor um plano previamente estabelecido (baseado em hipóteses claramente indicadas e variáveis que são objetos de definição operacional), a pesquisa interpretativa e qualitativa costuma ser direcionada, ao longo de seu desenvolvimento; além disso, não busca enumerar ou medir

eventos e, geralmente não emprega instrumental estatístico para análise dos dados; seu foco de interesse é amplo e parte de uma perspectiva diferenciada da adotada pelos métodos quantitativos [Neves 1996].

Nos estudos qualitativos faz parte a obtenção de dados mediante contato direto e interativo do pesquisador com a situação objeto de estudo. Nas pesquisas qualitativas, é frequente que o pesquisador procure entender os fenômenos, segundo a perspectiva dos participantes da situação estudada e, a partir daí, situe sua interpretação dos fenômenos estudados.

Os métodos qualitativos e quantitativos não se excluem; se complementam. Embora difira quanto à ênfase, o método qualitativo traz como contribuição ao trabalho de pesquisa uma mistura de procedimentos de cunho racional e intuitivo capazes de contribuir para a melhor compreensão dos fenômenos. Pode-se distinguir o enfoque qualitativo do quantitativo, mas não seria correto afirmar que guardam relação de oposição.

Na pesquisa em Engenharia de Software é preciso notar que tanto o processo de desenvolvimento de software quanto o uso da tecnologia criada são processos sociotécnicos e por isso é necessário “um olhar que busca apreender a Engenharia de Software sem fragmentá-la em ‘fatores ou aspectos técnicos’ de um lado, e ‘fatores ou aspectos não técnicos’ de outro” [Cukierman 2006]. De acordo com Cukierman e outros autores (2006), “o olhar sociotécnico busca o desejo descritivo, ou seja, o desejo de descrever, em detalhes; de particularizar; de localizar; de especificar; de produzir diferenças”.

Métodos de pesquisa próprios são necessários para capturar esse olhar sociotécnico e descrever aspectos e questões de pesquisa, ao invés de simplesmente simplificar e produzir similaridades. Neste sentido, métodos qualitativos são os mais indicados, pois eles permitem uma compreensão mais abrangente de todo o fenômeno em estudo [Seaman 1999].

A pesquisa qualitativa ainda vem enfrentando resistências no que diz respeito a sua aceitabilidade no tocante ao quesito cientificidade. Um argumento utilizado pelos pesquisadores positivistas é o problema da generalização, pois para estes numa

abordagem qualitativa os resultados encontrados não podem ser generalizados, uma vez que a pesquisa qualitativa preza pela localidade ao invés da universalidade, fazendo cortes pequenos para análise, tendo em vista o nível de profundidade alcançado nas interpretações dos achados de pesquisa. Esse argumento é contraposto por alguns pesquisadores [Viera 2004] ao afirmarem que a generalização pode ser feita, resguardando o fato de as duas situações que serão comparadas, possuírem características em comum, o que gera um grau maior de confiabilidade.

Para os sociólogos que a propuseram [Strauss, A., Corbin, J. 1998], a Teoria Fundamentada em Dados (do inglês, *Grounded Theory*) consiste na observação da sociedade a partir de seu ambiente natural antes de procurar descobrir os padrões de comportamento que poderiam ser utilizados subsequentemente na construção de teorias. A lógica da construção teórica é a indutiva, a partir da qual se pretende construir uma teoria substantiva baseada na realidade observada. Conceitua-se teoria substantiva como uma teoria de escopo específico a determinado fenômeno ou sujeitos pesquisados. Ela não se propõe a fazer uma generalização estatística, porém busca a generalização analítica apoiada na realidade objetivada pelos sujeitos da pesquisa e interpretada pelo próprio pesquisador.

A Teoria Fundamentada em Dados (TFD) pode ter diversas aplicações. Em primeiro lugar pode ser trabalhada para solucionar os problemas localizados, chegar a teorias novas, somá-las e/ou confrontá-las com as teorias que são repassadas para os pesquisadores, no sentido de expandir o entendimento sobre o tema de estudo.

Flick [Flick 1998] afirma que a TFD “quebra” com a pesquisa tradicional na medida em que não tem necessidade do pesquisador ir a campo com um modelo a priori e cheio de posições teóricas, nesse caso o pesquisador adotará uma postura construtiva no campo, reafirmando assim que o objetivo deste método não é reduzir a complexidade, fragmentando-a em variáveis, mas em vez disso aumentar a complexidade e incluir o contexto na análise. Uma informação importante que deve ser observada é que a teoria a ser criada não surge somente para explicar algum fenômeno, mas também provê um esquema de referência para a ação. Além disso, deve-se ressaltar que poderemos sempre combinar técnicas qualitativas e quantitativas.

1.4. Problema Tratado

Desenvolvimento de software é um processo social, pois se fundamenta na compreensão comum dos envolvidos no processo e em suposições [Pfleeger 1999]. As questões críticas – FATORES DE RISCOS - capazes de afetar o desenvolvimento de software e áreas correlatas envolvem não apenas aspectos tecnológicos, mas também aspectos de caráter organizacional e socioculturais.

Uma grande dificuldade para o gerenciamento dos riscos do processo de desenvolvimento de software é a existência de diversas visões parciais sobre as técnicas e formas de gerenciamento. Quando transportadas para a prática estas visões podem trazer muitos problemas e ineficiências. Isto porque qualquer desenvolvimento, por maior a hegemonia de um determinado conteúdo tecnológico, implica em conhecimento diversificado. Cada visão parcial carrega consigo também um vocabulário e determinados valores próprios, dificultando a integração entre os diversos profissionais pela ausência de padronização. Se compararmos as particularidades (cultura organizacional, objetivos financeiros, contexto político, etc.) existentes entre as organizações de âmbito público e privado essas visões tornam-se ainda mais distantes.

Temos como uma limitação atual da Gerência de Riscos na área de desenvolvimento de software, uma quantidade pequena de estudos práticos divulgados, apresentando indicadores de sucesso dos projetos de software desenvolvidos, conforme relato em pesquisadas disponibilizadas na área [Fontoura 2004, Leopoldino 2004, Coelho 2004, Machado 2002, Mielke 2003, Neves 2010, Pinto 2002, Souza 2006].

Na literatura encontramos iniciativas que visaram identificar e categorizar riscos no ambiente de desenvolvimento de software, mas a maioria representa as experiências específicas de uma organização de software do setor privado [Fontoura 2004, Leopoldino 2004, Machado 2002, Mielke 2003, Neves 2010, Pinto 2002, Souza 2006] ou instituição de consultoria [Taxonomy of Operations Risks – SEI 2005, Risk Management – TenStep 2005] e limitaram-se à identificação do perigo e não no fator de risco causador do perigo.

Não foram encontradas referências sobre fatores de riscos existentes em ambientes de desenvolvimento de software de organizações públicas bem como o tratamento

adequado a esses riscos. Sabe-se que órgãos públicos possuem características diversas ao âmbito privado que potencializam o aparecimento de fatores de riscos que não são encontrados ou possuem impactos diferenciados no setor privado. Podemos citar como exemplo os fatores políticos, sociais e legais.

1.5. Objetivos e Contribuições

O objeto principal desta dissertação de mestrado é propor solução direcionada ao contexto de uma Organização do Setor Público para identificação, análise e proposta de tratamento dos fatores de riscos existentes no ambiente de desenvolvimento de software da organização. Este trabalho será iniciado através do mapeamento dos principais perigos e seus fatores de riscos existentes no ambiente de desenvolvimento de software do departamento de tecnologia da informação utilizando como metodologia de pesquisa a Teoria Fundamentada em Dados.

A Teoria Fundamentada em Dados é aplicável em áreas que não foram previamente estudadas ou onde é necessário aprofundar o entendimento sobre um determinado fenômeno [Strauss e Corbin 1998]. A inexistência de estudos ou iniciativas prévias na organização em estudo para identificação dos fatores de riscos no ambiente de desenvolvimento de software e a ausência de referências na literatura sobre esse contexto motivaram a adoção desta metodologia.

Os perigos e os fatores de riscos identificados através da aplicação desta metodologia serão analisados e avaliados para que seja elaborado um Plano de Ação. Devido à importância da Norma ISO 31000:2009 para o gerenciamento de riscos e a relevância, adequação e reconhecimento do Método Brasiliano [Brasiliano 2009] para análise e avaliação de riscos, decidiu-se conduzir a investigação, nesta dissertação, com base na Norma internacionalmente reconhecida e na experiência dos profissionais atuantes na área de riscos corporativos no Brasil. O Método Brasiliano vem sendo amplamente adotado pelas Instituições Financeiras Brasileiras (Banco do Brasil, ITAU, Real, entre outros), organizações do Setor Público (Governo de São Paulo e Rio de Janeiro, Empresa Brasileira de Correios e Telégrafos, etc), grandes empresas como Petrobrás e Shell, além

de participação em projetos internacionais como a Câmara Federal e Senado do Paraguai e Base Edwards nos Estados Unidos. Soma-se a isso o fato da equipe envolvida no estudo, incluindo a autora da dissertação, ter sido capacitada e treinada no Método Brasiliano.

A realização de investigações sobre os fatores de riscos na área de desenvolvimento de software da Organização em estudo trará como resultado imediato uma fotografia atual do departamento através dos seus principais problemas, identificados pelos próprios membros que o compõe, e uma proposta de ação para esses problemas, além de contribuir para a pesquisa e prática de processos de Gerenciamento de Riscos no órgão supracitado.

1.6. Metodologia de trabalho

Para alcançar resultados satisfatórios em investigações na área gerenciamento de riscos, é fundamental aplicar estratégias adequadas de pesquisa.

Nesta pesquisa foi utilizada a Teoria Fundamentada em Dados como a metodologia qualitativa para a identificação dos riscos e seus fatores. A análise, avaliação dos riscos e elaboração do plano de respostas foi realizada através da aplicação do Método Brasiliano de análise e avaliação de riscos que implementa os processos definidos pela ISO 31000:2009 – Gestão de Riscos.

A metodologia de trabalho pode ser dividida nas seguintes macrofases que intercalam as etapas da Teoria Fundamentada em Dados com as etapas sugeridas pelo Método Brasiliano, conforme Tabela 2.

Tabela 2: Metodologia de Trabalho

Fase	Descrição	Objetivos
1ª	Definir o contexto e escopo do estudo	Definir contexto, limites da pesquisa e fontes de dados.
2ª	Definir e aplicar mecanismos	Elaborar questionário e realizar entrevistas com

	de coleta de dados	os usuários selecionados.
3ª	Realizar codificação dos dados	Quebra, análise, comparação, conceituação e categorização dos dados.
4ª	Identificação dos Perigos e Fatores de Riscos	Identificar os perigos encontrados na categorização dos dados, identificar os fatores de riscos através do Diagrama de Causa e Efeito (Diagrama de Ishikawa) e avaliar os fatores de riscos utilizando a Matriz SWOT (Strenghts, Weaknesses, Opportunities, Threats) para encontrar a motricidade de cada fator e a Matriz de Impacto Cruzado para hierarquizar os fatores mais determinantes e importantes entre os identificados.
5ª	Análise dos Riscos	Estabelecer o grau de probabilidade (através dos critérios "Fator de Risco" e "Exposição") e o nível de impacto de cada perigo.
6ª	Avaliação dos Riscos	Elaborar a Matriz de Riscos para priorização dos riscos analisados.
7ª	Resposta aos Riscos: Plano de Ação	Elaborar plano de ação com base nos Fatores de Riscos visando mitigar ou diminuir as probabilidades dos riscos.

Tabela 2 – Continuação: Metodologia de Trabalho

1.7. Organização da Dissertação

Após este capítulo introdutório cujo objetivo foi descrever a motivação e proposta da solução, a estrutura do documento tem o seguinte formato:

Capítulo 2 - **Referencial Teórico** – apresenta o referencial teórico, que contém a revisão dos conceitos e teorias bases da dissertação organizadas em três seções. A Seção 2.1 - **Gerenciamento de Riscos** - apresenta o tópico de Gerência de Riscos, contextualizando o trabalho realizado e identificando as principais técnicas de identificação e análise de riscos utilizadas. A Seção 2.2 – **Método Brasiliano de Análise de Riscos** - apresenta a Norma ISO 31000 – Gestão de Riscos e o Método Brasiliano de Análise de Riscos. E a Seção 2.3 - **Teoria Fundamentada em Dados (TFD)** - discorre sobre a Teoria Fundamentada em Dados, sua origem, objetivos e estrutura além de apresentar uma comparação entre pesquisas quantitativas e qualitativas.

Capítulo 3 – **Metodologia de Pesquisa** - detalha a estruturação da metodologia de trabalho utilizada para mapear os fatores de riscos e elaborar seus planos de respostas. Neste capítulo, descrevemos como adotaremos a Teoria Fundamentada em dados utilizando princípios e diretrizes da Norma ISSO 31000 através da proposta do Método Brasiliano.

Capítulo 4 – **Mapeamento dos Fatores de Riscos e Plano de Resposta** - apresenta a aplicação do plano de trabalho proposto no departamento de tecnologia da informação da organização pública em estudo e seus resultados, narrando passo a passo a contextualização, coleta, análise e estruturação dos fatores de riscos e seus planos de respostas.

Capítulo 5 – **Conclusões e Trabalhos Futuros** - apresenta as conclusões, trabalhos relacionados, trabalhos futuros e dificuldades encontradas para a realização desta dissertação.

2. Referencial Teórico

A base teórica necessária para a realização da pesquisa e o entendimento do estudo é apresentada nesse capítulo. O capítulo está organizado em três seções:

Seção 2.1 Gerenciamento de Riscos: nesta seção são apresentados conceitos e teorias referentes ao Gerenciamento de Riscos.

Seção 2.2 Método Brasiliano: nesta seção é apresentado o Método Brasiliano de Análise de Riscos, para a identificação, análise e avaliação dos riscos.

Seção 2.3 Teoria Fundamentada em Dados: nesta seção é apresentada a Teoria Fundamentada em Dados, sua origem, objetivos e estrutura.

2.1. Gerenciamento de Riscos

Se há um tema para o qual se encontrará uma vasta literatura é o risco. Abordagens financeiras, das ciências atuariais, operacionais, matemáticas, da administração financeira, econômica, tributária, etc., são algumas fontes de informações sobre riscos.

Nesta seção será exposta através de uma sucinta revisão da literatura, a teoria existente e relevante sobre riscos de uma forma geral e riscos de projetos. Serão apresentados os principais conceitos de riscos, incertezas, perigos, fatores de riscos e gestão de riscos.

2.1.1. História e Origens

As incertezas fazem parte do cotidiano humano. Desde os primórdios o homem procura defender-se dos riscos que o cercam, galgando níveis de satisfação das necessidades básicas, de segurança e culminando nas necessidades de cunho puramente profissional.

[Gusmão 2005]. As pessoas, em sua grande maioria, diariamente fazem escolhas, com graus diferenciados de riscos, mas também com um alto grau de oportunidade e benefícios associados.

Segundo Gusmão [Gusmão 2005], deste modo, tem-se que as incertezas incutem, geram e implicam em riscos e estes, são definidos como a probabilidade ou possibilidade da ocorrência de valores para determinados eventos e fenômenos, não desejáveis e, ou, adversos. Isto leva a estabelecer a convivência contínua e inevitável com inúmeros tipos de riscos. Porém, entende-se que esta convivência precisa ser explicitada, ou mesmo, elucidada. Fato que propiciará a identificação, análise e quantificação da intensidade dos riscos. Este conhecimento proporcionará o estabelecimento de estratégias que visem ações de prevenção, minimização e, ou, mitigação dos efeitos associados aos riscos, não obstante a reutilização do acúmulo de conhecimento através das situações vivenciadas.

Existem várias definições e usos para o termo risco. Frank Knight em seu livro - *Risk, Uncertainty and Profit* – define risco, em uma abordagem para o mercado financeiro, como sendo a exposição a eventos incertos com probabilidades conhecidas [Knight 1921]. No dicionário Houaiss, o termo risco é definido como: “probabilidade de perigo” [Houaiss 2001].

Peter Bernstein [Bernstein 1997], em seu livro - Desafio aos Deuses: A Fascinante História do Risco, apresenta que a origem da palavra risco vem do italiano antigo, *risicare* que significa “ousar”, que por sua vez, deriva do Latin *risicu*, *riscu*. Desta forma é uma escolha e não o destino. E ainda [Bernstein 1997] “... a capacidade de gerenciar riscos, a vontade de correr riscos e fazer opções ousadas são elementos-chave da energia que impulsiona o mundo”. Logo, sendo o risco uma opção, pode-se medi-lo, avaliar as consequências de sua ocorrência e consequentemente geri-lo.

Conforme Solomon e Pringle, citados por Rovai, risco é o grau de incerteza que se tem em relação a um evento. Onde há incerteza, sempre haverá risco [Rovai 2005].

A Gerência de Riscos, atualmente na prática, ainda utiliza vários de seus conceitos fundamentais apresentados desde o século XVII. Inicialmente o processo de gestão de riscos pode apresentar informações confusas, dúvidas e desconhecimentos, uma vez que, tudo no início do projeto é incerto. É baseada em teorias que provêm diferentes

estratégias para a tomada de decisões sob condições probabilísticas. Todas as estratégias esforçam-se em melhorar a qualidade das decisões com a avaliação de duas ou mais alternativas de ação [Clemen 1991].

Três séculos e meio atrás a ciência iniciou uma busca intelectual cujo objetivo era medir o acaso e, com isso, exercer um maior controle sobre os fenômenos naturais. A Figura 1, desenvolvida por Gusmão (2007) apresenta uma visão cronológica da importância da Gerência de Riscos.

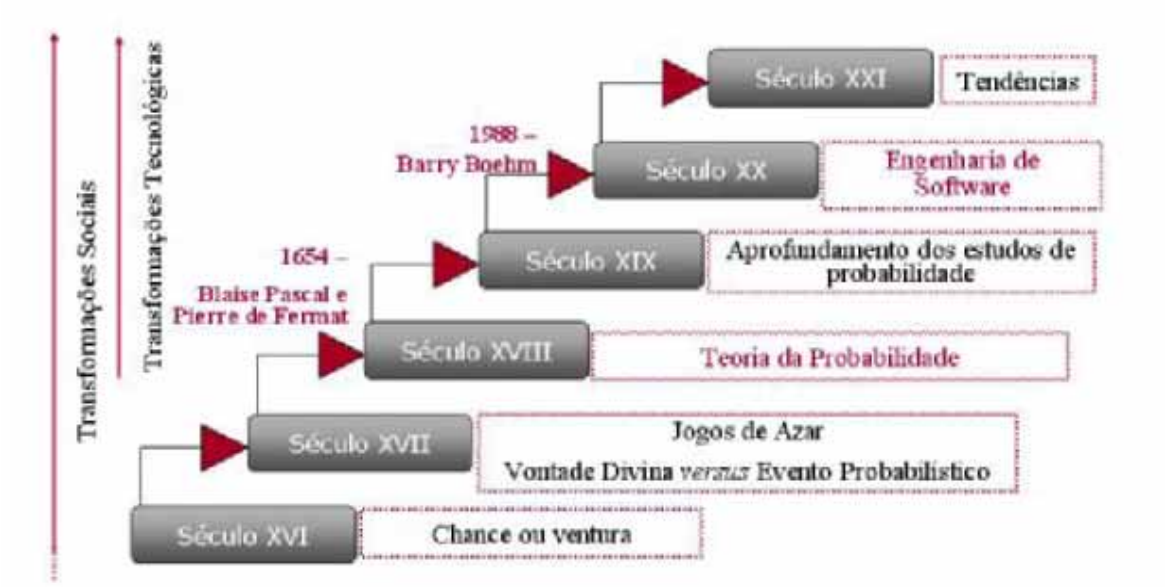

Figura 1: Cronologia da Gerência de Riscos [Gusmão 2007]

Pode-se dizer que esta jornada inicia-se com a Teoria da Probabilidade, criada por Blaise Pascal e Pierre de Fermat, seguindo pelos séculos XVIII e XIX que são caracterizados pelo aprofundamento nos estudos das probabilidades e no tratamento de situações de uma complexidade maior.

No final do século XIX e início do século XX, o objetivo concentrava-se na análise de fatos quantitativos sobre o Estado. A finalidade inicial, da primeira coleta de dados demográficos, era oferecer um levantamento de perspectivas de mercado ao comércio e de fornecer ao governo as primeiras estimativas de número de pessoas disponíveis para o serviço militar, "conhecimento este que pode tornar o comércio e o governo mais

seguros e regulares" [Bernstein 1997]. Seguindo este pensamento surgiu a necessidade de conhecer as bases tributárias, os gastos com benefícios sociais e assistenciais, era o início da importância da coleta de informações como subsídio para a tomada de decisão.

No século XX a Gerência de Riscos é formalmente apresentada à comunidade de Engenharia de Software através da proposta do modelo Espiral de Barry Boehm [Boehm 1988]. Seguindo-se a este evento muitas abordagens e modelos foram apresentados com características próprias e seguindo, de um modo geral, a proposição do uso das atividades da Gerência de Riscos.

No século XXI as tendências da área de gerenciamento de projetos vêm evoluindo e adaptando questões de melhoria a aplicação dos conhecimentos voltados para a área de gerenciamento de riscos. Muitas iniciativas da comunidade estão voltadas para o uso de modelos baseados em Escritório de Projetos e Modelos de Maturidade. Outros tratam abordagens do uso dos conceitos da Gerência de Riscos Integrada significando sua utilização em todos os processos de gestão da organização, além do enfoque em conceitos de cooperação. Essa visão corporativa é o objetivo da ISO 31000:2009.

Ainda que o conceito de risco esteja bastante associado a perigos e impactos negativos, já vem sendo utilizado como "exposição a consequências da incerteza", sendo cada vez mais aplicado tanto no gerenciamento de perdas como no de ganhos potenciais.

Eventos podem gerar impacto tanto negativo quanto positivo ou ambos. Os que geram impacto negativo representam riscos que podem impedir a criação de valor ou mesmo destruir o valor existente. Os de impacto positivo podem contrabalançar os de impacto negativo ou podem representar oportunidades, que por sua vez representam a possibilidade de um evento ocorrer e influenciar favoravelmente a realização dos objetivos, apoiando a criação ou a preservação de valor.

2.1.2. Perigo *versus* Risco *versus* Fatores de Risco

Segundo Brasiliano [Brasiliano, 2009] precisamos claramente diferenciar perigo, riscos e fatores de riscos.

Risco difere de perigo. Perigo é um evento, algo que está localizado no passado. Risco sempre se refere ao futuro, é sempre um elemento de incerteza. Dado um determinado evento - ou perigo – risco é a condição que cria ou aumenta o seu potencial de concretização. Exemplo: incêndio é um perigo, o risco são as condições de armazenagem, carga de incêndio, cultura de funcionários, entre outras. A violência urbana é um perigo, a concretização dela depende das condições.

A identificação dos perigos abrange a definição do conjunto de eventos, externos ou internos, que podem impactar os objetivos estratégicos e táticos da empresa, inclusive os relacionados aos ativos intangíveis.

Os fatores de risco são, na realidade, a origem e ou causa de cada perigo. São fatores internos ou externos que contribuem e/ou influenciam na ocorrência do risco. Para compreender o risco – a condição – a soma de todos os fatores, há a necessidade de dissecar o fluxo de cada processo. É de suma importância à compreensão dos fatores de risco e de suas origens, pois desta forma é que se poderá implementar medidas preventivas realistas.

A identificação dos perigos e de seus fatores significa a compreensão das origens de cada perigo. Deve-se buscar responder por que o perigo existe na empresa. Quais são as condições que potencializam a concretização do evento estudado. Em linhas gerais, podemos considerar que os Fatores de Riscos são condições “certas”, “concretas” existentes na organização que irão potencializar ou facilitar a ocorrência ou concretização de uma condição “incerta” – o perigo. Por exemplo, em uma determinada organização que desenvolve software não existe uma metodologia de desenvolvimento nem padrão de codificação, além de não existir políticas de treinamento. Essas condições fazem parte da organização, são “certezas” no cenário atual que podem favorecer a ocorrência, por exemplo, de retrabalho. Mas o retrabalho é algo que pode acontecer, não necessariamente irá. É um perigo. Essa situação está diagramada na Figura 2:

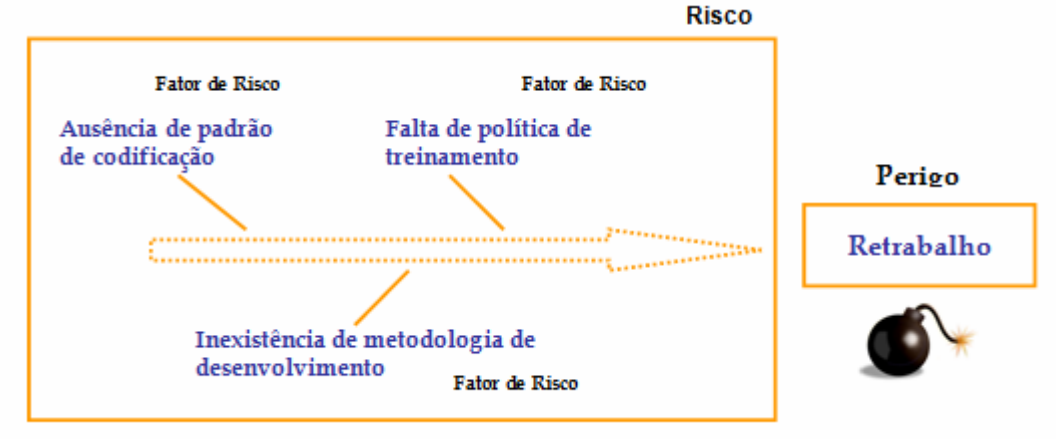

Figura 2: Perigo versus Riscos versus Fatores de Risco

A compreensão da origem do perigo é imperiosa para a eficácia no tratamento, na priorização que a empresa vai poder dedicar para mitigar aquela situação. Somente após o entendimento do porque da existência de cada perigo, é que se poderá sugerir medidas eficazes para mitigar, ou seja, minimizar a exposição ao mesmo.

2.1.3. Riscos em Engenharia de Software

Atualmente todos os ramos da atividade humana dependem de alguma forma da utilização de software para operar, dar suporte, controlar equipamentos e fluxos de informações, gravar ou processar atividades. A área de Engenharia de Software tem promovido vários estudos com a finalidade de produzir modelos de melhoria, processos, métodos e ferramentas para aumentar a probabilidade de sucesso na execução de projetos de software, garantindo a qualidade de seus produtos e minimizando possíveis problemas associados [SEI 2001, PMI 2008]. Portanto, na capacidade de prevenir e controlar essas variáveis pode estar o diferencial para gerir os riscos de projetos na indústria de software [Santana e Xisto 2009].

Todo projeto de software enfrenta problemas de qualidade, de cronograma, e de custo que estão sendo afetados por riscos que são inesperados, não planejados ou ignorados simplesmente pela falta de conhecimento.

As organizações estão tornando-se cada vez mais dependentes do sucesso ou do fracasso dos softwares que desenvolvem, devido às perspectivas globais de mercados. Neste contexto, a Gerência de Riscos não é apenas baseada em boas práticas para o desenvolvimento de software, mas sim, boas práticas para gerir seus negócios.

Cada dia fica mais clara a percepção de que gerenciar projetos é gerenciar riscos. Mas isto não basta. É necessário que o gerente de projetos seja capaz de identificar problemas concretos, e, de preferência, com a probabilidade de ocorrência. Além disso, há riscos e riscos! Determinados tipos de projetos são intrinsecamente mais arriscados do que outros. Possuir uma visão integrada do risco é fundamental para as organizações que buscam o desenvolvimento e a continuidade do negócio, e ainda dependem de uma infraestrutura operacional sob risco controlado.

Risco na área de software foi representado de forma sistemática por Barry W. Boehm, em 1988, através do Modelo Espiral [Boehm et al 2004], que tem como princípio ser incremental e dirigido à análise de riscos. O desenvolvimento incremental é uma estratégia para a obtenção de progresso em pequenos passos, pela divisão de um problema em subproblemas e a posterior combinação das soluções encontradas (alternativas definidas).

Atualmente, a área que trata riscos na Engenharia de Software evoluiu, passando de uma análise dentro das fases do modelo de desenvolvimento de software para se tornar uma gerência que permeia todos os processos do ciclo de vida do software.

Risco de software pode ser caracterizado como [Hall 1998]:

- **Riscos de Projeto de Software.** Define os parâmetros operacionais, organizacionais e contratuais do desenvolvimento de software. Inclui limites de recursos, interfaces, relacionamentos com fornecedores ou restrições de contratos.

- **Riscos de Processo de Software**. Relacionam-se os problemas técnicos e de gerenciamento. Nos procedimentos de gerência podem-se encontrar riscos em atividades como: planejamento, definição e contratação de equipe de trabalho, garantia de segurança e configuração de gerência. Nos procedimentos técnicos,

podem-se encontrar riscos nas atividades: análise de requisitos, projeto, codificação e testes, por exemplo.

- **Riscos de Produto de Software.** Contém as características intermediárias e finais do produto. Estes tipos de riscos têm origens nos requisitos de estabilidade do produto, desempenho, complexidade de codificação e especificação de testes.

Muitas classificações são encontradas na literatura relacionada à Gerência de Projetos [Car et al 1993, Gustafson 2002, Sommerville 2003, PMI 2004], uma delas é o uso de taxonomia de riscos (Taxonomy-Based Risk Identification) como a apresentada pelo Instituto de Engenharia de Software (SEI - Software Engineering Institute) onde os riscos são classificados dentro de categorias para melhor entendimento de sua natureza. Alguns estudos e abordagens na literatura, que tratam a área de Gerência de Riscos, evoluíram, ou mesmo adaptaram, as categorias de riscos inicialmente apresentadas na taxonomia proposta pelo SEI [Costa et al 2005, Gusmão et al 2005 e Webster et al 2005, TenStep 2009].

As categorias de riscos favorecem a identificação dos riscos em um ambiente promovendo uma classificação e organização dos riscos identificados em grupos lógicos.

De forma geral, nos modelos de processos de gerenciamento de riscos é solicitada a definição das categorias ou classes de riscos (classificações) de acordo com as características do ambiente de desenvolvimento em questão.

2.1.4. Gerência de Riscos e Tomada de Decisão

A incerteza é um fator que pode dificultar a tomada de decisão racional. A maioria das decisões, sobretudo aquelas importantes, está baseada em algum tipo de estimativa, colocando a incerteza como elemento do processo decisório. E mesmo que a situação não exija estimativa, deve-se considerar a insuficiência das informações para a tomada de decisão.

Um risco só deveria ser tratado quando o seu benefício potencial (oportunidade) para a organização e as chances de ganhos excedesse o valor do custo reparador de uma decisão mal sucedida e as chances de perdas dentro de uma margem satisfatória. Para que isso possa acontecer é preciso que o gerente de projeto, ou o profissional responsável pelo risco, encontre as respostas para algumas questões, tais como o motivo pelo qual o risco deve ser tratado; quais são os ganhos associados ou o que poderá ser perdido; as reais chances de sucesso (ou fracasso); o que poderá ser feito se os objetivos definidos não forem alcançados; se o custo de estratégias de tratamento vale o esforço para um risco em específico.

Dessa forma, torna-se importante fazer uma análise do grau de incerteza existente no processo de decisão, ou seja, procurar uma estimativa dos riscos envolvidos. Deve-se ressaltar a importância do uso de abordagens qualitativa e quantitativa na análise e desenvolvimento dos investimentos, de uma empresa, seja ela de pequeno, médio ou grande porte. A norma ISO 31000:2009 traz essa orientação através da abordagem conjunta de métodos qualitativos e quantitativos na gestão dos riscos. O método Brasiliano implementa essa questão utilizando de forma complementar análises subjetivas e estatísticas no processo de avaliação de riscos, como veremos na seção 2.3.

2.1.5. Gerenciamento de Projetos *versus* Gerenciamento de Riscos

A Gerência de Riscos tem uma aplicabilidade bastante ampla em ambientes organizacionais. Quando se fala em gerir projetos, é inevitável que se fale em gerir riscos. Por este motivo, muitas vezes, é difícil delimitar a fronteira existente entre as duas gerências.

Ainda não existe um consenso sobre o relacionamento entre a gerência de projetos e a gerência de riscos. Normas, padrões e modelos são apresentados, na área de Engenharia de Software, mas não tratam esse relacionamento de forma explícita. Não existe um padrão que descreva o elo existente entre a Gerência de Riscos e a Gerência de Projeto, nem tão pouco apresente o objetivo do processo e das atividades da Gerência de Riscos.

Isto evidencia a imaturidade da comunidade de Engenharia de Software, onde as normas e modelos deveriam consolidar este conhecimento já existente.

A falta de padronização dificulta o entendimento, a definição de processos e papéis em relação à Gerência de Riscos, o cumprimento dos objetivos organizacionais, pois não se tem uma visão integrada. De acordo com Stephen Grey existem três visões, de uma forma geral, para o relacionamento entre a Gerência de Riscos e a Gerência de Projeto [Grey 1995]:

- **Dependência** – A Gerência de Riscos é vista como parte da gerência de projeto. A execução é de responsabilidade do gerente de projeto ou é delegada a outro membro da equipe de projeto. Desta forma as atividades de gestão de riscos são realizadas em nível de projeto na organização (nível operacional);

- **Existência** – A motivação para a execução de um projeto é a gerência de seus riscos. A existência da gerência de projetos está condicionada à Gerência de Riscos. Se não existe risco, não existe necessidade da gerência de projeto. Neste caso tornar-se-ia uma mera atividade administrativa. Este tipo de abordagem é comumente conhecido como “gerência de projetos dirigida a riscos”;

- **Independência** – através desta visão, a Gerência de Riscos é um processo distinto e de apoio para todos os projetos da organização, desde o nível estratégico até o operacional.

Em 2005, David Hillson citava como uma das áreas de aperfeiçoamento futuro da Gerência de Riscos a integração desta com a cultura organizacional [Hillson 2005]. Esta visão direcionava o uso da Gerência de Riscos como parte integral do negócio organizacional sendo um processo construtivo e não repreensivo.

Esse é o objetivo da ISO 31000:2009 ao enfatizar uma gestão de riscos corporativa, imersa e parte integrante da cultura da organização. A ISO 31000:2009 não faz diferenciação entre gerenciamento de projetos e gerenciamento de riscos por abranger um contexto mais amplo – que é o da organização como um todo – permeando todos os níveis das atividades do negócio o que pode inclui entre outras as operações, projetos, processos, etc.

2.1.6. Atividades da Gerência de Riscos: Visão de Metodologias

Já com relação às atividades que compõem o processo de Gerência de Riscos, na literatura da área de Engenharia de Software [Higuera 1994] como na área corporativa, parece haver um consenso. Deve-se ressaltar que todas as atividades são baseadas e centradas na comunicação, devendo ser realizadas de forma cíclica e contínua dentro do processo de Gerência de Riscos utilizado.

Entre as principais abordagens encontradas na literatura para Gerenciamento de Riscos, destacamos: A metodologia de desenvolvimento RUP (Rational Unifed Process) [Kruchten 2003], O Instituto Internacional de Software - SEI através do CMMI (Capability Maturity Model Integration) [SEI 2001], o Instituto de Gerenciamento de Projetos – PMI [PMI 2009], a metodologia COSO – ERM (Enterprise Risk Management) [COSO 2004] e a recém lançada Norma ISO 31000:2009 de Gestão de Riscos [ISO 31000 2009] que, teve como base na sua criação a compilação, harmonização e estruturação de vários modelos, normas, processos e boas práticas da área, vem a ser o ponto focal em termos de Gestão de Riscos. De uma forma geral, os modelos e abordagens relacionados ao processo de Gerência de Riscos utilizam este conjunto de atividades:

Para efeito desta dissertação, optou-se em contextualizar as atividades ao escopo da Engenharia de Software, mesmo tendo como base normas mais abrangentes que visam o contexto organizacional como o COSO – ERM e a ISO 31000.

- **Planejar a Gerência de Riscos**. Esta atividade tem a finalidade de definir a estratégia da gestão de riscos, dos recursos necessários para a realização do processo e por fim, da efetivação das ações consideradas necessárias no plano de Gerência de Riscos.

- **Identificar Riscos**. A identificação dos riscos é a atividade inicial de um projeto de software. Objetiva um levantamento preliminar de todas as possibilidades de riscos existentes no projeto. O aspecto mais importante da atividade de identificação de riscos é compor uma documentação formalizando os dados coletados.

- **Analisar Riscos**. Nesta atividade são caracterizados os aspectos mais importantes de cada risco, com a finalidade de explorar as melhores estratégias de mitigação (eliminação). Em regra, os riscos são categorizados e priorizados, segundo algum critério específico estabelecido, para tornar a gerência concentrada nos riscos considerados prioritários.

  Para realizar a análise dos riscos de um projeto normalmente são utilizadas técnicas quantitativas e/ou qualitativas, como será visto no Método Brasiliano descrito na seção 2.3. No uso das técnicas qualitativas são desenvolvidas escalas de probabilidade e impacto que irão auxiliar na composição da Exposição ao Risco. Essas escalas são desenvolvidas dentro das atividades de planejamento da Gerência de Riscos.

- **Planejar Respostas aos Riscos**. O planejamento é uma atividade, da Gerência de Riscos, que envolve, em geral, (i) a determinação dos riscos a serem gerenciados, (ii) dos planos de ação para os riscos sob controle da gerência e (iii) dos planos de contingência para os riscos que se encontram além das capacidades de mitigação.

  Para realizar as atividades de Planejamento e Tratamento das Respostas aos Riscos é necessário que as estratégias e tolerância aos riscos estejam definidas. As estratégias são montadas por meio de uma análise dos custos das atividades e ações planejadas (preventivas e/ou corretivas). Por vezes uma determinada estratégia não pode ser utilizada porque seu custo de execução é mais alto do que a ocorrência do próprio risco.

- **Monitorar Riscos**. O monitoramento dos riscos é a observação da efetividade dos planos de ação na execução do desenvolvimento do projeto de software. O objetivo é prover informações precisas e contínuas para habilitar a Gerência de Riscos a atuar de forma preventiva e não reativa aos eventos adversos. Como benefício desta atividade, tem-se a melhor compreensão do andamento do projeto por parte dos membros das equipes de desenvolvimento. Cada risco monitorado possui um ciclo de atualização próprio. A frequência de atualização depende dos recursos disponíveis e da rapidez com que o produto se desenvolve.

- **Controlar Riscos**. A atividade de controle dos riscos avalia a situação corrente para determinar eventuais desvios do planejado. O controle dos riscos envolve alteração das estratégias de mitigação, quando se fizer necessário; utilização de ações previamente planejadas de contingência; encerramento de trabalhos relacionados a um determinado risco, quando este deixar de existir, entre outras. A utilização de cronogramas é essencial para a atividade de controle na Gerência de Riscos, pois o controle explícito de tarefas de mitigação de riscos facilita o acompanhamento do progresso e da eficácia destes planos.

- **Comunicar os Riscos**. A comunicação entre as equipes e membros do projeto de software é um dos fatores mais importantes para a realização bem sucedida da gerência de riscos. Riscos, problemas e crises podem aparecer, quando a estrutura de comunicação é debilitada em uma organização [Humphrey 1990].

2.1.7. Métodos de Identificação de Riscos

Uma grande variedade de métodos, para a identificação de riscos, está disponível na literatura de Engenharia de Software [Boehm 1991, Higuera 1994, Moynihan 1997, Machado 2002, Pressman 2006] e na área de Gestão de Riscos Corporativos [Brasiliano 2009, COSO 2004, ISO 31000 2009]. Alguns destes métodos, referenciados inclusive pelo Guia PMBOK [PMI 2009], são: B*rainstorming*, listas de verificação (checklist), comparação por analogia, análise de premissas, decomposição, técnicas de diagramação, técnica Delphi, revisão de documentação (plano e modelo de projeto) e entrevistas.

