UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

HERESSON JOÃO PAMPOLHA DE SIQUEIRA MENDES

UMA PROPOSTA DE METODOLOGIA PARA GERENCIAMENTO DE RISCOS EM PROJETOS DE SOFTWARE ADERENTE A MODELOS E NORMAS DE QUALIDADE DE PROCESSO DE SOFTWARE

Belém
2015

Heresson João Pampolha De Siqueira Mendes

UMA PROPOSTA DE METODOLOGIA PARA GERENCIAMENTO DE RISCOS EM PROJETOS DE SOFTWARE ADERENTE A MODELOS E NORMAS DE QUALIDADE DE PROCESSO DE SOFTWARE

Dissertação de Mestrado apresentada para a obtenção do grau de Mestre em Ciência da Computação no Programa de Pós-Graduação em Ciência da Computação do Instituto de Ciências Exatas e Naturais da Universidade Federal do Pará.
Área de Concentração Engenharia de Software.
Orientador Prof. Dr. Sandro Ronaldo Bezerra Oliveira.

Belém
2015

Mendes, Heresson João Pampolha de Siqueira

Uma proposta de metodologia para gerenciamento de riscos em projetos de software aderente a modelos e normas de qualidade de processo de software / Heresson João Pampolha de Siqueira Mendes; orientador, Sandro Ronaldo Bezerra Oliveira - 2015.

Dissertação (Mestrado) - Universidade Federal do Pará, Instituto de Ciências Exatas e Naturais, Programa de Pós-Graduação em Ciência da Computação, Belém, 2015.

1. Engenharia de Software. 2 Processo de Software. I. Oliveira, Sandro R. B orientador. II. Universidade Federal do Pará, Instituto de Ciências Exatas e Naturais, Programa de Pós-Graduação em Ciência da Computação. III. Título.

Heresson João Pampolha De Siqueira Mendes

UMA PROPOSTA DE METODOLOGIA PARA GERENCIAMENTO DE RISCOS EM PROJETOS DE SOFTWARE ADERENTE A MODELOS E NORMAS DE QUALIDADE DE PROCESSO DE SOFTWARE

Dissertação de Mestrado apresentada para a obtenção do grau de Mestre em Ciência da Computação no Programa de Pós Graduação em Ciência da Computação do Instituto de Ciências Exatas e Naturais da Universidade Federal do Pará.

Data da aprovação: Belém-PA. __-__-____

Banca Examinadora

Prof. Dr. Sandro Ronaldo Bezerra Oliveira
Programa de Pós Graduação em Ciência da Computação - UFPA – Orientador

Profª. Dra. Carla Alessandra Lima Reis
Faculdade de Computação - Instituto de Ciências Exatas e Naturais- UFPA – Membro Externo

Profª. Dra. Marcelle Pereira Mota
Faculdade de Computação - Instituto de Ciências Exatas e Naturais- UFPA – Membro Externo

AGRADECIMENTOS

Agradeço aos meus pais e familiares, que mesmo nas ausências e nas muitas madrugadas em claro, nunca deixaram de ter compreensão, e aquele carinho todo especial.

Aos professores do Mestrado, em especial ao professor Sandro, que contribuíram não somente para minha formação acadêmica, mas também com ensinamentos que levarei para a vida.

Aos colegas de trabalho do projeto SPIDER, que, sem exceção, contribuíram direta ou indiretamente para a realização deste trabalho.

Aos demais colaboradores, que revisaram os produtos desta dissertação ou participaram do experimento realizado, suas contribuições foram essenciais para a conclusão deste trabalho.

Aos amigos que já tinha e que ganhei ao longo desses dois anos. Tenham certeza que foi de grande importância seu apoio, contribuindo com palavras amigas ou mesmo uma simples conversa,vocês me ajudaram muito a manter o foco nos meus objetivos durante todo esse tempo.

Agradeço também a Deus pelo dom da vida e por sempre colocar pessoas incríveis no meu caminho.

"Que os vossos esforços desafiem as impossibilidades, lembrai-vos de que as grandes coisas do homem foram conquistadas do que parecia impossível"

Charles Chaplin

RESUMO

Projetos de software são atividades complexas que necessitam de um planejamento adequado, porém fatores inesperados podem ocorrer de modo que prejudiquem a execução das atividades conforme planejadas previamente. Para contornar esses eventos inesperados é necessário aplicar a gerência de riscos, que tem o objetivo de analisar a probabilidade e as consequências de cada um desses possíveis eventos, afim de evitar que se tornem um problema futuramente.

Existem na literatura várias recomendações de boas práticas de gerenciamento de riscos que podem ser aplicadas em um projeto de software, porém ao adotar as recomendações de apenas um guia, uma organização pode deixar de aproveitar outras oportunidades para alcançar a eficácia na gerência de riscos.

Neste contexto, este trabalho visa contribuir através de uma proposta de apoio à implementação da gerência de riscos em organizações que desenvolvem software, sendo composta por uma metodologia de processo e uma ferramenta para apoio à execução das tarefas sugeridas. Para alcançar tais resultados foi realizado um mapeamento entre os modelos MR-MPS-SW e CMMI-DEV, a norma ISO/IEC 12207, o guia PMBOK e o padrão internacional para gerenciamento de riscos ISO/IEC 16085, com o objetivo de identificar equivalências, agrupando-as em uma lista de boas práticas referenciadas em cada guia de qualidade envolvido.

PALAVRAS-CHAVE: Qualidade de Software, Melhoria de Processo de Software, Gerência de Riscos, Metodologia de Processo, Mapeamento de Modelos

ABSTRACT

Software projects are complex activities that require proper planning, but unexpected events may occur during the execution of the activities causing some damages. Risk management is an area responsible to avoid these unexpected events, which analyzes the probability and consequences of each of these possible events in order to avoid them becoming a problem in the future.

There are several recommendations of best practices related to risk management that can be applied in a software project, but adopting only one guide's recommendations an organization hardly can take advantage of other opportunities to achieve effectiveness in risk management.

In this context, this work aims to contribute through a proposal supporting the implementation of risk management in software development organizations, composed by a process methodology and a software tool. These results were achieved through a mapping between the MR-MPS-SW and CMMI-DEV models, ISO/IEC 12207 standard, the PMBOK guide, and the international standard ISO/IEC 16085, identifying equivalences, and grouping them in a list of best practices referenced in each quality guide involved.

KEYWORDS: Software Quality, Software Process Improvement, Risk Management, Process Methodology, Models Mapping

LISTA DE FIGURAS

Figura 2.1 - Elementos de uma estrutura de melhoria do processo de software (Pressman, 2011) 13
Figura 2.2 - Estrutura da norma ISO/IEC 12207, envolvendo processos, atividades e tarefas (adaptado de Koscianski e Soares, 2007) 16
Figura 2.3 - Componentes do modelo CMMI-DEV (adaptado de SEI, 2010) 18
Figura 2.4 - Construção do programa MPS.BR (Koscianski e Soares, 2007) 19
Figura 2.5 - Estrutura do MR-MPS-SW (adaptado de Koscianski e Soares, 2007) 19
Figura 2.6 - Grupos de processos de acordo com o ciclo de vida de um projeto (adaptado de PMI, 2014) 20
Figura 2.7 - Processo para gerenciamento de riscos sugerido pelo padrão ISO/IEC 16085:2006 (IEEE, 2006) 22
Figura 3.1 - Fases da metodologia proposta para gerenciamento de riscos 54
Figura 3.2 - Tarefas da fase de Planejamento. 56
Figura 3.3 - Exemplo de uma EAR (PMI, 2014) 57
Figura 3.4 - Tarefas da fase de Execução 58
Figura 3.5 - Tarefas da fase de Avaliação 60
Figura 4.1 - Visão geral da arquitetura da ferramenta Spider-RM 68
Figura 4.2 - Casos de Uso relacionados à fase de planejamento da metodologia sugerida 70
Figura 4.3 - Casos de Uso relacionados à fase de execução da metodologia sugerida 72
Figura 4.4 - Casos de Uso relacionados à fase de avaliação da metodologia sugerida 73
Figura 4.5 - Tela Principal da Spider-RM 75
Figura 4.6 - Tela de Política Organizacional 76
Figura 4.7 - Tela de Estrutura Analítica de Riscos Organizacional 77
Figura 4.8 - Tela de Portfólio 78
Figura 4.9 - Tela de Plano de Risco 79
Figura 4.10 - Tela da Estrutura Analítica de Riscos do Projeto 80
Figura 4.11 - Tela de Calendário 80
Figura 4.12 - Tela de Gerenciar Riscos 81
Figura 4.13 - Tela de Priorizar Riscos 82
Figura 4.14 - Tela da Seleção de Riscos para Monitoramento 82
Figura 4.15 - Tela de Apresentação de Riscos Ocorridos 83
Figura 4.16 - Tela de Seleção de Risco para Análise 83
Figura 4.17 - Tela da Análise de Risco 84
Figura 4.18 - Tela da Execução de Planos Pendentes 85
Figura 4.19 - Tela da Apresentação dos Planos Realizados 85
Figura 5.1 - Tempo de experiência dos participantes do experimento em projetos de software 93
Figura 5.2 - Nível de conhecimento em modelos de qualidade de software dos participantes do experimento 94
Figura 5.3 - Tempo de experiência dos participantes do experimento em modelos de qualidade de software 94
Figura 5.4 - Identificação de quantos participantes possuem ou não alguma certificação em modelos de qualidade de software 95

Figura 5.5 - Nível de conhecimento em gerência de riscos dos participantes do experimento 95
Figura 5.6 - Tempo de experiência dos participantes do experimento em gerência de riscos 96
Figura 5.7 - Percepção dos participantes com relação à importância da sistematização da gerência de riscos 97
Figura 5.8 - Respostas dos participantes quando perguntado se a ferramenta fornece suporte à identificação dos riscos 97
Figura 5.9 - Respostas dos participantes quando perguntado se a ferramenta fornece suporte à análise de riscos 98
Figura 5.10 - Respostas dos participantes quando perguntado se a ferramenta fornece suporte à priorização de riscos 98
Figura 5.11 - Respostas dos participantes quando perguntado se a ferramenta fornece suporte à mitigação de riscos 99
Figura 5.12 - Respostas dos participantes quando perguntado se a ferramenta fornece suporte ao monitoramento de riscos 99
Figura 5.13 - Respostas dos participantes quando perguntado se a ferramenta fornece suporte à contingência dos riscos 100
Figura 5.14 - Respostas dos participantes quando perguntado se a ferramenta possui usabilidade adequada 100
Figura 5.15 - Respostas dos participantes quando perguntado se consideram a ferramenta adequada ao uso em uma organização 101
Figura 5.16 - Percepção dos participantes com relação ao desempenho da ferramenta na execução de tarefas 101
Figura 5.17 - Percepção dos participantes com relação à aderência da ferramenta ao modelo MR-MPS-SW 102

LISTA DE QUADROS

Quadro 3.1 - Equivalência entre componentes das referências 35
Quadro 3.2 - Mapeamento entre o resultado esperado GRI1 e as tarefas da ISO 12207 37
Quadro 3.3 - Mapeamento entre o resultado esperado GRI2 e as tarefas da ISO 12207 38
Quadro 3.4 - Mapeamento entre o resultado esperado GRI3 e as tarefas da ISO 12207 40
Quadro 3.5 - Mapeamento entre o resultado esperado GRI4 e tarefas da ISO 12207.....41
Quadro 3.6 - Mapeamento entre o resultado esperado GRI5 e as tarefas da ISO 12207 43
Quadro 3.7 - Mapeamento entre o resultado esperado GRI6 e tarefas da ISO 12207.....44
Quadro 3.8 - Mapeamento entre o resultado esperado GRI7 e as tarefas da ISO 12207 45
Quadro 3.9 - Mapeamento entre o resultado esperado GRI8 e tarefas da ISO 12207.....47
Quadro 3.10 - Mapeamento entre o resultado esperado GRI9 e as tarefas da ISO 12207 48
Quadro 3.11 - Boas Práticas identificadas a partir do mapeamento de modelos de qualidade.....50
Quadro 4.1 - Comparativo entre as principais funcionalidades da ferramenta Spider-RM e ooutras ferramentas mencioadas em trabalhos relacionados 86
Quadro 5.1 -Plano de Realização das Fases 92

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas e Técnicas
BP	Boa Prática
CMMI	*Capability Maturity Model Integration*
CMMI-DEV	CMMI *for Development*
DAO	*Data Access Object*
EAR	Estrutura Analítica de Riscos
GPL	*General Public License*
GRI	Gerência de Riscos
IEEE	*Institute of Electrical and Electronics Engineers*
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
MA-MPS	Método de Avaliação MPS.BR
MN-MPS	Modelo de Negócio MPS.BR
MPS.BR	Melhoria do Processo de Software Brasileiro
MR-MPS-SW	Modelo de Referência MPS para Software
MVC	*Model-View-Controller*
PMBOK	*Project Management Body of Knowledge*
PMC	*Project Monitoring and Control*
PMI	*Project Management Institute*
PP	*Project Planning*
RUP	*Rational Unified Process*
SAM	*Supplier Agreement Management*
SEI	*Software Engineering Institute*
SG	*Specific Goals*
SGBD	Sistema de Gerenciamento de Banco de Dados
SOFTEX	Associação para Promoção da Excelência do Software Brasileiro
SP	*Specific Practices*
SPI	*Software Process Improvement*
SPIDER	*Software Process Improvement: Development and Research*
SWOT	*Strengths, Weaknesses, Opportunities And Threats*

SUMÁRIO

1 INTRODUÇÃO 1

1.1 Contexto do Trabalho 1
1.2 Motivação 3
1.3 Objetivos 5
1.4 Metodologia do Trabalho 6
1.5 Estrutura da Dissertação 8

2 FUNDAMENTAÇÃO TEÓRICA 10

2.1 Processo de Software: Uma Visão Geral 10
2.2 Normas, Modelos e Guias de Conhecimento para a Definição e Melhoria de Processos de Software 14
2.2.1 A Norma ISO/IEC 12207 15
2.2.2 O Modelo CMMI-DEV 16
2.2.3 O Modelo MR-MPS-SW 18
2.2.4 O Guia PMBOK 20
2.2.5 O Padrão Internacional ISO/IEC 16085:2006 21
2.3 Gerência de Riscos: Uma Visão Geral 22
2.3.1 A Gerência de Riscos no Contexto de Normas, Modelos e Guias 25
2.4 Trabalhos Relacionados 29
2.5 Considerações Finais 31

3 A METODOLOGIA DO PROCESSO DE GERÊNCIA DE RISCOS EM PROJETOS DE SOFTWARE 33

3.1 O Mapeamento entre Modelos de Qualidade 34
3.1.1 GRI1 - O escopo da gerência de riscos é determinado 36
3.1.2 GRI2 - As origens e as categorias de riscos são determinadas e os parâmetros usados para analisar riscos, categorizá-los e controlar o esforço da gerência de riscos são definidos 38
3.1.3 GRI3 - As estratégias apropriadas para a gerência de riscos são definidas e implementadas 39
3.1.4 GRI4 - Os riscos do projeto são identificados e documentados, incluindo seu contexto, condições e possíveis consequências para o projeto e as partes interessadas. 41
3.1.5 GRI5 - Os riscos são priorizados, estimados e classificados de acordo com as categorias e os parâmetros definidos 42
3.1.6 GRI6 - Planos para a mitigação de riscos são desenvolvidos 43
3.1.7 GRI7 - Os riscos analisados e a prioridade de aplicação dos recursos para o monitoramento desses riscos é determinada 45
3.1.8 GRI8 - Os riscos são avaliados e monitorados para determinar mudanças em sua situação e no progresso das atividades para seu tratamento 46
3.1.9 GRI9 - Ações apropriadas são executadas para corrigir ou evitar o impacto do risco, baseadas na sua prioridade, probabilidade, consequência ou outros parâmetros . 48
3.1.10 Práticas dos modelos de qualidade não relacionadas com nenhum resultado esperado do modelo MR-MPS-SW 49
3.2 As Boas Práticas Coletadas 50
3.3 Detalhamento da Metodologia Proposta 53
3.3.1 Fases Propostas 54