De acordo com pesquisa realizada em 2006 pelo PMI [PMI 2006], conforme Figura 3, as técnicas mais utilizadas para a identificação de riscos, em ordem de preferência são *Brainstorming*, Entrevista, Revisão de Documentos, Listas de Verificação, Técnica Delphi, Análise (Matriz) SWOT e Análise Causal (Diagrama de Ishikawa):

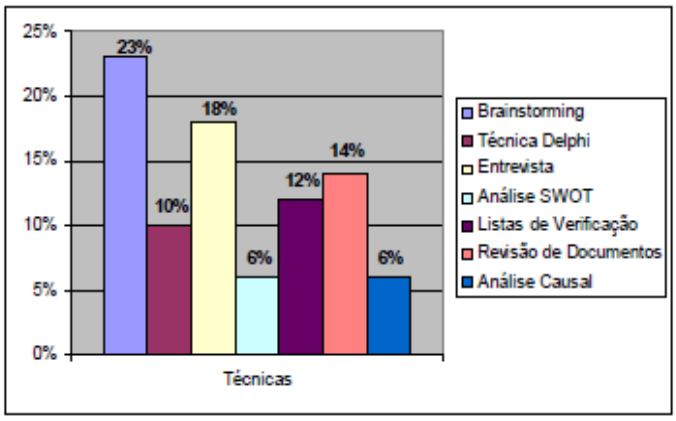

Figura 3: Técnicas para Identificação de Riscos [Gusmão 2007]

- *Brainstorming*

Técnica de geração de ideias em grupo dividida em duas fases: (1) fase criativa, onde os participantes apresentam o maior número possível de ideias (2) fase crítica, onde cada participante defende sua ideia com o objetivo de convencer os demais membros do grupo. Na segunda fase são filtradas as melhores ideias, permanecendo somente aquelas aprovadas pelo grupo.

A técnica é composta de quatro regras básicas: (1) As críticas devem ser banidas – a avaliação das ideias deve ser guardada para momentos posteriores; (2) A geração livre de ideias deve ser encorajada; (3) Foco na quantidade – quanto maior o número de ideias, maiores as chances de se ter ideias válidas; (4) Combinação e aperfeiçoamento de ideias geradas pelo grupo.

A meta do *brainstorming* é obter uma lista abrangente de riscos do projeto. A equipe do projeto normalmente realiza o *brainstorming*, frequentemente com um conjunto multidisciplinar de especialistas que não fazem parte da equipe. Ideias sobre os perigos, riscos e fatores de riscos do projeto são geradas sob a liderança de um facilitador.

É preferível que as pessoas que se envolvam nesse método sejam de setores e competências diferentes, pois suas experiências diversas podem colaborar com a "tempestade de ideias" que se forma ao longo do processo de sugestões e

discussões. Nenhuma ideia é descartada ou julgada como errada ou absurda. Todas as ideias são ouvidas e trazidas até o processo de *brainwriting*, que se constitui na compilação ou anotação de todas as sugestões ocorridas no processo de *brainstorming*, em uma reunião com alguns participantes da sessão de *brainstorming*, e assim evoluindo as ideias até a chegada da solução efetiva.

- **Listas de Verificação**

  As listas de verificação (checklists) são comumente usadas para identificar os riscos associados a um processo e para assegurar a concordância entre as atividades desenvolvidas e os procedimentos operacionais padronizados. Através deste método, diversos aspectos do sistema são analisados por comparação com uma lista de itens pré-estabelecidos, criada com base em processos similares, objetivando descobrir e documentar possíveis deficiências do sistema.

  Desvantagens estão associadas à impossibilidade de listar todos os riscos e a limitação da identificação aos itens constantes da lista pelo usuário (categorias e fatores de risco). Normalmente, as listas de verificação são utilizadas para embasar ou fortalecer os resultados obtidos por algumas técnicas de análise de riscos, por exemplo, *brainstorming*.

- **Comparação por Analogia**

  Este método tem por base a comparação entre projetos, identificando projetos similares para a efetiva comparação de acordo com os critérios determinadas.

  É um método de simples aplicação, mas devido à subjetividade na determinação das características para a comparação entre projetos, incute dependência na análise e interpretação dos dados históricos e no nível de detalhamento descrito.

- **Análise de Premissas**

  Além dos riscos envolvidos na execução de um projeto, existem os riscos associados às hipóteses e premissas utilizadas na definição do plano de projeto e no próprio ambiente organizacional. Estas premissas são identificadas e validadas ao longo do desenvolvimento, como forma de prevenção dos riscos

(imprecisão, inconsistência, incompletude), evitando a execução de um projeto baseado em premissas irreais [PMI 2009].

- **Entrevista com Especialistas**

  A entrevista com especialistas é um método de coleta de informações, utilizada no levantamento e na identificação de riscos. Inicialmente os especialistas são identificados, selecionados, a agenda é criada e o questionário é desenvolvido.

  A aplicação dos questionários pode ser desenvolvida através de entrevistas individuais ou da formação de grupos focais (formados por profissionais com perfis similares e existe a figura do facilitador para coletar as informações definidas) [Victoria et al. 2000]. A vantagem deste método é a obtenção de diversas visões de riscos, dentro do contexto escolhido, pela participação de profissionais de perfis e experiências distintas.

  Entre as desvantagens pode-se associar a criação do questionário, não limitando as respostas dos entrevistados, e a forte dependência existente entre entrevistado e entrevistador.

- **Análise Causal**

  Este método é baseado na análise entre um efeito e sua possível causa para que seja identificada a origem do risco. Entre os métodos que empregam a análise causal estão: Diagrama de Causa e Efeito, também conhecido com Espinha de Peixe (fishbone), e a técnica dos 6 W´s (Who, Why, What, Whichway, Wherewithal, When) [Boehm e De Marco 1997].

  O Diagrama de Causa e Efeito é também conhecido como Diagrama de Ishikawa ou Espinha de Peixe, e é útil para a identificação da causa dos riscos. O diagrama é montado organizando o efeito à direita e as causas à esquerda. Para cada efeito existem categorias de causas. As causas principais podem ser agrupadas por estas categorias. Assim, para cada perigo (efeito) identificado devem-se procurar os Fatores de Riscos (causas) [Brasiliano 2009].

- **Técnica Delphi**

Esta técnica é utilizada quando existe a necessidade de obter o consenso sobre determinado assunto, entre um grupo de especialistas. É uma variação dos grupos focais, onde especialistas são identificados, mas participam anonimamente [Victoria et al 2000]. Um facilitador usa um questionário para levantar ideias sobre os riscos mais importantes de um projeto em questão.

As respostas são apresentadas e circulam entre o grupo para que sejam inseridos comentários, caso desejem. O consenso é atingido através de diversas rodadas. Ao final um grupo de riscos avaliados e aprovados pelo grupo é apresentado e consolidado. Como vantagem desta técnica, tem-se a redução dos desvios nos dados e o equilíbrio mantido entre as influências dos especialistas [PMI 2009]. Como desvantagem, igualmente a entrevista com especialistas, tem dependência direta com as questões apresentadas (questionário), limitando a troca de ideias.

- **Análise SWOT**

A análise SWOT (Strength, Weakness, Opportunity and Threats) está mais voltada para uma avaliação organizacional do que para um projeto individualmente [Brasiliano 2009, PMI 2008, Heldman 2005].

Como o acrônimo especifica, é uma análise que procura aferir questões positivas e negativas da organização através dos pontos fortes e fracos encontrados.

A finalidade é identificar na organização onde existem vulnerabilidades e como potencializar e fortalecer determinado tipo de atividade realizada com perfeição. Como exemplo, pode-se citar uma situação em que uma organização desenvolvedora de software tem em seu histórico de atuação, sucesso em projetos de desenvolvimento, mas fracassos em projetos de montagem de laboratórios. Ora, se um novo projeto a ser executado é para montar um laboratório, o impacto dos riscos associados às atividades para execução deste projeto têm maiores consequências para a organização. De imediato devem ser tratados os pontos falhos neste cenário. [Gusmão 2007]

A análise SWOT foi adaptada por Brasiliano [Brasiliano 2009] para a área de Gestão de Riscos e é utilizada com o objetivo de ranquear fraquezas,

oportunidades, ameaças e forças: os fatores facilitadores dos perigos identificados.

Outras técnicas também encontradas na literatura são *Nominal Group Technique*, análise de negócio, análise causal, estudo de viabilidade e avaliação do documento de requisitos [Heldman 2005].

O Método Brasiliano Avançado de Análise de Risco [Brasiliano 2009] defende a utilização do *Brainstormin*g para identificar e listar os perigos da organização; O Diagrama de causa e efeito (Diagrama de Ishikawa) para identificar os Fatores de Riscos, que como já mencionado, são os eventos que podem potencializar a concretização dos perigos; e as ferramentas Matriz SWOT e Matriz de Impactos Cruzados para a avaliação dos Fatores de Riscos. Essa avaliação é a mensuração dos respectivos Fatores de Riscos com o objetivo de identificar quais os que possuem maior importância e motricidade (influência sobre os demais fatores). Veremos mais detalhes da utilização dessas ferramentas na seção 2.3 do Capítulo 2.

2.1.8. Técnicas de Análise e Avaliação de Riscos

Após a identificação dos riscos é realizada a análise e avaliação.

Prevenir, prever falhas e acidentes, minimizar consequências, auxiliar na elaboração de planos de contingência, estes são alguns dos objetivos da avaliação de riscos em ambientes de desenvolvimento de software. No entanto, a consagração destes resultados requer a adoção de uma metodologia sistemática e estruturada de identificação, análise e priorização de riscos.

A análise de riscos visa promover o entendimento do nível de risco e de sua natureza, auxiliando na definição de prioridades e opções de tratamento aos perigos identificados. Por meio dela, é possível saber qual a chance, a probabilidade dos riscos virem a acontecer e calcular seus respectivos impactos na organização.

É importante ressaltar que tanto a análise como a avaliação de riscos pode ser realizada com vários graus de detalhamento, dependendo do risco, da finalidade da análise e das

informações, dados e recursos disponíveis. A avaliação pode ser tanto quantitativa (objetiva) – baseada em estatísticas, aferindo base histórica dos registros de incidentes relatados – quanto qualitativa (subjetiva) – baseada em experiência (*know-how*), geralmente realizada por especialistas que têm profundos conhecimentos sobre o assunto, ou ainda uma combinação das mesmas, dependendo das circunstâncias.

A análise de riscos é tipicamente uma atividade de prevenção. As métricas são utilizadas para determinar a probabilidade da ocorrência e a perda associada. A partir deste conhecimento podem ser definidas estratégias de controle e monitoramento dos eventos, assegurando uma ação efetiva.

As principais técnicas quantitativas citadas para utilização em processos de Gerência de Riscos são: às árvores de decisão e simulações [Boehm 1991, PMI 2008]:

- **Árvore de decisão**: Uma técnica fundamental na análise de riscos é a árvore de decisão, pois segmenta o problema em vários subconjuntos, facilitando a elaboração da solução e a tomada de decisão [Boehm 1991, Clemen 1991, Keelling 2002].

- **Simulação:** As técnicas de simulação auxiliam na quantificação dos riscos associados ao projeto. Uma das mais comuns é a Análise de Monte Carlo [CSEP 1995, Heldman 2005].

  As técnicas de simulação são realizadas através de automação computacional, logo precisam de um programa específico que realize as funções necessárias.

  A análise de Monte Carlo analisa, individualmente e, com relação a todo projeto, as atividades sob os critérios de quantidade de horas e custos de execução. A análise é realizada através de variáveis definidas para o cronograma das atividades do projeto e para pacotes de serviços definidos através da WBS (Work Breakdown Structure). Estas variáveis são analisadas para situações onde os valores podem ser pessimistas, mais frequentemente, ou otimistas, levando em consideração um desvio padrão.

A natureza das interações que se estabelecem entre os diversos recursos que compõem um projeto de software é variada e nem sempre se processa do mesmo modo. Este é um

dos motivos pelos qual o uso exclusivo de métodos quantitativos pode falhar na área de gerência de projeto. Neste sentido tem crescido o uso de abordagens interpretativas e de técnicas qualitativa (subjetivas) nas atividades de gerenciamento de projetos [Holloway 1997, Victoria et al 2000, Silva 2002].

A investigação qualitativa constitui uma interpretação, uma aproximação naturalística do mundo, o que significa que este tipo de investigação estuda as coisas no seu ambiente natural, numa tentativa de compreender ou interpretar os fenômenos em termos do significado que as pessoas lhes dão.

A principal técnica qualitativa referenciada pelo Guia PMBOK [PMI 2009] é a utilização da Matriz de Riscos, que também é a técnica escolhida pelo Método Brasiliano. Essa matriz é composta pelo levantamento das probabilidades de ocorrência e gravidade dos riscos e consequente exposição do projeto ao risco:

- Como o risco implica uma perda potencial, dois elementos fundamentais devem ser estimados: a probabilidade de ocorrência e a gravidade (impacto) do risco.

  Uma das métricas mais comuns utilizadas para determinar a gravidade do risco é Cálculo de Exposição ao Risco [Boehm 1991, Brasiliano 2009]. A finalidade é definir um valor numérico que representa a potencialidade do risco para o alcance dos resultados do projeto. Esta avaliação utiliza escalas de probabilidade e impacto definidas pelo gerente para análise dos riscos. A partir desta análise é possível priorizar os riscos de maior exposição para o projeto e definir respostas para seu tratamento.

  Probabilidade - Saber qual a chance, a probabilidade, dos perigos virem a acontecer, frente à condição existente – risco.

  Impacto - Calcular o impacto com base na consequência.

  Definir escalas de probabilidade e o impacto é uma atividade subjetiva. O uso de escalas minimiza os riscos associados à subjetividade. Esta atividade está normalmente direcionada para o gerente de projeto, mas para organizações que possuem os escritórios de projetos em sua estrutura, estes passam a ter a responsabilidade pela elaboração e manutenção.

> O desenvolvimento das escalas de probabilidade e impacto deve levar em consideração critérios relacionados aos históricos dos projetos executados na organização, mais também, informações da literatura e a experiência dos profissionais envolvidos no ambiente de desenvolvimento (gerentes de projetos, engenheiros de software, analistas, entre outros).

O Guia PMBOK enfatiza o uso destas técnicas, em especial às qualitativas [PMI 2009]. A ISO 31000:2009 não prescreve critérios ou métodos para a análise e avaliação de riscos, deixando a cargo da organização a escolha, tendo em vista as características do negócio. O framework do Método Brasiliano combina técnicas quantitativas e qualitativas para avaliar os riscos.

Outras técnicas como: análise de cenários, métrica *Fuzzy*, aplicação de questionários também são relatados na literatura [Boehm 1991, Charette 2001, Moynihan 1997].

Resumo da Seção

Esta seção apresentou através de uma sucinta revisão da literatura os principais conceitos relacionados à Gerência de Riscos, sua história e origens, uma contextualização sobre os Riscos na área de Engenharia de Software, as principais atividades que compõe as metodologias para Gerenciamento de Riscos, focando as principais técnicas de Identificação e Análise de Riscos utilizadas.

2.2. Método Brasiliano de Análise de Riscos

Esta seção apresenta os objetivos, estrutura e processos da Norma ISO 3100 de Gestão de Riscos. Veremos em detalhes o Método Brasiliano de Análise de Riscos que fornece um processo, alinhado com a ISO 31000, para a identificação, análise e avaliação dos riscos.

2.2.1. ISO 31000:2009 – Gestão de Riscos

Durante os anos de 2007 e 2008, uma série de questões de riscos – desde a crise de liquidez nos mercados financeiros até as preocupações emergentes sobre terrorismo, clima, disponibilidade de alimentos, infraestrutura e energia – focou a atenção global na fragilidade sistêmica dos processos estratégicos das nações e, consequentemente, do mundo [Brasiliano 2009].

Uma conscientização do risco e gerenciamento de risco é cada vez mais vista como um pré-requisito para o controle efetivo, tanto no setor privado como público.

Dentro desse contexto, é que, em 2009, foi lançada oficialmente a ISO 31000, que teve como desafio integrar os diferentes conceitos da Gestão de Riscos Corporativos. A norma foi desenvolvida por uma comissão especial da ISO (International Organization for Standardization) e teve sua numeração definida como ISO 31000.

2.2.1.1. Objetivos

A ISO 31000 surgiu da necessidade de harmonizar padrões, regulamentações e frameworks publicados anteriormente e que de alguma forma estão relacionados com a gestão de riscos.

A origem da norma, que pode ser aplicada por empresas ou indivíduos, e fornece diretrizes para implementação de gestão de riscos em organizações de qualquer tipo, tamanho ou área de atuação, vem da necessidade das corporações de lidar com as incertezas que podem afetar os seus objetivos.

Esses objetivos podem ter diferentes aspectos (tais como metas financeiras, de saúde e segurança e ambientais) e podem aplicar–se em diferentes níveis (tais como estratégico, em toda a organização, de projeto, de produto e de processo). Assim, a norma pode ser aplicada aos vários tipos de riscos ligados aos diferentes setores da organização, tais como financeiro, saúde e meio ambiente, tecnologia da informação, segurança empresarial, seguros, de projetos, entre outros, incluindo a visão moderna de que risco também é oportunidade.

A ISO 31000 surgiu também para integrar as diversas metodologias e terminologias, pois ainda faltava um consenso em relação à nomenclatura e aos conceitos utilizados para a gestão de riscos.

Segundo Alberto Bastos, coordenador da Comissão de Estudo Especial de Gestão de Riscos – ABNT (Associação Brasileira de Normas Técnicas), “a ISO avaliou e descobriu que existiam mais de sessenta comitês técnicos ou grupos de trabalhos que desenvolviam normas em vários setores que, de alguma forma, diziam a respeito à gestão de riscos” e, vendo que “cada grupo desses ou cada norma, utilizava conceitos diferentes, terminologias diferentes”, percebeu “a necessidade de se criar, principalmente dentro de um organismo de normalização, um padrão para que se padronizassem todos esses documentos, todas essas práticas.” “O mais difícil foi se conseguir conciliar e chegar ao consenso diferentes áreas, diferentes termos utilizando a gestão de risco.” Esse objetivo foi alcançado e na norma existe um capítulo apenas para terminologia.

A ISO 31000 possui um processo consistente e uma estrutura abrangente para ajudar a assegurar um gerenciamento de risco de forma eficaz, eficiente e coerente.

Por esta razão, a abordagem é genérica fornecendo os princípios e diretrizes para gerenciar qualquer forma de risco de uma maneira sistemática, transparente e confiável, dentro de qualquer escopo e contexto.

2.2.1.2. Estrutura Geral da Norma

O sucesso da gestão de riscos depende da estrutura de gestão que fornece os fundamentos e os arranjos que irão incorporá-la através de toda a organização, em todos os níveis. A estrutura descreve os componentes necessários do esqueleto para gerenciar riscos e a forma como eles se inter-relacionam.

A Figura 4 apresenta a visão desta estrutura:

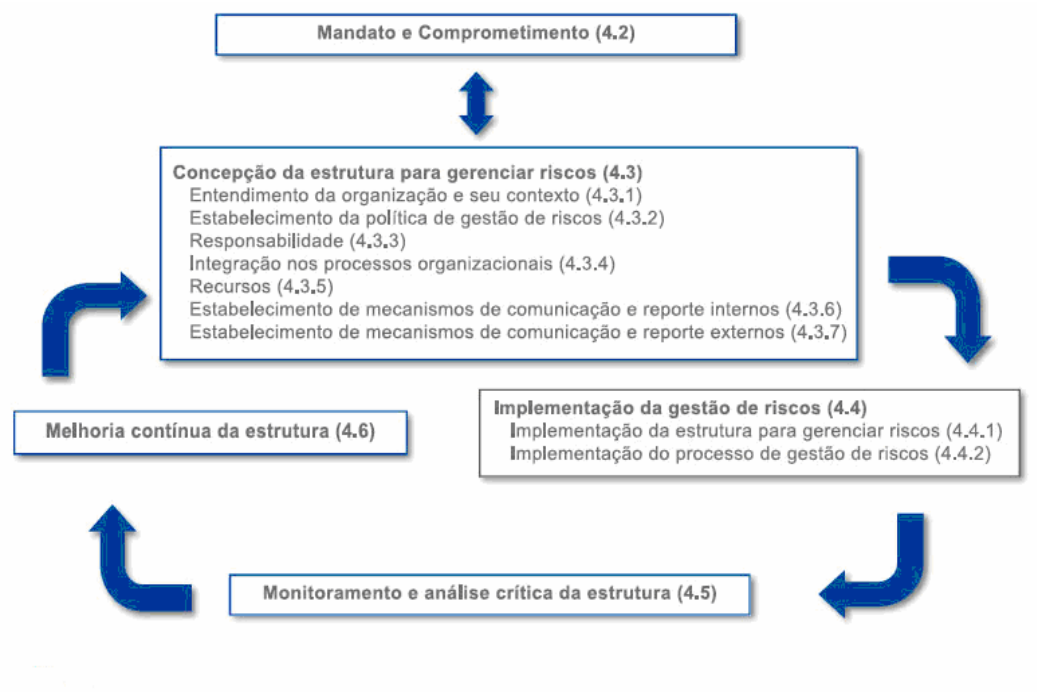

Figura 4: ISO 3100 – Estrutura

Esta estrutura não se destina a estabelecer um sistema de gestão, mas sim para ajudar a organização a integrar a gestão de risco em seu sistema de gestão global. Portanto, as organizações devem adaptar os componentes às suas necessidades específicas. Analisaremos sucintamente cada componente:

Mandato e compromisso

A introdução da gestão de risco é essencial para garantir a sua eficácia continuada, requer forte e sustentado compromisso da gestão da organização, bem como o planejamento estratégico e rigoroso para atingir empenho em todos os níveis.

Concepção da Estrutura para Gerenciar Riscos

- Compreender a organização e seu contexto

Antes de iniciar a concepção e implementação do quadro de gestão de risco é importante para avaliar e compreender tanto o contexto externo e interno da organização, uma vê que estes podem reduzir significativamente a influência do design do quadro.

- O estabelecimento da política de gestão de risco

A política de gestão de risco deve indicar claramente os objetivos da organização.

- Responsabilidade

A organização deve assegurar que haja responsabilidade, autoridade e competências adequadas à gestão de riscos, incluindo a implementação e manutenção do processo de gestão de risco e garantir a adequação, eficiência e eficácia dos controles.

- Integração em processos organizacionais

A gestão de riscos deve ser integrada em todas as práticas e processos organizacionais de uma forma que é relevante, eficaz e eficiente. O processo de gerenciamento de risco deve ser parte, não estão separados, os processos organizacionais.

- Recursos

A organização deve alocar recursos adequados para a gestão de risco. Deve ser levado em consideração: as pessoas, habilidades, experiência e competência; os recursos necessários para cada etapa do processo de gestão de riscos; os processos organizacionais, métodos e instrumentos utilizados na gestão de riscos; processos e procedimentos documentados; e os sistemas de informação e gestão do conhecimento e programas de treinamento.

- Mecanismos para comunicação interna e comunicação

A organização deve estabelecer a comunicação interna e os mecanismos para apoiar e incentivar a responsabilidade e a participação.

- Mecanismos para a comunicação externa e comunicação

A organização deve desenvolver e implementar um plano de como você irá se comunicar com o exterior as partes interessadas.

Implementação da Gestão de Riscos

- Aplicação de uma estrutura para o gerenciamento de risco

Como parte da implementação da organização para a gestão de riscos, a organização deve entre outros: Definir o calendário e estratégia para a implementação do quadro

regulamentar; implementar a política de gestão de riscos e processo de processos organizacionais; garantir que a tomada de decisões, incluindo o desenvolvimento e estabelecimento de objetivos, está alinhado com os resultados dos processos de gestão de risco;

- Implementação do processo de gestão de risco

A gestão dos riscos devem ser implementada para assegurar que o processo de gestão do risco descrito, é aplicado através de um plano de gestão de riscos em todos os níveis e funções relevantes da organização como parte de suas práticas e processos.

Monitoramento e Análise crítica da estrutura

Para garantir que a gestão do risco é eficaz e continua a apoiar o desempenho organizacional, a organização deve:

- Estabelecer indicadores de desempenho;
- Medir o progresso periodicamente contra, e o desvio do plano de gestão de risco;
- Revisar periodicamente se no âmbito da política de gestão de riscos e do plano ainda são adequados, tendo em conta as realidades internas e externas das organizações;
- Reportar sobre os riscos, o progresso do plano de gestão de risco e como a política de gestão de risco é seguido;
- Revisar a eficácia da estrutura de gerenciamento de risco.

Melhoria contínua da estrutura

Com base nos resultados da monitoração e avaliação, as decisões devem ser feitas sobre coma estrutura de gestão de risco, a política e o plano podem ser melhorados. Estas decisões devem levar a melhorias na organização de gestão de riscos e de sua cultura de gestão de risco.

2.2.1.3.Processos

A ISO 31000 defende que o Processo de Gerenciamento de Risco deve ser:

- Uma parte integrante da gestão;
- Incorporados na cultura e práticas, e;
- Adaptados para os processos de negócio da organização.

Genericamente, o processo estruturado sugerido possui sete atividades claramente identificadas, sendo um processo retroalimentativo. Ou seja, segue os princípios do ciclo da qualidade, PDCA – *Plan – Do – Check – Action*. A Figura 5 traz a visão estruturada das atividades da norma ISO 31000.

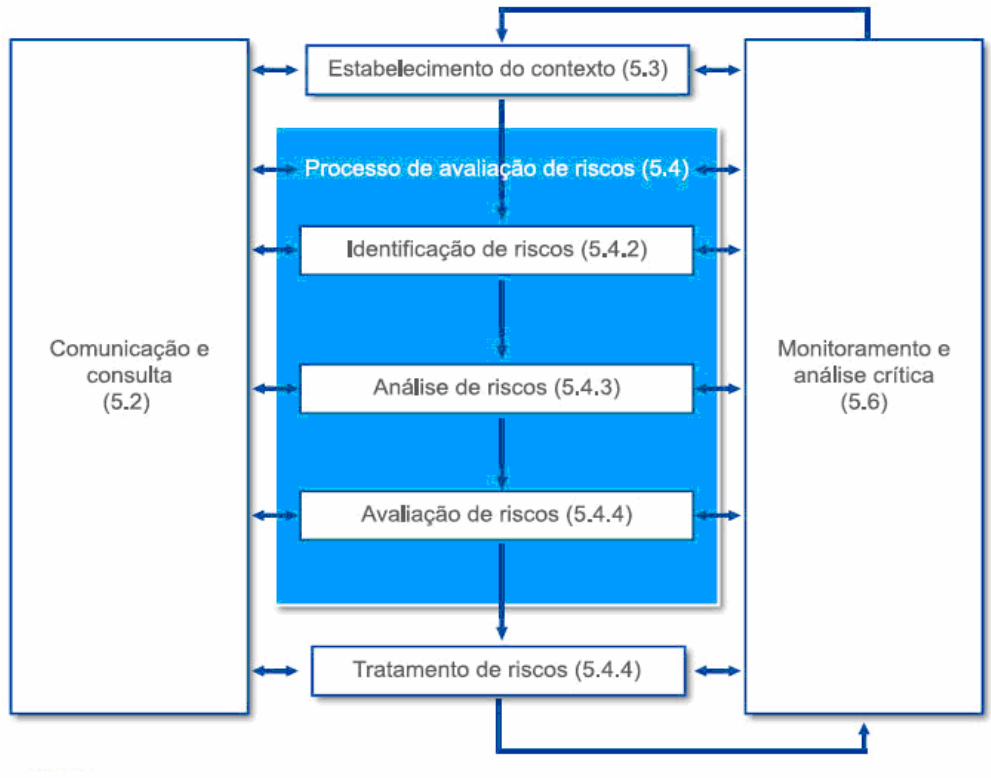

Figura 5: ISO 31000 – Processo de Gerenciamento de Riscos

A fase de COMUNICAÇÃO E CONSULTA abrange todas as demais fases e é inter-relacionada. A cobertura é tanto sobre a comunicação interna quanto a externa,

assegurando que os responsáveis e partes interessadas compreendam os fundamentos sobre os quais as decisões são tomadas e as respectivas razões.

A fase do ESTABELECIMENTO DO CONTEXTO preconiza entender os fatores e as variáveis externas, incluindo os fatores-chave, as tendências e as relações com as partes interessadas externas e suas percepções de valores. Já no contexto interno a preocupação está em entender: objetivos estratégicos, cultura, processos, estrutura e estratégia. No contexto geral, estabelece-se o processo de gestão de riscos com sua estrutura, seus critérios e métodos que a organização deverá utilizar. Definem-se metas e objetivos além de responsabilidades e o apetite ao risco que a organização quer possuir.

A fase da IDENTIFICAÇÃO DE RISCOS, no processo de avaliação de riscos, é a listagem dos perigos que o processo, departamento e ou empresa possui com as respectivas fontes de riscos. A identificação deve ser crítica, pois um risco que não é identificado nesta fase não será incluído em análises posteriores. Fica claro que essa é uma fase estratégica, pois favorece o entendimento dos fatores de riscos, fatores facilitadores da existência do risco na empresa.

A fase de ANÁLISE DE RISCOS desenvolve a compreensão dos riscos. Com a compreensão dos riscos é que a empresa poderá tomar decisões a respeito de seu tratamento. Nessa fase, estima-se a probabilidade e consequência do risco na empresa.

A análise envolve a apreciação das causas e as fontes de risco, suas consequências positivas e negativas, e a probabilidade de que essas consequências possam ocorrer. A norma não especifica critérios e métodos, pois organização é a responsável pela escolha, a qual deve respeitar as características do negócio.

A fase da AVALIAÇÃO DE RISCOS visa auxiliar na tomada de decisões – com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento, bem como sobre qual a prioridade para a implementação do mesmo. Na avaliação de riscos, que, envolve comparar o nível de risco encontrado durante a análise de riscos, deve-se utilizar uma Matriz de Riscos como ferramenta de gestão.

A fase de TRATAMENTO DE RISCOS envolve um processo cíclico composto por:

- Avaliação do tratamento já realizado;

- Decisão se os níveis de risco residual são toleráveis;
- Se não forem toleráveis, a definição e implementação de um novo tratamento;
- Avaliação e eficácia desse tratamento.

As opções de tratamento de riscos não são necessariamente mutuamente exclusivas, ou adequadas em todas as circunstâncias [Brasiliano 2009]. As opções podem incluir os seguintes aspectos:

- A ação de evitar o risco ao se decidir não iniciar, ou descontinuar, a atividade que dá origem ao risco;
- A tomada ou o aumento do risco na tentativa de tirar proveito de uma oportunidade;
- A remoção da fonte de risco;
- A alteração da probabilidade;
- A alteração das consequências;
- O compartilhamento do risco com outra parte ou partes (incluindo contratos e financiamento do risco);
- A retenção do risco por uma decisão consciente e bem embasada.

A última fase, MONITORAMENTO E ANÁLISE CRÍTICA é a fase da checagem ou das vigilâncias regulares. Podem ser regulares – periódicas ou acontecerem em resposta a um fato específico. Deve haver uma definição clara e direta das responsabilidades de quem vai realizar o monitoramento e a análise crítica.

2.2.2. Método Brasiliano

O Método Avançado de Análise e Resposta aos Riscos Corporativos – Método Brasiliano fornece um processo, alinhado com a ISO 31000, para a identificação dos perigos,

avaliação dos seus Fatores de Riscos, análise e avaliação dos riscos corporativos. Este método descreve passos a serem percorridos, ferramentas a serem utilizadas, critérios a adotar na probabilidade, impacto, além de estabelecer priorização de ações a serem executadas.

O Método será apresentado através das atividades do processo definido pela ISO 31000 (Figura 5) descritas na Seção 2.2.1.3: Comunicação e Consulta, Contextos Estratégicos, Processo de Avaliação de Riscos, Tratamento dos Riscos e Monitoração e Análise Crítica.

2.2.2.1.Comunicação e Consulta

A comunicação e consulta é a forma como vai estabelecer o processo e a estratégia de comunicação com as partes interessadas.

É uma fase que permeia todo o processo de planejamento e gestão de riscos. É extremamente estratégico, pois sem a comunicação não vai existir processo de gestão de riscos tendo em vista não sensibilizar os usuários do processo [Brasiliano 2009].

Nessa fase, há necessidade de elaborar campanhas de endomarketing, difundindo os critérios e metodologias que a empresa deve implantar.

2.2.2.2. Contextos Estratégicos

Segundo Brasiliano [Brasiliano 2009], o estabelecimento do contexto é dividido em três níveis. O primeiro nível diz respeito ao entendimento da empresa, através da compreensão dos objetivos estratégicos e organizacionais, a cultura e como ela – empresa – pensa sobre a questão de gestão de riscos. O segundo nível trata variáveis externas incontroláveis que poderão interferir ou expor os objetivos estratégicos da empresa. Na verdade, há a necessidade de se construir cenários de riscos estratégicos. O terceiro nível abarca a Política de Gestão de Riscos da empresa. O objetivo é detalhar a estrutura que será trabalhada, os critérios e metodologia que serão utilizados.

2.2.2.3. Processo de Avaliação de Riscos

O processo de Avaliação de Riscos pode ser dividido nas seguintes fases: Identificação dos Perigos e Fatores de Riscos, Análise dos Riscos e Avaliação dos Riscos – Nível de Risco. Detalharemos cada fase a seguir.

2.2.2.3.1. Identificação dos Perigos e Fatores de Riscos

Brasiliano divide esta fase em três objetivos: 1 - Identificar e listar os perigos; 2 – Identificar os Fatores de Riscos e 3 - Avaliar os Fatores de Riscos. Para alcançar cada objetivo são utilizadas técnicas e ferramentas específicas conforme detalhamento a seguir:

1. Identificar e listar os perigos a que a empresa, unidades, processos e ou departamentos estão expostos. A listagem deve ser realizada através de reuniões do tipo *brainstorming*, identificando tanto os perigos conhecidos como os desconhecidos. Os perigos desconhecidos são aqueles que nunca aconteceram, mas que podem ocorrer, mesmo que remotamente;

2. Identificar os Fatores de Riscos. Os Fatores de Riscos, também chamados de Fatores Facilitadores e ou Fontes de Riscos, são os eventos que podem potencializar a concretização dos perigos. São variáveis controláveis e incontroláveis. Utiliza-se para isso a ferramenta de gestão Diagrama de Causa e Efeito (Diagrama de Ishikawa).

O Diagrama de Causa e Efeito é uma notação simples para identificar fatores que causam o evento estudado. Em 1953 o Professor Karou Ishikawa, da Universidade de Tóquio - Japão sintetizou as opiniões dos engenheiros de uma fábrica na forma de um diagrama de causa e efeito, enquanto eles discutiam problemas de qualidade.

Na Gestão de Riscos da segurança patrimonial, Brasiliano realizou uma adaptação nos fatores de perigo, inserindo: Meios Organizacionais, Recursos Humanos da Segurança, Meios Técnicos Passivos, Meios Técnicos Ativos, Ambiente Interno e Ambiente Externo [Brasiliano 2009]. A Figura 6 mostra essa adaptação:

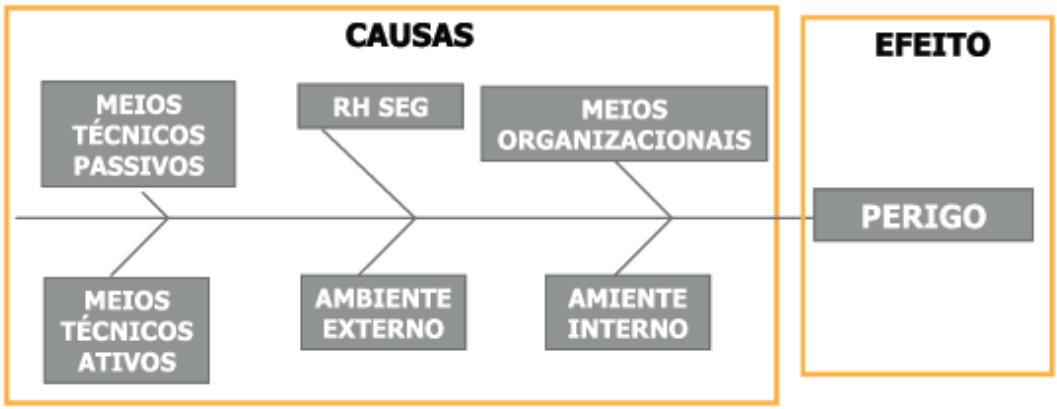

Figura 6: Diagrama de Causa e Efeito

A técnica para detalhar os fatores é fazendo a pergunta POR QUE? Até esgotar o respectivo fator. O objetivo é identificar quais subfatores influenciam na concretização do perigo. O risco passa ser então o somatório dos fatores. O Diagrama de Ishikawa é o risco, é a condição.

3. Avaliar os Fatores de Riscos. Após a identificação dos vários fatores de riscos o analista precisa enxergar estrategicamente quais são os fatores de riscos comuns a todos os perigos e quais são os mais motrizes, ou seja, quais são os que possuem maior influência no contexto.

A avaliação dos fatores de riscos é a mensuração dos respectivos fatores com o objetivo de identificar quais são os fatores de maior importância e ou motricidade. Ou seja, quais são os fatores que devem ser tratados e quais são os que interferem no contexto de riscos. Utiliza-se para isso duas Ferramentas de Gestão: a Matriz SWOT e ou a Matriz de Impactos Cruzados. Analisaremos cada uma detalhadamente:

- **Matriz SWOT**

A análise SWOT (Strenghts, Weaknesses, Opportunities, Threats) foi adaptada pelo administrador Antônio Celso Ribeiro Brasiliano, Diretor Executivo da empresa Brasiliano & Associados Gestão de Riscos Corporativos para área de gestão de riscos. O objetivo almejado com a adaptação continuou sendo praticamente o mesmo oferecido pela análise: o de aplicação na área de planejamento estratégico visando apresentar um

diagnóstico claro após a realização da análise, ou seja, promover uma visualização do todo, demonstrando uma fotografia da empresa que está sendo estudada.

Igualmente à aplicação na área de planejamento estratégico, a Matriz SWOT aplicada na área de gestão de riscos – chamada também de Matriz FOFA (Forças, Oportunidades, Fraquezas e Ameaças) – é utilizada com o objetivo de ranquear fraquezas, oportunidades, ameaças e forças: os fatores facilitadores dos perigos identificados.

A matriz (Figura 7) possui quatro células, avaliadas quantitativamente, utilizando-se dois parâmetros:

A. Magnitude significa o tamanho ou grandeza que a variável ou evento possui perante a empresa. Caso aconteça, positivamente ou negativamente, o quanto ela vai influenciar no contexto como um todo. A magnitude é ranqueada, utilizando-se uma pontuação, que varia de –3 a +3, dentro do seguinte parâmetro: + 3 (alto); + 2 (médio);+ 1 (baixo), para cada elemento positivo (força ou oportunidade) e –1 (baixo); -2 (médio); -3 (alto) para cada variável negativa (fraqueza e ameaça). No nosso caso podemos ter como parâmetro para poder dar a nota da magnitude na célula da fraqueza e ameaça o número de vezes que as variáveis aparecem no diagrama de causa e efeito. É uma forma mais objetiva de saber a magnitude do Fator de Risco, pois se um Fator de Risco aparece 5 vezes em seis perigos estudados, significa que esta variável é de “grande” magnitude.

B. Importância significa a prioridade que esta variável deve possuir perante a conjuntura da empresa. É uma nota subjetiva com base na experiência da equipe que está avaliando. Utilizamos também três níveis de pontuação: 3 (muito importante); 2 (média importância); 1 (pouca importância). Neste caso, não há contagem negativa para a importância, pois, tanto faz ela ser negativa ou positiva.

Figura 7: Matriz SWOT

Para ranquear os itens em cada célula, podemos multiplicar a avaliação da magnitude e da importância (R = [M]agnitude x [I]mportância). Os fatores de riscos ranqueados com maior numeração, positiva e negativa, são considerados motrizes. Motrizes porque devem receber maior atenção.

A matriz SWOT - FOFA demonstra o conjunto de Fatores de Riscos (Fraquezas e Ameaças), e seus pontos fortes e oportunidades. Com esta fotografia o analista enxergará seus pontos de maior fragilidade. Se formos observar sob o ponto de vista das fraquezas e ameaças contidas na Matriz SWOT, podemos afirmar que a Matriz SWOT é um resumo de todos os diagramas de causa e efeito, sem listar os fatores repetidos.

Ponto importante na matriz SWOT – FOFA é que as fraquezas são oriundas dos diagramas de causa e efeito, são os resumos dos fatores de riscos: recurso humano, ambiente interno, meios técnicos ativos, meios técnicos passivos, meios organizacionais. As ameaças são as variáveis incontroláveis do ambiente externo, também oriundas do diagrama de causa e efeito. As variáveis negativas (fraquezas e ameaças) da Matriz SWOT – FOFA são o resumo dos vários diagramas de causa e efeito, sendo a base para a definição do Plano de Ação.

A Matriz SWOT - FOFA adaptada para a gestão de riscos visualiza o todo, enquanto que o diagrama de causa e efeito visualiza somente o perigo estudado. Por esta razão há a necessidade de elaborar um diagrama para cada perigo. Essa matriz é o resumo estratégico dos fatores de riscos dos perigos, concentrados na fraqueza e ameaças identificadas.