3.3.2 Papéis Sugeridos 54
3.3.3 Descrição das Tarefas Propostas 56
3.4 Diferenciais da Proposta 61
3.5 A Avaliação da Metodologia Proposta 62
3.6 Considerações Finais 65
4 A FERRAMENTA SPIDER-RM 66
4.1 O Objetivo da Ferramenta Spider-RM 66
4.2 Projeto Técnico da Ferramenta Spider-RM 67
4.2.1 Arquitetura da Ferramenta 67
4.2.2 Casos de Uso da Ferramenta 69
4.2.3 Tecnologias utilizadas na Ferramenta 73
4.3 As Funcionalidades da Ferramenta Spider-RM 74
4.3.1 Visão Geral 75
4.3.2 Módulo Organizacional 75
4.3.3 Módulo de Escopo de Projetos 78
4.4 Diferenciais da Ferramenta 86
4.5 Considerações Finais 87
5 AVALIAÇÃO QUALITATIVA 89
5.1 Abordagem da Avaliação 89
5.2 Análise dos Resultados Obtidos 93
5.2.1 Perfil dos Participantes 93
5.2.2 Avaliação da Ferramenta 96
5.2.3 Análise do Apoio à Aprendizagem 103
5.3 Considerações Finais 104
6 CONCLUSÕES 105
6.1 Considerações Finais 105
6.2 Contribuições 106
6.3 Limitações 107
6.4 Trabalhos Futuros 108
6.4.1 Integração da metodologia com outras áreas de processos 108
6.4.2 Aprimoramento da metodologia para cenários específicos 109
6.4.3 Aprimoramento da ferramenta Spider-RM 109
6.4.4 Estudo de caso em cenário real 109
REFERÊNCIAS BIBLIOGRÁFICAS 110
APÊNDICE A – DETALHAMENTO DAS TAREFAS DA METODOLOGIA 114
APÊNDICE B – QUESTIONÁRIO DE AVALIAÇÃO DA METODOLOGIA POR UM ESPECIALISTA 134
APÊNDICE C – RASTREABILIDADE ENTRE METODOLOGIA E OS CASOS DE USO 139
APÊNDICE D – CENÁRIO DO EXPERIMENTO 139
APÊNDICE E – QUESTIONÁRIO DE PERFIL E AVALIAÇÃO DA SPIDER-RM 142
APÊNDICE F – QUESTIONÁRIO DE AVALIAÇÃO DO CONHECIMENTO 145

1 INTRODUÇÃO

Este capítulo apresenta a contextualização do trabalho, necessária para o entendimento da motivação que levou à elaboração do mesmo, abordada em seguida. Depois são apresentados os objetivos e a metodologia definida para a execução do trabalho, e finalmente é apresentada a estrutura desta dissertação.

1.1 Contexto do Trabalho

O aspecto não repetitivo do desenvolvimento de software torna essa atividade difícil e, sobretudo, em boa medida imprevisível (Koscianski e Soares, 2007). Na literatura, é reconhecida a alta complexidade envolvida nesta atividade, pois exige conformidade com as necessidades dos clientes, estando sujeito a constantes mudanças, mesmo sendo intangível (Brooks, 1986).

As dificuldades identificadas perduram até a atualidade, confirmadas por Pressman (2011), que evidencia a importância da gerência de riscos ao afirmar que software é uma empreitada difícil, muitas coisas podem dar errado, portanto entender riscos e tomar medidas proativas para evitá-los é essencial para um bom gerenciamento do projeto de software.

Além disso, o mercado exige que as organizações, para serem competitivas, entreguem software que satisfaçam as necessidades dos clientes, de forma a garantir confiança e satisfação (SOFTEX, 2012a). Consequentemente, a qualidade é uma variável importante a ser considerada em todo processo de produção de um software, da construção à entrega.

Uma forma de atingir a excelência no desenvolvimento de software é através da qualidade do processo de produção do mesmo (Sommerville, 2007), que se preocupa

com o gerenciamento e monitoramento das tarefas envolvidas da concepção à entrega do produto. O tópico relacionado à qualidade do processo preocupa-se em desenvolver aspectos gerenciais, de engenharia e de apoio ao desenvolvimento de um software.

Tendo em vista um melhor acompanhamento da evolução de um processo de software surgiram normas e modelos de qualidade, que recomendam o aperfeiçoamento gradual deste processo de forma categorizada. Entre as iniciativas internacionais destacam-se a norma ISO/IEC 12207 (ABNT, 2009a), o modelo CMMI-DEV - *Capability Maturity Model Integration for Development* (SEI, 2010), e no âmbito nacional o Modelo de Referência para Melhoria de Processo de Software para Software (MR-MPS-SW) (SOFTEX, 2012a).

A gerência de riscos é uma área de conhecimento estudada nos principais modelos e normas de qualidade, e trata de um fator importante para o sucesso de um projeto, pois gerencia a probabilidade de um evento inesperado ocorrer e suas consequências, denominado risco (IEEE, 2006).

Para alcançar o sucesso no gerenciamento de riscos de um projeto, pode ser utilizado como base as recomendações presentes nos modelos de qualidade citados anteriormente, além de outros, como o guia de gerenciamento de projetos PMBOK – *Project Management Body of Knowledge* (PMI, 2014) e o padrão internacional para gerência de riscos definido pelo IEEE e ISO/IEC, a norma ISO/IEC 16085:2006 (IEEE, 2006).

A diversidade de normas e padrões internacionais relativos ao gerenciamento de riscos provoca uma grande quantidade de boas práticas dispersas, que eventualmente podem não ser aproveitadas, caso se utilize apenas um dos modelos de qualidade para a implantação da melhoria do processo de software. Porém é importante as organizações terem alternativas para a implementação de quaisquer melhorias no processo, devido suas peculiaridades. Um caso de sucesso pode não ser replicado de forma satisfatória em outra organização, ou até mesmo em uma mesma organização, porém com equipe e cenário diferentes (Avison *et al.*, 1994).

Este trabalho tem o intuito de propor uma metodologia abrangente para a implantação da gerência de riscos em uma organização desenvolvedora de software. A metodologia a ser proposta deve agrupar boas práticas de modelos e normas de Gerenciamento de Riscos, porém estas práticas devem ser totalmente aderentes às

exigências do MR-MPS-SW, pois este projeto faz parte do escopo do Projeto SPIDER (Oliveira *et al.*, 2011). O projeto SPIDER tem como objetivo criar um suíte de abordagens de software livre aderente ao MR-MPS-SW para reduzir os custos de implementação deste modelo. Ambos têm objetivos alinhados, haja vista que o projeto SPIDER não possui estudos específicos na área de gerência de riscos.

1.2 Motivação

A qualidade em software pode ser alcançada através de dois fatores (Humphrey, 1989): (i) qualidade do produto, que busca definir diretrizes a partir das características tangíveis do produto; e (ii) qualidade do processo, que foca na melhoria dos processos geradores do produtos para alcançar a qualidade no produto final.

Desde meados dos anos 70 desenvolvedores vêm buscando melhorar a qualidade dos softwares, que apresentam até os dias atuais dificuldades como cronograma não observados, projetos abandonados, módulos que não operam conforme combinado, programas tão difíceis de usar que são descartados, entre outros (Koscianski e Soares, 2007). Obter resultados positivos em um software como: qualidade considerável, alta taxa de produtividade e entrega do produto dentro do prazo estabelecido sem a necessidade de alocar mais recursos; tem sido um dos grandes desafios da Engenharia de Software (Fiorini *et al.*, 1998).

Por ser considerado um projeto, o desenvolvimento de um software é não repetitivo e imprevisível, envolvendo alta complexidade, necessitando estar em conformidade com as necessidades do cliente, sujeito a constantes mudanças, além de ser intangível (Brooks, 1986). Uma maneira encontrada para tentar ultrapassar estas dificuldades é através de modelos e normas, que são guias para executar boas práticas em processos de software, fornecendo diretrizes em diversas disciplinas relacionadas ao desenvolvimento de software, entre elas está o gerenciamento de riscos.

Diversos modelos e guias de boas práticas para projetos e projetos de software, como MR-MPS-SW, PMBOK, ISO/IEC 12207 e CMMI-DEV possuem referência ao gerenciamento de riscos, embasando a importância deste processo. Cada modelo possui um conjunto de metas a serem alcançadas no Gerenciamento de Riscos e algumas

sugestões de como implementá-lo, porém organizações consideradas micro, pequenas e médias empresas muitas vezes não possuem recursos suficientes para implementar um processo e avaliá-lo (SOFTEX, 2012a).

No contexto nacional, o programa MPS.BR, que mantém o modelo MR-MPS-SW, decompõe a evolução de um processo organizacional de forma gradual, através de sete níveis de maturidade, iniciando-se no nível G até o nível A. Atualmente, existem cerca de 276 empresas avaliadas positivamente no MPS.BR e dentro do prazo de vigência de três anos. Deste total apenas 25 empresas foram avaliadas nos últimos três anos no nível C (SOFTEX, 2015), no qual está situada a gerência de riscos, ou seja, menos de 10% das organizações desenvolvedoras de software que comprovadamente buscam qualidade do processo no Brasil através do MPS.BR já possuem experiência na implantação do gerenciamento de riscos.

A evidência da pouca experiência prática no gerenciamento de riscos em projetos de software no Brasil e a variedade de modelos e práticas existentes relacionados a esta disciplina são fortes motivadores para este trabalho.

Profissionais e pesquisadores concordam que para a gerência de riscos ser efetiva, é necessário incluí-la desde as fases iniciais do processo de desenvolvimento (Islam, 2011), pois requisitos são uma das principais causas de falhas nos projetos (Glass, 1998). Uma vantagem de considerar a gerência de riscos desde as fases iniciais do processo de desenvolvimento do software é a possibilidade de identificar prematuramente futuros problemas que aumentariam os custos do projeto (Van Lamsweerde, 2009).

No entanto, a literatura carece de diretrizes abrangentes e evidências claras de como integrar o gerenciamento de riscos desde as fases iniciais do processo de desenvolvimento de um software (Islam, 2011).

Ademais, a taxa de fracasso de projetos de TI permanece inalterada em pesquisas ao logo de quinze a vinte anos, em torno de 40% a 50%. Apesar de novas tecnologias, métodos e ferramentas de apoio, é um processo cheio de riscos do começo ao fim (Avdoshin e Pesotskaya, 2011).

Logo, constata-se a importância do gerenciamento dos riscos em projetos de software, no qual ocupa um papel de destaque em normas e modelos de maturidade de processo de software. Além disso, a realidade brasileira apresentada evidencia a

necessidade de pesquisas em níveis de maturidades mais altos (incluindo-se a gerência de riscos), na tentativa de identificar a baixa aderência a estes níveis de maturidade no âmbito nacional, e como, através da redução dos custos de implementação, estes números podem ser aumentados.

Portanto, este trabalho visa fornecer uma metodologia ampla para a implantação do gerenciamento de riscos, totalmente aderente às boas práticas nos principais modelos e normas de qualidade do software, com principal foco no modelo MR-MPS-SW que possui maior popularidade no Brasil, associado a um conjunto de formas de implementação de cada prática.Também através de um apoio ferramental, formado por um software livre, passível de customização, respaldando a metodologia produzida nesta pesquisa, reduzindo assim possíveis custos extras da implementação da gerência de riscos em organizações desenvolvedoras de software.

1.3 Objetivos

Este projeto tem como objetivo geral propor uma metodologia para a implementação e a execução do processo de gerenciamento de riscos em projetos de software, baseada nos modelos, normas e guias de qualidade CMMI-DEV, MR-MPS-SW, ISO/IEC 12207, PMBOK, e ISO/IEC 16085. A metodologia deve agregar as boas práticas identificadas e ser apoiada por uma ferramenta de software livre, que sistematize um conjunto de tarefas geradas pelo estudo.

Para atender ao objetivo geral, devem ser contemplados os seguintes objetivos específicos:

- Investigar normas e modelos de qualidade que sugerem boas práticas em gerenciamento de riscos;
- Mapear boas práticas dos modelos e normas de qualidade selecionados;
- Desenvolver uma metodologia para implantação de um processo de gerenciamento de riscos baseado nas boas práticas selecionadas;
- Descrever papéis, tarefas, artefatos e procedimentos para o processo sugerido;
- Elicitar e especificar os requisitos funcionais e não funcionais para propor uma

ferramenta que dê suporte à metodologia de gerenciamento de riscos desenvolvida;

- Definir o projeto arquitetural com base nos requisitos especificados;
- Desenvolver uma ferramenta de software livre aderente à metodologia;
- Produzir, aplicar e analisar questionários para avaliar a metodologia e a ferramenta desenvolvidas;
- Analisar possíveis benefícios da metodologia e da ferramenta através de avaliação qualitativa.

1.4 Metodologia do Trabalho

A realização deste trabalho ocorreu através das etapas descritas a seguir:

a) Etapa de Estudo Inicial

- Análise de trabalhos relacionados ao gerenciamento de riscos, ao mapeamento de modelos de qualidade e à elaboração de *frameworks* para a gerência de riscos;
- Estudo de modelos , normas e guias mais citados nos trabalhos analisados na etapa anterior.

b) Etapa de Análise dos Modelos de Qualidade

- Estudo mais aprofundado dos modelos MR-MPS-SW e CMMI-DEV, da norma ISO/IEC 12207, do guia PMBOK e do padrão ISO/IEC 16085;
- Desenvolvimento do mapeamento entre os elementos que compõem as orientações sobre a gerência de riscos de cada um dos modelos, normas e guias de qualidade envolvidos;
- Consolidação de Boas Práticas identificadas em cada um dos documentos analisados para o mapeamento.

c) Etapa de Análise do Mapeamento

- Elaboração da metodologia para implantação da gerência de riscos em alto nível, descrevendo fases, papéis e tarefas;
- Detalhamento das tarefas elaboradas para a metodologia proposta;
- Avaliação da metodologia proposta com auxílio de um especialista em gerência de riscos e melhoria de processo;

- Análise das sugestões propostas pelo especialista que realizou a avaliação.

d) Etapa de Especificação e Construção da Ferramenta Sistematizada

- Definição dos requisitos funcionais e não funcionais da ferramenta Spider-RM, baseados na metodologia e no conjunto de Boas Práticas;
- Priorização e validação dos requisitos definidos junto a um consultor experiente certificado por alguma instituição relacionada à qualidade de software;
- Elaboração da estrutura arquitetural da ferramenta;
- Implementação e testes de acordo com requisitos e arquitetura planejados.

e) Etapa de Análise Qualitativa

- Planejamento das etapas do experimento;
- Execução de uma experimentação de uso da ferramenta Spider-RM em um cenário que simule o cenário real;
- Análise das respostas obtidas nos questionários entregues aos participantes do experimento;
- Análise do aprendizado obtido com uso da ferramenta através das respostas obtidas com o questionário.

f) Etapa de Documentação

- Redação final da dissertação.