- **Matriz de Impactos Cruzados**

Esta ferramenta é utilizada para avaliar a influência de um Fator de Riscos sobre outros Fatores de Riscos. Ou seja, leva em conta a interdependência entre várias questões formuladas, possibilitando que o estudo que se esteja realizando adquira um enfoque mais global, mais sistêmico e, portanto, mais de acordo com uma visão prospectiva.

Esta ferramenta técnica tem o objetivo de buscar e hierarquizar os Fatores de Riscos mais determinantes e importantes entre todos aqueles identificados no estudo.

A técnica de impactos cruzados pode ser descrita, sucintamente, do seguinte modo: Com base na lista de pertinência versus probabilidade dos fatores de riscos, estes são dispostos em uma configuração matricial, com o eixo horizontal significando às forças motrizes e o vertical as dependências. A diagonal principal da matriz é inutilizada. Os dados são adicionados sempre na VERTICAL, ou seja, de cima para baixo, onde é colocado um peso (valor numérico em uma escala ajustada) que representa a influência de cada evento coluna sobre a probabilidade incondicional do evento linha. A matriz de Impactos Cruzados deve ser preenchida, utilizando-se uma tabela, que permite que se atribuam valores de 0 a 3, para quantificar o efeito (impacto) que a ocorrência do evento destacado poderá causar sobre as probabilidades de ocorrência dos demais eventos, conforme pode ser visualizado na Tabela 3.

Tabela 3: Matriz de Impactos Cruzados – Grau de Impacto

Influência	Nota
ALTA	3
MÉDIA	2
BAIXA	1
NÃO INTERFERE	0

Se o fator coluna não interfere na probabilidade de ocorrência do fator linha será atribuída nota “0”. Se existe interferência, mas a mesma é baixa, nota “1”. Se o fator coluna interfere significamente no fator linha será atribuída nota “2”, e se essa interferência foi alta, nota “3”.

Ao somar os valores das colunas com as linhas, obtém-se, através dos resultados das colunas, a motricidade de cada fator de risco, e através das linhas horizontais o valor de sua dependência. Exemplificamos a matriz abaixo, conforme Figura 8, com seis eventos:

MATRIZ DE IMPACTOS CRUZADOS

	x1	x2	x3	x4	x5	x6	D
x1	0	1	1	1	1	1	5
x2	1	0	1	1	1	0	4
x3	0	1	0	0	1	1	3
x4	0	0	0	0	1	1	2
x5	0	1	1	0	0	1	3
x6	0	1	0	0	1	0	2
M	1	4	3	2	5	4	

D = Dependência M = Motricidade

Figura 8: Matriz de Impactos Cruzados – Exemplo de uso

Esta matriz possui de especial a influência da ocorrência de um evento sobre a probabilidade de outros, definindo-a como impacto. Pode-se então elaborar o gráfico da motricidade *versus* dependência. Para tanto, basta calcular os pontos médios de motricidade e de dependência, aplicando as fórmulas visualizadas na Equação 1, e construir o gráfico (Figura 9), onde o eixo dos "x" corresponde aos valores de dependência e o eixo dos "y" aos da motricidade.

$$PM = \frac{VM + vM}{2}$$

PM = Ponto Médio da Motricidade
VM = Valor mais alto de motricidade
vM = Valor mais baixo da motricidade

$$PD = \frac{VD + vD}{2}$$

PD = Ponto Médio da Dependência
VD = Valor mais alto da dependência
vD = Valor mais baixo da dependência

Equação 1: Cálculo dos pontos médios de motricidade e de dependência

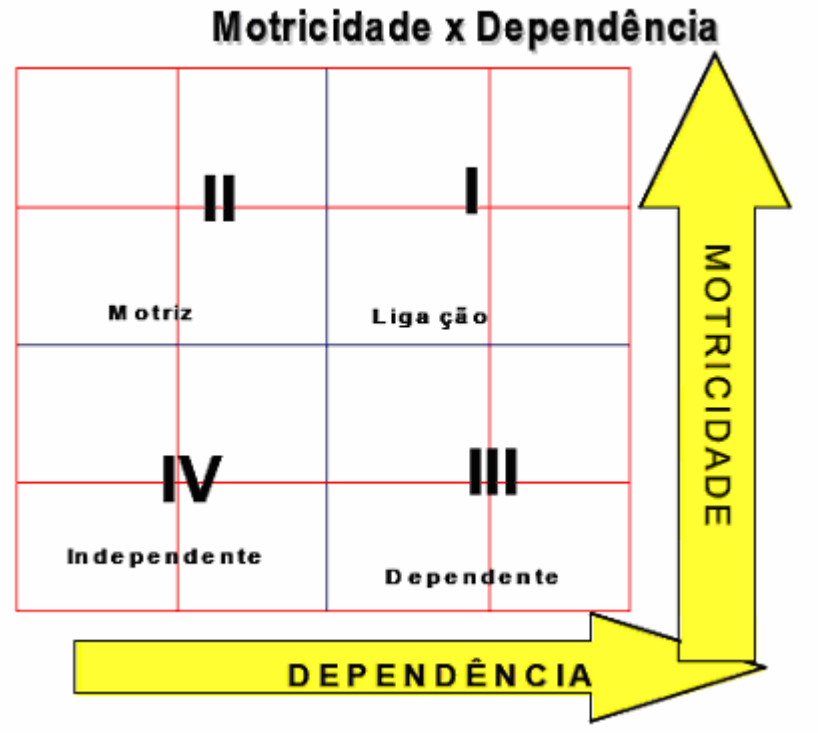

Figura 9: Gráfico - Motricidade x Dependência

As variáveis motrizes (quadrante II) são as que condicionam o restante do sistema. Já as variáveis de ligação (quadrante I) são muito motrizes, mas têm grande dependência das

demais. São as que fazem a ligação entre as variáveis motrizes e as dependentes (quadrante III). Por sua natureza instável, qualquer ação sobre elas terá repercussão sobre as outras e um efeito de retorno sobre si próprio que virá ampliado ou atenuado em função da impulsão inicial.

As variáveis dependentes (quadrante III) são pouco motrizes e muito dependentes, seu comportamento é explicado pelo das variáveis motrizes e de ligação. Já as variáveis independentes (quadrante IV) são aquelas pouco motrizes e pouco dependentes. São geralmente tendências de peso ou fatores relativamente desligados do sistema, e que não constituem determinantes do futuro, podendo ser excluídas da análise.

Análise e Interpretação

- As variáveis consideradas de ligação são as mais importantes, devendo ser tratadas com maior criticidade, pois são interdependentes.
- As variáveis motrizes também devem ser olhadas com criticidade, pois são elas que alavancam as outras variáveis.
- As varáveis dependentes são as menos críticas, pois dependem de outras para que possa a acontecer. As variáveis independentes são consideradas franco atiradoras.

O resultado da Matriz SWOT pode ser diferente do resultado encontrado na Matriz de Impactos Cruzados. Isso ocorre devido à diferença na avaliação de cada uma. Na Matriz SWOT a avaliação é feita de forma mais simples e objetiva buscando identificar os fatores motrizes de acordo com a frequência e a importância dada pela equipe que está analisando, nela não é avaliada a influência de um fator sobre os demais, foco da Matriz de Impactos Cruzados, cuja execução é mais custosa e complexa.

A organização pode optar pelo uso de uma ou ambas. A utilização das duas matrizes de forma complementar possibilita uma melhor priorização dos fatores de riscos críticos.

2.2.2.3.2. Análise dos Riscos

Nesta fase se estabelecem critérios para os dois parâmetros universais: a probabilidade e o impacto. Os critérios para os dois parâmetros são de suma importância para a

elaboração do estudo de análise de riscos. O cruzamento destes dois parâmetros tem como resultado uma Matriz de Riscos.

A metodologia a ser utilizada para a avaliação de riscos possui dois parâmetros claros a serem estudados:

A. Saber qual a chance, a probabilidade, dos perigos virem a acontecer, frente à condição existente – risco;

B. Calcular o impacto / consequência;

O Método Brasiliano possui como diferencial a obtenção do **GRAU DE PROBABILIDADE - GP** do perigo.

O **GP** possui dois critérios: (i) Fatores de Riscos e o (ii) Exposição. O **GP** está alicerçado em uma fórmula simples, que calcula de forma direta, através da multiplicação dos dois critérios, o nível de possibilidade do perigo e ou evento vir a acontecer, frente à situação de segurança e sua exposição. O **GP** pode ser classificado tanto de forma subjetiva como de forma objetiva. Com base nesta classificação e cruzando com o grau do impacto, pode-se obter a Matriz de Riscos da Unidade de Negócio, que podemos chamar de Matriz de Vulnerabilidade. **O Grau de Probabilidade – GP** - é a consequência da multiplicação dos fatores de riscos versus o critério da exposição. É uma multiplicação direta, onde cada critério possui uma escala de valoração 1 a 5.

Critério do Fator de Riscos – "FR"

Este critério possui seis subcritérios, estudados na fase da identificação da origem de cada perigo. Os subcritérios possuem uma escala de valoração que mede o grau de influência para a concretização do perigo. Neste caso julgamos qual o nível de influência, por subcritério, para que o perigo seja concretizado. É uma nota subjetiva, com base no diagrama de causa e efeito. Ou seja, a nota deve estar coerente com o diagrama de causa e efeito realizado. Conforme apresentados no Diagrama de Ishikawa adaptado por Brasiliano, os subfatores de riscos propostos para a área de segurança patrimonial são:

FR AMBIENTE INTERNO: este critério projeta a influência das variáveis internas na concretização do perigo em estudo.

FR AMBIENTE EXTERNO: este critério projeta a influência das variáveis externas incontroláveis, ambiência – cenários, na concretização do perigo em estudo.

FR RECURSOS HUMANOS – SEGURANÇA: este critério projeta o nível da equipe de segurança da empresa, na concretização do perigo em estudo. Deve-se levar em consideração o efetivo existente, perfil, qualificação e posicionamento tático.

FR MEIOS ORGANIZACIONAIS: este critério projeta a influência da formalização das normas e políticas, não existentes na empresa, na concretização do perigo em estudo.

FR MEIOS TÉCNICOS ATIVOS: este critério projeta a influência dos equipamentos e sistemas eletrônicos, não existentes na empresa, na concretização do perigo em estudo.

FR MEIOS TÉCNICOS PASSIVOS: este critério projeta a influência dos recursos físicos, não existente na empresa, na concretização do perigo em estudo.

Os seis fatores de riscos mencionados anteriormente possuem uma escala de valoração que mede o nível e o grau de influência de cada aspecto para a materialização do risco, conforme pode ser observado na Tabela 4.

Tabela 4: Nível do Fator de Risco

Nível do Fator de Risco	
Escala	Pontuação
Influencia Muito	5
Influencia	4
Influencia Medianamente	3
Influencia Pouco	2
Influencia Muito Pouco – quase nada	1

Após a pontuação das questões pertinentes aos respectivos fatores de risco, é necessário efetuar a soma do resultado / média dos seis fatores e dividir por seis para determinar o grau final (média) desta variável, conforme demonstrado a seguir, por meio da Equação 2.

$$FR = \frac{MO + RH + MTA + MTP + AE + AI}{6}$$

MO = Meios Organizacionais
RH = Recursos Humano
MTA = Meios Técnicos Ativos
MTP = Meios Técnico Passivos
AE = Ambiente Externo
AI = Ambiente Interno

Equação 2: Cálculo do Críterio do Fator de Risco

Critério da Exposição

Assim como no tópico anterior, e ainda considerando o contexto da Gestão de Riscos na segurança patrimonial, o critério de exposição possui uma escala de valoração que mede a frequência que as ameaças costumam manifestar-se na empresa ou em empresas similares, conforme pode ser observado na Tabela 5.

Tabela 5: Escala do Critério da Exposição

Critério da Exposição	
Escala	Pontuação
Uma ou mais vezes por mês	5
Uma ou mais vezes por ano	4
Uma ou mais vezes a cada 5 anos	3
Uma ou mais vezes a cada 10 anos	2
Remotamente possível	1

Grau de Probabilidade

O GP é o resultado da multiplicação do valor final do fator de risco *versus* o critério da exposição, conforme demonstrado a seguir, na Equação 3:

$$GP = FR \times E$$

Equação 3: Cálculo do Grau de Probabilidade

Esta multiplicação direta representa o grau de probabilidade, sendo que o valor máximo obtido é 25, com a classificação dividida em cinco níveis. Essa classificação foi realizada por Brasiliano com base em suas experiências de consultoria e práticas encontradas na literatura. Para transformar esta classificação subjetiva em uma classificação objetiva, basta multiplicar pelo fator 4. Por que fator 4? Porque se faz uma equivalência entre o número máximo obtido na multiplicação direta entre os dois fatores (fator de riscos x fator de exposição) que é 25 e a porcentagem da probabilidade máxima que é 100%. Desta forma temos a tabela a seguir (Tabela 6):

Escala	Nível de Probabilidade	
1 - 5	Baixa	4% a 20%
5,01 - 10	Média	20,01 a 40%
10,1 - 15	Alta	40,01 a 60%
15,01 - 20	Muito Alta	60,01 a 80%
20,01 - 25	Elevada	80,01 a 100%

Tabela 6: Classificação do Nível de Probabilidade

Relevância do Impacto

Para mensurar o impacto, não devemos levar em consideração somente a questão financeira. Com o objetivo de o gestor obter uma visão holística do impacto há a necessidade de projetar

todos os custos que os perigos causam. Ao calcular o impacto, é possível identificar o quanto cada tipo de risco pode prejudicar a competitividade empresarial. Dentro deste foco calculamos o impacto no negócio da organização através de quatro fatores de impacto – FI. Cada fator de impacto terá um peso diferenciado, tendo em vista seu grau de importância para a organização. A Figura 10 mostra os fatores de impacto e seus respectivos pesos sugeridos por Brasiliano para a Gestão de Riscos em segurança patrimonial seguidos pelas respectivas escalas (Tabela 7 a Tabela 10):

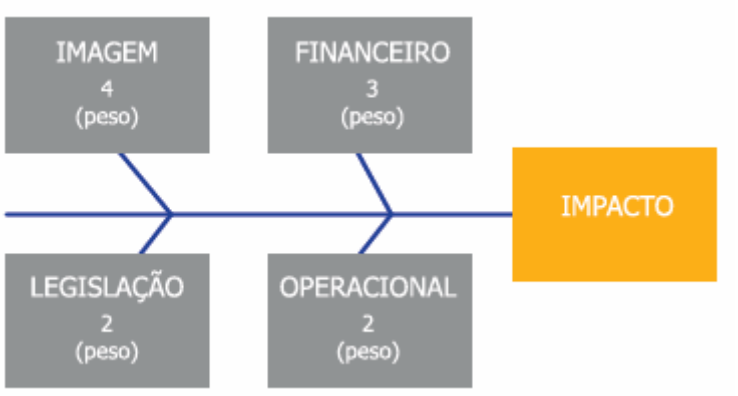

Figura 10: Fatores de Impacto

IMAGEM:

Escala	Pontuação
De Caráter Internacional	05
De Caráter Nacional	04
Regional	03
Local	02
De Caráter Individual	01

Tabela 7: Escala do Fator Impacto "Imagem"

FINANCEIRO:

Escala	Pontuação
Massivo	05
Severo	04
Moderado	03
Leve	02
Insignificante	01

Tabela 8: Escala do Fator Impacto "Financeiro"

LEGISLAÇÃO:

Escala	Pontuação
Perturbações Muito Graves	05
Graves	04
Limitadas	03
Leves	02
Muito Leves	01

Tabela 9: Escala do Fator Impacto "Legislação"

OPERACIONAL:

Escala	Pontuação
Perturbações Muito Graves	05
Graves	04
Limitadas	03
Leves	02
Muito Leves	01

Tabela 10: Escala do Fator Impacto "Operacional"

Determinação do Nível de Impacto

O Nível de Impacto é o resultado da soma dos resultados de cada fator de impacto (multiplicação do peso versus a nota), dividido pela soma dos pesos, conforme demonstrado abaixo (Equação 4):

$$\text{Nível de Impacto} = \frac{\text{Imagem} + \text{Financeiro} + \text{Operacional} + \text{Legislação}}{11 (\text{soma dos pesos } 4+3+2+2)}$$

Equação 4: Cálculo do Nível de Impacto

O nível de impacto possui a seguinte classificação (Tabela 11):

Grau de Impacto	Nível de Impacto
4,51 – 5,00	Catastrófico
3,51 – 4,50	Severo
2,51 – 3,50	Moderado
1,51 – 2,50	Leve
1,00 – 1,50	Insignificante

Tabela 11: Escala de Classificação do Nível de Impacto

2.2.2.3.3. Avaliação dos Riscos – Nível de Risco

Comparar os níveis de riscos em relação ao critério pré-estabelecido. A relevância dos riscos possui como parâmetro a Matriz de Riscos. O resultado da matriz de riscos é o grau de criticidade, ou seja, qual é a priorização com que a empresa deve tratar cada risco, frente ao seu apetite ao risco. A matriz é dividida em quadrantes, e, para cada quadrante, há uma estratégia de tratamento e priorização. Cabe ressaltar que é nessa fase também que estabelece o Grau de Riscos dos Processos estudados e ou das Unidades / Sites Empresariais.

Com o objetivo de visualizar e, ao mesmo tempo, implementar uma forma de tratamento de cada risco, o resultado da avaliação dos riscos será apresentado em um mapa de riscos (Matriz de Vulnerabilidade), permitindo o acompanhamento da mitigação ou elevação dos riscos.

A matriz de Vulnerabilidade (Figura 11) demonstra os pontos de cruzamento (horizontal e vertical) da probabilidade de ocorrência e do impacto. Desta forma, pela divisão da matriz em quatro níveis de criticidade podemos avaliar o nível de vulnerabilidade e sua influência nos objetivos da Unidade de Negócio da empresa. Quanto maior for à probabilidade e o impacto de um risco, maior será o nível do risco. Os riscos plotados em cada nível terão um tratamento específico, a saber:

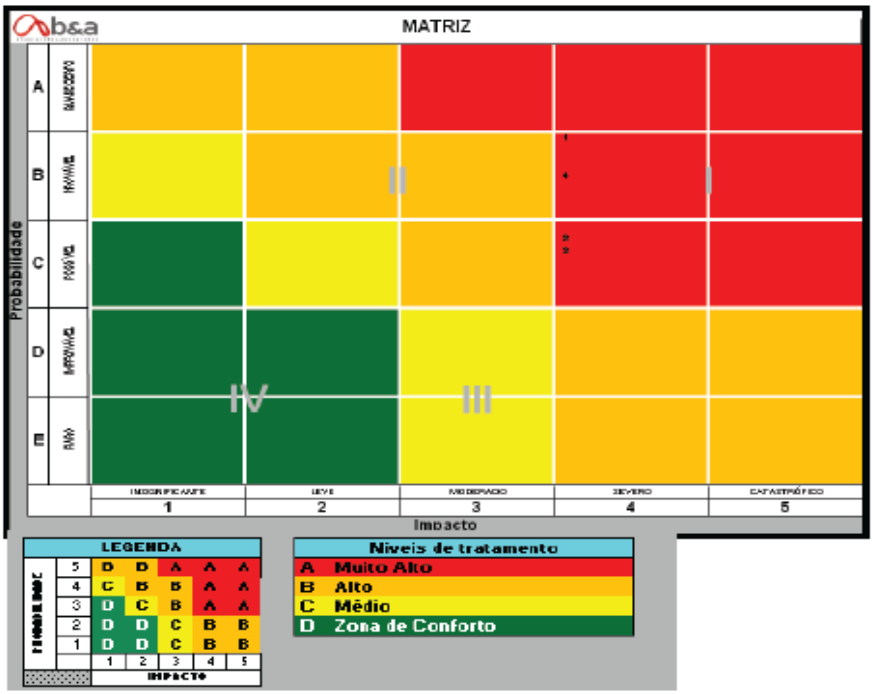

Figura 11: Matriz de Vulnerabilidade

Os riscos terão os seguintes tratamentos, de acordo com o quadrante em que estiver localizado:

Quadrante I (Vermelho): Os riscos existentes no quadrante I são aqueles que têm alta probabilidade de ocorrência e poderão resultar em impacto extremamente severo,

caso ocorram. Exigem a implementação imediata das estratégias de proteção e prevenção, ou seja, ação imediata;

Quadrante II (Laranja): No quadrante II, localizam-se ameaças que poderão ser muito danosas à empresa, podendo possuir muito baixa probabilidade e alto impacto como baixo impacto e alta probabilidade. Estas ameaças devem possuir respostas rápidas, que para isso devem estar planejadas e testadas em um plano de contingência, emergência, continuidade de negócios, além de ações preventivas. A diferença do quadrante I é que as ações podem ser implementadas com mais planejamento e tempo. São eventos que devem ser constantemente monitorados;

Quadrante III (Amarelo): No quadrante III, estão os riscos com alta probabilidade de ocorrência, mas que causam consequências gerenciáveis à empresa. Os riscos classificados neste quadrante devem ser monitorados de forma rotineira e sistemática, podendo também possuir planos de emergência;

Quadrante IV (Verde): Os riscos classificados no quadrante IV possuem baixa probabilidade e pequeno impacto, representando pequenos problemas e prejuízos. Estes riscos somente devem ser gerenciados e administrados, pois estão na zona de conforto.

2.2.2.4. Resposta aos Riscos – Plano de Ação

Depois de identificados, avaliados e mensurados, deve-se definir qual o tratamento que será dado aos riscos. Na prática, a eliminação total dos riscos é impossível. Nesse contexto, a Matriz de Riscos e a Classificação do Nível de Riscos apoiam a priorização e visa direcionar os esforços relativos a novos projetos e planos de ação elaborados, a fim de minimizar os eventos que possam afetar adversamente e maximizar aqueles que possam trazer benefícios para a organização. As várias alternativas para tratamento dos riscos são descritas abaixo, iniciando-se pelo dilema básico: evitar ou aceitar o risco.

Evitar o Risco: decisão de não se envolver ou agir de forma a se retirar de uma situação de risco. Exemplo: a organização decide não iniciar o projeto.

Aceitar o Risco: neste caso, apresentam-se quatro alternativas: reter, reduzir, transferir/compartilhar ou explorar o risco.

- **Reter**: manter o risco no nível atual de impacto e probabilidade. Exemplo: a diretoria da empresa decide nada investir em melhorias da área de informática, assumindo que as perdas e erros atualmente sabidos e esperados de informações internas para o processo de decisão e de gestão são (riscos) toleráveis.

  Reduzir: ações são tomadas para minimizar a probabilidade e/ou o impacto do risco. Exemplo: uma organização financeira identificou e avaliou o risco de seus sistemas permanecerem inoperantes por um período superior a três horas e concluiu que não aceitaria o impacto dessa ocorrência. A organização investiu no aprimoramento de sistemas de autodetecção de falhas e de backup para reduzir a probabilidade de indisponibilidade do sistema.

- **Transferir e/ou Compartilhar**: atividades que visam reduzir o impacto e/ou a probabilidade de ocorrência do risco através da transferência ou, em alguns casos, do compartilhamento de uma parte do risco. Exemplo: a organização identificou e avaliou os riscos de falhas naturais com danos elétricos em seus Centros de Processamento de dados (Data Centers). Após analisar a melhor estratégia a ser adotada no que tange às despesas possíveis, constitui-se um seguro destes equipamentos junto ao mercado, transferindo este risco operacional categorizado como de alto impacto e baixa frequência, inerente ao processo de operação e manutenção.

  Devem ser transferidos por meio de seguro os riscos tidos como catastróficos (riscos de baixa frequência e alta severidade), os riscos de alta freqüência que provoquem cumulativamente perdas relevantes e todos aqueles cujo custo de transferência seja inferior ao custo de retenção. A transferência do risco não necessariamente elimina todas as potenciais perdas e, por isto, é necessário dispor de um adequado plano de contingência.

- **Explorar**: aumentar o grau de exposição ao risco na medida em que isto possibilita vantagens competitivas. Exemplo: uma empresa produtora de petróleo

usa as informações sobre o mercado futuro para especular no mercado de derivativos, aumentando sua exposição ao preço da commodity.

O Plano de Ação é o tratamento dos riscos, ou seja, qual será a resposta que a empresa terá que operacionalizar. Aceitar, reter, reduzir, transferir, explorar e ou evitar? Desenvolver e implementar um plano específico de gerenciamento o qual inclui consideração de provimento de fundos. O Plano de Ação é o conjunto de medidas organizacionais, sistemas técnicos de prevenção e monitoração, recursos humanos que gerenciarão os riscos. O Plano de Ação é elaborado com base nos Fatores de Riscos visando mitigar e diminuir as probabilidades dos riscos.

O Plano de Ação deverá ser elaborado utilizando-se a técnica das perguntas: 5W e 2 H. As perguntas detalhadas são (Figura 12):

WHAT	WHO	WHEN	WHERE	WHY	HOW	HOW MUCH
O QUE?	QUEM?	QUANDO?	ONDE?	POR QUE?	COMO?	QUANTO CUSTA?

Figura 12: Plano de Ação - Técnica 5W-2H

WHAT = O QUE FAZER?

Nesta pergunta respondemos quais são as variáveis que iremos tratar, quais sistemas integrados iremos implantar. Exemplo: treinaremos nossa equipe; implantaremos um novo sistema de acesso; e assim por diante. O importante é estar lincado com a Matriz de Vulnerabilidade e SWOT – FOFA.

WHO = QUEM FAZER?

Nesta pergunta respondemos quem é o responsável, podendo ser uma pessoa, grupo de pessoas e ou um departamento. Exemplo: Recursos Humanos, Segurança; João da Silva. Esta pergunta é muito importante, pois sem designar responsáveis, o plano não terá chance de ser implementado.

WHEN = QUANDO?

Nesta pergunta respondemos o horizonte temporal que deveremos implantar cada variável e ou sistema. Exemplo: até 31 de agosto de 2008. O ideal é que coloque-se uma data limite, evitando horizontes temporais sem limite de data, como exemplo implantar o sistema de acesso num prazo de seis meses. Este tipo de horizonte é considerado vago. Todas as variáveis devem ter um horizonte temporal específico.

WHERE = ONDE?

Nesta pergunta respondemos quais são os departamentos e locais da empresa que os sistemas / ações serão implantados. Exemplo: Portaria Principal; Acesso da Diretoria. O importante é deixar claras as áreas específicas, com o objetivo do Plano de Ação não se tornar genérico.

WHY = POR QUE?

Nesta pergunta respondemos quais são os perigos que estamos mitigando, tendo em vista a implantação das variáveis. A pergunta pode suprir mais de um perigo, fazendo desta forma a otimização da ação. Exemplo: fuga de informação, instabilidade de requisitos.

HOW = COMO?

Nesta pergunta respondemos de que forma poderemos implantar o sistema. Pode ser em fases ou de uma única vez.

HOW MUCH = QUANTO CUSTA?

Esta pergunta, para os gestores, é a mais importante. Dará a projeção de investimento por sistema e variável a ser implantado. É recomendável que também nesta pergunta tenhamos a opção de investimento, se será a vista, a prazo ou se a empresa vai optar em realizar um aluguel. O importante é estar relacionado com a Matriz de Vulnerabilidade SWOT – FOFA.

2.2.2.5. Monitoração e Análise Crítica

Esta fase diz respeito ao monitoramento e revisão do desempenho das ações e do sistema de gerenciamento de risco e ao procedimento a mudanças que possam afetá-lo.

O monitoramento e a análise crítica devem ser planejados como parte do processo de Gestão de Riscos e deve envolver a checagem ou vigilância regulares. Podem ser periódicos ou acontecer em resposta a um fato específico.

De forma clara e objetiva o monitoramento envolve dois processos: o primeiro é a verificação se o Plano de Ação proposto está sendo executado. Também devem ser acompanhados os resultados das ações e medidas propostas. Devem ser acompanhadas para saber se seus objetivos foram atingidos e se não foram quais as dificuldades encontradas e as ações corretivas. Este é um processo de monitoração.

O segundo processo de monitoração diz respeito à evolução das condições de riscos identificados e estudados. Neste caso deve-se montar um processo de acompanhamento se as condições listadas no diagrama de causa e efeito sofrem mudanças e ou alterações do ambiente.

Resumo da Seção

Esta seção apresentou sucintamente os objetivos, estrutura e processos da Norma ISO 3100 de Gestão de Riscos. Vimos que o Método Brasiliano fornece um processo, alinhado com a ISO 31000, para a identificação dos perigos, avaliação dos seus Fatores de Riscos, análise e avaliação dos riscos. O método foi descrito através de seus processos, ferramentas e atividades. Foi dada ênfase no processo de Avaliação de Riscos por ter maior aplicabilidade para o escopo deste trabalho. Foram descritas as principais atividades do processo de Avaliação de Riscos: Identificação dos Riscos, Análise dos Riscos e a Avaliação dos Riscos Resposta aos Riscos (Plano de Ação).

2.3. Teoria Fundamentada em Dados

O desenvolvimento de uma pesquisa deve ser amparado por uma metodologia para que os resultados obtidos possuam credibilidade perante a comunidade científica. Métodos científicos clássicos normalmente constituem-se de formulação do problema, definição da hipótese, verificação da hipótese e conclusão.

A Teoria Fundamentada em Dados (TFD), uma metodologia aplicada em pesquisas qualitativas, não parte de nenhuma hipótese, buscando estruturar uma teoria que sustenta-se sobre uma análise sistemática dos dados coletados durante a pesquisa, os quais podem ser baseados em referências bibliográficas e/ou conclusões a respeito de questionários e/ou entrevistas respondidas por um grupo de pessoas ou, ainda, observações sobre o ambiente que constitui o foco do trabalho.

Esta seção apresenta uma breve comparação entre métodos qualitativos e quantitativos, suas características e diferenças e explana com mais detalhes a Teoria Fundamentada em Dados, metodologia escolhida para esta guiar este trabalho.

2.3.1. Métodos Qualitativos *versus* Métodos Quantitativos

Para alcançar resultados satisfatórios em investigações na área de gerenciamento de riscos, e em particular para levantar os fatores de riscos existentes, é fundamental aplicar estratégias adequadas de pesquisa. Uma estratégia de pesquisa na área de ciências sociais corresponde a uma forma diferente de coletar e analisar evidências produzidas em contextos específicos [Yin 2003]. Os métodos e técnicas de coleta e análise de dados podem ser agrupados em dois conjuntos, métodos quantitativos e métodos qualitativos [Creswell 2003].

Métodos quantitativos de pesquisa envolvem a coleta e análise de dados numéricos e são fortemente apoiados em estatística. Esses métodos podem ser aplicados eficientemente

em estudos experimentais para medir a correlação entre as variáveis de um estudo. Variáveis são coisas que podem ser medidas, controladas ou manipuladas em uma pesquisa. A aplicação dos métodos quantitativos para coleta e análise de dados em estudos experimentais de tipo *survey* ou casos de estudo buscam realizar pesquisas correlacionais entre as variáveis procurando não influenciar nenhuma delas, mas apenas medindo-as e procurando por relações (correlações) com outras variáveis [Montoni 2010].

Quanto mais complexo for o fenômeno, sob investigação, maior deverá ser o esforço para se chegar a uma quantificação adequada, em parte porque algumas atividades são inerentemente difíceis de serem mensuradas e quantificadas e, outra, porque, até o presente momento, descrições matemáticas excessivamente complicadas são extremamente intratáveis, do ponto de vista de solução, para que tenham algum valor prático.

Métodos qualitativos de pesquisa envolvem a coleta e análise de dados como palavras (por exemplo, questionários de entrevistas), imagens (por exemplo, vídeo), ou objetos (por exemplo, um artefato). Métodos de pesquisa qualitativos foram desenvolvidos principalmente por pesquisadores na área de educação e outros cientistas sociais para estudar a complexidade do comportamento humano, por exemplo, motivação, comunicação e entendimento humano [Seaman 1999].

No entanto, uma questão que afeta a qualidade das pesquisas com métodos qualitativos, está relacionada às dificuldades associadas à adoção desses métodos. Métodos qualitativos exigem maior esforço e são mais exaustivos do que métodos quantitativos [Seaman 1999]. Alguns autores apontam, também, que a experiência, o conhecimento do domínio e as habilidades dos investigadores afetam a qualidade do resultado da pesquisa com métodos qualitativos [Pandit 1996, Coleman e O'Connor 2008].

Alguns autores criticam o uso extensivo de métodos quantitativos em pesquisas na área de Engenharia de Software [Bertelsen 1997, Coleman e O'Connor 2008]. Esse questionamento é apoiado na premissa de que Engenharia de Software é um fenômeno sociocultural e não puramente técnico. Pode-se considerar, então, que métodos qualitativos são mais indicados quando o foco da pesquisa é o estudo do comportamento humano e do contexto sociocultural do fenômeno em questão [Myers 1997]. Isso não significa que métodos quantitativos são inadequados e não devem ser utilizados. Alguns

autores reconhecem a importância de adotar métodos quantitativos e qualitativos em conjunto nas pesquisas de estudos de comportamentos sociais [Strauss e Corbin 1998, Seaman 1999, Matavire e Brown 2008].

A aplicação de métodos qualitativos em pesquisas sociais tem como objetivo criar e avaliar teorias por meio da coleta e análise de dados visando explorar, descrever e explicar fenômenos do mundo real [Ragin 1994]. No entanto, teorias sociais não devem ser tratadas como verdades absolutas, pois a obtenção de uma visão realista de um fenômeno considera a interpretação dos indivíduos baseada em seus valores pessoais [Adolph et al. 2008]. Consequentemente, os resultados dos estudos de comportamentos sociais são dependentes de contexto e, portanto, não podem ser generalizados [Niazi et al. 2006, Coleman e O'Connor 2007].

Seamen apresenta vários métodos de pesquisa para coleta e análise de dados qualitativos, descrevendo como os mesmos podem ser utilizados em estudos experimentais em Engenharia de Software [Seaman 1999]. Desde então, é possível notar o crescente uso de métodos qualitativos em pesquisas sobre diferentes tópicos em Engenharia de Software. Alguns exemplos são: (i) Taipale e outros autores apresentam um estudo qualitativo com o objetivo de compreender a prática de teste de software [Taipale et al 2007]; Montoni discute os resultados de análises qualitativas com o objetivo de identificar fatores críticos de sucesso em iniciativas de melhoria de processo de software [Montoni 2010]; De Souza e outros autores detalham um estudo qualitativo sobre como desenvolvedores utilizam APIs (Application Programming Interface ou Interface de Programação de Aplicações), apresentando pontos importantes sobre desenvolvimento colaborativo [De Souza et al. 2004].

2.3.2. Métodos Qualitativos

Creswell aponta 5 tipos de métodos qualitativos: (i) pesquisa narrativa, (ii) pesquisa fenomenológica, (iii) pesquisa com Teoria Fundamentada em Dados (Grounded Theory), (iv) pesquisa etnográfica e (v) pesquisa baseada em estudo de caso [Creswell 1997]. Um tipo bastante adotado em estudos na área de Engenharia de Software é o método

Grounded Theory ou Teoria Fundamentada em Dados (TFD) [Adolph et al., 2008]. Em linhas gerais:

- Etnografia: Estuda um grupo cultural intacto - por tempo prolongado- processo flexível;
- Estudos de caso: Exploração aprofundada;
- Pesquisa fenomenológica: Identifica a "essência" das experiências humanas relativas a um fenômeno - Experiências de vida;
- Teoria embasada (Fundamentada em Dados): deduzir uma teoria geral e abstrata de um processo, ação ou interação com base nas visões dos participantes de estudo;
- Pesquisa narrativa: Estuda a vida da pessoa, combina visões da vida do participante com as visões do pesquisador em uma cronologia narrativa.

Decidiu-se utilizar a TFD, segundo a linha straussiana [Strauss e Corbin 1998], para guiar a condução da investigação, nesta dissertação, pois esse método estabelece um conjunto de procedimentos para condução de pesquisa qualitativa em áreas pouco exploradas, bem como é um método com efetividade comprovada para apoiar a coleta e análise de experiências de profissionais da área de software, visando à construção de teorias substantivas sobre o comportamento humano [Orlikowski, 1993; Coleman e O'Connor, 2007, Crabtree et al., 2009, Montoni 2010].

2.3.3. Métodos Quantitativos

A pesquisa quantitativa vem da tradição das ciências naturais, onde as variáveis observadas são poucas, objetivas e medidas em escalas numéricas. Filosoficamente, a pesquisa quantitativa baseia-se numa visão dita positivista onde:

- As variáveis a serem observadas são consideradas objetivas, isto é, diferentes observadores obterão os mesmos resultados em observações distintas;
- Não há desacordo do que é melhor e o que é pior para os valores dessas variáveis objetivas;

- Medições numéricas são consideradas mais ricas que descrições verbais, pois se compatibilizam à manipulação estatística.

As pesquisas quantitativas são mais adequadas para apurar opiniões e atitudes explícitas e conscientes dos entrevistados, pois utilizam instrumentos estruturados (questionários). Devem ser representativas de um determinado universo de modo que seus dados possam ser generalizados e projetados para aquele universo. Seu objetivo é mensurar e permitir o teste de hipóteses (visando à obtenção de respostas que atendam aos objetivos do levantamento), já que os resultados são mais concretos e, consequentemente, menos passíveis de erros de interpretação. Em muitos casos geram índices que podem ser comparados ao longo do tempo, permitindo traçar um histórico da informação.

A seguir a Tabela 12 apresenta um quadro comparativo entre os Métodos Quantitativos e Métodos Qualitativos sob os aspectos: foco, objeto de estudo, papel do pesquisador, objetivos da pesquisa, amostra para estudo, tratamento / análise dos dados, instrumentos de pesquisa, critério de confiabilidade, apresentação dos resultados e discussão dos resultados.

Tabela 12: Métodos Quantitativos versus Métodos Qualitativos: Quadro Comparativo

Característica	Quantitativa	Qualitativa
Foco	Busca explicação: o "por quê": preocupa-se com as causas	Busca compreensão: o "como": preocupa-se em compreender os fenômenos, se refere ao mundo dos símbolos / significados
Objeto de estudo	Fatos naturais descritos	Fenômenos humanos apreendidos (significados)
Papel do pesquisador	Distancia-se do fato pesquisado	Olha a luz da sua subjetividade Envolve-se no fenômeno de interesse
Objetivos da pesquisa	Teste de hipóteses Descrição e estabelecimento de correlações matemáticas (estatísticas) e causais entre	Compreensão; explanação Apreensão e interpretação da relação de significações de fenômenos para os indivíduos e a

	fatos	sociedade
Amostra / grupo para estudo	Randômica: representativa estatisticamente de uma população	Proposital, Intencional: sujeitos individualmente eleitos; tamanho pequeno
Tratamento / análise dos dados	Técnicas estatísticas, habitualmente feitas por especialistas	Análise de conteúdo: categorias por relevância teórica de repetição
Instrumentos de pesquisa	Experimentos e *surveys* Observação dirigida Questionários fechados Escalas Exames laboratoriais D ados randomizados em prontuários	Pesquisador como instrumento, com seus sentidos Observação Entrevistas Coleta intencional em prontuários Testes psicológicos eventuais Diário de campo Seminários (atas, sínteses) Oficinas (material)
Critério de confiabilidade	Fidedignidade atribuída ao rigor da reprodutibilidade dos resultados	Validade atribuída ao rigor da validade dos dados / achados
Apresentação dos resultados	Em linguagem matemática (tabelas, quadros), habitualmente em separado no relatório	Tópicos redigidos, com observações do campo e citações literais (falas), não separados da discussão
Discussão dos resultados e conclusões	Confirmação ou refutação das hipóteses previamente definidas. Generalização dos resultados e conclusões	Interpretação simultânea à apresentação de resultados, revisão de hipóteses, conceitos ou pressupostos

Tabela 12 – Continuação: Métodos Quantitativos versus Métodos Qualitativos: Quadro Comparativo

Por objetivarmos um estudo exploratório, sem hipóteses pré-estabelecidas, com o propósito de entender o ambiente em questão buscando os fatores de riscos que ocorrem na área de desenvolvimento de software e que os resultados sejam primordialmente específicos para a organização (não generalização), vemos que a opção mais adequada para a condução deste trabalho é através da metodologia qualitativa.

2.3.4. A Teoria Fundamentada em Dados

A Teoria Fundamentada em Dados (TFD) é um método de pesquisa qualitativo aplicável em áreas que não foram previamente estudadas ou onde é necessário aprofundar o entendimento sobre um determinado fenômeno [Strauss e Corbin 1998].