A pesquisa realizada pode ser caracterizada de várias formas, utilizando a definição de Silva e Menezes (2001) é possível classificá-la da seguinte maneira:

- **Quanto à natureza:** pesquisa aplicada, pois tem o objetivo de gerar conhecimentos para a aplicação prática focando na solução de problemas específicos;
- **Quanto à abordagem do problema:** pesquisa quantitativa e qualitativa são utilizadas, devido a necessidade de se traduzir em números as opiniões e as informações obtidas com o uso de questionários, além disso em outras situações o pesquisador tende a analisar os dados de maneira indutiva;
- **Quanto aos objetivos:** trata-se de uma pesquisa exploratória e descritiva, pois proporciona um maior entendimento do problema, relacionando levantamentos bibliográficos, entrevistas com pessoas com experiência prática e por utilizar questionários para verificar as características e percepções de uma população;

- **Quanto aos procedimentos técnicos**: pesquisa bibliográfica, devido ter sido elaborada com base em materiais já publicados, como artigos de periódicos e eventos, livros, dissertações, teses e materiais disponibilizados na Internet.

1.5 Estrutura da Dissertação

Este capítulo introdutório aborda a visão geral a respeito do trabalho desenvolvido nesta dissertação, identificando o contexto, a motivação, os objetivos e a metodologia utilizada para sua execução.

O Capítulo 2 apresenta a fundamentação teórica abordando conceitos relacionados a processos de software e detalhando a norma ISO/IEC 12207, os modelos CMMI-DEV e MR-MPS-SW, o guia de gerenciamento de projetos PMBOK e o padrão internacional para gerenciamento de riscos em projetos de software ISO/IEC 16085. Também são abordados conceitos relacionados ao gerenciamento de riscos e é realizada uma apresentação de como esses modelos, normas padrões e guias tratam deste tema. Além disso, são apresentados os trabalhos relacionados às abordagens executadas nesta dissertação.

O Capítulo 3 apresenta a metodologia desenvolvida nesta dissertação, que pretende auxiliar a implantação da gerência de riscos nas organizações. Inicialmente é apresentado o mapeamento realizado entre os documentos de qualidade envolvidos, depois são destacadas as boas práticas coletadas. Em seguida as fases, papéis e tarefas da metodologia proposta são apresentadas, juntamente com seu diferencial. E, finalmente, é realizado o detalhamento de como a avaliação desta metodologia foi realizada.

No Capítulo 4 a ferramenta de apoio à metodologia, Spider-RM, é apresentada através do seu objetivo e do projeto técnico elaborado para seu desenvolvimento. Também são expostas as funcionalidades da ferramenta, junto com as telas que representam cada funcionalidade evidenciando quais tarefas da metodologia foram responsáveis pelo seu desenvolvimento.

O Capítulo 5 aborda a avaliação qualitativa realizada através de um experimento, para analisar a ferramenta e a metodologia desenvolvidas. São

apresentados os aspectos gerais para a realização da avaliação e a análise dos resultados obtidos após o experimento.

Finalmente, o Capítulo 6 apresenta as considerações finais, contribuições, limitações e trabalhos futuros desta dissertação.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta a fundamentação teórica deste trabalho, esclarecendo algumas terminologias relacionadas ao processo de software. Em seguida, apresenta normas, modelos e guias de conhecimento utilizados para apoiar a melhoria do processo de software. Por fim, são abordados conceitos relacionados ao gerenciamento de riscos e apresentados trabalhos relacionados às temáticas aqui tratadas.

2.1 Processo de Software: Uma Visão Geral

Processo de software é denominado por Pressman (2011) como uma metodologia para as atividades, ações e tarefas necessárias para desenvolver um software de alta qualidade, que tem sua importância por propiciar estabilidade, controle e organização para um atividade, que pode se tornar bastante caótica. O guia PMBOK – *Project Management Body of Knowledge* (PMI, 2014), define processo como uma combinação de atividades inter-relacionadas realizadas, com o intuito de atingir um objetivo, como alcançar resultados, produtos ou serviços.

Para o modelo de qualidade CMMI – *Capability Maturity Model Integration* (SEI, 2010), um processo é definido quando existe documentação que detalha o que é feito (produto), quando (etapas), por quem (papéis), os itens utilizados e os itens produzidos (insumos e resultados, respectivamente). A definição de Fuggeta (2000) para processo é de um conjunto de políticas, estruturas organizacionais, tecnologia, procedimentos e artefatos coerentes, necessários para conceber, desenvolver implantar e manter um produto de software. Humphrey (1989) interpreta o conceito de processo de software dando enfoque às necessidades do cliente, definindo como um conjunto de atividades relacionadas de Engenharia de Software, que são necessárias para produzir software a partir dos requisitos do usuário.

Sommerville (2007) define um processo de software como um conjunto de

atividades relacionadas que levam a um produto de software, além disso classifica os processos nas seguintes categorias:

a) **Processos informais:** a organização não possui uma definição concreta do processo de software, logo cada equipe de desenvolvimento de diferentes projetos escolhe qual processo irá utilizar;
b) **Processos gerenciados:** é utilizado um modelo de processo padrão instanciado para cada projeto, com o intuito de direcionar futuras evoluções;
c) **Processo metódicos:** possui alguns métodos definidos, que são utilizados para normatizar o processo de software parcialmente ou totalmente;
d) **Processos melhorados:** processos de software que possuem orçamento e procedimentos específicos visando sua melhoria, ou seja, têm como principal objetivo a melhoria contínua.

As classificações para processos, determinadas por Sommerville (2007) não são exclusivas, ou seja, um mesmo projeto de uma mesma organização podem ter mais de um tipo de processo, de acordo com as necessidades demandadas.

Falbo (1998) e Travassos (1994) identificam em seus trabalhos alguns dos principais conceitos relacionados à definição de processo de desenvolvimento software:

a) **Atividades:** tarefas ou trabalhos a serem realizados, que requerem recursos e podem consumir ou produzir um artefato. Para sua realização, uma atividade pode adotar um procedimento. Uma atividade pode ser decomposta em outras atividades. Além disso, atividades, em qualquer nível, podem depender da finalização de outras atividades;
b) **Artefatos:** produtos de software produzidos ou consumidos por atividades durante sua realização. Alguns exemplos são: manuais de qualidade, manuais de revisão, diagramas de fluxo de dados, diagramas de objetos, código fonte, etc.;
c) **Procedimentos:** são condutas bem estabelecidas e ordenadas para a realização de atividades. Alguns procedimentos podem ser parcialmente automatizados por ferramentas de software. São exemplos de procedimentos: técnicas de avaliação da qualidade, tais como inspeções e *walkthroughs*, roteiros diversos para a produção de documentos, normas de programação, etc.;
d) **Recursos:** pessoas, ferramentas de software, equipamentos ou quaisquer outros

recursos necessários à execução de uma atividade. Um recurso humano, especificamente, desempenha um papel na execução das atividades do processo;

e) **Processos:** agrupamento de atividades relacionadas que têm lugar durante o desenvolvimento de um produto.

Em resumo, as inúmeras definições para processo de desenvolvimento de software abrangem o conceito de que existem um conjunto de atividades relacionadas que têm o objetivo de desenvolver um produto de software.

O relacionamento entre atividades e componentes podem apresentar grande complexidade na coordenação de tarefas durante o ciclo de vida do software. Assim, a definição de um processo de software possibilita que profissionais da Engenharia de Software trabalhem de forma ordenada (Humphrey,1989). Partindo deste inferência, Humphrey (1989) identificou que a busca por um software de qualidade tem sido realizada em duas vertentes: a qualidade do processo e a qualidade do produto. A qualidade do processo tem foco nas tarefas e processos geradores do produto, através do controle e gerenciamento do ciclo de vida do software, enquanto a qualidade do produto dedica-se em identificar características tangíveis dos produtos resultantes de um processo, estabelecendo assim critérios que auxiliarão na avaliação do software produzido.

A qualidade do processo de software é uma abordagem comumente utilizada para alcançar a qualidade de software (Humphrey, 1989), isto acontece através da melhoria do processo de software (*Software Process Improvement* - SPI). Pressman (2011) identifica que SPI envolve três fatores: (1) elementos de um processo de software podem ser definidos de maneira eficaz; (2) uma abordagem organizacional existente para o desenvolvimento de software pode ser avaliada em relação aos elementos do processo; e (3) uma estratégia significativa para a melhoria pode ser definida, transformando a abordagem para o processo de desenvolvimento em algo mais focado, com melhor repetibilidade e mais confiável.

A Figura 2.1 apresenta uma visão geral de uma estrutura SPI típica, no qual tem-se como elemento principal a definição do processo de software, que: é avaliado com o intuito de levar à determinação da capacidade; identifica pontos fortes e fracos do processo; e leva à estratégia de melhoria, que identifica mudanças e sugere abordagens de melhoria para o processo.

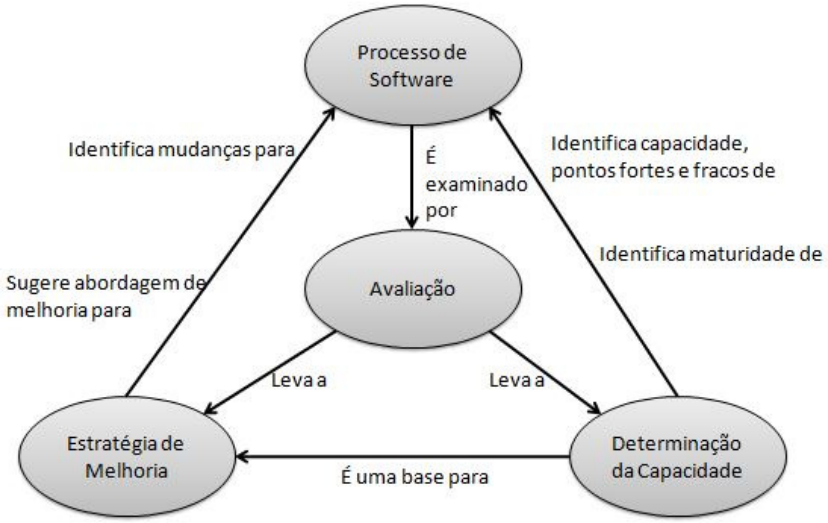

Figura 2.1 Elementos de uma estrutura de melhoria do processo de software (Pressman, 2011)

Conradi (1996) classifica seis grupos distintos de suporte à SPI, porém que podem ser complementares:

a) **Certificadores de qualidade**: a abordagem desse grupo enfatiza que a qualidade do processo leva à qualidade do produto, enfatizando métodos de avaliação e encaminhando um conjunto bem definido de características que lhes permitem determinar se o processo apresenta qualidade;
b) **Formalistas**: pretende entender e, se possível, otimizar o fluxo de trabalho do processo, através da utilização de linguagens de modelagem do processo, para criar um modelo de processo existente e então projetar extensões ou modificações que tornarão o processo mais eficaz;
c) **Defensores das ferramentas**: grupo que insiste em uma abordagem assistida por ferramenta para melhoria do processo, modelando fluxo de trabalho e outras características do processo, de maneira a ser analisada para melhoria;
d) **Profissionais**: através de uma abordagem pragmática, esse grupo enfatiza no gerenciamento básico do projeto, qualidade e produto, aplicando planejamento e métricas em nível de projeto, mas com pouca modelagem formal;
e) **Reformadores**: têm como objetivo a mudança organizacional que pode levar a um melhor processo de software, concentrando-se mais nos aspectos humanos;
f) **Ideologistas**: focaliza na adequação de um modelo particular de processo para um domínio de aplicação específico ou estrutura organizacional. Têm interesse maior em um processo voltado para reutilização ou reengenharia.

Independentemente do foco geral adotado no suporte à melhoria do processo de software, os grupos que a patrocinam devem, segundo Pressman (2011) estabelecer mecanismos para: (1) suportar transição de tecnologia; (2) determinar o grau segundo o qual uma organização está pronta para absorver mudanças de processo propostas; e (3) medir o grau segundo o qual as mudanças foram adotadas.

Um modelo de maturidade é aplicado no contexto de uma estrutura SPI com a finalidade de proporcionar uma indicação geral do nível de maturidade do processo, para tanto utiliza-se geralmente algum tipo de escala ordinal (Pressman, 2011).

Entre os padrões que incentivam SPI através de um modelo de maturidade destaca-se internacionalmente o CMMI-DEV – *CMMI for Development* (SEI, 2010), e no âmbito nacional o MR-MPS-SW – Modelo de Referência para a Melhoria do Processo de Software, integrante do programa MPS.BR (SOFTEX, 2012a). Além disso, algumas normas ou guias de qualidade também podem contribuir para a melhoria do processo de software de uma organização, como por exemplo a norma ISO/IEC 12207 (ABNT, 2009a) e o guia PMBOK (PMI, 2014), considerado como uma referência em práticas no gerenciamento de projetos, porém de forma mais abrangente, ele determina boas práticas para projetos de quaisquer natureza, não especificamente para software. No contexto do gerenciamento de riscos, há ainda o padrão internacional mantido pelo IEEE – *Institute of Electrical and Electronic Engineers* em parceria com ISO/IEC – *International Organization for Standardization and International Electrotechnical Commission*, denominado ISO/IEC 16085:2006 (IEEE, 2006), que fornece diretrizes para práticas de gerenciamento de riscos em projetos de software, alinhadas à norma ISO/IEC 12207.

2.2 Normas, Modelos e Guias de Conhecimento para a Definição e Melhoria de Processos de Software

Modelos de melhoria de processos auxiliam as organizações na evolução da capacidade em cumprir prazos ao construir software (Paulk, 2004). Além disso, os modelos e normas possuem um olhar genérico, têm como objetivo não se preocuparem com características individuais de cada projeto, fornecendo assim um olhar genérico sobre as organizações como um todo (Spinola *et al.*, 2008).

As normas, os modelos e os guias de agregam um conteúdo substancial de

conhecimento e indicam boas práticas para as diversas disciplinas envolvidas na Engenharia de Software, através da exposição de um caminho gradual na evolução do processo de software organizacional. É importante ressaltar que as boas práticas descritas por estes materiais de apoio à melhoria do processo não têm o intuito de definir o processo na organização, pois este deve se adequar à realidade de cada organização.

As subseções a seguir apresentam normas, modelos e guias de conhecimento relacionados à melhoria do processo de software, que estão no âmbito do trabalho aqui apresentado.

2.2.1 A Norma ISO/IEC 12207

Criada pelas entidades internacionais ISO e IEC, através de um esforço conjunto. Originou-se em 1989, tendo sua primeira versão publicada em 1995. Após sofrer algumas emendas e algumas revisões para alinhamento a outras normas, tem sua versão mais atual datada em 2008 (Koscianski, 2007).

Seu objetivo é a definição de um padrão para o ciclo de vida do software, estabelecendo terminologias e práticas de processos envolvidos na produção do software e que podem ser referenciadas pela indústria. Pode ser aplicada à aquisição de sistemas, produtos e serviços de software, para o fornecimento, desenvolvimento, operação e manutenção de produtos de software executados de forma internamente ou externamente a uma organização (ABNT, 2009a).