Nas próximas subseções, são discutidas as principais linhas de pesquisa e os conceitos da Teoria Fundamentada em Dados, destacando os aspectos relevantes do método, bem como os problemas comuns identificados nos relatos da literatura e algumas recomendações para garantir a adoção adequada do método em estudos qualitativos.

2.3.4.1. Linhas de Pesquisa

A Teoria Fundamentada em Dados (TFD) foi criada em 1967 pelos pesquisadores Glaser e Strauss como uma resposta à noção vigente na época de que o objetivo das ciências sociais era derivar explicações únicas ou teorias formais e abrangentes do comportamento social [Glaser e Strauss 1967]. Esses autores acreditavam que teorias sociais não devem ser verdades absolutas já que pessoas interpretam a realidade baseadas em seus valores pessoais e, portanto, esses valores não devem ser ignorados em estudos qualitativos [Adolph et al. 2008].

Em "*The Discovery of Grounded Theory: Strategies for Qualitative Research*", os autores apresentam a TFD como um conjunto de procedimentos para gerar, elaborar e validar teorias substantivas sobre fenômenos essencialmente sociais no contexto de um determinado grupo de pessoas ou situação [Glaser e Straus, 1967].

No entanto, os criadores da TFD divergiram sobre alguns pontos e o método dividiu-se em duas linhas. A linha defendida por Glaser enfatiza a característica de emergência do método e os processos indutivos desenvolvidos pelo Departamento de Sociologia da Universidade de Columbia nos anos 50 e 60 [Glaser 1992]. A outra linha, desenvolvida por Strauss e posteriormente consolidada em conjunto com Corbin, sistematiza o método de coleta e análise de dados [Straus 1987, Corbin 1998].

Não é relevante para os pesquisadores compreenderem os argumentos filosóficos por trás das diferenças entre as duas principais linhas da TFD, bastando para esses apenas definir, de forma clara, o método escolhido e garantir que os diferentes métodos não são misturados na condução de pesquisas qualitativas.

A característica prescritiva da linha defendida por Strauss é tida como uma das razões pelas quais essa linha tem sido mais amplamente adotada em estudos qualitativos na área de Engenharia de Software [Adolph et al. 2008]. Portanto, no contexto desta pesquisa, a linha de pesquisa adotada é a defendida por Strauss e Corbin.

2.3.4.2. Princípio da Emergência

O princípio de emergência da Teoria Fundamentada em Dados define que, tanto o produto final da pesquisa (a teoria fundamentada em dados), quanto a definição do processo de pesquisa, devem ser emergentes, ou seja, devem ser desenvolvidos ao longo do processo de pesquisa [Strauss e Corbin 1998, Matavire e Brown 2008].

Segundo o princípio de emergência, os pesquisadores não devem iniciar a investigação com conceitos pré-concebidos ou com algum framework teórico de guia. Na pesquisa baseada em TFD, os conceitos e a própria teoria devem emergir dos dados, ou seja, pesquisadores devem permitir que os "dados falem por si" [Strauss e Corbin 1998]. O princípio de emergência garante, então, que a teoria derivada do estudo representa de forma confiável tanto a visão das pessoas participantes do estudo, quanto o contexto da investigação [Duchsher e Morgan 2004].

De forma análoga, o princípio de emergência também deve ser aplicado na definição do processo de pesquisa. A utilização de um processo pré-definido e com uma visão dos

resultados que se pretende alcançar em cada etapa do estudo, inibe a natureza emergente da pesquisa [Strauss e Corbin 1998, Matavire e Brown 2008]. De fato, isso pode ser observado em alguns dos relatos de aplicação da TFD, como o de Coleman e O'Connor, nos quais a pesquisa é conduzida em fases constituindo um processo exploratório iterativo de coleta e análise de dados [Coleman e O'Connor 2007]. Os resultados produzidos em cada fase são utilizados, na fase seguinte, para aprofundar a investigação em tópicos de interesse ou mesmo para verificar a teoria em desenvolvimento.

2.3.4.3. Comparação Constante

A técnica principal da Teoria Fundamentada em Dados para descobrimento de teorias é a comparação constante. Essa técnica é utilizada para (i) determinar a exatidão dos dados, (ii) estabelecer os limites de generalização empírica, (iii) especificar um conceito, (iv) gerar a teoria e (v) verificar a teoria [Glasner e Strauss 1967, Matavire e Brown 2008]. A exatidão dos dados é determinada por meio da comparação de cada elemento de dado (ou incidente) com outro. Vale ressaltar que a imprecisão de alguns dados não deve ser tratada como um problema no processo de análise, porque o aspecto relevante é determinar a categoria conceitual ou propriedade conceitual associada ao dado analisado. O estabelecimento dos limites de generalização empírica é alcançado por meio da comparação de incidentes de dados com outros incidentes coletados em diferentes contextos, por exemplo, a comparação de dados coletados em entrevistas com membros de diferentes organizações pode servir para indicar que (i) o conceito associado aos dados é aplicável em ambas organizações ou (ii) os dados apontam para diferentes variações dimensionais de um mesmo conceito. A verificação da teoria é realizada por meio da comparação dos dados com outros casos que confirmem a existência das categorias e proposições da teoria [Glaser e Strauss 1967].

No entanto, o objetivo principal da comparação constante é a geração de uma teoria. Uma teoria é gerada pela quebra dos dados em incidentes que são comparados procurando identificar similaridades e diferenças. Neste processo, o pesquisador deve questionar qual o conceito ou propriedade de uma categoria que o dado representa [Glaser 1992, Matavire e Brown 2008]. O objetivo é atribuir um significado comum para

múltiplos incidentes de dados, formando uma categoria [Locke 2001]. À medida que conceitos emergem e são nomeados, estes são comparados com outros incidentes nos dados, levando à definição de uma propriedade de uma categoria. Portanto, a teoria é gerada por meio de uma iteração constante entre nomeação e comparação de incidentes de dados com outros incidentes, bem como entre incidentes de dados e conceitos na ótica de uma categoria [Glaser 1992, Locke 2001].

A comparação constante está alinhada ao princípio de emergência, pois permite a adequação das questões da pesquisa à medida que a análise é iniciada, possibilitando que sejam reveladas as questões e os problemas essenciais do fenômeno que está sendo estudado [Adolph et al. 2008]. Para tanto, pesquisadores não devem iniciar a pesquisa com ideias e noções pré-concebidas sobre o fenômeno. Apesar de ser impossível ignorar o conhecimento possuído, o pesquisador deve procurar que esse conhecimento não limite sua criatividade na nomeação e na identificação de conceitos e categorias [Locke 2001].

2.3.4.4. Amostragem Teórica

A validade e confiabilidade dos resultados de um estudo dependem da adequação da amostra dos dados utilizados na análise [Yin 2003]. No caso de um estudo conduzido com base na TFD, a população estudada é o conjunto de conceitos que constitui um fenômeno e não o conjunto de indivíduos envolvidos no fenômeno em si [Adolph et al. 2008]. Portanto, a estratégia de amostragem adotada deve possibilitar a descoberta de conceitos suficientes para desenvolver uma teoria substantiva conceitualmente densa. A amostragem teórica é aplicada na TFD como forma de apoiar a coleta, codificação e análise conjunta de dados, bem como apoiar a tomada de decisão sobre quais serão os próximos dados a serem coletados e como obtê-los [Glaser 1978].

A amostragem teórica na Teoria Fundamentada em Dados é direcionada pelas categorias e proposições emergentes, isto é, a decisão sobre as amostras de dados a serem coletadas é um processo contínuo que não pode ser determinado a priori [Adolph et al. 2008]. No entanto, é difícil determinar quando o pesquisador deve finalizar a investigação, pois não se conhece o tamanho real da população (conceitos do fenômeno), acarretando em um aumento inesperado do esforço e prazo da pesquisa. Esse problema é comum em estudos

qualitativos conduzidos com base na TFD. Uma possível consequência disso é o término prematuro da pesquisa devido, por exemplo, a restrições de tempo e custo da investigação. Neste caso, há chances da teoria estar incompleta, as categorias não terem sido saturadas, não haver densidade teórica adequada ou as variações comportamentais não serem cobertas de forma adequada pelas proposições da teoria [Adolph et al. 2008].

A coleta e análise de dados devem, então, ser realizadas de forma contínua até que todas as categorias (conceitos) estejam saturadas, ou seja, quando a coleta de mais dados não indica nenhuma nova categoria [Strauss e Corbin 1998].

Recomenda-se que os pesquisadores escolham amostras teóricas capazes de fornecer a máxima cobertura do fenômeno estudado por meio da seleção de casos ou indivíduos de acordo com o seu potencial para o desenvolvimento de novos conceitos ou para o refinamento de conceitos previamente identificados [Morse e Richards 2002].

2.3.4.5. Procedimentos de Codificação

Apesar de Strauss e Corbin reconhecerem que o conhecimento científico e as experiências pessoais do pesquisador são importantes para o desenvolvimento de teorias fundamentadas em dados, o uso de ideias preconcebidas no processo de investigação pode limitar os resultados da pesquisa [Bandeira e Cunha 2003].

Para minimizar os preconceitos do pesquisador no processo interpretativo, os autores definiram um conjunto de princípios e procedimentos de análise por meio da codificação dos dados coletados nos estudos qualitativos. A codificação pode ser interpretada como um processo analítico a partir do qual dados são quebrados, conceituados e integrados para formar uma teoria.

Os tipos de procedimentos de codificação são: codificação aberta, codificação axial e codificação seletiva. Apesar desses três tipos serem descritos de maneira sequencial na TFD, a aplicação é realizada de forma iterativa de acordo com as necessidades do estudo.

Codificação aberta é o processo analítico a partir do qual conceitos e categorias são identificados e suas propriedades e dimensões são descobertas nos dados. As atividades

chaves deste procedimento são nomeação de categorias, comparação de dados e escrita de anotações [Locke 2001, Matavire e Brown 2008].

Conceitos são os blocos construtores básicos de uma teoria e, portanto, o primeiro passo na descoberta de uma teoria é abrir os dados para revelar e nomear esses conceitos. Isso pode ser obtido por meio da técnica de comparação constante a partir da qual comparações quanto às similaridades e diferenças entre os dados incidentes são realizadas para derivar conceitos, nomeando-os em seguida. No caso dos nomes das categorias terem sido atribuídos diretamente dos dados, esses são referidos como códigos "in-vivo" [Strauss e Corbin 1998].

Codificação axial é definida como o processo de relacionamento entre as categorias e suas respectivas subcategorias. Este procedimento recebe esse nome, pois a codificação é realizada ao redor do eixo axial de uma categoria, no qual outras categorias podem ser relacionadas no nível de propriedades e dimensões. Uma subcategoria é subordinada a uma categoria principal ou fenômeno possibilitando responder questões do tipo quem, onde, quando, por que e como sobre uma categoria"[Strauss e Corbin 1998].

Para facilitar a codificação axial, deve ser utilizado um modelo de paradigma que defina como uma categoria se relaciona com suas subcategorias. Esse modelo ajuda a integrar a estrutura (o contexto condicional no qual um fenômeno ocorre) com o processo (sequencias de ações/interações pertencentes ao fenômeno) [Strauss e Corbin 1998].

O modelo de paradigma sugerido por Strauss e Corbin tem a seguinte estrutura: dado um determinado fenômeno (categoria principal), a realização de ações/interações resulta em determinadas consequências; condições causais são as categorias que exercem algum tipo de influência não apenas no fenômeno, mas também nas ações/interações dos atores, enquanto que condições intervenientes limitam o impacto causado pelas condições causais no fenômeno. No entanto, o pesquisador pode definir os próprios conectores entre os códigos, utilizando-os para examinar as relações entre as categorias que formam as proposições da teoria substantiva [Bandeira e Cunha 2006].

Codificação seletiva envolve a identificação de uma categoria central a partir da qual todas as demais categorias estão relacionadas. A categoria central deve representar a

essência do processo social que ocorre entre os envolvidos, podendo ser uma categoria existente ou uma nova categoria deve ser criada [Strauss e Corbin 1998].

Durante a codificação seletiva, todo o processo é refinado por meio da revisão do esquema conceitual, procurando validar internamente a teoria e estabelecer uma lógica plausível. Esse refino também deve envolver o preenchimento de categorias pouco desenvolvidas, além da remoção de categorias em excesso. A teoria final pode, então, ser representada na forma de um conjunto de proposições ou uma narração da discussão teórica [Strauss e Corbin 1998, Matavire e Brown 2008].

2.3.4.6. Aplicação da Teoria Fundamentada em Dados na Área de Software

Na área de software, métodos qualitativos têm sido mais utilizados para guiar investigações em Sistemas de Informação [Coleman e O'Connor 2007]. O objetivo da maioria desses estudos é apoiar a aplicação da Tecnologia de Informação para tratar questões gerenciais e de cunho organizacional [Hevner e March 2003]. O uso de métodos qualitativos em pesquisas na área de Engenharia de Software é bem menor se comparado ao seu uso em Sistemas de Informação [Glass et al. 2002]. Apesar disso, os resultados apresentados por esses estudos demonstram que métodos qualitativos podem trazer diversos benefícios para a pesquisa e prática de Engenharia de Software e áreas correlatas, como melhoria de processos de software.

Orlikowski realizou um dos trabalhos pioneiros na utilização da Teoria Fundamentada em Dados para conduzir investigações na área de software [Orlikowski 1993]. O autor utilizou o método para desenvolver um framework teórico capaz de explicar as questões organizacionais relacionadas à adoção e ao uso de ferramentas CASE (Computer-Aided Software Engineering) em duas organizações de software.

Nasirin e outros autores [Nasirin et al. 2003] descrevem a aplicação da TFD para investigar fatores críticos de sucesso na implementação de sistemas de informação geográfica (GIS, do inglês Geographical Information Systems) [Nasirin et al. 2003]. Apesar desse estudo não focar em desenvolvimento de software, os resultados

apresentados demonstram os benefícios e a viabilidade da aplicação da Teoria Fundamentada em Dados em estudos qualitativos, conduzidos para compreender os fatores críticos de sucesso e as estratégias de implementação de mudanças organizacionais.

Existem, também, alguns estudos que relatam a aplicação da TFD para investigar questões relacionadas à melhoria de processo de software. Coleman e O'Connor investigaram a prática de melhoria de processos de software na indústria Irlandesa, realizando conclusões sobre as causas da resistência à implementação de modelos de referência para melhoria de processo [Coleman e O'Connor 2007].

Matavire e Brown fazem um levantamento da produção acadêmica da área de Informática que empregam a Teoria Fundamentada em Dados em seus trabalhos publicados em periódicos como *Information Technology & People*, *Journal of Management Information Systems, Information Research* e *MIS Quarterly* [Matavire e Brown 2008].

Crabtree apresentou a aplicação do método em um estudo exploratório para investigar como as pessoas descrevem processos de software usando linguagem natural [Crabtree 2009].

Conte, Cabral e Travassos apresentaram o resultado da aplicação da Teoria Fundamentada em Dados na análise qualitativa de um estudo de observação em Engenharia de Software, visando compreender o processo de aplicação de uma técnica de inspeção de usabilidade em aplicações Web [Conte et al. 2009].

Montoni relata a aplicação da Teoria Fundamentada em Dados para investigar os fatores críticos de sucesso em iniciativas de melhoria de processos de software [Montoni 2010].

Algumas características comuns nos trabalhos destacados acima estão relacionadas à metodologia de pesquisa adotada. A maioria dos estudos foi conduzida em duas fases, sendo que o propósito da primeira fase foi explorar questões de pesquisa gerais e abertas, enquanto a condução da fase seguinte foi direcionada com base nos resultados obtidos na fase anterior da investigação.

Como relação às fontes de dados, a maioria dos estudos, destacados acima, realizou entrevistas semiestruturadas e revisões da literatura. O propósito das revisões da

literatura foi identificar conceitos relevantes da área que pudessem orientar a investigação, por exemplo, por meio da definição dos tópicos a serem discutidos nas entrevistas com os especialistas no problema ou fenômeno de interesse.

Resumo da Seção

Esta Seção expôs as principais características, objetivos, critérios e diferenças encontradas nas Pesquisas Qualitativas e Quantitativas. A Teoria Fundamentada em dados, metodologia qualitativa escolhida para guiar este trabalho, foi apresentada através de uma breve descrição de seu surgimento, seus princípios, linhas de pesquisas, estrutura e procedimentos. Foram apresentados alguns exemplos de aplicação desta metodologia na Área da Engenharia de Software.

2.4. Resumo do Capítulo

Este capítulo apresentou o referencial teórico utilizado para a condução deste trabalho. Na Seção 2.1 foram apresentados conceitos relativos ao Gerenciamento de Riscos. O Método Brasiliano de Análise de Riscos foi descrito em detalhes na Seção 2.2. E na Seção 2.3 a Teoria Fundamentada em dados foi apresentada dos seus princípios, estrutura e procedimentos.

3. Metodologia de Pesquisa

Conforme contextualizado e justificado nos capítulos anteriores, o objetivo deste trabalho é mapear Fatores de Riscos existentes no ambiente de desenvolvimento de software de uma Organização do Setor Público e elaborar um Plano de Respostas para esses fatores.

A metodologia de pesquisa adotada para alcançar esse objetivo foi estruturada na Teoria Fundamentada em Dados aplicada em conjunto com o processo de Avaliação de Riscos (Seção 2.2.2.3 do Capítulo 2) do Método Brasiliano. Podemos dividir a pesquisa – estruturada e apresentada na Tabela 2 (Capítulo 1) em seus principais componentes - em duas grandes fases que serão apresentadas em suas estratégias e ações a seguir.

3.1. Estratégias e Ações

A primeira fase objetivou o entendimento inicial das condições e processos do Centro de Desenvolvimento de software do Departamento de Tecnologia da Informação da Organização do Setor Público em estudo (Tabela 2 – 1ª fase).

Nesta fase também foi realizado um estudo na literatura sobre as principais metodologias de pesquisa além de abordagens e processos para avaliação e análise de riscos. Conforme apresentado e justificado, a metodologia de pesquisa escolhida foi a Teoria Fundamentada em Dados e para avaliação de riscos o Método Brasiliano.

Após a contextualização do escopo do estudo, a escolha da metodologia de pesquisa e o método para avaliação de riscos, o próximo passo foi estruturar a investigação de modo a combinar os insumos necessários à execução do Método Brasiliano através da aplicação da Teoria Fundamentada em Dados.

O primeiro insumo necessário é a listagem e identificação dos Perigos e Fatores de Riscos, primeira etapa do processo de Avaliação de Riscos (Seção 2.2.2.3, Capítulo 2). Brasiliano descreve como técnica para essa etapa o *Brainstorming* [Brasiliano 2009]. Em nossa pesquisa, utilizamos a Teoria Fundamentada em Dados cujo objetivo foi

desenvolver uma teoria capaz de representar de forma confiável a visão e perspectivas das pessoas envolvidas na investigação (Tabela 2 – 2ª fase). Procurou-se, então, aplicar a metodologia de pesquisa de forma a evitar que ideias preconcebidas sobre o fenômeno estudado, exercessem algum tipo de influência no resultado da investigação. Para tanto, foram definidas as seguintes questões de pesquisa de forma aberta, sem focar em um problema específico:

• QP1 – Quais são os Perigos ou Fatores capazes de influenciar o insucesso em projetos de software e qual a frequência de ocorrência desses perigos / fatores?

• QP2 – Como os desenvolvedores / gerentes tratam os perigos ou fatores capazes de influenciar o insucesso dos projetos de software?

A primeira questão visou também identificar a frequência com que os Perigos ou Fatores de Riscos costumam manifestar-se no ambiente em questão. Essa resposta servirá como insumo para a elaboração de uma escala de frequência que será utilizada para o cálculo da exposição no processo de Análise de Riscos (Seção 2.2.2.3.2, Capítulo 2 / Tabela 5).

A segunda questão buscou investigar possíveis sugestões de respostas aos Perigos e Fatores de Riscos levantados, visando auxiliar na elaboração do Plano de Respostas aos Riscos (Seção 2.2.2.4).

Na 2ª fase, após a codificação dos dados realizada na 1ª fase (Tabela 2 – 3ª fase), obteremos uma listagem categorizada dos Perigos e / ou Fatores de Riscos com suas respectivas definições. Por ser uma metodologia investigativa, o resultado da codificação realizada na 1ª fase será composto por Perigos, Fatores de Riscos e possíveis sugestões de tratamento para esses problemas. Com este resultado, daremos início ao processo de Avaliação de Riscos do Método Brasiliano (Tabela 2 – 4ª a 7ª fase).

Veremos em detalhes nos tópicos a seguir cada passo que será realizado nas duas fases da pesquisa.

3.2. 1ª Fase - Descrição dos Passos

Essa fase é fundamentada nos princípios e conceitos da Teoria Fundamentada em Dados (TFD), segundo a linha de pesquisa defendida por [Strauss e Corbin 1998]. No entanto, os autores do método não estabelecem uma descrição rígida de como o método deve ser aplicado, permitindo adaptações para contextos específicos de pesquisa. Por exemplo, os autores Goulding e Schots, apresentam abordagens para operacionalizar a aplicação da TFD com diferentes propósitos de investigação qualitativa [Goulding 2002, Schots 2010]. A Figura 13 apresenta a estrutura geral sugerida por Montoni e adotada como guia para esta fase [Montoni 2010].

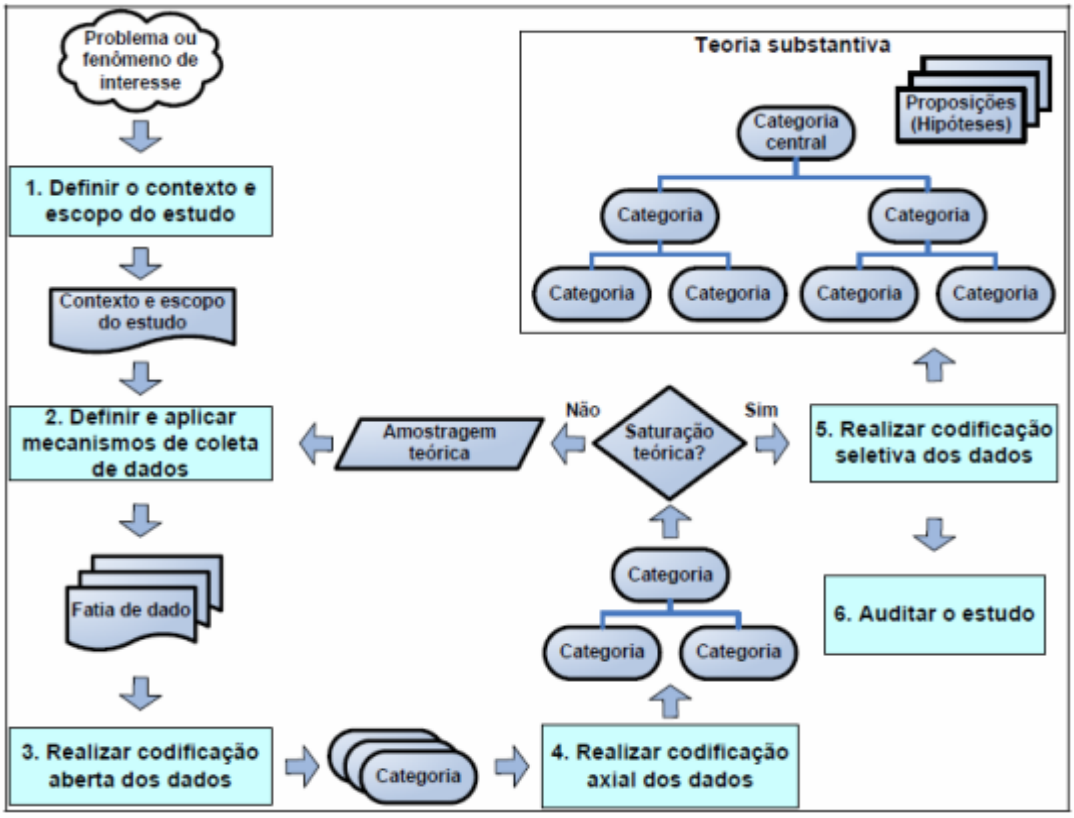

Figura 13: 1ª Fase: Estrutura Geral - Teoria Fundamentada em Dados

Conforme a Figura 13, o ponto inicial da metodologia é a definição de um problema ou fenômeno de interesse. A capacidade de generalização de uma teoria substantiva é dependente do quanto o contexto e escopo representam o problema ou fenômeno estudado [Strauss e Corbin 1998].

Em seguida, é necessário definir e aplicar mecanismos de coleta de dados. Segundo os criadores da TFD, tanto dados subjetivos, quanto objetivos, são passíveis de serem coletados desde que sejam relevantes para o problema ou fenômeno de interesse [Glaser 1992].

Após a coleta dos dados, deve ser executado um conjunto de passos para aplicar os três tipos de procedimentos de análise propostos no método (codificação aberta, axial e seletiva). Apesar da aplicação desses procedimentos ser proposta de maneira sequencial, na prática, há uma forte interação entre a coleta e a análise de dados. Essa interação é representada, na Figura 13 na forma de um ciclo contínuo de amostragens teóricas, definidas ao longo do processo de pesquisa, segundo o princípio de emergência do Método. A execução do processo interativo da investigação é encerrada quando a coleta e análise de novos dados não agregam novo conhecimento à teoria, alcançando-se a saturação teórica.

O passo final da metodologia é a realização de uma auditoria do estudo para avaliar, tanto o processo de investigação, quanto a teoria desenvolvida. Veremos mais detalhes de cada etapa dessa estrutura a seguir.

3.2.1. 1º Passo – Definir o contexto e escopo do estudo

Vimos pela estrutura apresentada na Figura 13, que inicialmente, devem ser definidos o contexto e o escopo para estudo de um problema ou fenômeno de interesse. A definição do contexto e escopo deve possibilitar que múltiplas fontes de dados sejam utilizadas, visando aumentar a capacidade de generalização, bem como facilitar a captura do conhecimento, visão e perspectiva das pessoas envolvidas no problema ou fenômeno estudado [Bandeira e Cunha 2003, Carvalho et al. 2003].

Alguns autores, como Goulding, recomendam que o contexto e escopo do estudo sejam definidos em áreas substantivas nas quais não existe uma literatura extensa de base

empírica com credibilidade assegurada [Goulding 1999]. Caso contrário, o investigador deve tomar cuidado para que a literatura não prejudique ou influencie suas percepções. No entanto, isso não significa que a literatura deve ser totalmente ignorada [Suddaby 2006]. Estudos empíricos, relacionados ao fenômeno ou problema estudado, podem ser úteis para ajudar a definir os conceitos da teoria emergente ou para testar ideias no processo de investigação [Nasirin et al. 2003].

Segundo o princípio de emergência da Teoria Fundamentada em Dados, as questões de pesquisa devem ser definidas, nas etapas iniciais da investigação, de forma aberta e geral, e não devem ser formalizadas a priori na forma de hipóteses específicas [Bandeira e Cunha 2003]. À medida que a investigação é conduzida, questões de pesquisa mais fechadas devem ser definidas para focar as etapas da pesquisa em tópicos de interesse ou para verificar a teoria.

Nesse ponto, estaremos adquirindo as informações necessárias para o estabelecimento do contexto organizacional que irá auxiliar o processo de Avaliação de Riscos.

3.2.2. 2º Passo – Definir e aplicar mecanismos de coleta de dados

Este passo envolve a definição e aplicação dos mecanismos de coleta de dados. Os mecanismos apontados como sendo os mais comuns e aplicáveis em estudos qualitativos são: (i) estudos experimentais do tipo *survey*, (ii) revisão da literatura e (iii) entrevistas estruturadas e/ou semiestruturadas [Strauss e Corbin 1998, Carvalho et al. 2003]. A aplicação desses mecanismos permite criar um repositório de dados (ou fatias de dados) que servirá de base para investigação de um determinado fenômeno. No entanto, é importante fazer algumas considerações práticas quanto à aplicação desses mecanismos.

Os *surveys* são pesquisas de opinião de caráter quantitativo. A coleta de dados é feita por meio de questionários estruturados. Exige rígidos procedimentos internos de controle a fim de garantir a eficiência no levantamento de campo e a fidedignidade dos resultados. O tamanho e a representatividade da amostra devem assegurar resultados

estatisticamente confiáveis. O rigor metodológico desse mecanismo deve ser considerado durante a estruturação da metodologia de pesquisa. [Montoni 2010]

Um aspecto negativo da revisão da literatura é a tendência dos pesquisadores, autores e editores de revistas em publicar apenas resultados positivos. Resultados contraditórios de pesquisas, geralmente, não são publicados [Biolchini et al. 2005]. Para tratar essas questões, abordagens mais rigorosas podem ser aplicadas na revisão da literatura. A revisão sistemática da literatura é uma dessas abordagens.

O termo Revisão Sistemática da Literatura (RSL) é usado para se referir a uma metodologia de pesquisa, desenvolvida para coletar e avaliar evidências disponíveis relacionadas a um tema específico [Kitchenham 2004]. A aplicação da RSL requer que seja seguido um conjunto bem definido e sequencial de passos metodológicos segundo um protocolo de pesquisa desenvolvido apropriadamente. Este protocolo é construído considerando um tema específico que representa o elemento central da investigação. Os passos metodológicos, as estratégias definidas para coletar as evidências e o foco das questões de pesquisa são definidas explicitamente de tal forma que outros pesquisadores são capazes de reproduzir o mesmo protocolo de pesquisa e também de julgar a adequação dos padrões adotados no estudo [Biolchini et al. 2005].

Um cuidado que se deve ter ao empregar a revisão da literatura no processo de investigação do problema ou fenômeno de interesse, é evitar forçar os dados coletados em uma teoria pré-concebida ao invés de facilitar o surgimento do problema e da teoria diretamente dos dados. Esse problema é chamado de *Forcing* e conflita com o princípio de emergência da TFD [Glaser 1992, Adolph et al. 2008].

Em relação às entrevistas, na aplicação da Teoria Fundamentada em Dados, os pesquisadores devem evitar a condução de entrevistas muito estruturadas por meio de um conjunto fechado de questões pré-definidas [Goulding 1999]. No entanto, isso traz certa dificuldade ao método. Entrevistas totalmente desestruturadas podem causar confusão, falta de coerência e resultados sem significado para a teoria emergente. O pesquisador deve, então, procurar um balanceamento adequado que permita ao entrevistado expandir suas respostas com base nas suas experiências, sem que o

pesquisador tenha que perguntar precisamente o que deve ser dito pelos entrevistados [Goulding 1999]. Assim, para a condução este trabalho foi escolhido como mecanismo de coleta a realização de entrevistas semiestruturadas.

3.2.3. 3º Passo – Realizar codificação aberta dos dados

Após a coleta dos dados, a análise pode ser iniciada. A relação dinâmica entre a análise e a coleta de dados é uma característica significativa da Teoria Fundamentada em Dados [Carvalho et al. 2003]. A análise de dados orientada pelo método é realizada por meio da codificação dos dados. Conforme descrito anteriormente, e também observados na Figura 13, são previstos três tipos de codificação: codificação aberta, axial e seletiva. A codificação aberta ou rotulação (labeling) envolve a quebra, análise, comparação, conceituação e categorização dos dados. A codificação axial examina as relações entre as categorias e subcategorias dos dados. Na codificação seletiva, todo o processo é refinado, procurando identificar uma categoria central da teoria, com a qual todas as outras estão relacionadas.

Os objetivos deste passo são os seguintes: (i) realizar a codificação aberta dos dados coletados e (ii) agrupar os códigos em categorias e subcategorias. A codificação, neste passo, compreende o processo de gerar rótulos (ou códigos) para descrever conceitos e aspectos relevantes de certas passagens de textos nas fontes dos dados [Seaman 1999].

A codificação é iniciada com a leitura de uma seção de dados por vez. Em seguida, deve ser feita uma nova leitura, atribuindo rótulos a trechos de passagens no texto. Após a rotulação dos dados, o texto é novamente lido, procurando por consistência nos códigos utilizados e garantindo que nenhuma informação relevante foi perdida. A análise dos dados é realizada por meio da busca por similaridades e diversidades entre os dados, coletando um número de indicadores que apontem para múltiplos aspectos qualitativos de um conceito potencialmente significativo [Strauss e Corbin 1998]. Na execução deste passo, os códigos gerados devem ser classificados como: códigos de primeira ordem, diretamente associados às citações (chamados códigos “in vivo”); e códigos abstratos ou teóricos, associados a outros códigos, sem necessariamente estarem ligados a alguma citação [Strauss e Corbin 1998, Bandeira e Cunha 2003].

Podem ser utilizados códigos pré-definidos, que podem ser identificados a partir dos objetivos do estudo, bem como das questões de pesquisa e variáveis de interesse pré-estabelecidas [Seaman 1999]. No entanto, códigos também podem ser criados após o início do estudo, caso os objetivos sejam abertos e sem foco. Em ambos os casos, novos códigos podem ser adicionados à medida que o estudo é executado, como também podem ser excluídos, modificados, integrados e subdivididos.

Os rótulos de trechos de textos criados devem ser agrupados por meio da análise de padrões. A criação dessas categorias de agregação dos códigos visa reduzir a quantidade de itens de análise. Os grupos (ou categorias) identificados devem ser analisados, procurando entender o seu significado e fornecer explicações sobre o problema ou fenômeno de estudo [Carvalho et al. 2003].

Neste passo, é importante considerar também que haja poucos códigos abstratos relacionados a muitos códigos "in-vivo", evitando o excesso de complexidade e facilitando o entendimento, aprendizado e aplicação do conhecimento teórico construído [Biffl et al. 2006]

3.2.4. 4º Passo – Realizar codificação axial dos dados

O objetivo deste passo é agregar conhecimento sobre a teoria. Na Teoria Fundamentada em Dados o processo investigativo de construção de uma teoria é guiado por um modelo chamado de Modelo de Paradigma [Strauss e Corbin 1998]. Segundo esse modelo, conhecimento é agregado a uma teoria por meio da análise e construção das relações entre as categorias e subcategorias que devem ser testadas novamente nos dados. A TFD denomina esse tipo de análise de codificação axial.

Conforme descrito anteriormente, as relações entre as categorias e subcategorias da teoria são definidas na forma de proposições (ou hipóteses), representando condições causais, fenômeno, contexto, condições intervenientes, estratégias de ação/interação e consequências. A execução deste passo visa construir uma teoria por meio da busca de

conexões entre as instâncias desses elementos, representados na forma de proposições ou hipóteses fundamentadas nos dados coletados.

Segundo Bandeira e Cunha, o pesquisador pode definir os próprios conectores entre os códigos, utilizando-os para examinar as relações entre as categorias que formam as proposições da teoria substantiva [Bandeira e Cunha 2006].

3.2.5. 5º Passo – Realizar codificação seletiva dos dados

O objetivo deste passo é refinar o conhecimento sobre a teoria construída por meio do que a TFD denomina de codificação seletiva. Neste passo, todo o processo de construção da teoria é refinado pela identificação de uma categoria central capaz de integrar todas as outras categorias e expressar a essência do processo social que ocorre entre os envolvidos [Bandeira e Cunha 2003]. A execução deste passo envolve, também, a revisão das categorias mal formuladas, bem como a resolução de falhas na lógica da teoria.

A construção de uma teoria fundamentada em dados deve ser realizada de forma iterativa à medida que os dados são coletados. Em cada iteração do processo de pesquisa, mais conhecimento sobre a teoria é agregado e refinado até que a coleta e análise de mais dados não proporcionem ganhos significativos à teoria, ou seja, novas categorias e relações não sejam mais encontradas no processo de codificação, alcançando a saturação teórica [Strauss e Corbin 1998].

No entanto, é comum, nos relatos da literatura, a não execução do procedimento de codificação seletiva e / ou não seleção de uma categoria central [Adolph et al. 2008]. Outro problema é a falta de descrição do processo social de como os envolvidos no fenômeno estudado resolvem suas questões principais [Adolph et al. 2008]. Suddaby aponta que o uso mecânico do método para identificação de categorias revela uma “ênfase excessiva e neurótica em codificação” [Suddaby 2006]. Uma teoria fundamentada em dados não é um inventário de conceitos anotados com comentários dos participantes, mas sim um conjunto integrado de categorias que explica o processo pelo qual os participantes da pesquisa resolvem suas questões principais [Adolph et al. 2008].

Caso não tenha sido alcançada a saturação teórica ao final de uma iteração do processo de pesquisa, uma nova amostragem teórica de dados deve ser realizada, seguida de mais uma iteração de análise de dados. A estratégia de amostragem adotada deve possibilitar a descoberta de conceitos suficientes para desenvolver uma teoria substantiva conceitualmente densa. O investigador deve, então, utilizar as categorias e proposições emergentes para direcionar a coleta de dados de forma a maximizar a cobertura da exploração conceitual do problema ou fenômeno de estudo [Adolph et al. 2008].

3.2.6. 6º Passo – Auditar o estudo

O objetivo deste passo é avaliar o estudo para garantir validade dos resultados encontrados. Para tanto, é fundamental que sejam registradas anotações ao longo de todo o processo de pesquisa, desde a etapa de coleta dos dados até a codificação e análise dos elementos construtores da teoria.

A avaliação do resultado da investigação deve ser guiada por um conjunto de critérios definidos para garantir objetividade. Um conjunto de critérios sugerido por Strauss e Corbin [Strauss e Corbin 1998] para avaliar teorias substantivas fundamentadas em dados é o seguinte [Strauss e Corbin 1998]: (i) adequação (fit) – a teoria deve ser adequada à área de pesquisa substantiva e deve corresponder aos dados, (ii) entendimento (understanding) – a teoria tem sentido para profissionais da área estudada, (iii) generalidade (generality) – a teoria deve ser abstrata o suficiente para servir de guia geral sem perder sua relevância, e (iv) controle (control) – a teoria atua como um guia geral e possibilita a uma pessoa entender completamente a situação. Existem alguns relatos que evidenciam a aplicação desses critérios para avaliar teorias desenvolvidas com base na Teoria Fundamentada em Dados [Coleman e O'Connor 2007, Crabtree et al. 2009].

3.3. 2ª Fase - Descrição dos Passos

Após a codificação dos dados realizada na 1ª fase obteremos uma listagem categorizada dos Perigos e/ou Fatores de Riscos com suas respectivas definições. Por ser uma metodologia investigativa, o resultado da codificação realizada na fase anterior será composto por Perigos, Fatores de Riscos e possíveis sugestões de tratamento para esses problemas. Com este resultado, daremos início ao processo de Avaliação de Riscos do Método Brasiliano.

Como o objetivo desta pesquisa não abrange a implantação de um Processo de Gestão de Riscos na organização, os processos Comunicação e Consulta (Seção 2.2.2.1, Capítulo 2) e Contexto Estratégico (Seção 2.2.2.2, Capítulo 2), descritos pelo Método Brasiliano, não serão abordados.

Para a execução do processo de Avaliação de Riscos realizaremos os seguintes passos:

3.3.1. 1º Passo – Identificar os Fatores de Riscos

Como visto na Seção 2.2.2.3.1 é necessário o desmembramento de cada perigo em fatores ou causas. A codificação dos dados obtidas na 1ª fase identificou tanto Perigos quanto os seus Fatores de Riscos relacionados. Após analisar os Perigos e Fatores de Riscos levantados, iremos identificar as principais macrocausas que serão usadas para adaptar o Diagrama de Ishikawa (Figura 6, Seção 2.2.2.3.1). Aplicaremos então o diagrama para organizar os Fatores de Riscos e Perigos encontrados.

3.3.2. 2º Passo – Identificar a Motricidade dos Fatores de Riscos

Após a identificação dos Fatores de Riscos iremos avaliar quais são os fatores comuns a todos os perigos e quais são os mais motrizes. Conforme descrito pelo Método Brasiliano (Seção 2.2.2.3.1) as ferramentas utilizadas serão a Matriz SWOT e a Matriz de Impacto Cruzado.

Vimos que para a aplicação da Matriz SWOT será necessário pontuar subjetivamente, com base na experiência da equipe que está avaliando, cada Fator de Risco através do parâmetro "Importância". Essa avaliação será realizada em uma 2ª entrevista, após termos listados e categorizados todos os Fatores de Riscos. (1º Passo)

Teremos a mesma necessidade para a utilização da Matriz de Impacto Cruzado, onde o critério "Grau de Interdependência" entre os Fatores de Riscos é subjetivamente informado pela equipe responsável pela análise. Essa avaliação será realizada conjuntamente com a Matriz SWOT na 2ª entrevista.

3.3.3. 3º Passo – Cálculo do Grau de Probabilidade

O próximo passo é a realização da Análise de Riscos através do cálculo do Grau de Probabilidade (Seção 2.2.2.3.2). A fórmula para esse cálculo está alicerçada em dois critérios: Critério dos Fatores de Riscos (FR) e o Critério da Exposição (E).

3.3.3.1. Critério do Fator de Risco (FR)

Conforme visto na descrição do Método Brasiliano o FR é uma nota subjetiva, com base no diagrama de causa e efeito. Os subcritérios - estudados na fase da identificação da origem de cada perigo (1º Passo) - serão pontuados (seguindo a escala proposta na Tabela 4, Seção 2.2.2.3.2) para medir o grau de influência para a concretização do perigo.

Como exposto anteriormente, para efeito deste trabalho, o Diagrama de Ishikawa e por consequência os subcritérios que serão utilizados neste cálculo serão adaptados para se adequar ao contexto da área de desenvolvimento de software.

3.3.3.2. Critério da Exposição (E)

O critério da Exposição possui uma escala de valoração que mede a frequência que os perigos costumam manifestar-se na organização. Essa escala (Tabela 5, Seção 2.2.2.3.2.)

será ajustada com as informações sobre ocorrência dos perigos levantados na 1ª Fase da pesquisa juntamente com a experiência profissional da autora da dissertação.

3.3.4. 4º Passo – Definição da Relevância do Impacto

Vimos que para mensurar o impacto, não devemos levar em consideração apenas a questão financeira. O Método Brasiliano sugere estudar a relevância do impacto considerando quatro fatores: imagem, financeiro, operacional e legal. (Figura 10, Seção 2.2.2.3.2). Faremos uma entrevista direcionada com a gerência do Departamento de Tecnologia da Informação da organização para avaliar a importância e relevância desses fatores.

3.3.5. 5º Passo – Determinação do Nível de Impacto

Após definirmos os fatores de impacto iremos calcular o Nível de Impacto conforme fórmula apresentada na Equação 4: O resultado é a soma dos resultados de cada fator de impacto (multiplicação do peso x nota), divido pela soma dos pesos.

3.3.6. 6º Passo – Construção da Matriz de Riscos

O resultado da avaliação dos riscos realizado nos passos anteriores será apresentado em um mapa de riscos (Matriz de Riscos) que permitirá a priorização e o acompanhamento da dinâmica dos riscos. Será utilizada a Matriz (Figura 11) apresentada na Seção 2.2.2.3.3.

3.3.7. 7º Passo – Elaboração do Plano de Ação

Uma vez identificados, avaliados e mensurados, o próximo passo é definir qual o tratamento será dado aos riscos. Com a Matriz de Riscos saberemos a priorização a ser dada em relação aos riscos e através das Matrizes SWOT e de Impactos Cruzados teremos a informação sobre quais fatores de riscos devem ser atacados com criticidade. Com base nesses dados iremos estabelecer a estratégia de tratamento adequada e

direcionar os esforços. Para elaborar o plano de ação utilizaremos a técnica 5W e 2H descrita na Seção 2.2.2.4.

3.4. Resumo do Capítulo

Este capítulo apresentou as estratégias e ações adotadas para estruturar a metodologia de pesquisa para alcançar os objetivos deste trabalho. Essa pesquisa foi divida em duas fases estruturadas na Teoria Fundamentada em Dados aplicada em conjunto com o processo de Avaliação de Riscos do Método Brasiliano. A primeira fase objetivou essencialmente a listagem e identificação dos Perigos e Fatores de Riscos através dos princípios da Teoria Fundamentada em Dados. O resultado dessa fase será entrada para a 2ª fase da pesquisa que usará os processos e atividades descritos pelo Método Brasiliano para avaliar os Riscos obtendo no final do processo o Plano de Ação.

4. Mapeamento dos Fatores de Riscos e Plano de Respostas

Este capítulo apresenta os resultados obtidos através da execução da metodologia de pesquisa estruturada e apresentada no Capítulo 3. A metodologia foi dividida em duas fases: a primeira estruturada nos princípios e diretrizes da Teoria Fundamentada em Dados objetiva a identificação dos principais perigos e fatores de riscos existentes no ambiente de desenvolvimento de software da Organização do Setor Público em estudo. Uma visão do contexto da organização também é apresentada. A segunda fase utiliza os processos e ferramentas descritos no Método Brasiliano para realizar a Análise e Avaliação de Riscos que resultará na elaboração do Plano de Ação dos Riscos.

4.1. Resultados da 1ª Fase – Teoria Fundamentada em Dados

Na primeira fase, a investigação teve caráter exploratório, motivada pela experiência pessoal da autora da dissertação na área de riscos e no ambiente de desenvolvimento de software. Uma investigação inicial sobre o contexto, organização e o processo de desenvolvimento de software foi realizado através de entrevistas informais com diferentes membros e da leitura da documentação disponível do Centro de Desenvolvimento de Sistemas da Organização em estudo. Em seguida foi aplicada a Teoria Fundamentada em Dados com o objetivo de elaborar a lista de perigos e fatores de riscos existentes no ambiente de desenvolvimento de software.

4.1.1. Contexto Organizacional

Descreveremos em linhas gerais o contexto e estrutura organizacional do Departamento de Tecnologia da Informação (DTI) que coordena o Centro de Desenvolvimento de Sistemas, unidade responsável pelo desenvolvimento de software da organização que é o foco deste trabalho.

4.1.1.1. Departamento de Tecnologia da Informação

Ao DTI cabe a prestação de serviços às unidades da organização nas áreas de consolidação e de manutenção da gestão única das atividades de tecnologia da informação. Seu organograma é apresentado na Figura 14:

Figura 14: Organizacional do Departamento de Tecnologia da Informação

A diretoria do DTI encontra-se no Gabinete responsável pela coordenação de todos os centros. O escopo deste trabalho será essencialmente direcionado ao Centro de Desenvolvimento de Sistemas (CDS), responsável pelo desenvolvimento de softwares, porém veremos que diversos perigos ou fatores de riscos são oriundos ou possuem participação dos demais centros. Descreveremos sucintamente as atribuições de cada centro a seguir:

Centro de Projetos e Processos: Centro responsável pela gestão de portfólios, definição de processos e metodologias para gestão de projetos. Atua também como ponto focal para solicitações de demandas dos demais departamentos e coordenadorias para o DTI.

Centro de Arquitetura e Inovação: Centro responsável por estruturar e manter uma arquitetura única de tecnologia da informação para o DTI. Também atua em pesquisa e desenvolvimento com foco em inovação.

Centro da Segurança da Informação: Centraliza e gerencia todas as atividades relativas à segurança da informação. Defini políticas e procedimentos para toda organização.

Centro de Operações e Infraestrutura: Centro responsável pelo suporte e operação de toda infraestrutura de tecnologia da informação da organização.

Centro de Administração e Orçamento: Responsável por todas as questões administrativas relacionadas aos contratos, aquisições, licitações e orçamentação relativas à tecnologia da informação.

Centro de Desenvolvimento de Sistemas: Centro responsável pelo desenvolvimento e manutenção dos sistemas de informação da organização. Esse centro também é responsável pela gestão das fábricas de softwares terceirizadas que prestam serviços à organização. Veremos em detalhes sua estrutura e processos.

4.1.1.2. Centro de Desenvolvimento de Sistemas

O Centro de Desenvolvimento de Sistemas é a unidade responsável por centralizar e coordenar todo o desenvolvimento de software da organização, gerir os recursos e entregas das fábricas de softwares contratadas que prestam serviços à organização além de prestar manutenção em todos os sistemas de informações legados que estão hospedados no DTI.

O CDS conta com cerca de 80 membros entre servidores da própria organização e prestadores de serviços contratados ou cedidos de outros órgãos que trabalham exclusivamente e sob a coordenação do DTI. Atualmente o CDS está dividido em duas subunidades: Núcleo de Serviços Tributários e Núcleo de Serviços Financeiros e Administrativo.

O Núcleo de Serviços Tributários atende exclusivamente à Coordenadoria responsável pelos assuntos tributários e seus departamentos. Existe um departamento dedicado a realizar o intermédio entre os departamentos solicitantes desta Coordenadoria e a DTI, esse departamento é responsável pelo levantamento e documentação dos requisitos dos

sistemas, execução dos testes, homologação e controle da qualidade dos sistemas desenvolvidos pelo CDS. Todo o contato com o usuário é realizado por este departamento que se comunica com o CDS através dos casos de usos. Este departamento possui uma metodologia própria para levantamento e elaboração dos casos de usos, limitando a atuação do CDS apenas com o desenvolvimento do software.

O Núcleo de Serviços Financeiros e Administrativo é responsável pelo atendimento às demais coordenadorias da organização. Por não existir formalmente nenhum departamento que desempenhem funções semelhantes ao departamento da Coordenadoria de assuntos tributários, todo o levantamento, documentação e gestão dos requisitos são realizados diretamente pelo CDS. Não existe uma equipe dedicada à realização destes trabalhos, a alocação de recursos é feita dinamicamente de acordo com a demanda.

A tecnologia de desenvolvimento predominante é a plataforma Microsoft .NET. Não existe uma metodologia de desenvolvimento única para o CDS. Cada uma das subunidades utiliza informalmente práticas e procedimentos distintos. Não existe uma equipe responsável por testes ou pelo controle de qualidade de software. Essa função é realizada pelos próprios desenvolvedores dentro do escopo de cada projeto.

A gestão das fábricas de softwares terceirizadas é realizada pelo CDS que acompanha os termos do contrato de serviços, a execução dos projetos, realiza inspeção de código e arquitetura, realiza testes de integração e solicita/aprova requisições de mudanças solicitadas pelos usuários.

4.1.2. Mecanismo de coleta de dados

Vimos no Capítulo 3 – Seção 3.1 – que as questões de pesquisa foram definidas de forma aberta de forma a evitar que ideias preconcebidas, exercessem algum tipo de influência no resultado da investigação:

• QP1 – Quais são os Perigos ou Fatores capazes de influenciar o insucesso em projetos de software e qual a frequência de ocorrência desses perigos / fatores?

• QP2 – Como os desenvolvedores / gerentes tratam os perigos ou fatores capazes de influenciar o insucesso dos projetos de software?

Morse e Richards recomendam que os pesquisadores escolham amostras teóricas capazes de fornecer a máxima cobertura do fenômeno estudado por meio da seleção de casos ou indivíduos de acordo com o seu potencial para o desenvolvimento de novos conceitos ou para o refinamento de conceitos previamente identificados [Morse e Richards 2002]. Assim para a seleção dos entrevistados procurou-se obter uma amostra abrangente de todos os envolvidos no processo de desenvolvimento de software. Essa amostragem foi composta por: desenvolvedores (6), líderes técnicos (3) e analistas de requisitos (3), totalizando 12 entrevistados. As entrevistas duraram, em média, 1h. Os questionários, preenchidos nas entrevistas, continham, no total, mais de 40 páginas de informações.

4.1.3. Codificação dos dados

Concluídas as entrevistas, deu-se início à análise dos dados por meio da execução dos procedimentos de codificação aberta e axial da Teoria Fundamentada em Dados.

Segundo Suddaby e Nasirin, estudos da literatura, relacionados ao fenômeno ou problema estudado, podem ser úteis para ajudar a definir os conceitos da teoria emergente ou para testar ideias no processo de investigação [Nasirin et al. 2003, Suddaby 2006]. No entanto, novos códigos podem ser adicionados à medida que o estudo é executado assim como podem ser excluídos, modificados, integrados e subdivididos. Assim, inicialmente foram adotados os conceitos definidos por Brasiliano para serem utilizados como códigos pré-definidos: Perigo, Fator de Risco e Plano de Ação. Essa decisão objetivou que o mapeamento e estruturação dos dados fossem realizados na estrutura trabalhada pelo Método Brasiliano.

Decidiu-se iniciar a codificação pelo questionário de um líder técnico, pois se considerou que a alta experiência do líder, em comparação aos demais entrevistados, permitiria uma

maior exploração das questões da pesquisa. A codificação foi acompanhada por um líder técnico buscando diminuir o fator de subjetividade existente neste procedimento.

O questionário foi inicialmente analisado pela aplicação do procedimento de codificação aberta. Cada passagem de texto (citações) do questionário foi analisada linha a linha procurando identificar similaridades e diferenças entre os dados. A partir dessa análise, foi possível classificar os dados de acordo com sua evidência sobre a existência de riscos existentes no processo de desenvolvimento de software. Essas categorias, códigos *in vivo*, foram denominadas de "Achado de Risco". No Anexo I temos a lista com todas as categorias encontradas. A tabela 13 mostra alguns dessas categorias identificadas no primeiro questionário.

Tabela 13: Exemplos de categorias de "Achado de Risco" identificadas na codificação axial

Achado de Risco
[A01] Os requisitos não são formalizados
[A04] Existe uma alta rotatividade de membros da equipe
[A07] Falta de documentação dos sistemas
[A08] Falta de compartilhamento de informações entre equipes

Também foram identificadas categorias do tipo "Plano de Ação" decorrente das respostas fornecidas pela questão de pesquisa QP2. Exemplos dessa categoria são listados na Tabela 14. A listagem completa se encontra no Anexo I.

Tabela 14: Exemplos de categorias de "Plano de Ação" identificadas na codificação axial

Plano de Ação
[PA01] Realizar reuniões para validar requisitos
[PA03] Planejar e agendar a implantação dos sistemas
[PA04] Utilização de métricas para estimar esforço

Esse conjunto inicial de códigos pré-definidos e i*n vivo* foi revisado para confirmar sua adequação, e após essa revisão inicial, foi iniciada a codificação aberta dos outros onze questionários, com a análise de seus dados e associação de códigos às citações do texto.

Os procedimentos da codificação aberta estimulam a constante criação de novos códigos e a fusão com os códigos existentes quando novos dados de evidência e interpretação emergem. Em nossa análise não foi necessário criar mais códigos durante a codificação dos demais questionários.

Após a finalização da codificação aberta foram contabilizadas 71 categorias de “Achado de Risco” e 12 categorias de “Plano de Ação”. Os demais tipos “Perigo” e “Fator de Risco” não foram utilizados neste ponto e isso já era esperado para este passo da codificação, por se tratarem de códigos referentes às categorias mais abstratas que são identificadas durante a codificação axial.

Em seguida, foi executado o procedimento de codificação axial que visa estabelecer categorias mais abstratas dos códigos de achados de risco. A codificação axial ocorreu em três iterações. Na prática, os passos da codificação aberta e axial se sobrepõem e se unem, devido à interatividade do processo.

Na primeira iteração, os códigos de achados de risco foram agrupados nas categorias “Fator de Risco”, essa agrupação se deu através da percepção de “evidência”. Os fatores de riscos são evidenciados pela da existência de um ou mais achado de risco.

A segunda iteração envolveu a análise dos achados de risco e dos fatores de riscos buscando a identificação de perigos categorizados no código pré-definido “Perigo”, essa iteração também envolveu a agregação das categorias de fatores de risco nas categorias de perigo, partindo do princípio que um perigo é uma possível consequência de um conjunto de fatores de risco.

Não foi necessária a realização da codificação seletiva em busca de uma categoria central. O objetivo de identificar os perigos e fatores de riscos foi alcançado já nas iterações da codificação axial. Essa situação, no entanto, é comum, conforme relatos da literatura [Adolph et al. 2008].

A Tabela 15 apresenta exemplos de categorias e tipos de categorias identificados pela aplicação dos procedimentos de codificação aberta e axial nos dados coletados.

Tabela 15: Passos da codificação *versus* Tipo de categorias identificadas

Passo da Análise	Tipo de Categoria	Categoria
1. Codificação Aberta	Achado de Risco	[A01] Os requisitos não são formalizados
	Plano de Ação	[PA05] Institucionalizar equipe de testes
2. Codificação Axial (1ª iteração)	Fator de Risco	[FR17] Ausência de processo e equipe de Testes
3. Codificação Axial (2ª iteração)	Perigo	[P12] Requisitos mal entendidos e/ou definidos

Foi observado que os códigos pré-definidos estabelecidos antes do início da codificação e o código *in vivo* criado na codificação do primeiro questionário foram adequados e que todos os dados e citações dos demais questionários analisados se encaixavam em um desses códigos e os mesmos representavam fidedignamente a relação entre eles.

Os códigos e categorias identificados passaram por sucessivas revisões, sendo que, ao final da presente versão da análise, foram identificadas 71 categorias de Achado de Risco, 17 categorias de Perigo, 32 categorias de Fatores de Riscos e 12 categorias de Plano de Ação. A relação de todas as categorias é apresentada no Anexo I.

Para facilitar o entendimento, foram desenvolvidos cinco esquemas gráficos no processo de análise dos dados para estabelecer os relacionamentos entre as categorias identificadas. Foram escolhidas as seguintes categorias de perigos: “Fuga da Informação” “Estimativas de tempo e prazo irreais”, “Requisitos mal entendidos e/ou definidos”, “Indisponibilidade de sistemas durante a implantação” e “Perda da motivação da equipe”. Essas categorias foram escolhidas por terem as menores quantidades de relacionamento de modo que a diagramação não ficasse visualmente complexa. Seus esquemas gráficos são apresentados pelas Figuras 15, 16, 17, 18 e 19 respectivamente e as descrições das categorias de achados de riscos abreviadas podem ser consultadas nas tabelas do Anexo I.

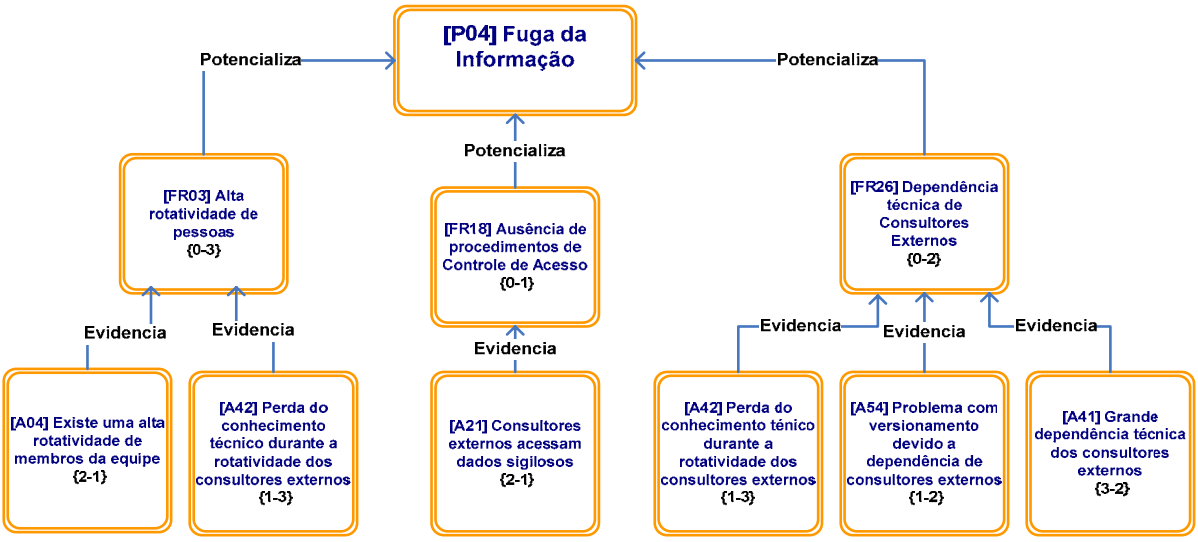

Figura 15: Esquema gráfico com as associações relacionadas ao Perigo [P04] Fuga da Informação.

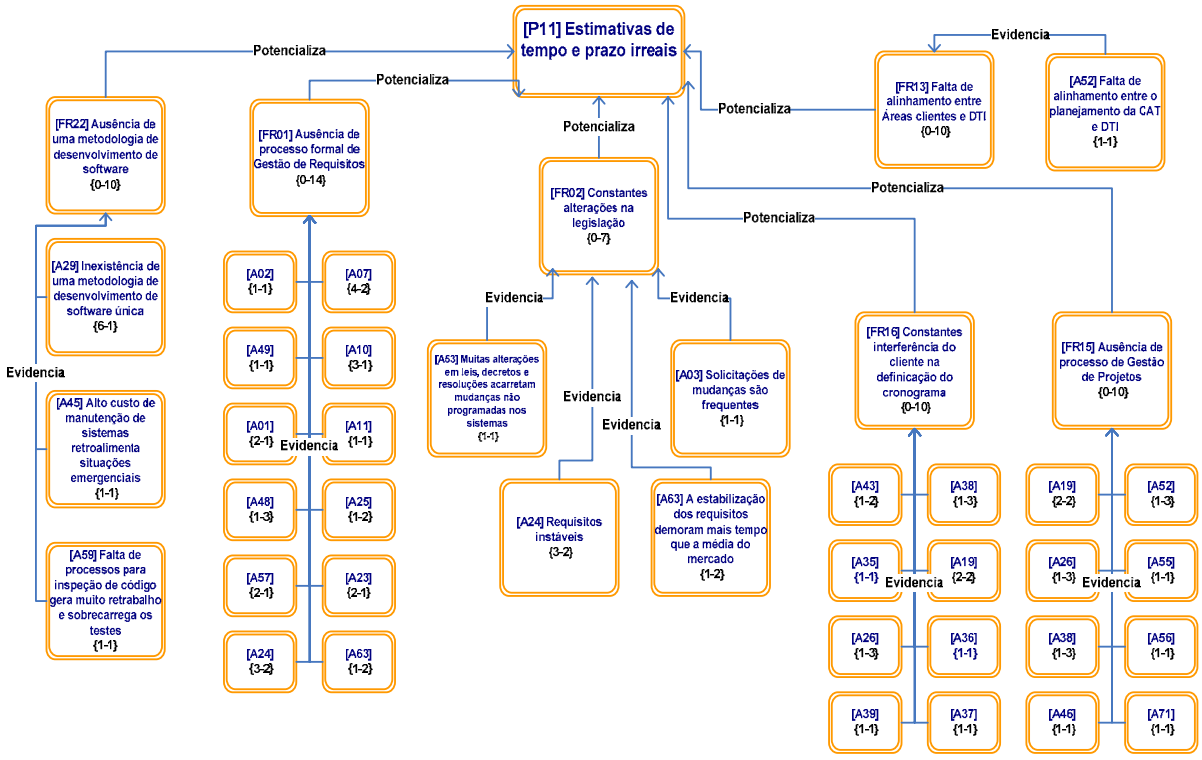

Figura 16: Esquema gráfico com as associações relacionadas ao Perigo [P11] Estimativas de tempo e prazo irreais.

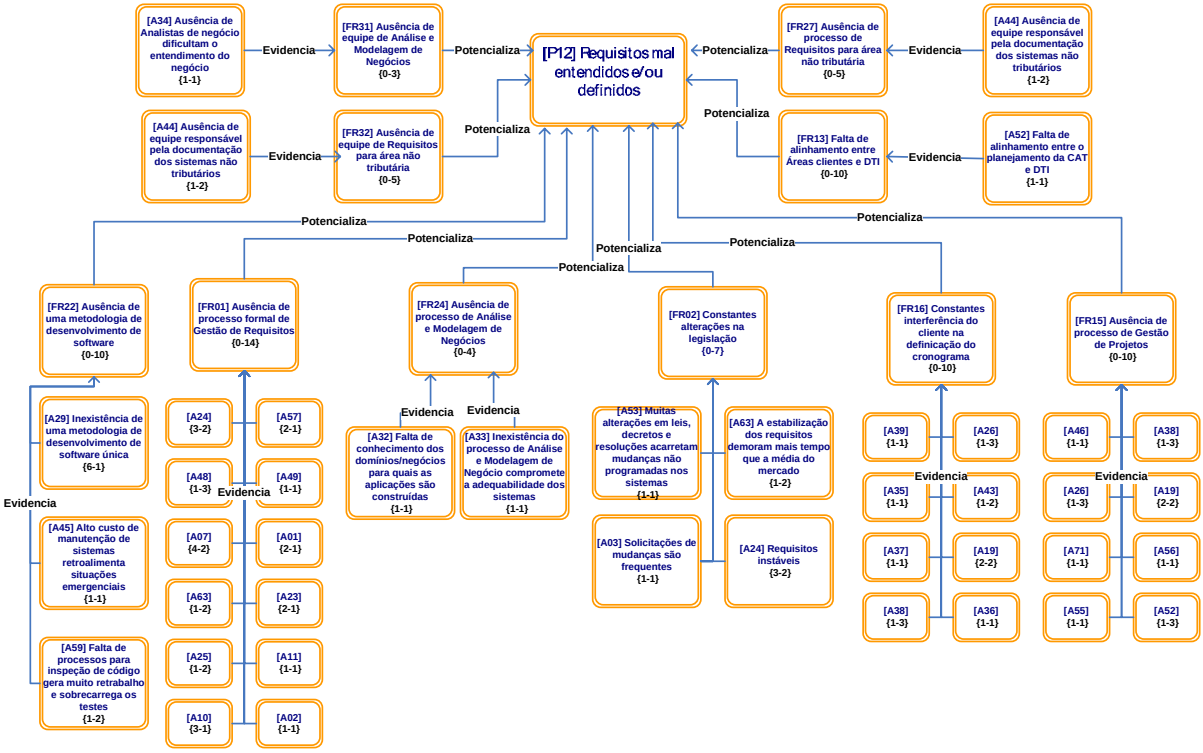

Figura 17: Esquema gráfico com as associações relacionadas ao Perigo [P12] Requisitos mal entendidos e/ou definidos.

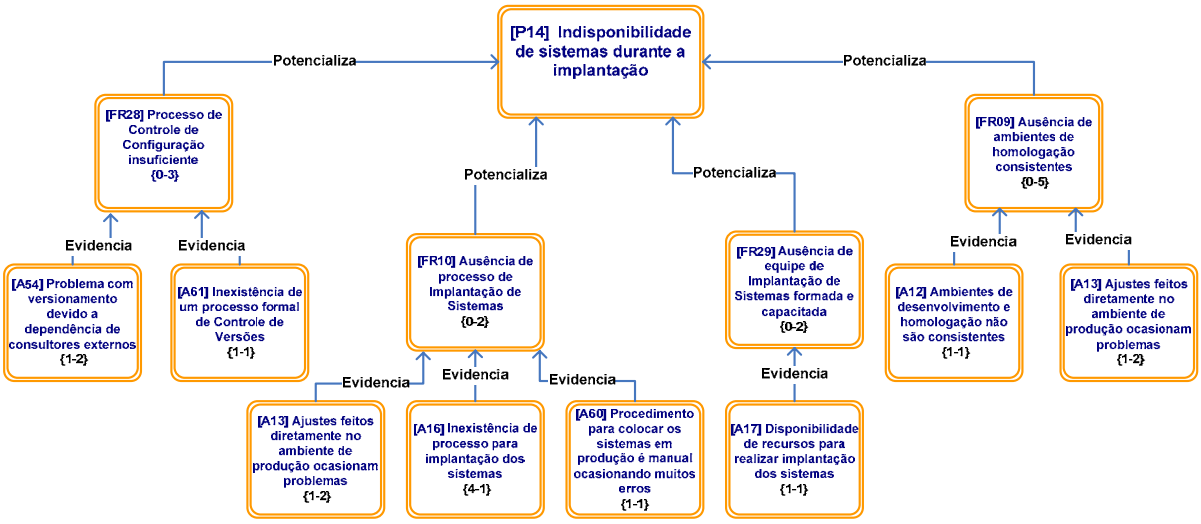

Figura 18: Esquema gráfico com as associações relacionadas ao Perigo [P14] Indisponibilidade de sistemas durante a implantação.

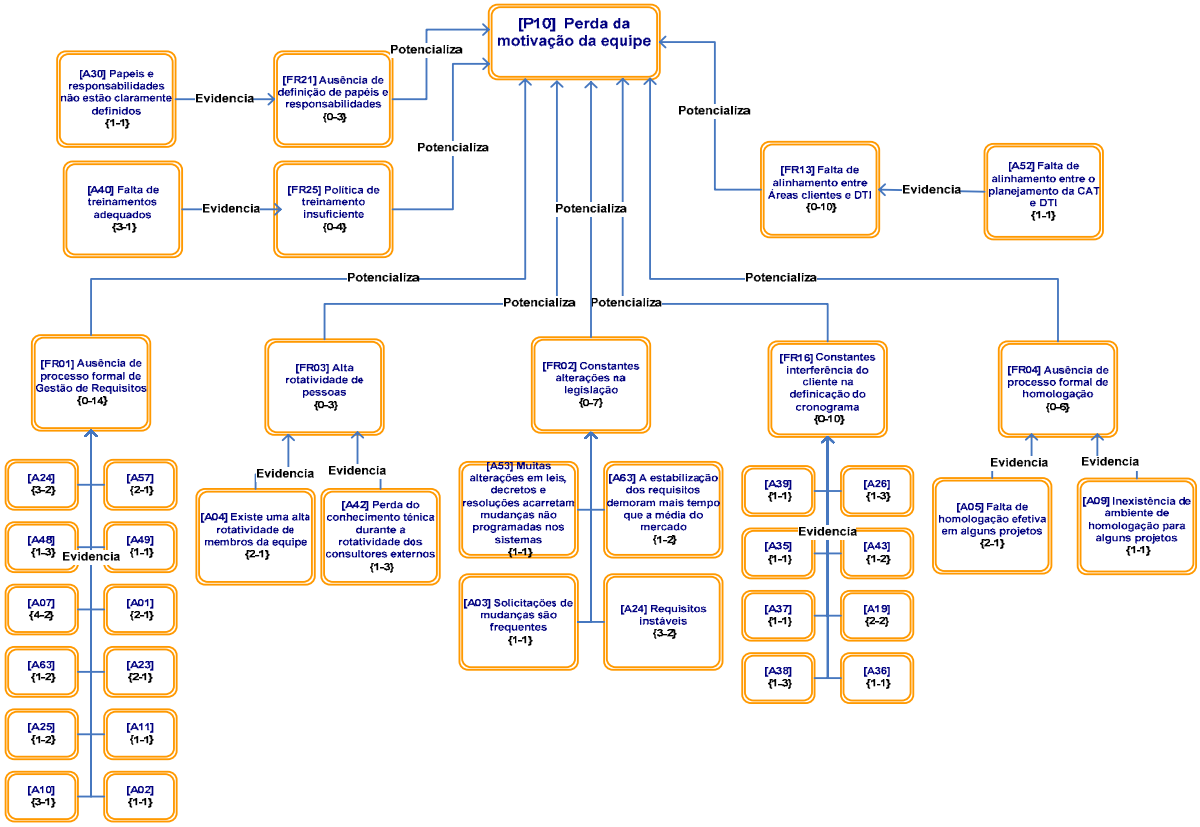

Figura 19: Esquema gráfico com as associações relacionadas ao Perigo [P10] Perda da motivação da equipe.

Como exemplo de análise dos esquemas gráficos, na Figura 15 a representação dos códigos das variações dimensionais do perigo “[P04] Fuga da Informação”.

Na Figura 15, os códigos são apresentados seguidos de dois números que representam, respectivamente, o grau de fundamentação (groundness) e o de densidade teórica (density). O grau de fundamentação (groundness) mostra o número de passagens de texto associadas ao código. O grau de densidade teórica (density) mostra o número de relacionamentos do código com outros códigos. Nessa figura, os códigos são precedidos por “[XX]”, sendo que XX é uma sigla de identificação única da categoria.

Observa-se na Figura 15 em relação ao fator de risco “[FR03] Alta rotatividade de pessoas” que existem dois tipos de achados de riscos associados (evidências). O achado “[A04] Existe uma alta rotatividade de membros da equipe {2-1}” representa uma evidência de da existência do fator de risco sendo fundamentado em duas passagens de texto (grau de fundamentação do código é igual a dois) e está relacionado apenas com o

fator de risco FR03 (densidade teórica do código é igual a um). O achado de risco "[A42] Perda do conhecimento técnico durante a rotatividade dos consultores externos {1-3}" representa uma evidência da existência do fator de risco está fundamentado em apenas uma passagem do texto, porém está relacionado a três fatores de risco (FR03, FR08, FR26) como pode ser visto nas tabelas descritivas do Anexo I. As categorias de fatores de riscos possuem sempre grau de fundamentação igual a zero por serem categorias abstratas e não possuírem citações diretas no texto, para essa categoria o grau de densidade teórica é a quantidade de relacionamentos com as categorias dos códigos de perigo. Com a mesma diretriz, vemos que as categorias de perigo possuem tanto o grau de fundamentação quanto a densidade teórica iguais a zero, e por isso omitiu-se sua apresentação.

Optou-se por não incluir as categorias referentes ao código "Plano de ação" na diagramação por ser uma informação que não integra diretamente a estruturar de fator de risco e perigo. Esse dado, conforme justificado na seção 3.1 do Capítulo 3, foi coletado visando auxiliar na elaboração do Plano de Respostas.

Por fim foi realizada a auditoria com o objetivo de avaliar o estudo para garantir validade dos resultados encontrados. Conforme descrito na Seção 3.2.6 do Capítulo 3, a avaliação do resultado da investigação deve ser guiada por um conjunto de critérios definidos para garantir objetividade. Um conjunto de critérios sugerido por Strauss e Corbin é: (i) adequação - adequação à área de pesquisa e deve corresponder aos dados, (ii) entendimento – ter sentido para profissionais da área estudada, (iii) generalidade abstração suficiente para servir de guia geral sem perder sua relevância, e (iv) controle – possibilidade de atuar como um guia geral e possibilita a uma pessoa entender completamente a situação.

A auditoria foi realizada através da avaliação dos líderes técnicos da área de desenvolvimento e foram considerados e avaliados os critérios de adequação, entendimento e controle. O resultado foi positivo para todos os critérios. O critério de generalidade não foi considerado devido à limitação do escopo de pesquisa, ficando como possibilidade de trabalho futuro a verificação de aplicação do resultado em um contexto similar.

4.2. Resultados da 2ª Fase – Método Brasiliano de Análise de Riscos

Com o resultado obtido na primeira fase – perigos e seus fatores de riscos relacionados- iniciou-se a execução do Método Brasiliano de Análise de Riscos com o objetivo de analisar e avaliar os riscos buscando a identificação da priorização e direcionamento de esforços na construção do plano de respostas.

4.2.1. Identificação dos Perigos e Fatores de Riscos

Na primeira fase da Avaliação de Riscos proposta por Brasiliano está a identificação dos riscos através dos perigos e fatores de riscos existentes através da utilização da técnica de *brainstorming* e do uso do Diagrama de Ishikawa. Essa etapa foi concluída com o resultado da aplicação da Teoria Fundamentada em Dados na 1ª fase, onde obtivemos a listagem dos perigos e dos fatores de riscos já relacionados entre si.

Uma adaptação no diagrama de Ishikawa foi feita considerando as principais macrocausas encontradas no ambiente de desenvolvimento de software de acordo com as principais categorias dos fatores de riscos coletados. Foram utilizadas apenas quatro macrocausas: Processos, Recursos Humanos (RH), Tecnologia e Meio Organizacional. A Figura 6.7 apresenta a representação do Perigo “Requisitos mal entendidos e/ou definidos” e seus fatores de riscos utilizando o Diagrama de Ishikawa adaptado. Os demais perigos estão esquematizados no Anexo II.

A distribuição dos fatores de riscos no Diagrama de Ishikawa, para o nosso caso, facilitará a identificação da macrocausa que possui maior influência sobre o perigo. Essa influência é considerada para o cálculo do critério “Fator de Risco” que compõe o cálculo do grau de probabilidade.

4.2.2. Identificação da Motricidade dos Fatores de Riscos

Após a identificação dos Fatores de Riscos avaliamos quais são os fatores comuns a todos os perigos e quais são os mais motrizes. Para isso utilizou-se como ferramentas a Matriz SWOT e a Matriz de Impacto Cruzado com os critérios estabelecidos na Seção 2.2.2.3.

Para a aplicação da Matriz SWOT utilizou-se como parâmetro para a nota da magnitude a seguinte escala: 1 (influência em 1 a 6 perigos), 2 (influência em 7 a 12 perigos) e 3 (influência acima de 13 perigos). Pontuaram-se subjetivamente cada Fator de Risco através do parâmetro "Importância" com a avaliação de alguns líderes técnicos que participaram da 1ª fase da pesquisa. Nesta Matriz foi apenas utilizado o campo de fraqueza, pois todos os fatores de riscos identificados eram relacionados ao contexto interno, no qual a organização possui autonomia. A ausência de forças e oportunidades é justificada pelo direcionamento dado durante a aplicação da Teoria Fundamentada em Dados na 1ª fase, onde se buscou essencialmente a identificação dos problemas. Já a ausência de ameaças (variáveis incontroláveis do ambiente externo) é possivelmente justificada pela ausência de Cultura em Gerenciamento de Riscos na organização, visto que a concepção de risco ainda está limitada em analisar apenas os riscos e problemas inerentes às atividades operacionais, não conseguindo visualizar o âmbito corporativo e os fatores externos. A Tabela 16 apresenta o resultado da Matriz SWOT.

Tabela 16: Matriz SWOT – Cálculo da Motricidade

Matriz SWOT – Fraquezas				
Fator de Risco	**Magnitude**	**Importância**	**TOTAL**	**Qte**
[FR01] Ausência de processo formal de Gestão de Requisitos	3	3	**9**	14
[FR02] Constantes alterações na legislação	2	2	**4**	7
[FR03] Alta rotatividade de pessoas	1	2	**2**	3
[FR04] Ausência de processo formal de	1	2	**2**	6

Homologação				
[FR05] Sistemas legados sem documentação	1	2	**2**	6
[FR06] Sistemas legados desenvolvidos em plataformas não conhecidas pela equipe	1	1	**1**	4
[FR07] Ausência de práticas de documentação dos sistemas	1	3	**3**	6
[FR08] Ausência de processo de Gestão do Conhecimento	1	2	**2**	3
[FR09] Ausência de ambientes de homologação consistentes	1	2	**2**	5
[FR10] Ausência de processo de Implantação de Sistemas	1	2	**2**	2
[FR11] Adoção da prática de *early-adopter*	1	1	**1**	1
[FR12] Baixa Qualidade de código e Documentação das Fábricas de Software	1	3	**3**	5
[FR13] Falta de alinhamento entre Áreas clientes e DTI	2	3	**6**	10
[FR14] Ausência de Padrão de Codificação	1	2	**2**	5
[FR15] Ausência de processo de Gestão de Projetos	2	3	**6**	10
[FR16] Constantes interferências do cliente na definição do cronograma	2	3	**6**	10
[FR17] Ausência de processo de Testes	2	3	**6**	7
[FR18] Ausência de procedimentos de Controle de Acesso	1	2	**2**	1
[FR19] Ausência de práticas em Arquitetura de Software	1	2	**2**	2
[FR20] Existência de outras unidades administrativas que desenvolvem software	1	2	**2**	4
[FR21] Ausência de definição de papéis e	1	3	**3**	3

responsabilidades				
[FR22] Ausência de uma metodologia de desenvolvimento de software	2	3	**6**	10
[FR23] Falta de capacitação na elaboração de editais	1	3	**3**	2
[FR24] Ausência de processo de Análise e Modelagem de Negócios	1	2	**2**	5
[FR25] Política de treinamento insuficiente	1	2	**2**	4
[FR26] Dependência técnica de Consultores Externos	1	2	**2**	2
[FR27] Ausência de processo de Requisitos para área não tributária	1	3	**3**	6
[FR28] Processo de Controle de Configuração insuficiente	1	2	**2**	3
[FR29] Ausência de equipe de Implantação de Sistemas formada e capacitada	1	2	**2**	2
[FR30] Ausência de equipe de Testes formada e capacitada	2	2	**4**	7
[FR31] Ausência de equipe de Análise e Modelagem de Negócios formada e capacitada	1	2	**2**	5
[FR32] Ausência de equipe de Requisitos para área não tributária formada e capacitada	1	2	**2**	6

Analisando o resultado da Matriz SWOT, identificamos que os cinco fatores mais pontuados como mais motrizes são: FR01 - Ausência de processo formal de Gestão de Requisitos (motricidade 14), FR13 - Falta de alinhamento entre Áreas clientes e DTI (motricidade 10), FR15 - Ausência de processo de Gestão de Projetos (motricidade 10), FR16 - Constantes interferências do cliente na definição do cronograma (motricidade 10) e FR22 - Ausência de uma metodologia de desenvolvimento de software (motricidade 10).

Com o resultado da Matriz SWOT já se tem uma base para priorizar as ações no Plano de Resposta aos Riscos. Contudo, para uma visão mais prospectiva e sistêmica da situação, foi realizada também a Matriz de Impacto Cruzado.