A norma possui um estrutura que envolve todo o ciclo de vida do software, desde a concepção de idéias até a descontinuação do software, e é formada por um conjunto de processos, compostos por outros processos, atividades, tarefas e notas, que foram projetados para serem adaptados de acordo com cada projeto de software. A adaptação consiste na supressão de processos, atividades e tarefas não aplicáveis à organização ou ao projeto instanciado.

A Figura 2.2 apresenta uma representação da estrutura da norma, na qual cada área do conhecimento da Engenharia de Software é denominada processo, tendo nome, propósito e resultados. Cada processo contém um conjunto de atividades, sendo as atividades divididas em grupos de tarefas.

Os processos representados na norma estão associados nos sete grupos de processos identificados a seguir: (i) processos de estabelecimento de acordos; (ii) processos organizacionais; (iii) processos de projeto; (iv) processos técnicos; (v) processos de implementação do software; (vi) processos de apoio; e (vii) processos de reutilização.

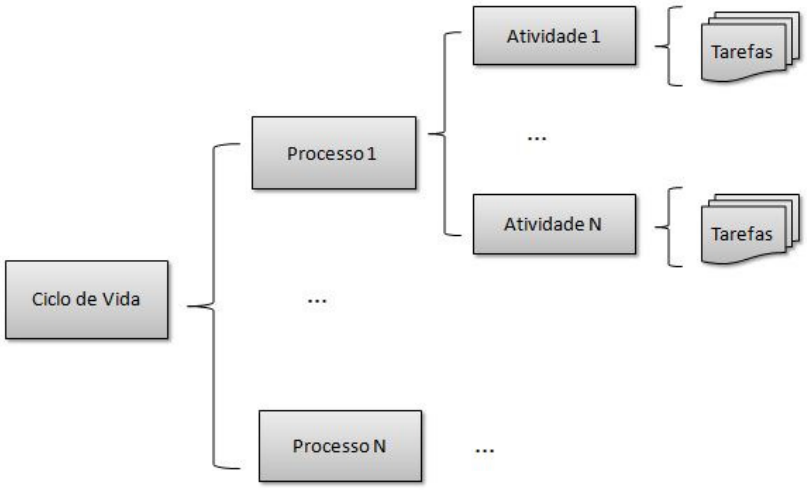

Figura 2.2 Estrutura da norma ISO/IEC 12207, envolvendo processos, atividades e tarefas (adaptado de Koscianski e Soares, 2007)

2.2.2 O Modelo CMMI-DEV

Criado a partir de um estudo desenvolvido pelo SEI – *Software Engineering Institute*, originalmente chamava-se CMM – *Capability Maturity Model* exercendo forte influência no convencimento da comunidade de Engenharia de Software em considerar seriamente o aprimoramento dos processos (Pressman, 2011).

Posteriormente, ao tentar integrar uma grande quantidade de modelos existentes, inclusive as subdivisões do CMM, foi desenvolvido o CMMI, substituindo os modelos CMM de Engenharia de Sistemas e de Software. O modelo tem a intenção de ser um *framework* de aprimoramento de processos que tem aplicabilidade ampla por meio de uma variedade de empresas (Ahern *et al.*, 2001).

Especificamente para o desenvolvimento de software, existe o guia CMMI-DEV, atualmente na versão 1.3, que contém práticas que abrangem gerência de projetos, gerência de processos, engenharia de sistemas, engenharia de hardware, engenharia de software e outros processos de suporte ao desenvolvimento e manutenção de software (SEI, 2010). Possui duas formas de representação:

a) **Representação por estágios**: áreas de processos são agrupadas com o intuito de serem avaliadas em níveis de maturidade de 1 a 5;
b) **Representação contínua:** permite uma classificação mais fina de cada área de processo individualmente, na qual a melhoria ocorre por níveis de capacidade em uma escala de 0 a 3.

O Quadro 2.1 apresenta um comparativo entre os níveis de maturidade e capacidade do CMMI-DEV, no qual um nível de capacidade está relacionado a uma área de processo e um nível de maturidade está relacionado a um conjunto de áreas de processo. Ambas representações utilizam níveis cumulativos, ou seja, um nível de capacidade mais alto inclui os atributos dos níveis mais baixos.

Quadro 2.1 Níveis do CMMI-DEV (adaptado de SEI, 2010)

Nível	Nível de Capacidade	Nível de Maturidade
0	Incompleto	*Inexistente*
1	Realizado	Inicial
2	Gerenciado	Gerenciado
3	Definido	Definido
4	*Inexistente*	Gerenciado Quantitativamente
5	*Inexistente*	Em Otimização

O CMMI-DEV está estruturado em 22 áreas de processo, cada uma contendo um propósito, algumas notas introdutórias, as áreas de processo relacionadas e os objetivos específicos. A Figura 2.3 apresenta graficamente a estrutura, que também é composta por objetivos genéricos, relacionados de forma igual a todas as áreas de processos.

Os objetivos (genéricos e específicos) são compostos por práticas (genéricas e específicas, respectivamente), que fornecem diretrizes para o alinhamento aos resultados desejados de cada área de processo. Apenas como aspecto informativo, cada prática específica possui subpráticas e produtos típicos de trabalho sugeridos, assim como cada prática genérica possui orientações para a aplicação e, também, subpráticas.

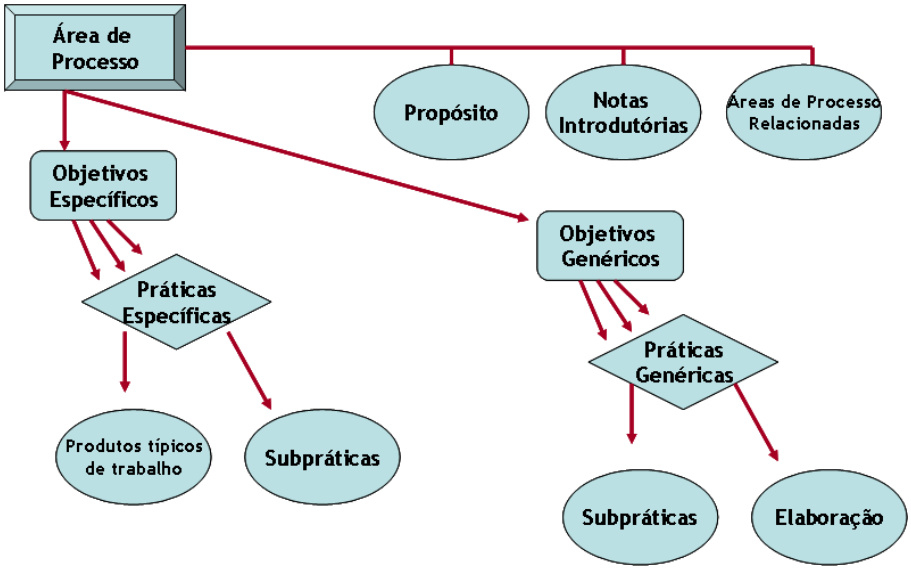

Figura 2.3 Componentes do modelo CMMI-DEV (adaptado de SEI, 2010)

2.2.3 O Modelo MR-MPS-SW

Criado no Brasil, em 2003, através de um parceria entre as instituições SOFTEX, Riosoft, COPPE/UFRJ, CESAR, CenPRA e CELEPAR, este Modelo de Referência MPS para software é integrante do programa MPS.BR (Melhoria do Processo de Software Brasileiro), mantido pela SOFTEX (Associação para Promoção da Excelência do Software Brasileiro) (SOFTEX, 2012a).

O modelo defende a melhoria do processo gradual, através de níveis de maturidade. Por ser voltado para a realidade brasileira, no qual é bastante custoso evoluir diversos processos concomitantemente, possui mais níveis de maturidade que o CMMI-DEV. Está dividido em três principais componentes: Modelo de Referência (MR-MPS), Método de Avaliação (MA-MPS) e Modelo de Negócio (MN- MPS). Cada componente é descrito por meio de guias e/ou documentos do modelo MPS (SOFTEX, 2012a).