Para a Matriz de Impacto Cruzado, o critério "Grau de Interdependência" entre os Fatores de Riscos também foi avaliado subjetivamente pela mesma equipe de líderes técnicos considerando os critérios estabelecidos na Tabela 3. A soma dos valores das colunas com as linhas resultou, através dos resultados das colunas, a motricidade de cada fator de risco, e através das linhas horizontais o valor de sua dependência. O resultado da Matriz de Impacto Cruzado é apresentado na Figura 20.

FATORES	FR01	FR02	FR03	FR04	FR05	FR06	FR07	FR08	FR09	FR10	FR11	FR12	FR13	FR14	FR15	FR16	FR17	FR18	FR19	FR20	FR21	FR22	FR23	FR24	FR25	FR26	FR27	FR28	FR29	FR30	FR31	FR32	D
FR01		0	0	1	0	0	1	0	0	0	0	0	0	0	2	0	1	0	0	0	1	2	0	1	0	0	1	0	0	0	0	1	11
FR02	0		0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
FR03	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
FR04	2	0	0		0	0	0	0	1	0	0	0	0	0	2	0	1	0	0	0	1	2	0	1	0	0	2	0	0	0	0	1	13
FR05	0	0	0	0		2	2	1	0	0	1	2	0	1	0	1	0	0	0	1	0	1	1	1	0	0	0	0	0	0	0	0	14
FR06	0	0	2	0	2		0	2	0	0	1	1	0	0	0	0	0	0	0	2	0	0	0	0	3	0	0	0	0	0	0	0	13
FR07	2	0	0	0	1	0		1	0	1	1	0	0	0	1	1	1	0	1	0	0	2	0	1	0	0	2	0	0	0	0	1	16
FR08	0	0	0	0	0	0	0		0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
FR09	1	0	0	2	0	1	1	0		2	1	1	0	0	1	0	2	0	1	1	0	2	0	0	0	0	0	3	1	0	0	0	20
FR10	0	0	0	0	0	0	0	0	0		0	0	0	0	1	0	1	0	0	0	0	2	0	0	0	0	0	1	1	0	0	0	6
FR11	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FR12	1	0	0	0	0	0	2	0	0	0	1		0	1	1	0	2	0	0	1	0	1	2	0	0	0	1	0	0	2	0	1	16
FR13	1	1	0	0	0	0	0	0	0	0	0	0		0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	1	0	7
FR14	0	0	0	0	0	1	2	0	0	0	1	0	0		0	0	1	0	1	1	0	2	0	0	0	0	0	0	0	0	0	0	9
FR15	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FR16	1	2	0	0	0	0	0	0	0	0	0	0	3	0	2		0	0	0	0	1	1	0	1	0	0	1	0	0	0	0	1	13
FR17	1	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0		0	0	0	0	2	0	1	0	0	0	0	1	0	1	8
FR18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FR19	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0		0	0	2	0	0	2	0	0	0	0	0	0	0	5
FR20	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0		1	0	0	0	0	0	0	0	0	0	0	0	3
FR21	1	0	0	2	0	0	0	0	0	1	0	0	2	0	2	0	1	1	0	1		1	0	1	0	0	1	1	1	1	1	1	19
FR22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0		0	1	0	0	0	0	0	0	0	0	3
FR23	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0		0	3	0	0	0	0	0	0	0	5
FR24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		1	0	0	0	0	0	1	0	2
FR25	0	0	0	0	0	0	0	2	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	3
FR26	0	0	2	0	1	3	1	3	0	0	2	1	0	0	0	0	0	0	0	1	0	0	0	0	3		0	1	1	0	0	0	19
FR27	3	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0	0	0	0	0	2	0	1	0	0		0	0	0	0	1	10
FR28	1	0	0	0	0	0	0	0	0	2	0	0	0	0	2	0	0	0	0	0	0	2	0	0	1	0	0		0	0	0	0	8
FR29	0	0	1	0	0	0	0	0	0	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0		0	0	0	5
FR30	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	2	0	0	0	0	0	0	0	1	0	0	0	0		0	0	5
FR31	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0		0	4
FR32	2	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	1	1	0	2	0	0	0	0		9
M	16	3	8	5	4	8	9	11	1	8	8	5	10	2	25	2	13	1	3	9	5	24	3	13	18	0	10	6	4	4	3	8	

Figura 20: Matriz de Impactos Cruzados - Resultado

Com as dados obtidos pela Matriz de Impactos Cruzados elaborou-se o gráfico da motricidade *versus* dependência (Figura 21). Para tanto, foram calculados os pontos

médios de motricidade e de dependência, aplicando as fórmulas apresentadas na Equação 1 da seção 2.2.2.3.1.

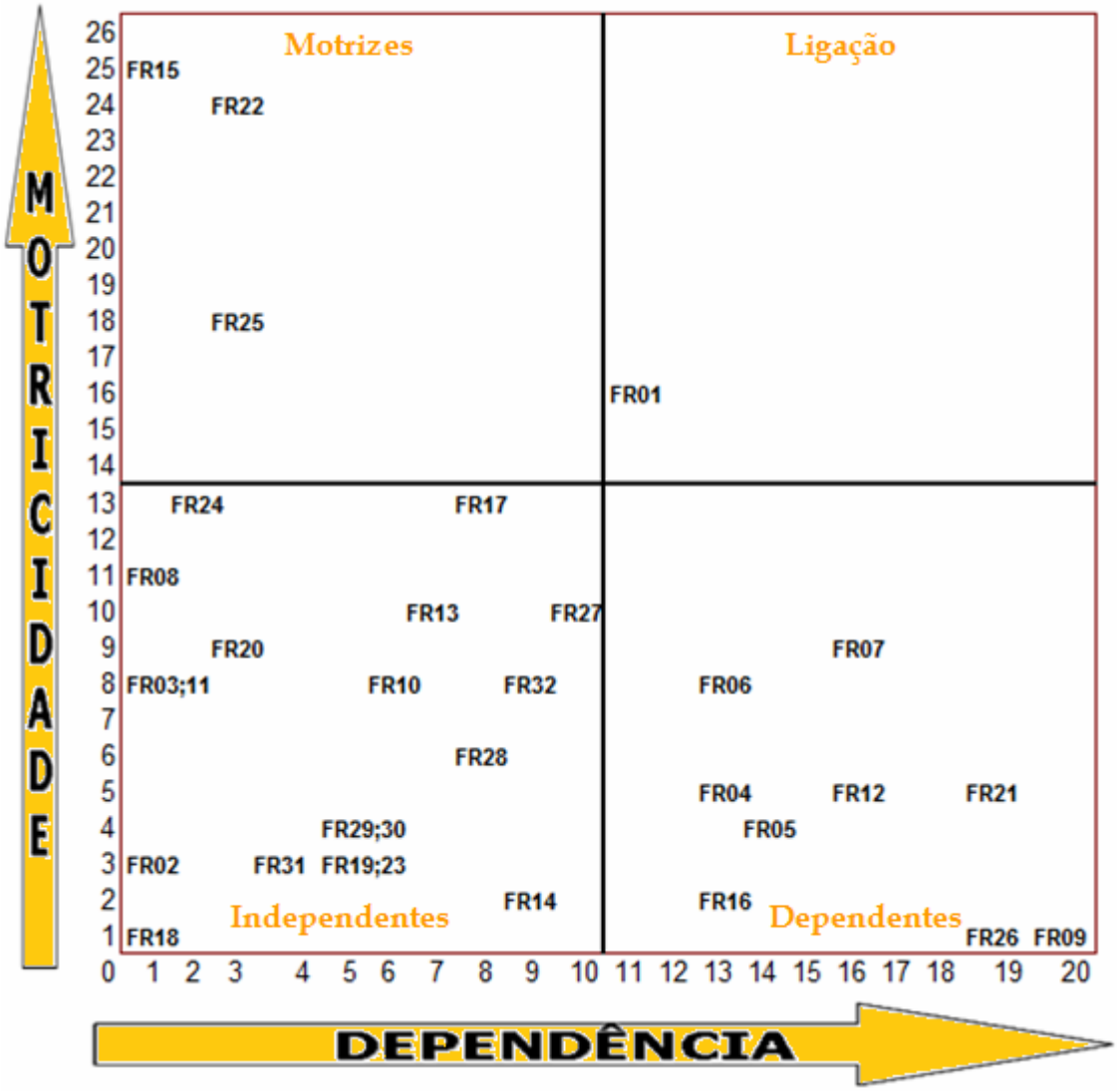

Figura 21: Matriz Motricidade x Dependência - Resultado

Analisando a Figura 21, vemos que o fator de risco FR11 - Ausência de processo formal de Gestão de Requisitos, localizado no quadrante de ligação, é muito motriz, mas tem grande dependência dos demais. Esse fator faz a ligação entre os fatores motrizes e os dependentes. Por sua ação instável, qualquer ação sobre ele terá repercussão sobre os outros e um efeito sobre si próprio que virá ampliado ou atenuado em função da impulsão inicial. Fatores de ligação são os mais importantes, assim o FR11 deve ser tratado com maior criticidade.

Os fatores motrizes são os que condicionam o restante do sistema. Assim, os fatores FR15 - Ausência de processo de Gestão de Projetos, FR22 - Ausência de uma metodologia de desenvolvimento de software e FR25 - Política de treinamento insuficiente também devem ser olhados com criticidade, pois são eles que alavancam os outros fatores.

Os fatores dependentes FR04 - Ausência de processo formal de homologação, FR05 - Sistemas legados sem documentação, FR06 - Sistemas legados desenvolvidos em plataformas não conhecidas pela equipe, FR07 - Ausência de práticas de documentação dos sistemas, FR09 - Ausência de ambientes de homologação consistentes, FR12 - Baixa Qualidade de código e Documentação das Fábricas de Software, FR16 - Constantes interferências do cliente na definição do cronograma, FR21 Ausência de definição de papéis e responsabilidades e FR26 - Dependência técnica de Consultores Externos são pouco motrizes e muito dependentes, seu comportamento é explicado pelos fatores motrizes e de ligação. Esses fatores são menos críticos, pois dependem de outros para que possa a acontecer. Assim, esses fatores não necessitam de ação imediata devendo apenas ser monitorados.

Os demais fatores, independentes, são pouco motrizes e pouco dependentes. Ações sobre esses fatores não tem grande repercussão sobre os demais. Assim devem ser tratados apenas os mais críticos, os que representam no momento um grande problema para organização. São geralmente tendências de peso ou fatores relativamente desligados do sistema e que não constituem determinantes do futuro. São considerados franco-atiradores e a recomendação é que sejam excluídos de uma análise prospectiva.

Segundo O CGEE [CGEE 2011], a análise de impacto cruzado é uma técnica altamente qualitativa e dependente da opinião de especialistas para identificar estimativas significativas da probabilidade da ocorrência de um evento. Assim, para o mesmo conjunto de fatores analisado, poderíamos obter resultados diversos dependendo da equipe envolvida na análise. A forma encontrada para diminuir o impacto da subjetividade se deu primeiramente através da seleção dos líderes técnicos que possuíam uma visão mais abrangente dos fatores envolvidos, em seguida durante a execução da análise foram amplamente debatidas todas as opiniões, através de exemplificação e casos passados visando à elaboração de um consenso, além da escolha de um “mediador” para decidir em caso de divergência.

Vemos que o resultado da Matriz SWOT foi diferente do resultado encontrado na Matriz de Impactos Cruzados. Conforme observado na seção 2.2.2.3.1 essa divergência ocorre devido à diferença no foco da avaliação realizada por cada. A opção de utilização das duas matrizes de forma complementar foi possibilita uma melhor priorização dos fatores de riscos críticos.

Os resultados obtidos pela Matriz SWOT e a Matriz de Impactos Cruzados possuem como pontos de convergência os fatores FR01 - Ausência de processo formal de Gestão de Requisitos, FR15 - Ausência de processo de Gestão de Projetos e FR22 - Ausência de uma metodologia de desenvolvimento de software. Esses terão tratados com criticidade e priorizados no Plano de Ação.

A Matriz SWOT também priorizou FR13 - Falta de alinhamento entre Áreas clientes e DTI e FR16 - Constantes interferências do cliente na definição do cronograma, considerados respectivamente como independente e dependente pela Matriz de Impactos Cruzados. Assim, o FR13 será tratado com prioridade, mas o FR16 será apenas monitorado, pois é claramente dependente dos fatores FR15 e FR12 que já serão priorizados. Isso é facilmente visualizado e justificado: implantando um processo formal de gestão de projetos e institucionalizando uma metodologia de desenvolvimento de software a interferência do cliente na definição do cronograma tenderá a diminuir / acabar.

A Matriz de Impactos Cruzados identificou o fator FR25 - Política de treinamento insuficiente como motriz. Embora na Matriz SWOT esse fator tenha pontuação baixa (motricidade igual a 2), esse fator também será considerado prioritário, pois como visto ele exerce grande influência sobre os demais fatores.

4.2.3. Análise dos Riscos

A análise de riscos visa auxiliar na definição de prioridades e opções de tratamento aos perigos identificados. Nesta fase foram calculadas a probabilidade e o impacto. O cruzamento destes dois parâmetros teve como resultado uma Matriz de Riscos.

4.2.3.1. Cálculo do Grau de Probabilidade

O próximo passo foi a realização da Análise de Riscos através do cálculo do Grau de Probabilidade (Seção 2.2.2.3.2). Como visto a fórmula para esse cálculo está alicerçada em dois critérios: Critério dos Fatores de Riscos (FR) e o Critério da Exposição (E).

4.2.3.1.1. Cálculo do Critério "Fator de Risco"

O critério FR é uma nota subjetiva, com base no diagrama de causa e efeito. Em nosso caso, realizamos uma adaptação na proposta do Método Brasiliano e este critério foi composto por quatro subcritérios referentes às macro causas identificadas:

FR RECURSOS HUMANOS: este critério projeta o nível da equipe de envolvida, na concretização do perigo em estudo. Deve-se levar em consideração o efetivo existente, perfil, qualificação e posicionamento tático.

FR MEIOS ORGANIZACIONAIS: este critério projeta a influência da formalização das normas e políticas, não existentes na organização, na concretização do perigo em estudo.

FR TECNOLOGIA: este critério projeta a influência da tecnologia, plataformas, ambientes de desenvolvimento e equipamentos não existentes ou deficientes no departamento, na concretização do perigo em estudo.

FR PROCESSOS: este critério projeta a influência dos processos, procedimentos e padrões não existente no departamento, na concretização do perigo em estudo.

Os subcritérios possuem uma escala de valoração (escala proposta na Tabela 4, Seção 2.2.2.3.3) que mede o grau de influência para a concretização do perigo. Neste caso julgamos qual o nível de influência, por subcritério, para que o perigo seja concretizado. É uma nota subjetiva, com base no diagrama de causa e efeito.

Para o cálculo desta influência foram consideradas as informações fornecidas pela Matriz SWOT, através do valor da motricidade, de modo que a nota fosse a mais coerente

possível. Assim, para cada macro fator do diagrama, foram somadas todas as motricidades dos seus fatores de riscos, obtendo assim uma pontuação para cada macrofator (subcritério). De acordo com a pontuação obtida por cada subcritério, foi usada a escala de valoração para estabelecer o grau de sua influência na concretização do perigo. Um exemplo dessa avaliação é apresentado na Figura 22. Os diagramas dos demais perigos são apresentados no Anexo II.

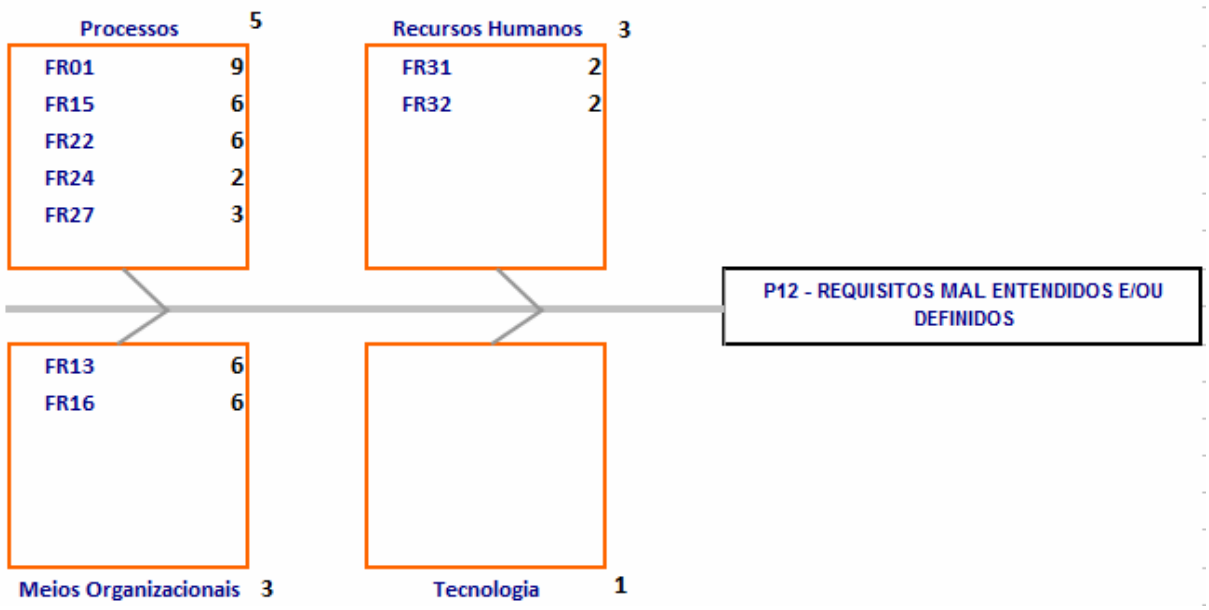

Figura 22: Perigo "Requisitos mal entendidos e/ou definidos" - Diagrama de Causa e Efeito.

Na Figura 22, a motricidade – calculada na Matriz SWOT – está indicada ao lado direito de cada fator de risco. Nota-se que a maior pontuação para este perigo se encontra no macrofator "Processos" (soma das motricidades igual a 26) e a menor no macrofator "Tecnologia" (soma das motricidades igual a 0). Assim, a maior influência está em Processos, atribuído grau 5, e para Tecnologia, menor influência, foi atribuído grau 1.

Após o cálculo do grau de influência de cada macro fator foi calculado o critério FR com base na fórmula apresentada na Equação 5:

$$FR = \frac{RH + TE + PR + MO}{4}$$

RH = Recursos Humanos

TE = Tecnologia

PR = Processos

MO = Meios Organizacionais

Equação 5: Cálculo do Critério "Fator de Risco".

Ainda usando como exemplo a Figura 22, temos para este perigo o FR igual 3,00 (FR = (3 + 1 + 5 + 3) / 4) .

4.2.3.1.2. Cálculo do Critério da Exposição

O critério da Exposição possui uma escala de valoração que mede a frequência que os perigos costumam manifestar-se na organização. A escala apresentada na Tabela 6, Seção 2.2.2.3.2 foi ajustada com as informações sobre ocorrência dos perigos levantados na 1ª Fase da pesquisa considerando a quantidade de projetos concluídos ou em desenvolvimento. A Tabela 17 apresenta a escala utilizada:

Tabela 17: Critério da Exposição adaptado

Critério da Exposição	
Escala	Pontuação
Em quase todos os projetos (80,01% a 100%)	5
Na maioria dos projetos (60,01% a 80%)	4
Em boa parte dos projetos (40,01% a 60%)	3
Em poucos projetos (20% a 40%)	2
Remotamente possível (até 20%)	1

O Grau de Probabilidade GP foi calculado através da multiplicação do valor final do fator de risco versus o critério da exposição, conforme demonstrado, na Equação 3 da seção 2.2.2.3.2.

Na Figura 23 que apresenta o resultado final da Análise de Riscos, é possível visualizar a pontuação obtida para cada subcritério e o valor final do critério "Fator de Risco", a pontuação para exposição de cada perigo – critério "Exposição" - e o Grau de Probabilidade obtido pela multiplicação dos dois critérios.

PERIGOS	FATOR DE PERIGO					E	GP	CLASSIFICAÇÃO GRAU PROBABILIDADE	PROBABILIDADE DE ACONTECER
	PRO	TI	RH	OR	FR		FRxE		
[P01] Sistemas não atendem às expectativas do cliente	5	1	2	3	2,75	5	13,8	ALTA	55%
[P02] Retrabalho	5	1	2	3	2,75	5	13,8	ALTA	55%
[P03] Perda do conhecimento técnico e do negócio	5	1	2	1	2,25	3	6,8	MÉDIA	27%
[P04] Fuga de informação	4	1	3	1	2,25	2	4,5	BAIXA	18%
[P05] Alto custo em manutenção dos sistemas	5	2	2	3	3,00	4	12,0	ALTA	48%
[P06] Alto custo em engenharia reversa	5	2	1	2	2,50	3	7,5	MÉDIA	30%
[P07] Problemas e não conformidades detectados apenas em produção	5	2	4	1	3,00	5	15,0	ALTA	60%
[P08] Alto índice de erros nos sistemas	5	2	2	2	2,75	5	13,8	ALTA	55%
[P09] Aumento da curva de aprendizado na adoção de novas tecnologias	3	4	1	1	2,25	2	4,5	BAIXA	18%
[P10] Perda da motivação da equipe	2	1	1	5	2,25	4	9,0	MÉDIA	36%
[P11] Estimativas de tempo e prazo irreais	5	1	1	3	2,50	5	12,5	ALTA	50%
[P12] Requisitos mal entendidos e/ou definidos	5	1	3	3	3,00	5	15,0	ALTA	60%
[P13] Gerenciamento impróprio de mudanças	5	2	1	4	3,00	4	12,0	ALTA	48%
[P14] Indisponibilidade de sistemas durante a implantação	5	2	3	1	2,75	3	8,3	MÉDIA	33%
[P15] Sistemas com baixa qualidade e confiabilidade	5	3	1	4	3,25	4	13,0	ALTA	52%
[P16] Transferência de responsabilidades	5	1	2	4	3,00	4	12,0	ALTA	48%
[P17] Alto custo com Fábricas de Software	5	2	4	1	3,00	3	9,0	MÉDIA	36%

Figura 23: Análise dos Riscos - Probabilidade

4.2.3.2. Definição da Relevância do Impacto

Para mensurar o impacto, não devemos levar em consideração a questão financeira. O Método Brasiliano sugere estudar a relevância do impacto levando em consideração quatro fatores: imagem, financeiro, operacional e legal. (Figura 10, Seção 2.2.2.3.2).

Foi realizada uma consulta com representantes da gerência do Departamento de Tecnologia da Informação para avaliar a importância e relevância desses fatores. O resultado foi: Imagem (peso 3), Financeiro (peso 4), Operacional (peso 5) e Legal (peso 2).

4.2.3.3. Determinação do Nível de Impacto

Após definirmos os fatores de impacto calculamos o Nível de Impacto conforme fórmula apresentada na Equação 4, Seção 2.2.2.3.3: O resultado é a soma dos resultados de cada fator de impacto (multiplicação do peso x nota), divido pela soma dos pesos. A escala de notas para cada fator de impacto foi apresentada na seção 2.2.2.3.2: Tabelas 7 a 10. Para o fator de impacto "Imagem" foi considerada a percepção da imagem do Departamento de Tecnologia da Informação perante a organização.

Tabela 18: Escala do Fator "Imagem" adaptada

Nível de Impacto – Imagem	
Escala	Pontuação
Estado sede da Organização	5
Toda a Organização	4
Demais Coordenadorias	3
Coordenadoria Sede	2
DTI	1

As notas atribuídas a cada fator de impacto e o nível de impacto de cada perigo são apresentadas na Figura 24:

PERIGOS	RELEVÂNCIA DE IMPACTO						
	Imagem	Financeiro	Legislação	Operacional	NOTA	Média	Nível de impacto
	3	4	2	5	14	Ponderada	
[P01] Sistemas não atendem às expectativas do cliente	4,0	3,0	1,0	3,0	41,0	2,93	MODERADO
[P02] Retrabalho	2,0	3,0	1,0	4,0	40,0	2,86	MODERADO
[P03] Perda do conhecimento técnico e do negócio	1,0	2,0	1,0	2,0	23,0	1,64	LEVE
[P04] Fuga de informação	5,0	3,0	3,0	2,0	43,0	3,07	MODERADO
[P05] Alto custo em manutenção dos sistemas	2,0	4,0	1,0	2,0	34,0	2,43	LEVE
[P06] Alto custo em engenharia reversa	1,0	3,0	1,0	3,0	32,0	2,29	LEVE
[P07] Problemas e não conformidades detectados apenas em produção	4,0	2,0	1,0	4,0	42,0	3,00	MODERADO
[P08] Alto índice de erros nos sistemas	3,0	4,0	1,0	4,0	47,0	3,36	MODERADO
[P09] Aumento da curva de aprendizado na adoção de novas tecnologias	1,0	1,0	1,0	2,0	19,0	1,36	INSIGNIFICANTE
[P10] Perda da motivação da equipe	2,0	1,0	1,0	4,0	32,0	2,29	LEVE
[P11] Estimativas de tempo e prazo irreais	3,0	2,0	1,0	4,0	39,0	2,79	MODERADO
[P12] Requisitos mal entendidos e/ou definidos	3,0	3,0	1,0	3,0	38,0	2,71	MODERADO
[P13] Gerenciamento impróprio de mudanças	2,0	2,0	1,0	4,0	36,0	2,57	MODERADO
[P14] Indisponibilidade de sistemas durante a implantação	3,0	3,0	1,0	4,0	43,0	3,07	MODERADO
[P15] Sistemas com baixa qualidade e confiabilidade	4,0	2,0	1,0	2,0	32,0	2,29	LEVE
[P16] Transferência de responsabilidades	4,0	1,0	2,0	3,0	35,0	2,50	LEVE
[P17] Alto custo com Fábricas de Software	2,0	4,0	1,0	3,0	39,0	2,79	MODERADO

Figura 24: Análise dos Riscos - Impacto

4.2.4. Avaliação de Riscos

Com o objetivo de visualizar e implementar uma forma de tratamento de cada risco, o resultado da análise será utilizado para montar a Matriz de Riscos.

4.2.4.1. Construção da Matriz de Riscos

A Matriz de Riscos demonstra os pontos de cruzamento da probabilidade de ocorrência e do impacto (calculados na análise de riscos). Desta forma, pela divisão da matriz em quatro níveis de criticidade podemos avaliar o nível de vulnerabilidade e sua influência nos objetivos da organização. Quanto maior for a probabilidade e o impacto, maior será o nível do risco. O apetite ao risco considerado para a organização foi conservador. A Figura 25 mostra o resultado da Matriz de Riscos considerando esse perfil.

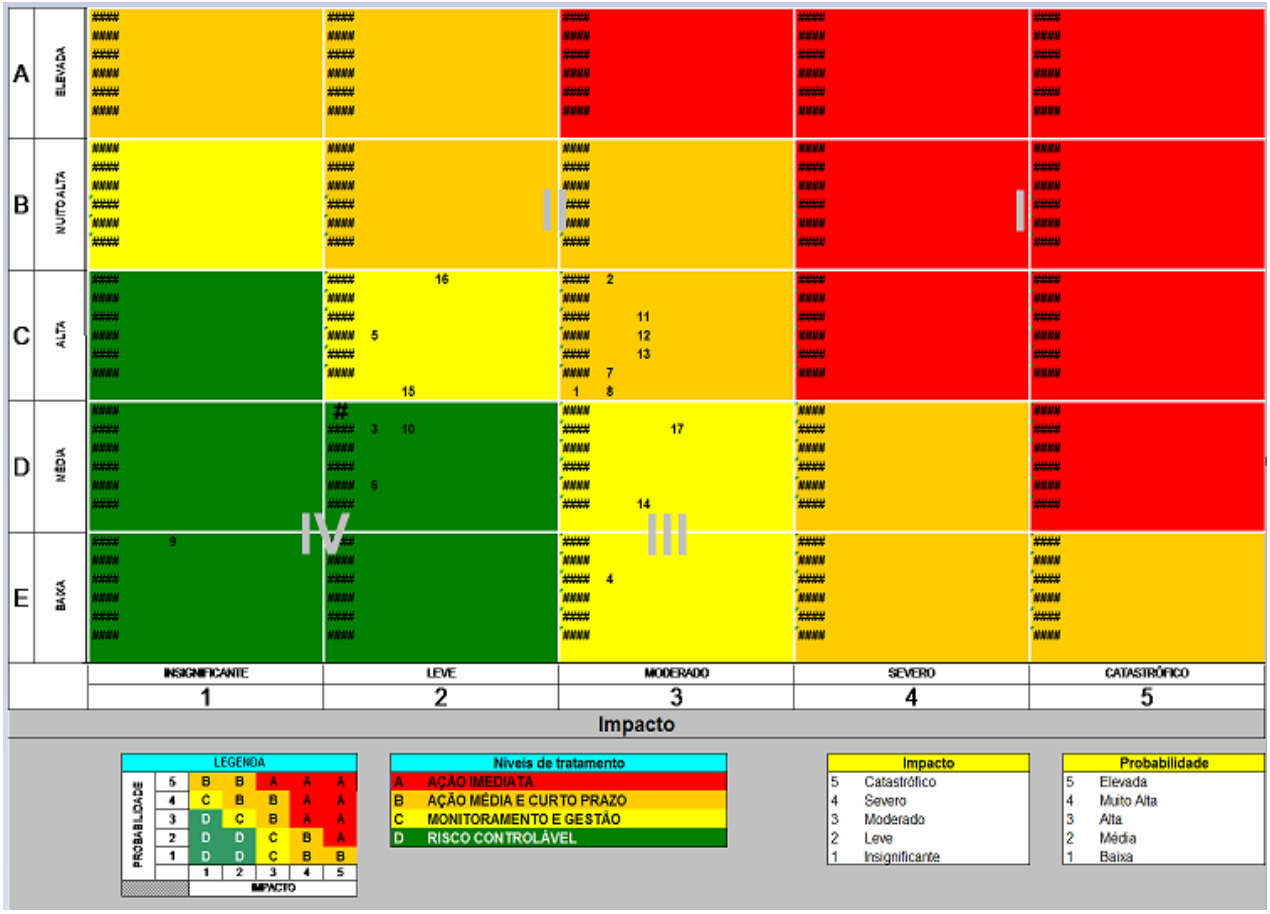

Figura 25: Matriz de Riscos - Resultado

Analisando a Figura 25, vemos que os riscos P01- Sistemas não atendem às expectativas do cliente, P02 – Retrabalho, P07 - Problemas e não conformidades detectados apenas em produção, P08 - Alto índice de erros nos sistemas, P11 - Estimativas de tempo e prazo irreais, P12 - Requisitos mal entendidos e/ou definidos e P13 - Gerenciamento impróprio de mudanças, localizados no quadrante II (laranja), poderão ser muito danosos à organização, possuindo baixa probabilidade e alto impacto ou baixo impacto e alta probabilidade. Estas ameaças devem possuir respostas rápidas, que deverão estar planejadas, além de ações preventivas.

No quadrante III (amarelo) estão os riscos P04 - Fuga de informação, P05 - Alto custo em manutenção dos sistemas, P14 - Indisponibilidade de sistemas durante a implantação, P15 - Sistemas com baixa qualidade e confiabilidade, P16 - Transferência de responsabilidades e P17 - Alto custo com Fábricas de Software. São riscos com alta

probabilidade de ocorrência, mas que causam consequências gerenciáveis à organização. Estes riscos irão ser monitorados de forma rotineira e sistemática, podendo posteriormente possuir planos de emergência.

E finalmente, os riscos [P03] Perda do conhecimento técnico e do negócio, [P06] Alto custo em engenharia reversa, [P09] Aumento da curva de aprendizado na adoção de novas tecnologias e P10 - Perda da motivação da equipe, quadrante IV (verde), possuem baixa probabilidade e pequeno impacto, representando pequenos problemas e prejuízos. Estes riscos somente serão apenas gerenciados e administrados, pois estão na zona de conforto.

4.2.5. Resposta aos Riscos: Plano de Ação

Uma vez identificados, avaliados e mensurados, o próximo passo foi definir qual o tratamento que será dado aos riscos. Com a Matriz de Riscos em conjunto com as Matrizes SWOT e de Impactos Cruzados identificamos a priorização a ser dada e a estratégia de tratamento adequada e assim direcionar os esforços.

4.2.5.1. Elaboração do Plano de Ação

Para elaborar o plano de ação utilizamos a técnica 5W e 2H descrita na Seção 2.2.2.4. As evidências das categorias de “Plano de Ação”, identificadas na primeira fase da pesquisa, foram utilizadas como consulta para avalias as possibilidades de ações e estratégias a serem adotadas.

Com o resultado da Matriz de Riscos sabemos quais as ameaças devem ser priorizadas. E, conforme visto cada ameaça é potencializada por um ou mais fatores de riscos. São nos fatores de riscos que devem ser concentradas e direcionadas as ações, com o objetivo de reduzir a probabilidade de ocorrência da ameaça ou em reduzir seu impacto. Contudo, apenas alguns fatores devem ser prioritariamente trabalhados: os motrizes e de ligação. São eles que condicionam os demais fatores.

Assim, os riscos prioritários, identificados na Matriz de Riscos (quadrante laranja) que terão ações imediatas são:

- P01 - Sistemas não atendem às expectativas do cliente
- P02 – Retrabalho
- P07 - Problemas e não conformidades detectadas apenas em produção
- P08 - Alto índice de erros nos sistemas
- P11 - Estimativas de tempo e prazo irreais
- P12 - Requisitos mal entendidos e/ou definidos
- P13 - Gerenciamento impróprio de mudanças

E dentre os fatores de riscos que potencializam a concretização dessas ameaças serão atacados de acordo com os resultados da Matriz SWOT e da Matriz de Impactos Cruzados:

- FR01 - Ausência de processo formal de Gestão de Requisitos
- FR13 - Falta de alinhamento entre Áreas clientes e DTI
- FR15 - Ausência de processo de Gestão de Projetos
- FR22 - Ausência de uma metodologia de desenvolvimento de software
- FR25 - Política de treinamento insuficiente

Para cada fator de risco foram utilizadas algumas evidências (“Achados de Risco”) encontradas na 1º fase da pesquisa, através da Teoria Fundamentada em Dados, para compor as ações de curto prazo. Foram apenas consideradas as evidências que podiam ser traduzidas e implementadas no plano de ação como respostas imediatas.

A Figura 26 apresenta o plano de ação proposto para os riscos e seus os fatores de riscos priorizados:

O QUE?	QUEM?	QUANDO?	ONDE?	PORQUE?	COMO?	QUANTO?	EVIDÊNCIAS
[FR01] Ausência de processo formal de Gestão de Requisitos							
Definir procedimento inicial para documentar, formalizar e aprovar os requisitos	Líder Técnico I	Até julho/2011	CDS	Mitigar os riscos P01, P02, P07, P08, P11, P12 E P13	Definindo um procedimento inicial para documentar, formalizar e aprovar os requisitos, através da definição de um template padrão e estabelecimento de reuniões para aprovação dos requisitos junto ao cliente.	20 horas - Servidor da Organização	[A01]; [A02]; [A07]; [A49]
Palestras de Divulgação sobre Gestão de Requisitos	Líder Técnico I	Até outubro/2011	CDS e Coordenadorias SEFAZ	Mitigar os riscos P01, P02, P07, P08, P11, P12 E P13	Palestras institucionais para divulgar a importancia e objetivos da Gestão de Requisitos	30 horas - Servidor da Organização	
Contratar consultoria especializada para diagnóstico, treinamento e proposta de processo formal	Diretor Adjunto do CDS	Até dezembro/2011	CDS	Mitigar os riscos P01, P02, P07, P08, P11, P12 E P13	Pesquisa de mercado e processo licitatório	A avaliar	[A01]; [A02]; [A07]; [A49]; [A63]; [A57]; [A23]; [A11]; [A10];
Implantar e institucionalizar processo de Gestão de Requisitos	Diretor Adjunto do CDS	Até dezembro/2012	CDS e Coordenadorias SEFAZ	Mitigar os riscos P01, P02, P07, P08, P11, P12 E P13	Divulgação e treinamento	Incluso no preço da prestação de servico	
[FR13] Falta de alinhamento entre Áreas clientes e o DTI							
Elaborar relatorio situacional do DTI visando obter alinhamento e comprometimento das Coordenadorias	Diretor DTI	Até julho/2011	Coordenadorias SEFAZ	Mitigar os riscos P01, P02, P07, P11, P12 E P13	Mapear e analisar o contexto do DTI	20 horas - Servidor da Organização	[A52]
Realizar Reuniões de alinhamento com as Coordenadorias	Diretor DTI	Até dez/2011	Coordenadorias SEFAZ	Mitigar os riscos P01, P02, P07, P11, P12 E P13	Realizar Reuniões e workshops para alinhamento entre as Coordenadorias	20 horas - Servidor da Organização	
[FR15] Ausência de processo de Gestão de Projetos							
Envolver equipe do projeto na elaboração do cronograma	Diretor Adjunto do CDS	Até agosto/2011	CDS	Mitigar o risco P11 e minimizar as ocorrências das evidências A19 E A26	Estabelecer procedimento para que a equipe do projeto seja envolvida na elaboração do cronograma através da obtenção de comprometimento com o Clientes e Gerentes de Projeto	30 horas - Servidor da Organização	[A19]; [A26]
Definir modelo de acompanhamento e Disponibilizar periodicamente informações sobre andamento dos proejtos	Diretor Adjunto do CDS	Até dez/2011	CDS	Minimizar as ocorrências das evidências A55 e A56	Definir modelo para acompanhamento dos projetos e Disponibilizar em área compartilhada do departamento informações sobre o andamentos dos projetos	80 horas - Servidor da Organização	[A55]; [A56]
Contratar consultoria especializada para diagnóstico e proposta de processo	Diretor Adjunto do CDS	Até dezembro/2011	CDS	Mitigar os riscos P01, P02, P07, P11, P12 E P13	Pesquisa de mercado e processo licitatório	A avaliar	
Palestras de Divulgação sobre Gestão de Projetos	Líder Técnico II	Até julho/2011	Coordenadorias SEFAZ	Mitigar os riscos P01, P02, P07, P11, P12 E P13	Palestras institucionais para divulgar a importancia e objetivos da Gestão de Projetos	60 horas - Servidor da Organização	
Implantar e institucionalizar processo de Gestão de Projetos	Diretor Adjunto do CDS	Até julho/2012	CDS e Coordenadorias SEFAZ	Mitigar os riscos P01, P02, P07, P11, P12 E P13	Divulgação e treinamento	Incluso no preço da prestação de servico	
[FR22] Ausência de uma metodologia de desenvolvimento de software							
Estabelecer procedimento inicial para inspeção de código	Líder Técnico III	Até agosto/2011	CDS	Mitigar os riscos P02, P08 e minimizar as ocorrências da evidência A59	Estabelecer o uso de um padrão de codificação e obrigatoriedade da revisão do código por outro membro da equipe de desenvolvimento	20 horas - Servidor da Organização	[A59]
Contratar consultoria especializada para diagnóstico e proposta de processo	Diretor Adjunto do CDS	Até dezembro/2011	CDS	Mitigar os riscos P01, P02, P08, P11, P12 E P13	Pesquisa de mercado e processo licitatório	A avaliar	[A29]; [A45]; [A59]
Palestras de Divulgação sobre Metodologia de Desenvolvimento de Software	Líder Técnico III	Até julho/2011	CDS	Mitigar os riscos P01, P02, P08, P11, P12 E P13	Palestras institucionais para divulgar a importancia e objetivos da Gestão de Projetos	60 horas - Servidor da Organização	
Implantar e institucionalizar Metodologia de Desenvolvimento de Software	Diretor Adjunto do CDS	Até dezembro/2012	CDS	Mitigar os riscos P01, P02, P08, P11, P12 E P13	Divulgação e treinamento	Incluso no preço da prestação de serviço	
[FR25] Política de treinamento insuficiente							
Levantar necessidades de treinamento	Líder Técnico IV	Até abril/2011	CDS	Medida estratégica visando reduzir probabilidade/impacto de outros fatores	Identicar e avaliar necessidades de treinamento atraves de entrevistas	30 horas - Servidor da Organização	[A40]
Contratar consultoria especializada nas necessidades levantadas	Diretor Adjunto do CDS	Até dezembro/2011	CDS	Medida estratégica visando reduzir probabilidade/impacto de outros fatores	Pesquisa de mercado e processo licitatório	A avaliar	
Realizar Treinamentos	Líder Técnico IV	Até dezembro/2012	CDS	Medida estratégica visando reduzir probabilidade/impacto de outros fatores	Divulgação e treinamento	Incluso no preço da prestação de serviço	

Figura 26: Plano de Ação Proposto

4.3. Resumo do Capítulo

Esse capítulo apresentou os resultados obtidos na execução das estratégias e ações adotadas no Capítulo 3 que estruturaram a metodologia de pesquisa para alcançar os objetivos deste trabalho. O resultado obtido na primeira fase da pesquisa, estruturada na Teoria Fundamentada em Dados, foi o mapeamento dos perigos e dos fatores de riscos relacionados e seus relacionamentos. Na segunda fase da pesquisa aplicamos o Método Brasiliano para analisar e avaliar os riscos e então obter um Plano de Ação para as ameaças e os fatores de riscos priorizados.

5. Conclusões e Trabalhos Futuros

Este capítulo apresenta os resultados obtidos, as limitações encontradas durante a execução deste trabalho, as conclusões e sugestões de trabalhos futuros. Apresenta também os estudos relacionados com este trabalho.

5.1. Resultados

O produto dessa dissertação foi o mapeamento dos Fatores de Riscos existentes no ambiente de Desenvolvimento de Software de uma Organização do Setor Público e uma Proposta de Tratamento para esses fatores.

A abordagem escolhida para conduzir a primeira fase da pesquisa, que objetivou a identificação dos perigos e fatores de riscos, através da Teoria Fundamentada em Dados, foi considerada adequada, pois foram diagnosticadas na análise dos dados as correlações entre os diversos fatores de risco e os perigos identificados. As correlações também demonstraram que o que faz com que o projeto não tenha sucesso em relação a um problema é um conjunto de fatores e não somente um fator, e que esses fatores não são apenas tecnológicos, e que a maioria está relacionada com processos, recursos humanos e aspectos administrativos da organização, como por exemplo, a influência política da organização e do cliente no projeto.

Observou-se também que muitos fatores de riscos estão intimamente ligados às características do órgão e seu contexto, por exemplo, as constantes alterações na legislação e a adoção da prática de *early-adopter*, confirmando assim a preocupação que se deve considerar as particularidades de cada organização durante a identificação dos riscos. A utilização da Teoria Fundamentada em Dados favoreceu a colaboração ativa dos participantes através do grande envolvimento de cada entrevistado na construção da teoria que considerou essencialmente a análise das evidências fornecidas no lugar do lançamento de hipóteses pré-estabelecidas.

A estratégia adotada na segunda fase da pesquisa para analisar e avaliar os riscos identificados também foi considerada satisfatória. O Método Brasiliano se preocupa em utilizar tanto aspectos objetivos quanto subjetivos para avaliar os riscos, oferecendo assim uma abordagem mais completa de análise. A avaliação da motricidade dos fatores de riscos através de duas ferramentas diferentes (Matriz SWOT e Matriz de Impactos Cruzados) ofereceu mais critérios de análise possibilitando uma melhor priorização dos fatores de riscos críticos a serem tratados. As adaptações realizadas para o cálculo da probabilidade e para a relevância do impacto proporcionaram uma melhor adequação às condições e características da organização. O plano de ação levou em consideração toda a análise realizada favorecendo assim o direcionamento das ações aos fatores considerados prioritários.

5.2. Limitações

O direcionamento dado na primeira fase da pesquisa limitou a identificação dos riscos relacionados apenas aos aspectos negativos. Os riscos chamados “positivos” – oportunidades – não foram relatados.

Pouco foi informado sobre medidas para a composição do plano de ação pelos entrevistados. Naturalmente houve uma concentração maior no levantamento de problemas e dificuldades. Esse fato limitou a participação das opiniões e experiências dos envolvidos na elaboração das ações.

Em relação à avaliação do resultado obtido com a Teoria Fundamentada em Dados, não foi possível a verificação do critério de auditoria “generalidade” (indicativo da abstração necessária da teoria para servir de guia geral sem perder sua relevância), devido à restrição do escopo da pesquisa.

A ausência de Cultura em Gerenciamento de Riscos na organização limitou a identificação de perigos e fatores de riscos ligados essencialmente às atividades operacionais, pouco se conseguindo em relação às influências do âmbito corporativo e os fatores externos.

A Matriz de Impactos Cruzados se confirmou altamente subjetiva dificultando sua execução. Consideráveis divergências foram levantadas em determinados cruzamentos e optou-se pelo consenso da maioria dos envolvidos na análise.

5.3. Conclusões

As Organizações que desenvolvem software, devem ser capazes de implementar, continuamente, a Gestão de Riscos, para prevenir-se dos aspectos críticos associados aos seus negócios. Executar corretamente os processos envolvidos na identificação, análise e tratamento dos riscos do projeto promove a potencialização dos resultados das ocorrências positivas e minimização das consequências negativas. Essa execução deve ser suportada por metodologias - processos, métodos e ferramentas – estruturadas para que o resultado seja adequado, otimizado e confiável.

Assim como em outros estudos [Fontoura 2004, Mielke 2003, Neves 2010, Pinto 2002] foram percebidas questões críticas relacionadas às particularidades e aos aspectos individuais da organização, como fatores de riscos relacionados à legislação, estrutura organizacional, práticas de adoção de tecnologias específicas e capacitação em elaboração de editais. Os resultados desta investigação permitiram identificar que esses fatores sofrem influência de outros fatores, e que o plano de ação deve considerar essas influências.

Os resultados desta pesquisa confirmaram que o desenvolvimento de software é de fato um processo social. Essa constatação pode ser comprovada pela identificação de questões críticas (fatores de riscos) associadas ao relacionamento entre os consultores externos e os membros da organização, nas constantes interferências dos clientes nos projetos, na ausência de alinhamento entre os departamentos da organização, entre outros. A própria construção da teoria - mapeamento dos fatores de riscos – mostrou as diferentes preocupações e prioridades através do ponto de vista de cada um dos entrevistados, e no processo de análise dos riscos, explicitamente na construção da Matriz de Impactos Cruzados, foram notáveis as particularidades e subjetivismos das opiniões dos envolvidos.

5.4. Trabalhos Futuros

Sugere-se para pesquisas futuras:

Ampliar o escopo da pesquisa para analisar todo o Departamento de Tecnologia da Informação da organização. Avaliar individualmente os demais centros (Segurança, Infraestrutura, Administração e Contratos, Segurança da Informação e Arquitetura e Inovação) buscando identificar os fatores de riscos de nível operacional e a influência entre eles, obtendo assim uma visão tática e estratégica de todo o departamento.

Direcionar a pesquisa buscando identificar também as oportunidades (riscos positivos) e a influência de fatores externos à organização, obtendo assim uma visão prospectiva do Gerenciamento dos Riscos.

Avaliar a aplicabilidade dos resultados obtidos pela Teoria Fundamentada em Dados através de um estudo similar em uma organização com características semelhantes buscando comparar os fatores de riscos identificados.

Refinar os fatores de riscos identificados em uma estrutura analítica de riscos (Risk Breakdown Structure) que irá favorecer a elaboração de um processo abrangente para identificar sistematicamente os riscos até um nível consistente de detalhes e contribui para a eficácia e qualidade da identificação de riscos. Um benefício desta abordagem é a classificação dos principais riscos da organização por meio de uma estrutura analítica.

Definir estrutura, política e indicadores de riscos (Risk Driven) baseados em fatores de riscos dinâmicos para auxiliar no suporte à tomada de decisão da organização.

5.5. Trabalhos Relacionados

Nesta seção descrevemos os principais trabalhos relacionados com o escopo desta dissertação. Foram categorizados basicamente em: Relacionados à Identificação e Avaliação de riscos no ambiente de Desenvolvimento de Software e relacionados a uso da Teoria Fundamentada em Dados na Engenharia de Software.

5.5.1. Avaliação de Riscos em Desenvolvimento de Software

Alguns trabalhos relacionados com a identificação e avaliação de riscos em desenvolvimento de software são relatados a seguir.

Fontoura utilizou GQM (Goal Question Metric) para Gerenciar Riscos em Projetos de Software. Em sua pesquisa foi exibido um conjunto dos principais riscos que afetam os projetos de software, elaborado a partir de uma comparação entre os riscos identificados na literatura e utilizou-se a abordagem GQM para serem elaboradas metas visando à eliminação ou a avaliação da existência e monitoramento dos fatores de riscos. [Fontoura 2004]

O A-RISK define um método de gerência de risco. É focado na identificação e quantificação de riscos de prazo de projeto, que pode ser aplicado antes e durante o desenvolvimento do projeto. Para a descoberta desses cenários, foram conduzidas duas pesquisas de campo, uma para a indústria nacional e outra para uma empresa específica, que trouxeram para o método de cálculo de risco a influência dos fatores e seus efeitos nos prazos dos projetos [Machado 2002].

Pinto através de uma revisão da literatura e entrevistas com especialistas de mercado procurou identificar quais os fatores mais relevantes que influenciam o sucesso de projetos de Sistemas de Informação [Pinto 2002].

De maneira semelhante, Mielke através de entrevistas com profissionais do setor privado, procurou identificar os problemas e ações adotadas por empresas da área de tecnologia da informação. [Mielke 2003]

Neves analisou a integração de técnicas de gestão do conhecimento à atividade de análise de riscos em projetos de desenvolvimento de software de micro e pequenas empresas de base tecnológica incubadas.[Neves 2010]

5.5.2. Utilização da Teoria Fundamentada em Dados

Os trabalhos relacionados com o uso da Teoria Fundamentada em Dados na área de Engenharia de Software são relatados a seguir. Nem foram encontradas referências da utilização da TFD na área de Riscos em Desenvolvimento de Software.

Matavire e Brown fazem um levantamento da produção acadêmica da área de Informática que empregam a Teoria Fundamentada em Dados em seus trabalhos publicados em periódicos como Information Technology & People, Journal of Management Information Systems, Information Research e MIS Quarterly [Matavire e Brown 2008].

Orlikowski realizou um dos trabalhos pioneiros na utilização da Teoria Fundamentada em Dados para conduzir investigações na área de software [Orlikowski 1993]. O autor utilizou o método para desenvolver um framework teórico capaz de explicar as questões organizacionais relacionadas à adoção e ao uso de ferramentas CASE (Computer-Aided Software Engineering) em duas organizações de software.

Crabtree apresentou a aplicação do método em um estudo exploratório para investigar como as pessoas descrevem processos de software usando linguagem natural [Crabtree 2009].

Nasirin e outros autores [Nasirin et al. 2003] descrevem a aplicação da TFD para investigar fatores críticos de sucesso na implementação de sistemas de informação geográfica (GIS, do inglês Geographical Information Systems) [Nasirin et al. 2003].

Conte, Cabral e Travassos apresentaram o resultado da aplicação da Teoria Fundamentada em Dados na análise qualitativa de um estudo de observação em Engenharia de Software, visando compreender o processo de aplicação de uma técnica de inspeção de usabilidade em aplicações Web [Conte et al. 2009].

Montoni relata a aplicação da Teoria Fundamentada em Dados para investigar os fatores críticos de sucesso em iniciativas de melhoria de processos de software [Montoni 2010].

Referências

[Adolph et al 2008] ADOLPH, S., HALL, W., KRUCHTEN, P., 2008, "*A methodological leg to stand on: Lessons learned using grounded theory to study software development*", pp. IBM Toronto Software Lab.; IBM Centers for Advanced Studies, CAS, Richmond Hill, ON, Canada.

[Alencar e Viera 2003] ALENCAR, A.; VIEIRA, L. A Informática, a Informação Pública a Terceirização de Serviços: Uma Questão Estratégica.

[Bandeira e Souza 2003] BANDEIRA-DE-MELLO, R., CUNHA, C., 2003, "Operacionalizando o método da *Grounded Theory* nas Pesquisas em Estratégia: técnicas e procedimentos de análise com apoio do software ATLAS/TI", Curitiba, Brazil.

[Bandeira e Souza 2006] BANDEIRA-DE-MELLO, R., CUNHA, C., 2006, "*Grounded Theory*". In: GODOI, C.K., BANDEIRA-DE-MELLO, R., SILVA, A.B.D. (eds), Pesquisa Qualitativa em Estudos Organizacionais: Paradigmas, Estratégias e Métodos, São Paulo, Saraiva.

[Bauer 1969] BAUER, L. FRIEDRICH. NATO Conference on Software Engineering 1968. Disponível em: http://homepages.cs.ncl.ac.uk/brian.randell/NATO/

[Bertelsen 1997] BERTELSEN, O.W., 1997, "*Toward a unified field of SE research and practice*", IEEE Software, v. 14, n. 6, pp. 87-88.

[Biffl et al. 2006] BIFFL, S., AURUM, A., BOEHM, B., et al., 2006, *Value-Based Software Engineering*, 1 ed.,Springer.

[Biolchini et al. 2005] BIOLCHINI, J., MIAN, P., NATALI, A.C., et al., 2005, *Systematic Review in Software Engineerin*g, RT-ES 679/05, COPPE/UFRJ, Rio de Janeiro, RJ, Brasil.

[Boehm 1991] Boehm, B. W. (1991) *Software Risk Management: Principles and Practices*, IEEE Software, Volume 8. No1. pp 32-40.

[Boehm et al 2004] Boehm, B. W.; Brown, A. W; Basili, V; Turner, R. (2004) *Spiral Acquisition of Software-Intensive Systems of Systems, Cross talh – The Journal of Defense Software Engineering*, DoD – Department of Defense. pp 4-9.

[Brasiliano 2009] BRASILIANO, C. Antonio. (2009) Método Brasiliano Avançado – Gestão e Análise de Risco Corporativo. Sicurezza.

[Carr 1993] Carr, M. J., Konda, S.L., Monarch, I., Ulrich, F. C., Walker, C. F. (1993) *Taxonomy Based Risk Identification*. Tecnical Report CMU/SEI-93-TR-6. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. USA.

[Carvalho et al. 2003] CARVALHO, L., SCOTT, L., JEFFERY, R., 2003, *Exploring the use of Techniques from Grounded Theory in Process Engineering, 03/1, Centre for Advanced Software Engineering Research* (CAESER), Sydney, Australia.

[CGEE 2011] Centro de Gestão e Estudos Estratégicos: Acessado em Dezembro de 2010. Disponível em:
http://www.cgee.org.br/prospeccao/index.php?operacao=Exibir&serv=textos/topicos/texto_exib&tto_id=4&tex_id=1

[Charette 2001] Charette, R. (2001*) Implementing Risk Management Best Practices*. Carole Edrich.

[Creswell 2003] CRESWELL, J.W., 2003, *Research Design: Qualitative, Quantitative, and Mixed Methods Approache*s, 2nd ed. Beverly Hills, CA, Sage.

[Clemen 1991] Clemen, R. (1991) Making Hard Decision. I*ntroduction to decision Analysis*. Belmont, CA: Wadsworth.

[Coelho 2004] Coelho, P. G. (2004) Identificação das Estratégias de Aprendizado utilizadas pelos PMP´s e Aspirantes a Certificação PMP. Projeto PMK – Environment Learning. CIn/UFPE – Centro de Informática – Universidade Federal de Pernambuco.

[Coleman e O'Connor 2008] COLEMAN, G., O'CONNOR, R., 2008, "*Investigating software process in practice: A grounded theory perspective*", Journal of Systems and Software, v. 81, n. 5, pp. 772-784.

[Corbin 1998] CORBIN, J.M., 1998, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, 2nd ed., Sage Publications.

[COSO 2004] Committee of Sponsoring Organizations. (2004). *Enterprise Risk Management — Integrated Framework.*

[Cote et al. 2009] CONTE, T., CABRAL, R., TRAVASSOS, G.H., 2009, "Aplicando Grounded Theory na Análise Qualitativa de um Estudo de Observação em Engenharia de Software – Um Relato de Experiência". In: V Workshop Um Olhar Sociotécnico sobre a Engenharia de Software – WOSES, pp. 26-37.

[Crabtree 2009] CRABTREE, C.A., SEAMAN, C.B., NORCIO, A.F., 2009, "*Exploring language in software process elicitation: A grounded theory approach*", IEEE Computer Society.

[Cukierman 2006] CUKIERMAN, H., TEIXEIRA, C. A. N., RUBERG, N., 2006. "Apresentação". In: WOSES 2006 Um Olhar Sociotécnico sobre a Engenharia de Software., pp. iii-iv, Vila Velha, Brasil

[De Marco 1997] De Marco, T. (1997) *The Deadline: A Novel About Project Management*. Nova Iorque: Dorset House Publishing.

[Duchscher e Morgan 2004] DUCHSCHER, J.E.B., MORGAN, D., 2004, "*Grounded theory: reflections on the emergence vs. forcing debate*", Journal of Advanced Nursing, v. 48, n. 6, pp. 605-612.

[Ferreira 2010] FERREIRA, R. Roni, Minimizando riscos na terceirização. disponível em: http://www1.serpro.gov.br/publicacoes/tema/171/materia12.htm . Acessado em janeiro de 2010.

[Flick, 1998] FLICK, U. *An introduction to qualitive research*. London: Sage. 1998

[Fontoura 2004] FONTOURA, M. Lisandra Usando GQM para Gerenciar Riscos em Projetos de Software. 18º Simpósio Brasileiro de Engenharia de Software. Acessado em dezembro de 2001. Disponível em: http://www.lbd.dcc.ufmg.br:8080/colecoes/sbes/2004/004.pdf

[Freitas 2002] FREITAS, S. C. Roberto. “Gestão de Risco: Possibilidades de Utilização pelo Setor Público e por Entidades de Fiscalização Superior”. Revista do Tribunal de Contas da União. R. TCU. Brasília. V.33, n.93. jul/st 2002. Disponível em: https://acessoseguro.tcu.gov.br/portal/pls/portal/docs/683666.PDF

[Glass et al. 2002] GLASS, R.L., VESSEY, I., RAMESH, V., 2002, "*Research in software engineering: An analysis of the literature*", Information and Software Technology, v. 44, n. 8, pp. 491-506.

[Glaser e Straus 1967] GLASER, B.G., STRAUSS, A., 1967, *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago / Illinois, Aldine.

[Glaser 1992] GLASER, B.G., 1992, *Basics of Grounded Theory Analysis: Emergence vs Forcing*, Sociology Press.

[Greg Shipley 2010] http://www.networkcomputing.com/people/gshipley.html

[Grey 1995] Grey, S. (1995) *Practical Risk Assessment for Project Management*. John Wiley & Sons.

[Goulding 1999] GOULDING, C., 1999, "*Grounded Theory: Some Reflections on Paradigm, Procedures and Misconceptions*", Management Research Centre, University of Wolverhampton, WP006/99.

[Gusmão et al 2005] Gusmão, C.M.G. et al. (2005) “Ontologia de Domínio de Riscos”, In Suppera Solutions Relatório Técnico, Centro de Informática, Universidade Federal de Pernambuco, Recife, Brasil.

[Gusmão 2007] Gusmão, C (2007) Um Modelo de Processo de Gestão de Riscos para Ambientes de Múltiplos Projetos de Desenvolvimento de Software. Tese de Doutorado. Universidade Federal de Pernambuco. Recife – PE, Brasil.

[Gusmão e Moura 2004] Gusmão, C. M. G.; Moura, H. P. (2004) Gerência de Risco em Processos de Qualidade de Software: uma Análise Comparativa. Anais do III Simpósio Brasileiro de Qualidade de Software. Brasília – DF – Brasil.

[Heldman 2005] Heldman, K. (2005) *Project Manager's Spotlight on Risk Managament. Harbor Light Press*. Sybex Inc. San Francisco. USA.

[Hevner e March 2003] HEVNER, A.R., MARCH, S.T., 2003, "*The Information Systems Research Cycle*", IEEE Computer Society Press, v. 36, n. 11, pp. 111-113.

[Higuera 1994] Higuera, P.R. (1994) *An Introduction to Team Risk Management, Technical Report*. Software Engineering Institute, Carnegie Mellon University. USA.

[Holloway 1997] Holloway, I. (1997) *Basic Concepts for Qualitative Research*. Oxford Blackwell Science, Oxford. Reino Unido.

[ISO 31000 2009] ISO / IEC 31000. (2009) ISO *Risk management -- Principles and guidelines.* International Standard Organization – ISO / IEC

[Keelling 2002] Keelling, R. (2002) Gestão de Projetos: Uma abordagem global . Ed. Saraiva: São Paulo.

[Kruchten 2003] Kruchten, P. (2003) Introdução ao Rup: Rational Unified Process. 2ª Ed. Ciência Moderna. São Paulo. pp 25-36.

[Leopoldino 2004] Leopoldino, C. B. (2004) Avaliação de Riscos em Desenvolvimento de Software. Dissertação de Mestrado. Universidade Federal do Rio Grande do Sul – Escola de Administração. Porto Alegre. Brasil.

[Locke 2001] LOCKE, K., 2001, *Grounded Theory in Management Research* London, Sage.

[Machado 2002] MACHADO, F. A. Cristina (2002). A-RISK: Um Método para Identificar e Quantificar Riscos de Prazo em Projetos de Software. Dissertação de Mestrado. Curso de pós-graduação em Informática Aplicada - PPGIA, Centro de Ciências Exatas e de Tecnologia - CCET, Pontifícia Universidade Católica do Paraná - PUCPR.

[Matavire e Brown 2008] MATAVIRE, R., BROWN, I., 2008, "*Investigating the use of "Grounded Theory*" in information systems research", ACM, Wilderness, South Africa.

[Mielke 2003] MIELKE, R. Eduardo. Fatores de Riscos em Administração de Projetos: Visões e Ações no Desenvolvimento de Software. Dissertação submetida ao Programa de Pós-Graduação em Administração da Universidade Federal do Rio Grande do Sul.

[Myers 1997] MYERS, M.D., 1997, "*Qualitative research in information systems*", MIS Quarterly: Management Information Systems, v. 21, n. 2, pp. 241-242.

[Montoni 2010] UMA INVESTIGAÇÃO SOBRE OS FATORES CRÍTICOS DE SUCESSO EM INICIATIVAS DE MELHORIA DE PROCESSOS DE SOFTWARE. Montoni, Mariano Angel. Tese de doutorado. Programa de Pós-graduação em Engenharia de Sistemas e Computação, COPPE, da Universidade Federal do Rio de Janeiro

[Morse e Richards 2002] MORSE, J.M., RICHARDS, L., 2002, *README FIRST for a User's Guide to Qualitative Methods*, Sage Publications.

[Moynihan 1997] Moynihan, T. (1997) *How experienced Project Managers* Access Risk. IEEE Software. Volume 14. Nº 3. 35-41.

[Nasirin et al. 2003] NASIRIN, S., BIRKS, D.F., JONES, B., 2003, "*Re-examining fundamental GIS implementation constructs through the grounded theory approach*", Telematics and Informatics, v. 20, n. 4, pp. 331-347.

[Neves 2010] NEVES, M. Sandra. "Análise de Riscos em Projetos de Desenvolvimento de Software por Meio de Técnicas de Gestão do Conhecimento.". Dissertação submetida ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de Itajubá.

[Niazi et al 2007] NIAZI, M., WILSON, D., ZOWGHI, D., 2006, "*Critical success factors for software process improvement implementation: An empirical study*", Software Process Improvement and Practice, v. 11, n. 2, pp. 193-211.

[Oliveira e Santos 2006] OLIVEIRA, C. Francisco, SANTOS, L. Joselias, Fatores de riscos associados à terceirização de TI no setor público Francisco Correia de Oliveira. Universidade de Fortaleza (UNIFOR), Mestrado em Administração, Fortaleza – CE, Brasil

[Orlikowski 1993] ORLIKOWSKI, W.J., 1993, "*CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development*", Management Information Systems Quarterly, v. 17, n. 3.

[Pandit 1996] PANDIT, N.R., 1996, "*The Creation of Theory: A Recent Application of the Grounded Theory Method*", The Qualitative Report, v. 2, n. 4 (December).

[Pinto 2002] PINTO, O. A. Sérgio. Gerenciamento de Projetos: Análise dos Fatores de Risco que influenciam o sucesso de projetos de Sistemas de Informação. Dissertação de Mestrado. Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo.

[Pratico 2010] PRATICO, Processo de aquisição de produtos e serviços de tecnologia da informação: Aplicação no estado de MG (PrATIco). Disponível em http://www.synergia.dcc.ufmg.br/pratico. Acessado em setembro de 2010

[Pressman 2006] Pressman, R. S. (2006) Engenharia de Software. 6ª edição. São Paulo: McGraw-Hill. Pp 577-595.

[Ragin 1994] RAGIN, C., 1994, *Constructing Social Research* Beverly Hills, CA, Sage.

[RIMS 2008] RMM - Risk Matury Model. (2008). The Risk Management Society. Disponível em: http://www.rims.org/erm/pages/RiskMaturityModel.aspx.

[Rovai 2005] ROVAI L. RICARDO, (2005) Modelo Estruturado para Gestão de Riscos em Projetos: Estudo de Múltiplos Casos. Tese de Doutorado. Escola Politécnica da Universidade de São Paulo. São Paulo, Brasil.

[Santana e Xisto 2009] SANTANA, Hyago. XISTO, Railan. Visão da Gerencia de Riscos na Engenharia de Software. Artigo disponível em: http://eng-softwares.blogspot.com/2009/07/visao-da-gerenca-de-riscos-na.html

[Schots 2010] SCHOTS, N.C.L., 2010, Uma Abordagem para a Identificação de Causas de Problemas Utilizando Grounded Theory, Tese de M.Sc., COPPE, UFRJ, Rio de Janeiro.

[Seaman 1999] SEAMAN, C.B., 1999, "*Qualitative methods in empirical studies of software engineering*", IEEE Transactions on Software Engineering, v. 25, n. 4, pp. 557-572.

[SEI 2001] SEI - Software Engineering Institute. (2001) CMMI - Capability Maturity Model Integration version 1.1 Pittsburgh, PA. Software Engineering Institute, Carnegie Mellon University. USA.

[Silva 2004] SILVA, A. F. da. Gestão estratégica na informática pública – um fator crítico de sucesso para os governos do século XXI. 2004, 177f. Dissertação (Mestrado). Universidade de Fortaleza – UNIFOR, CMA, 2004.

[Sommerville 2003] Sommerville, I. (2003) Engenharia de Software. São Paulo: Addison Wesley, Brasil.

[Souza 2006] Souza, F. C. (2006) Análise da Gerência de Riscos: Fator de Desenvolvimento Econômico na área de Serviços de Desenvolvimento de Software em Pernambuco. Trabalho de Conclusão de Curso. Curso de Sistemas de Informação. Faculdade Integrada do Recife.

[Standish Group 2009] The Standish Groupa – Chaos Report 2009. Disponível em: http://www1.standishgroup.com/newsroom/chaos_2009.php

[Strauss 1987] STRAUSS, A., 1987, Qualitative Analysis for Social Sciences, Cambridge University Press.

[Strauss e Corbin 1997] STRAUSS, A., CORBIN, J.M., 1998, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, 2nd ed., Sage Publications.

[Suddaby 2006] SUDDABY, R., 2006, "*From the Editors: What Grounded Theory is Not*", Academy of Management Journal, v. 49, n. 4, pp. 633-642.

[TCU 2010] Segurança da Informação – Boas Práticas. Disponível em: http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/boas_praticas

[TenStep 2009] Project Risk Factors Checklist. Disponível em: http://www.tenstep.com/open/7.0ManageRisk.html

[PMBOK 2009] PMI - Project Management Institute. (2009) *A Guide to the Project Management Body of Knowledge*. Project Management Institute. Four Campus Boulevard. Newtown Square. USA

[PMI 2006] PMI - Project Management Institute. (2006*) Best approach to identify risks results*. Disponível em: http://www.pmi.org.

[PMI 2009] PMI - Project Management Institute. (2009) A Guide to the Project Management Body of Knowledge.. Project Management Institute. Four Campus Boulevard. Newtown Square. USA.

[Taipale et al 2007] TAIPALE, O., KARHU, K., SMOLANDER, K., 2007. *"Observing Software Testing Practice from the Viewpoint of Organizations and Knowledge Management*". In: Proceedings of the First International Symposium on Empirical Software Engineering and Measurement, pp. 21 – 30

[Victoria et al 2000] Victoria, C.G. et al. (2000) Pesquisa Qualitativa em Saúde: uma introdução ao tema. Porto Alegre: Tomo Editorial. pp. 33 – 78.

[Viera, 2004] VIEIRA, Marcelo Milano Falcão. ZOUAIN, Deborah Moraes. Pesquisa Qualitativa em Administração. Rio De Janeiro: FGV. 2004

[Webster 2005] Webster, K. P. B. et al. (2005) Taxonomia de Riscos para Manutenção de Software. In Anais do IV Simpósio Brasileiro de Qualidade de Software. Porto Alegre – RS – Brasil.

[YIN 2003] YIN, R.K., 2003, *Case Study Research: Design and Methods*, 3rd ed. London, SAGE Publications.

Anexo I

Plano de Ação	*Groundness*
[PA01] Realizar reuniões para validar requisitos	3
[PA02] Fortalecer a gestão de contratos	2
[PA03] Planejar e agendar a implantação dos sistemas	2
[PA04] Utilização de métricas para estimar esforço	1
[PA05] Institucionalizar equipe de testes	4
[PA06] Implantar políticas e diretrizes de TI únicas para a organização	1
[PA07] Definir e institucionalizar metodologia para desenvolvimento de sistemas	4
[PA08] Institucionalizar processo de Análise e Modelagem de negócio	1
[PA09] Implantar a Gestão de Conhecimento	2
[PA10] Definição de equipe responsável por realizar *refactoring* em projetos	1
[PA11] Institucionalizar equipe responsável por melhorias em sistemas já desenvolvidos	1
[PA12] Institucionalizar Equipe de SQA	2

Tabela 19: TFD - Categorias de "Plano de Ação"

Achado de Risco	*Groundness*	*Density*
[A01] Os requisitos não são formalizados	2	1
[A02] Não conseguimos provar as solicitações dos clientes	1	1
[A03] Solicitações de mudanças são frequentes	1	1
[A04] Existe uma alta rotatividade de membros da equipe	2	1
[A05] Falta de homologação efetiva em alguns projetos	2	1

[A06] Dificuldade em realizar integrações em sistemas legados devido a tecnologias desconhecidas e falta de documentação	2	2
[A07] Falta de documentação dos sistemas	4	2
[A08] Falta de compartilhamento de informações entre equipes	1	1
[A09] Inexistência de ambiente de homologação para alguns projetos	1	1
[A10] Requisitos incompletes	3	1
[A11] Documentação não reflete as necessidades dos clientes	1	1
[A12] Ambientes de desenvolvimento e homologação não são consistentes	1	1
[A13] Ajustes feitos diretamente no ambiente de produção ocasionam problemas	1	2
[A14] Má qualidade do código entregue pelas Fábricas de Software prejudica manutenção	2	2
[A15] Prática de *early-adopter* aumenta a curva de aprendizado	1	1
[A16] Inexistência de processo para implantação dos sistemas	4	1
[A17] Disponibilidade de recursos para realizar implantação dos sistemas	1	1
[A18] Ausência de padrão de codificação	6	1
[A19] Cronogramas com metas irreais	2	2
[A20] Ausência de equipe e processo de testes	6	2
[A21] Consultores externos acessam dados sigilosos	2	1
[A22] Má qualidade do código entregue pelas Fábricas de Software ocasiona retrabalho	1	1
[A23] Requisitos mal definidos	2	1
[A24] Requisitos instáveis	3	2
[A25] Decisões erradas na arquitetura do sistema por causa de requisitos mal especificados	1	2

[A26] Prazos são definidos de cima para baixo sem participação da equipe	1	3
[A27] Confiabilidade do sistema é comprometida pela falta de qualidade de código das Fábricas de Software	1	1
[A28] Mais de uma unidade administrativa na organização com a finalidade de prover serviços de TI	1	1
[A29] Inexistência de uma metodologia de desenvolvimento de software única	6	1
[A30] Papeis e responsabilidades não estão claramente definidos	1	1
[A31] Contratos de prestação de serviço mal elaborados não permitem a punição de erros das Fábricas de Software	1	1
[A32] Falta de conhecimento dos domínios / negócios para quais as aplicações são construídas	1	1
[A33] Inexistência do processo de Análise e Modelagem de Negócio compromete a adequabilidade dos sistemas	2	1
[A34] Ausência de Analistas de negócio dificultam o entendimento do negócio	1	1
[A35] Necessidades de desenvolvimento emergenciais comprometem a qualidade dos testes	1	1
[A36] Necessidades de desenvolvimento emergenciais comprometem a validação dos requisitos	1	1
[A37] Necessidades de desenvolvimento emergenciais comprometem a elaboração de documentação técnica	1	1
[A38] Ciclo vicioso de situações emergenciais	1	3
[A39] Falta de tempo disponível para levantamento de requisitos	1	1
[A40] Falta de treinamentos adequados	3	1
[A41] Grande dependência técnica dos consultores externos	3	2
[A42] Perda do conhecimento técnico durante a rotatividade dos consultores externos	1	3

[A43] Falta de tempo para preparação de ambiente de testes	1	2
[A44] Ausência de equipe responsável pela documentação dos sistemas não tributários	1	2
[A45] Alto custo de manutenção de sistemas retroalimenta situações emergenciais	1	1
[A46] Tratamento de problemas é sempre feito de forma reativa	1	1
[A47] Recebemos sistemas desenvolvidos em outros departamentos para dar suporte	1	1
[A48] Muito tempo é gasto com manutenção corretiva	1	3
[A49] Documento de requisitos sem padrão, uns com muitos detalhes outros sem	1	1
[A50] Grande esforço com engenharia reversa para obter uma documentação consistente	1	2
[A51] Inexistência de ambiente de testes	1	1
[A52] Falta de alinhamento entre o planejamento da CAT e DTI	1	3
[A53] Muitas alterações em leis, decretos e resoluções acarretam mudanças não programadas nos sistemas	1	1
[A54] Problema com versionamento devido à dependência de consultores externos	1	2
[A55] Não temos uma visão completa dos projetos além da codificação	1	1
[A56] Pouca visibilidade sobre a condução dos projetos	1	1
[A57] Inexistência de processo de controle dos requisitos	2	1
[A58] Não existe formalização da arquitetura do sistema	2	
[A59] Falta de processos para inspeção de código gera muito retrabalho e sobrecarrega os testes	1	1
[A60] Procedimento para colocar os sistemas em produção é manual ocasionando muitos erros	1	1
[A61] Inexistência de um processo formal de Controle de	1	1

Versões		
[A62] Testes são feitos pelo próprio desenvolvedor prejudicando a qualidade e cobertura dos mesmos	1	2
[A63] A estabilização dos requisitos demora mais tempo que a média do mercado	1	2
[A64] Processo de contratação muito engessado dificultando a penalização dos fornecedores	1	1
[A65] Documentação gerada pelas Fábricas de Software possui muitos erros e não seguem uma padronização	1	1
[A66] Documentação deficiente das Fábricas de software gera revisões muito demoradas	1	1
[A67] Sistemas entregues pelas Fábricas contém muitos erros primários	1	2
[A68] Inexistências de testes de regressão aumentam a possibilidade de erros colaterais que não são identificados	1	1
[A69] É comum as fábricas de software corrigirem erros apenas de forma reativa	1	1
[A70] Testes realizados pelos usuários são sobrecarregados devidos a grande quantidade de erros gerados pelas Fábricas de Software	1	3
[A71] Altos custos de manutenção de sistemas devido ao mal planejamento	1	1

Tabela 20: TFD – Categorias de "Achados de Risco"

Por ser uma categoria abstrata, não possuindo citação direta dos textos analisados, o valor "*groundedness*" foi omitido.

Fator de Risco	*Density*	Achados de Riscos Relacionados
[FR01] Ausência de processo formal de Gestão de Requisitos	14	[A01], [A02], [A07], [A10], [A11], [A23],

		[A24], [A25], [A49], [A48], [A57], [A63]
[FR02] Constantes alterações na legislação	7	[A03], [A24], [A38], [A52] [A53], [A63]
[FR03] Alta rotatividade de pessoas	3	[A04], [A42]
[FR04] Ausência de processo formal de Homologação	6	[A05] [A09]
[FR05] Sistemas legados sem documentação	6	[A06], [A50]
[FR06] Sistemas legados desenvolvidos em plataformas não conhecidas pela equipe	4	[A06]
[FR07] Ausência de práticas de documentação dos sistemas	6	[A50], [A07]
[FR08] Ausência de processo de Gestão do Conhecimento	3	[A08], [A41], [A42]
[FR09] Ausência de ambientes de homologação consistentes	5	[A12], [A13],
[FR10] Ausência de processo de Implantação de Sistemas	2	[A13], [A16], [A60]
[FR11] Adoção da prática de *early-adopter*[1]	1	[A15]
[FR12] Baixa Qualidade de código e Documentação das Fábricas de Software	5	[A14], [A27], [A48], [A65], [A66], [A67], [A69], [A70]
[FR13] Falta de alinhamento entre Áreas clientes e DTI	10	[A52]
[FR14] Ausência de Padrão de Codificação	5	[A14], [A18], [A22]
[FR15] Ausência de processo de Gestão de Projetos	10	[A19], [A26], [A38], [A46], [A52], [A55], [A56], [A71]
[FR16] Constantes interferências do cliente na definição do cronograma	10	[A19], [A26], [A35], [A36], [A37], [A38], [A39], [A43]
[FR17] Ausência de processo de Testes	7	[A20], [A43], [A51], [A48], [A59], [A62], [A67], [A68], [A70]
[FR18] Ausência de procedimentos de Controle de Acesso	1	[A21]

[FR19] Ausência de práticas em Arquitetura de Software	2	[A25], [A58]
[FR20] Existência de outras unidades administrativas que desenvolvem software	4	[A28], [A47]
[FR21] Ausência de definição de papéis e responsabilidades	3[1]	[A30]
[FR22] Ausência de uma metodologia de desenvolvimento de software	10	[A29], [A45], [A59]
[FR23] Falta de capacitação na elaboração de editais	2	[A31], [A64]
[FR24] Ausência de processo de Análise e Modelagem de Negócios	5	[A32], [A33]
[FR25] Política de treinamento insuficiente	4	[A40]
[FR26] Dependência técnica de Consultores Externos	2	[A41], [A42], [A54]
[FR27] Ausência de processo de Requisitos para área não tributária	6	[A44]
[FR28] Processo de Controle de Configuração insuficiente	3	[A54], [A61]
[FR29] Ausência de equipe de Implantação de Sistemas formada e capacitada	2	[A17]
[FR30] Ausência de equipe de Testes formada e capacitada	7	[A20], [A62], [A70]
[FR31] Ausência de equipe de Análise e Modelagem de Negócios formada e capacitada	5	[A34]
[FR32] Ausência de equipe de Requisitos para área não tributária formada e capacitada	6	[A44]

Tabela 21: TFD – Categorias de "Fator de Risco"

Por ser a categoria mais abstrata dos dados e possuir valores de "groundedness" e "density" iguais a zero foram apresentados apenas os Fatores de Riscos de relacionados.

[1] *Early-adopter*: Prática em aderir, testas e divulgar novas tecnologias ainda não lançadas oficialmente no mercado

Perigo	Fatores de Riscos Relacionados
[P01] Sistemas não atendem às expectativas do cliente	[FR01], [FR02], [FR04], [FR07], [FR09], [FR15], [FR13], [FR16], [FR17], [FR21], [FR22], [FR24], [FR27], [FR30], [FR31], [FR32]
[P02] Retrabalho	[FR01], [FR02], [FR05], [FR07], [FR08], [FR12], [FR15], [FR13], [FR14], [FR16], [FR17], [FR19], [FR20], [FR22], [FR24], [FR27] [FR28], [FR30], [FR31], [FR32]
[P03] Perda do conhecimento técnico e do negócio	[FR01], [FR03], [FR05], [FR07], [FR08], [FR15], [FR20], [FR24], [FR26], [FR31]
[P04] Fuga de informação	[FR03], [FR18], [FR26]
[P05] Alto custo em manutenção dos sistemas	[FR01], [FR05], [FR06], [FR07], [FR12], [FR14], [FR13], [FR16], [FR17], [FR19], [FR20], [FR22], [FR25], [FR27], [FR30], [FR32]
[P06] Alto custo em engenharia reversa	[FR01], [FR02], [FR05], [FR06], [FR07], [FR14], [FR22]
[P07] Problemas e não conformidades detectados apenas em produção	[FR01], [FR04], [FR07], [FR09], [FR13], [FR15], [FR16], [FR17], [FR24], [FR27], [FR30], [FR31], [FR32]
[P08] Alto índice de erros nos sistemas	[FR01], [FR04], [FR12], [FR14], [FR16], [FR17], [FR22], [FR25], [FR30]
[P09] Aumento da curva de aprendizado na adoção de novas tecnologias	[FR08], [FR11]
[P10] Perda da motivação da equipe	[FR01], [FR02], [FR03], [FR04], [FR13], [FR16], [FR21], [FR25]
[P11] Estimativas de tempo e prazo irreais	[FR01], [FR02], [FR15], [FR13],

	[FR16], [FR22]
[P12] Requisitos mal entendidos e/ou definidos	[FR01], [FR02], [FR15], [FR13], [FR16], [FR22], [FR24], [FR27] [FR31], [FR32]
[P13] Gerenciamento impróprio de mudanças	[FR01], [FR02], [FR05], [FR06], [FR09], [FR10], [FR13], [FR15], [FR16], [FR22], [FR28], [FR29]
[P14] Indisponibilidade de sistemas durante a implantação	[FR10], [FR28], [FR09],[FR29]
[P15] Sistemas com baixa qualidade e confiabilidade	[FR01], [FR02], [FR04], [FR05], [FR06], [FR09], [FR12], [FR14], [FR15], [FR13], [FR16], [FR17], [FR22], [FR22], [FR25], [FR30]
[P16] Transferência de responsabilidades	[FR01], [FR04], [FR15], [FR13], [FR20], [FR21], [FR23], [FR27], [FR32]
[P17] Alto custo com Fábricas de Software	[FR01], [FR12], [FR15], [FR17], [FR22], [FR23], [FR30]

Tabela 22: TFD – Categorias de "Perigo"

Anexo II

Diagramas de Causa e Efeito dos perigos identificados com as motricidades de cada fator de risco calculadas a partir da Matriz SWOT.

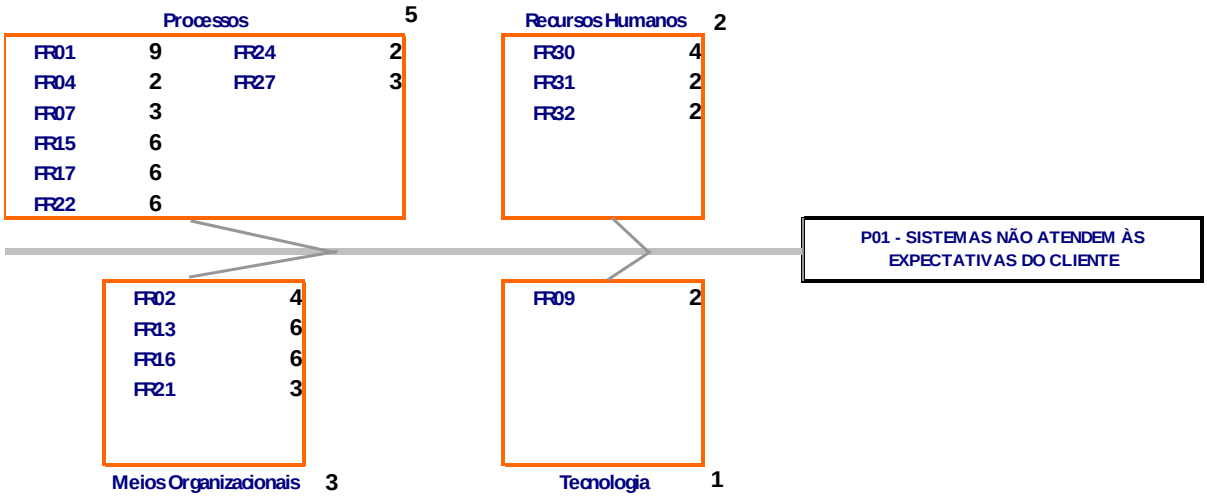

Figura 27: P01 – Diagrama de Causa e Efeito

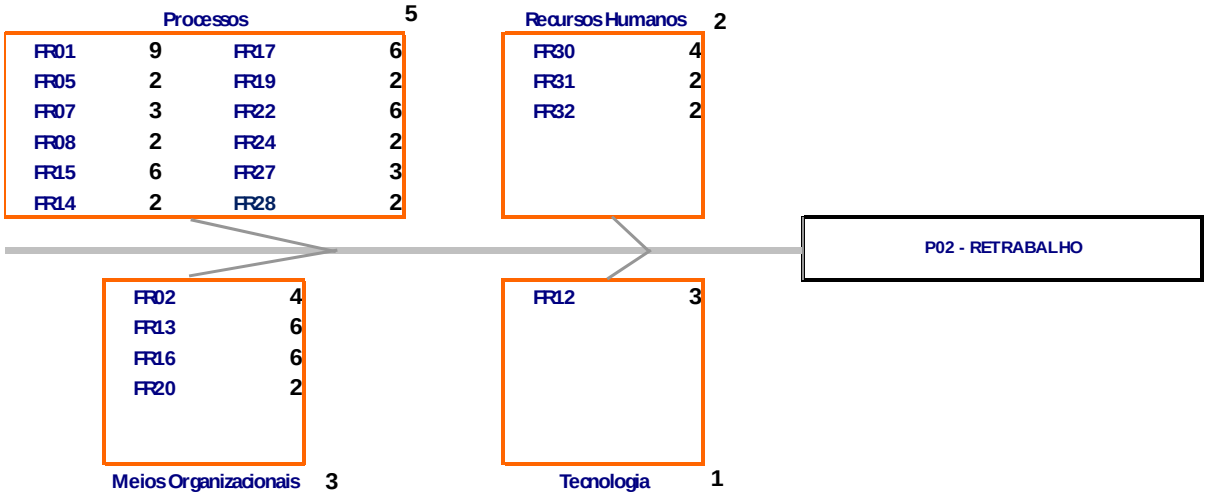

Figura 28: P02 – Diagrama de Causa e Efeito

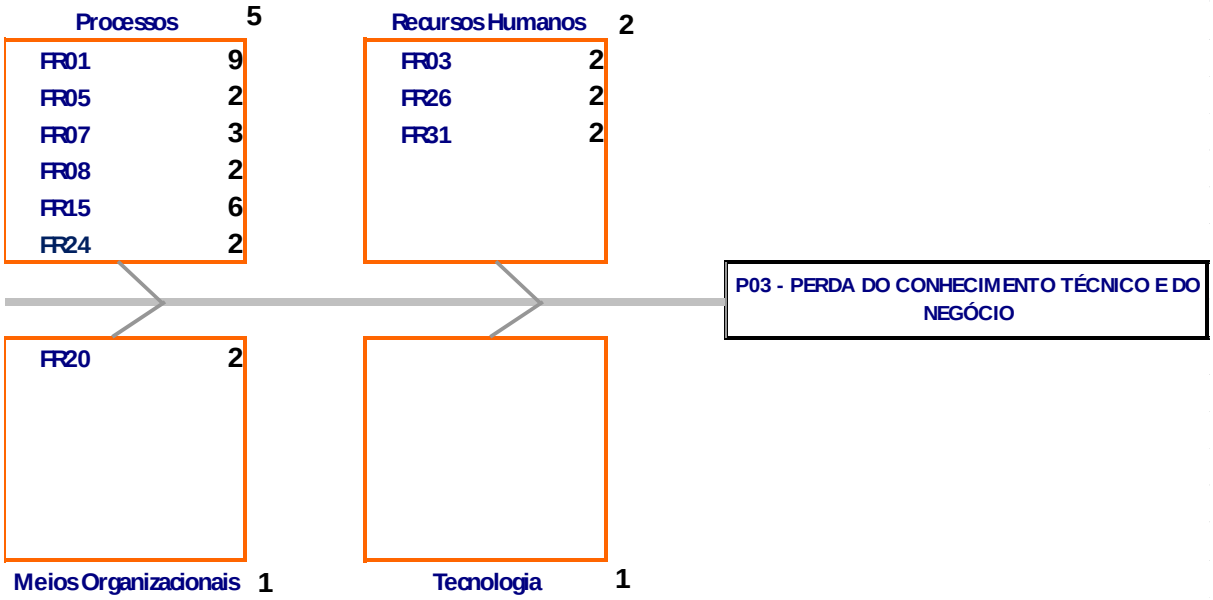

Figura 29: P03 – Diagrama de Causa e Efeito

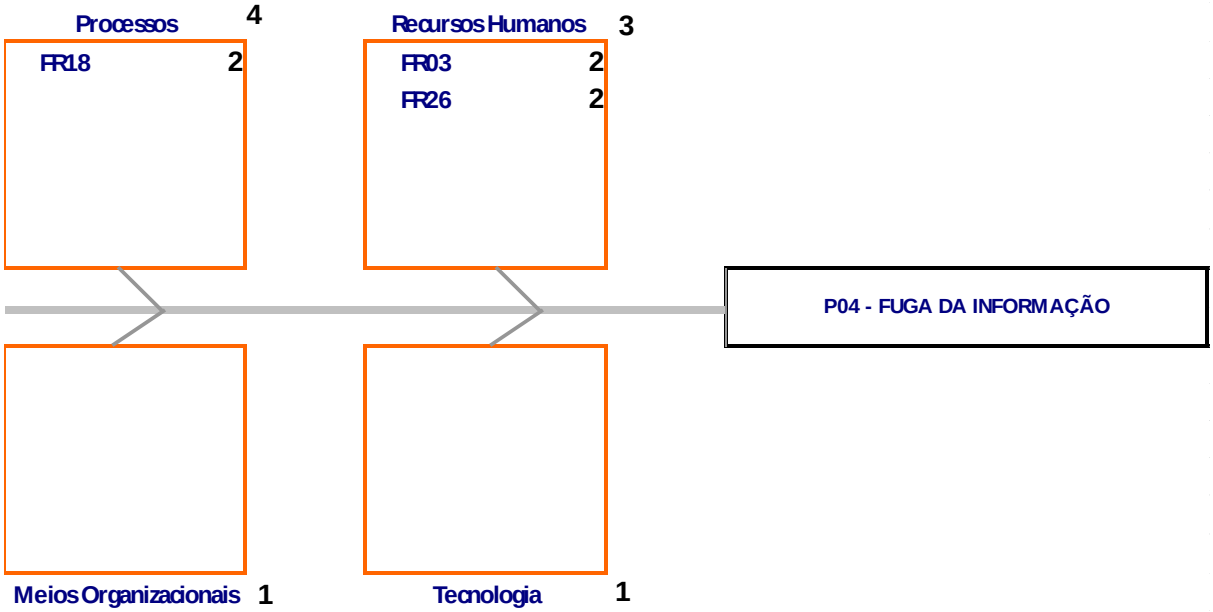

Figura 30: P04 – Diagrama de Causa e Efeito

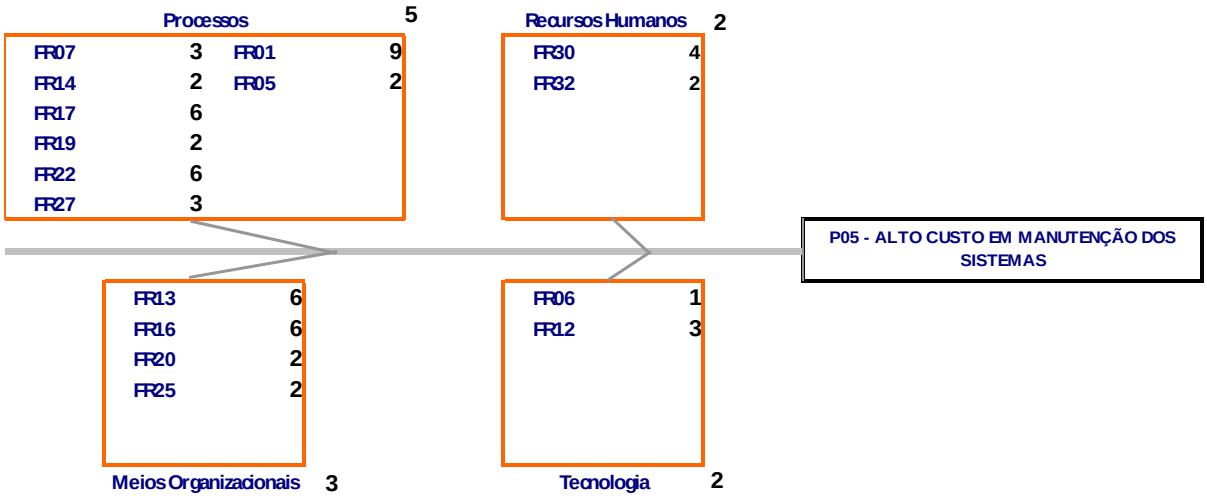

Figura 31: P05 – Diagrama de Causa e Efeito

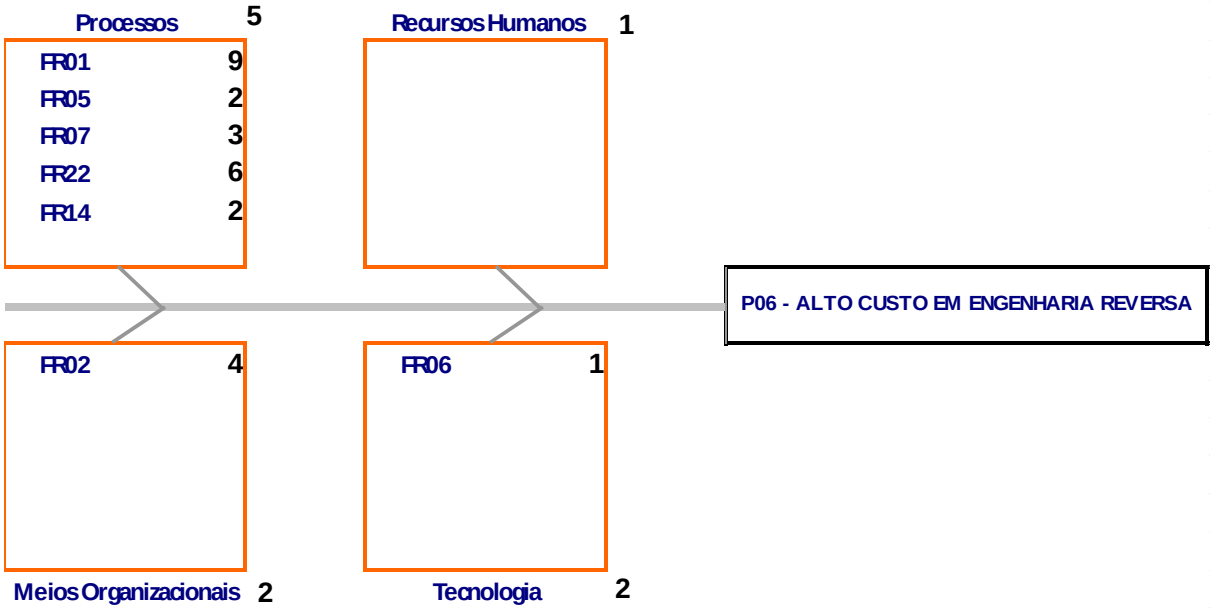

Figura 32: P06 – Diagrama de Causa e Efeito

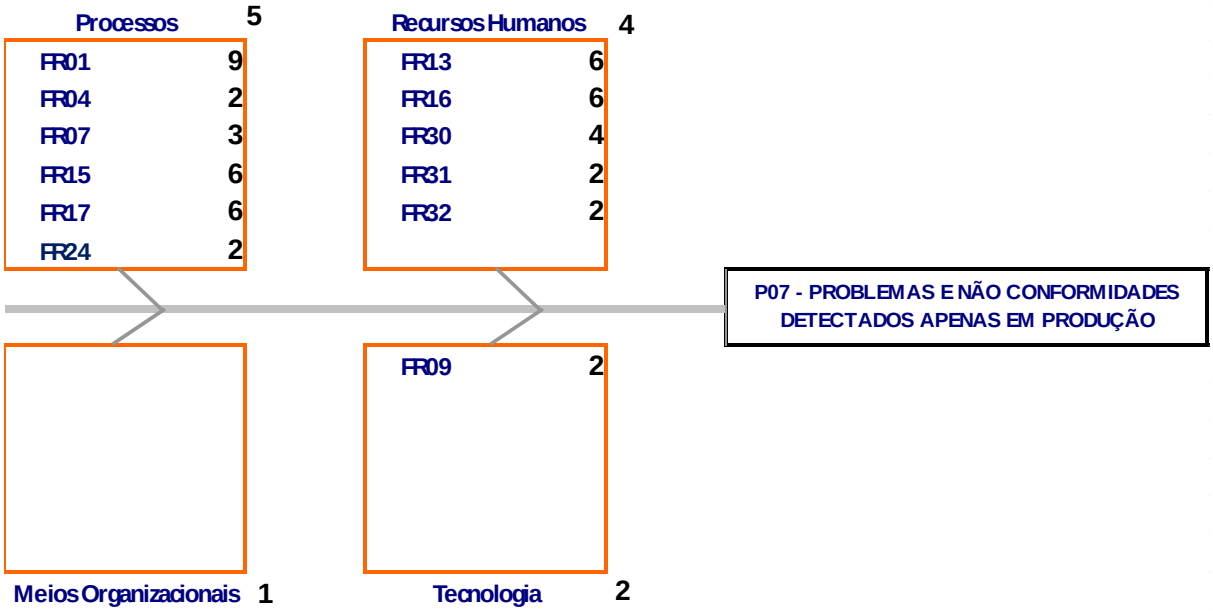

Figura 33: P07 – Diagrama de Causa e Efeito

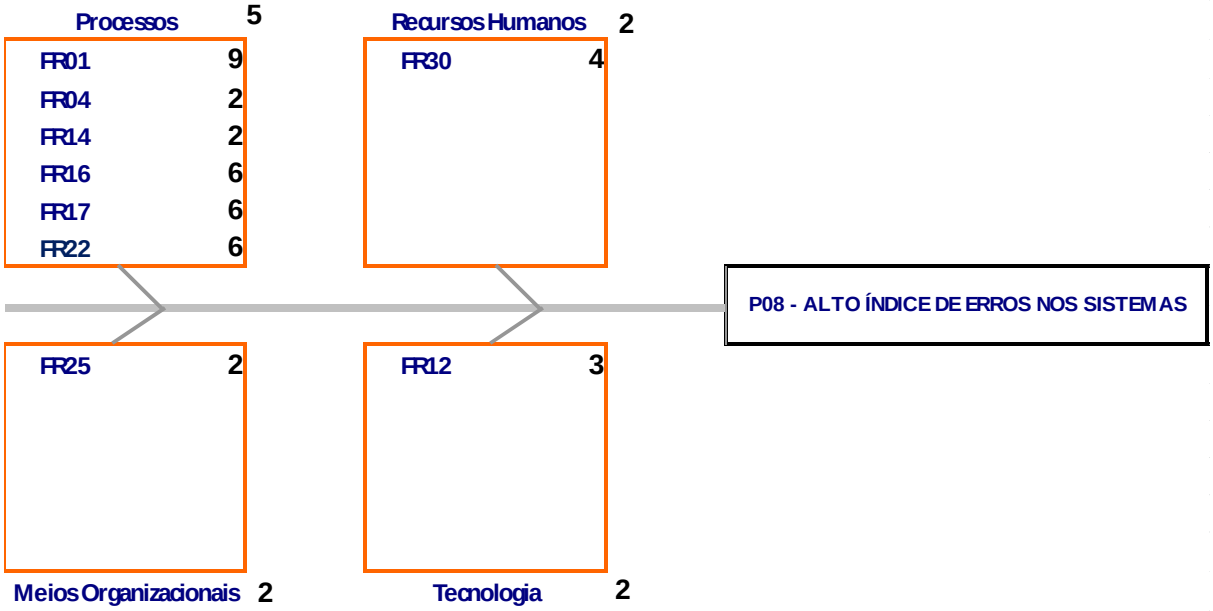

Figura 34: P08 – Diagrama de Causa e Efeito

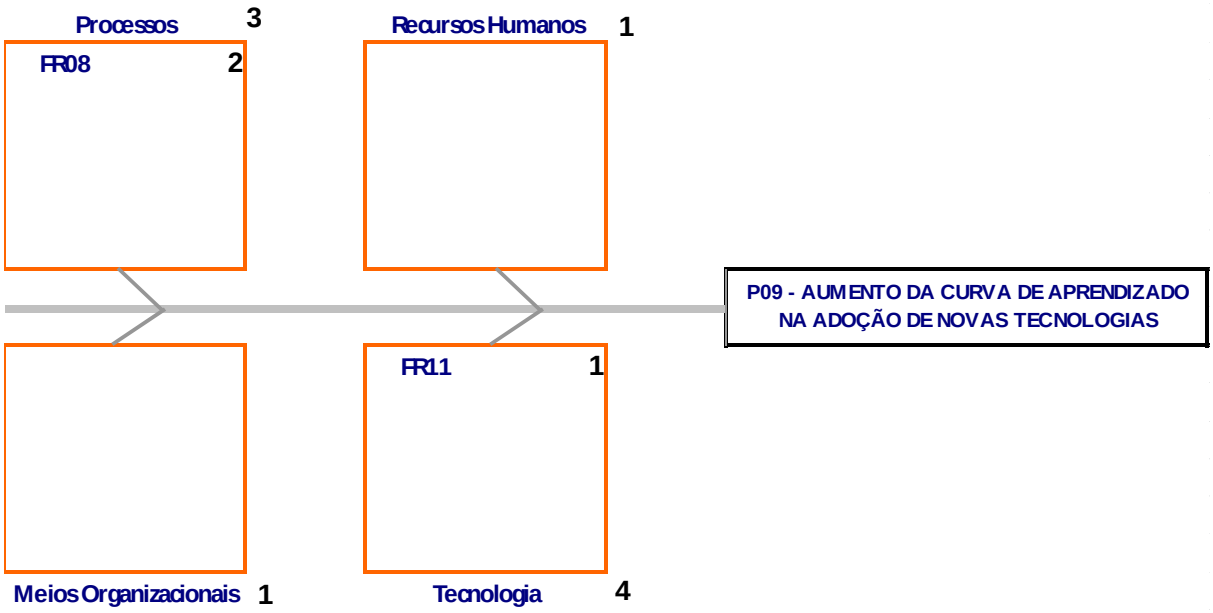

Figura 35: P09 – Diagrama de Causa e Efeito

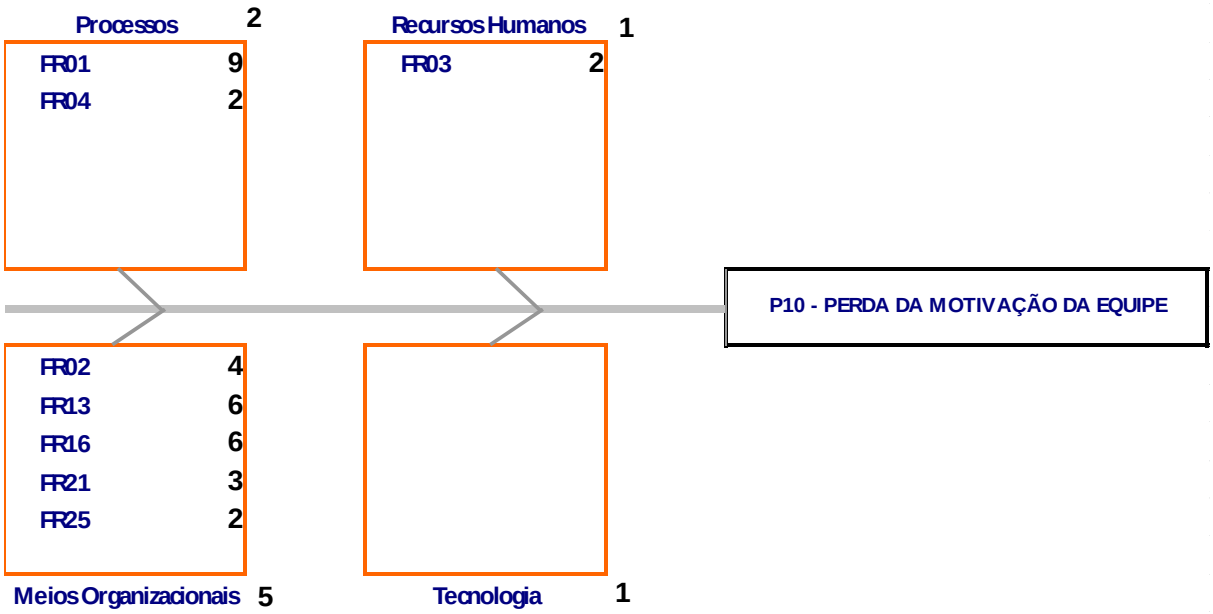

Figura 36: P10 – Diagrama de Causa e Efeito

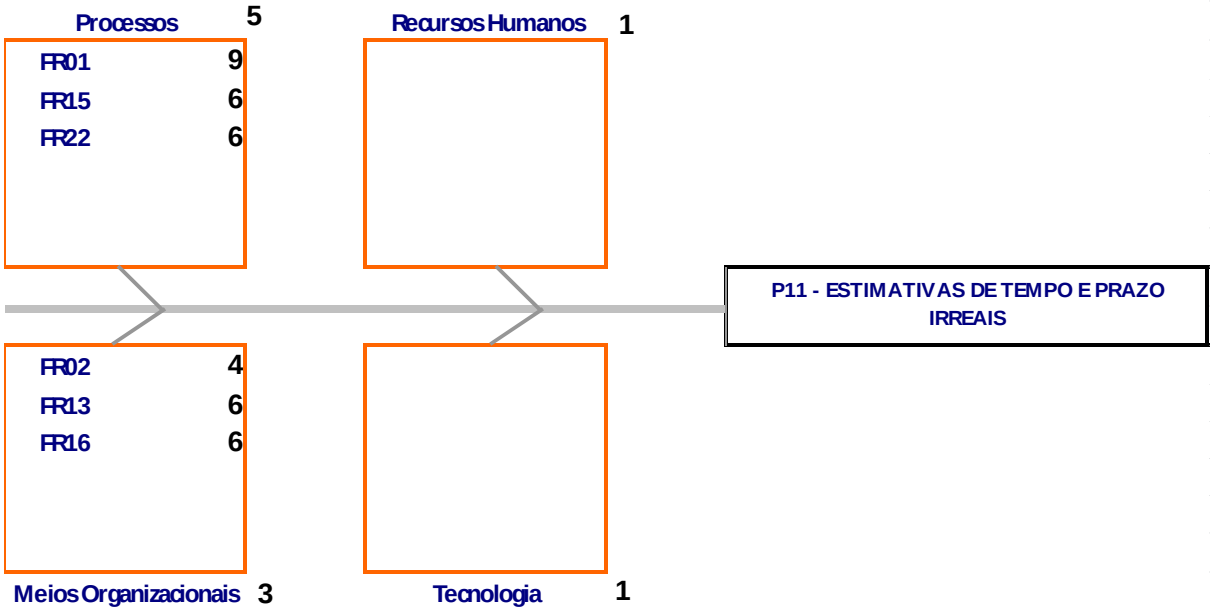

Figura 37: P11 – Diagrama de Causa e Efeito

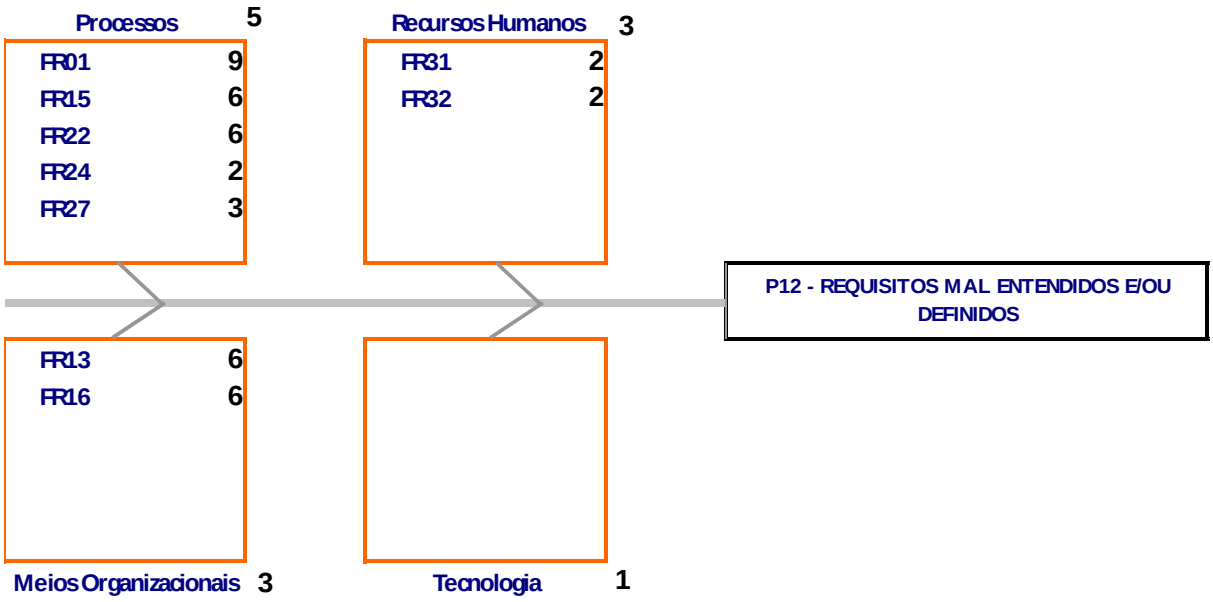

Figura 38: P12 - Diagrama de Causa e Efeito

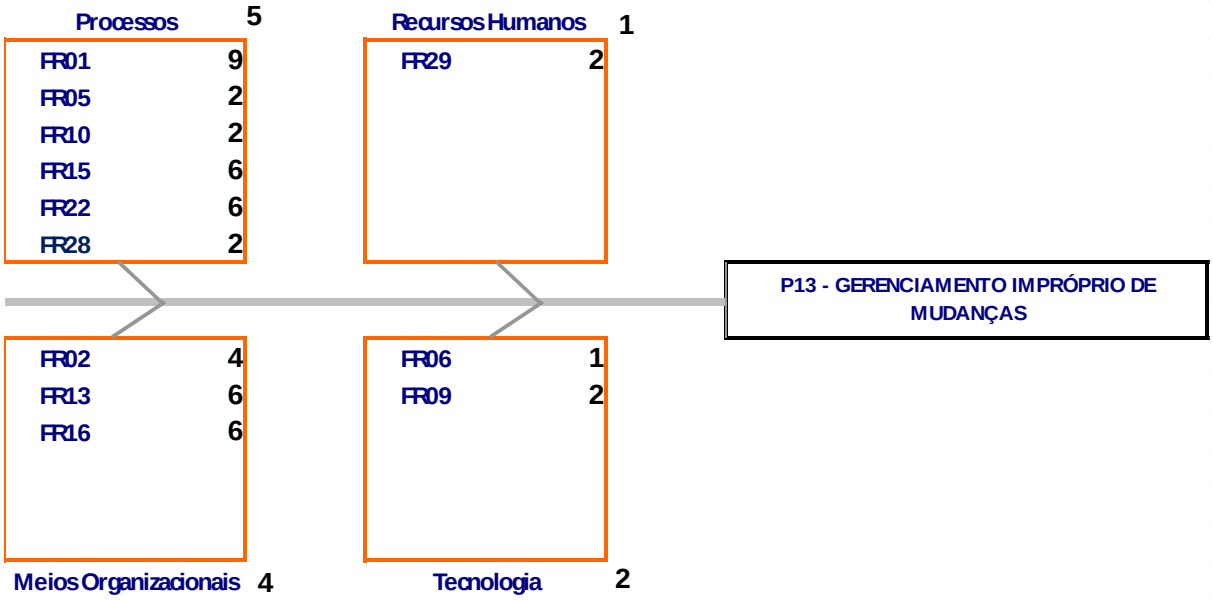

Figura 39: P13 – Diagrama de Causa e Efeito

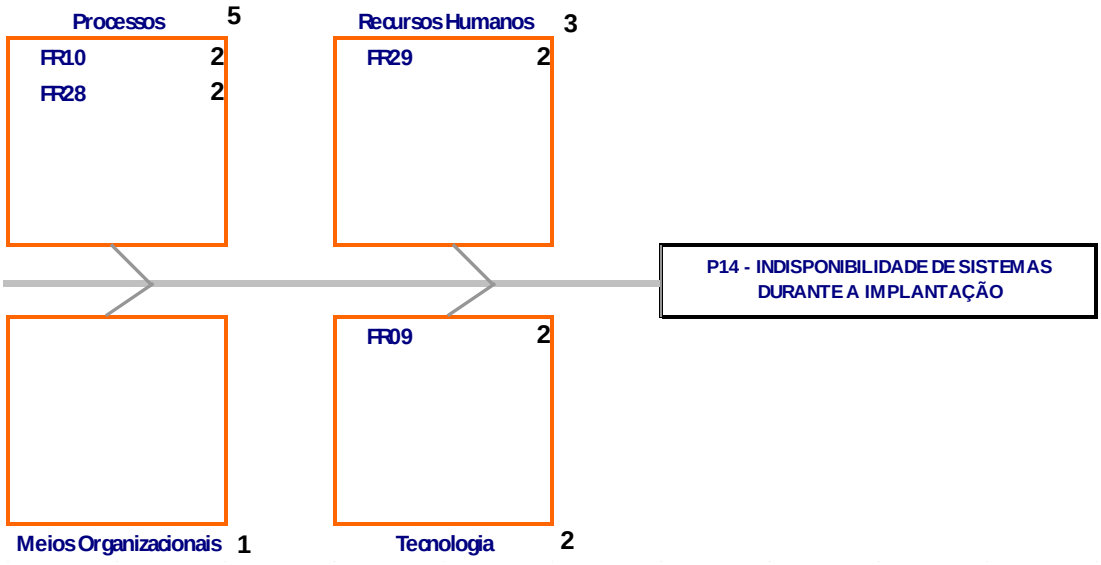

Figura 40: P14 – Diagrama de Causa e Efeito

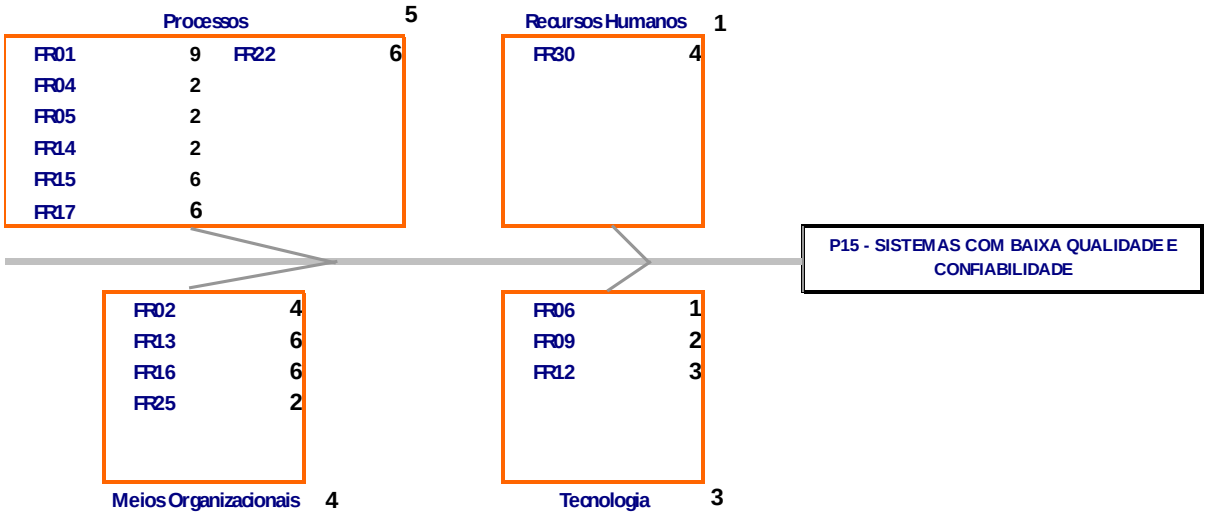

Figura 41: P15 – Diagrama de Causa e Efeito

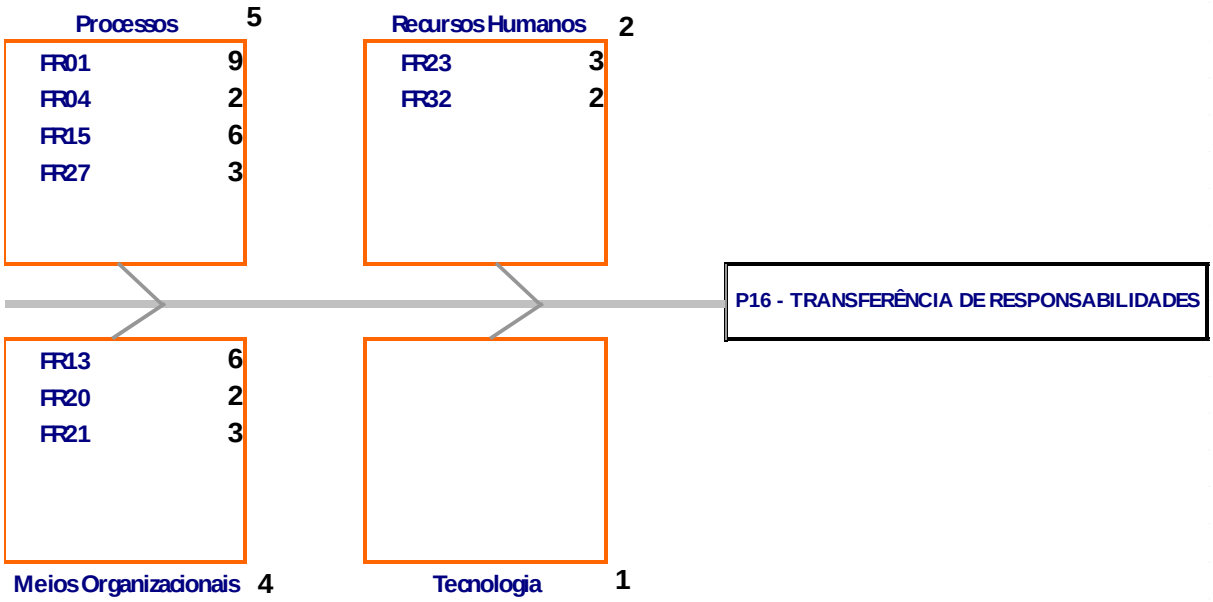

Figura 42: P16 – Diagrama de Causa e Efeito

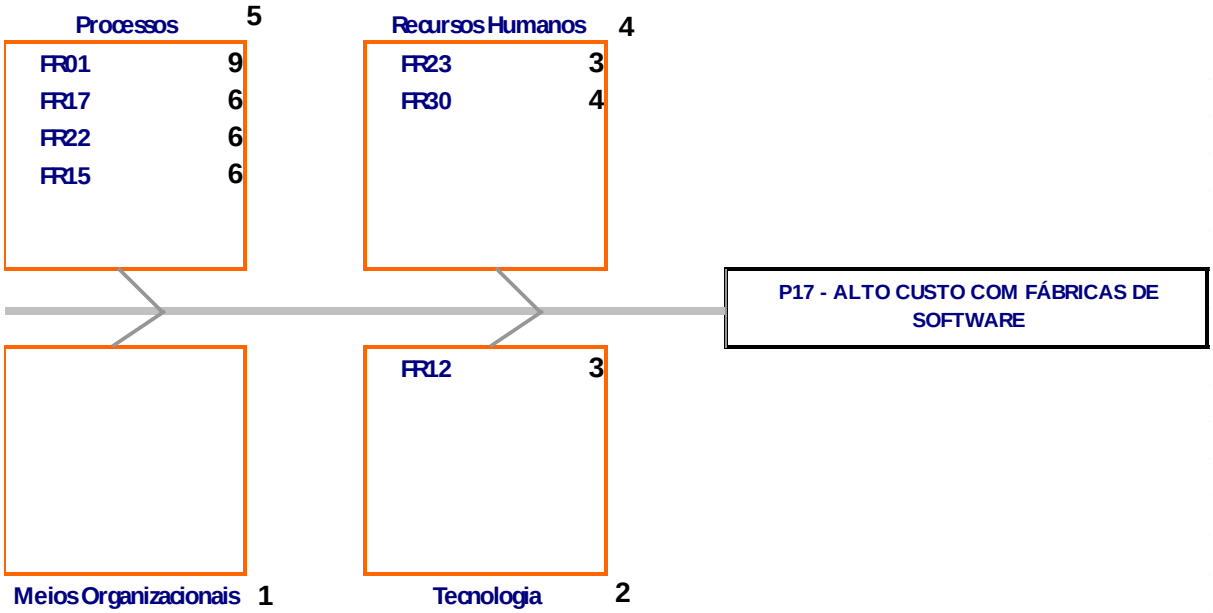

Figura 43: P17 – Diagrama de Causa e Efeito