A estrutura do modelo baseia-se nas normas NBR ISO/IEC 12207, ISO/IEC 15504 (ISO/IEC, 2004) e no modelo internacional CMMI, adaptadas à realidade das empresas brasileiras através de parcerias entre a SOFTEX, o Governo e as Universidades, como indicado na Figura 2.4.

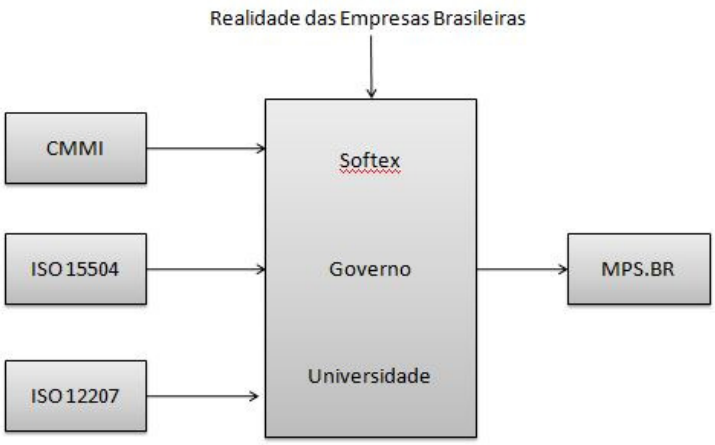

Figura 2.4 Construção do programa MPS.BR (Koscianski e Soares, 2007)

Composto por sete níveis de maturidade graduais e cumulativos, denominados por letras do alfabeto, segundo (SOFTEX, 2012a): G (Parcialmente Gerenciado), F (Gerenciado), E (Parcialmente Definido), D (Largamente Definido), C (Definido), B (Gerenciado Quantitativamente), A (Em Otimização).

Para cada um destes níveis de maturidade é atribuído um perfil de processo, indicando onde devem ser direcionados esforços de melhoria. O alcance de determinado nível de maturidade é obtido quando são atendidos os propósitos e todos os resultados esperados de cada processo do nível designado e os resultados esperados dos atributos de processos estabelecidos para aquele nível (vide Figura 2.5).

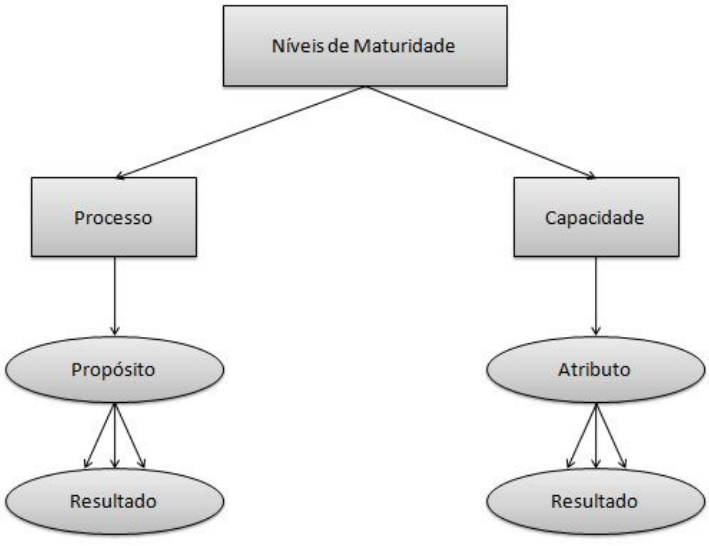

Figura 2.5 Estrutura do MR-MPS-SW (adaptado de Koscianski e Soares, 2007)

2.2.4 O Guia PMBOK

Criado pela instituição PMI – *Project Management Institute*, teve sua primeira publicação datada em 1996, atualmente encontra-se na quinta edição publicada em 2013. O Guia PMBOK trata-se de uma extensa documentação, que provê *guidelines* para o gerenciamento de projetos e definição de conceitos correlatos (PMI, 2014).

Segundo o próprio guia (PMI, 2014), seu propósito é identificar um subconjunto de conhecimentos em gerenciamento de projetos que geralmente são reconhecidos como boas práticas. "Geralmente reconhecidos" significa que os conhecimentos e as práticas descritos são aplicáveis na maioria dos projetos e há um consenso sobre seus valores e utilidades. "Boas práticas" significa que existe um consenso entre os especialistas que a aplicação do conhecimento, habilidade, ferramenta e/ou técnica pode aumentar a chance de sucesso de muitos projetos.

O guia descreve as tarefas a serem realizadas em um projeto através de processos, onde cada processo possui três elementos: (i) Entradas (documentos, planos, diagramas, etc.); (ii) Ferramentas e técnicas (mecanismos aplicados às entradas); e (iii) Saídas (documentos, planos, diagramas, etc.).

Cada um dos 47 processos definidos no guia PMBOK possuem dois tipos de classificações que agrupam um conjunto de processos. A primeira está relacionada ao ciclo de vida do projeto, que divide-o em cinco categorias: "Iniciação", "Planejamento", "Execução", "Monitoramento e Controle" e "Encerramento" (Vide Figura 2.6).

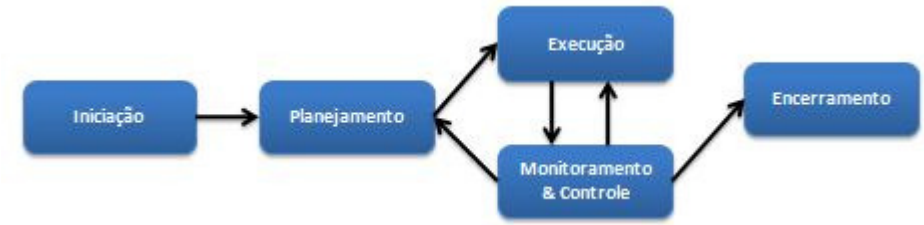

Figura 2.6 Grupos de processos de acordo com o ciclo de vida de um projeto (adaptado de PMI, 2014)

O outro tipo de classificação dos processos está relacionado ao agrupamento por áreas de conhecimento. São 10 grupos de processos, divididos em: "Integração", "Escopo", "Tempo", "Custo", "Qualidade", "Recursos Humanos", "Comunicações", "Riscos", "Aquisições" e "*Stakeholders*".

2.2.5 O Padrão Internacional ISO/IEC 16085:2006

Este padrão, específico para gerenciamento de riscos, descreve as atividades relacionadas à gerência de riscos executadas durante a aquisição, fornecimento, desenvolvimento e manutenção de sistemas ou softwares. Seu propósito é prover um conjunto único de requisitos de processos, adequados para a administração de uma ampla variedade de riscos que possam ocorrer em um projeto de software (IEEE, 2006).

Não é foco deste padrão prover o detalhamento das práticas relacionadas à gerência de riscos, seu foco está na definição do processo de gestão de riscos durante o ciclo de vida do software, identificando quais práticas são mais indicadas a serem aplicadas em cada atividade do processo.

O padrão ISO/IEC 16085 possui compatibilidade com a implantação da norma ISO/IEC 12207, podendo ser implantados em conjunto ou de forma independente. Caso seja utilizada a implantação conjunta, há a estruturação de ambos os documentos de forma semelhante.

O documento de especificação sugere um processo padrão (Figura 2.7), contendo 6 atividades diretamente relacionadas ao tratamento de riscos: "Planejar e Implementar a Gerência de Riscos", "Gerenciar o Perfil de Risco do Projeto", "Realizar Análise de Riscos", "Realizar Monitoramento de Riscos", "Realizar Tratamento de Riscos" e "Avaliar o Processo de Gerência de Riscos".

Para cada atividade apresentada é identificado um conjunto de tarefas, que possuem sugestões de quais documentos, práticas, técnicas ou ferramentas podem ser utilizadas para o alcance dos objetivos esperados.

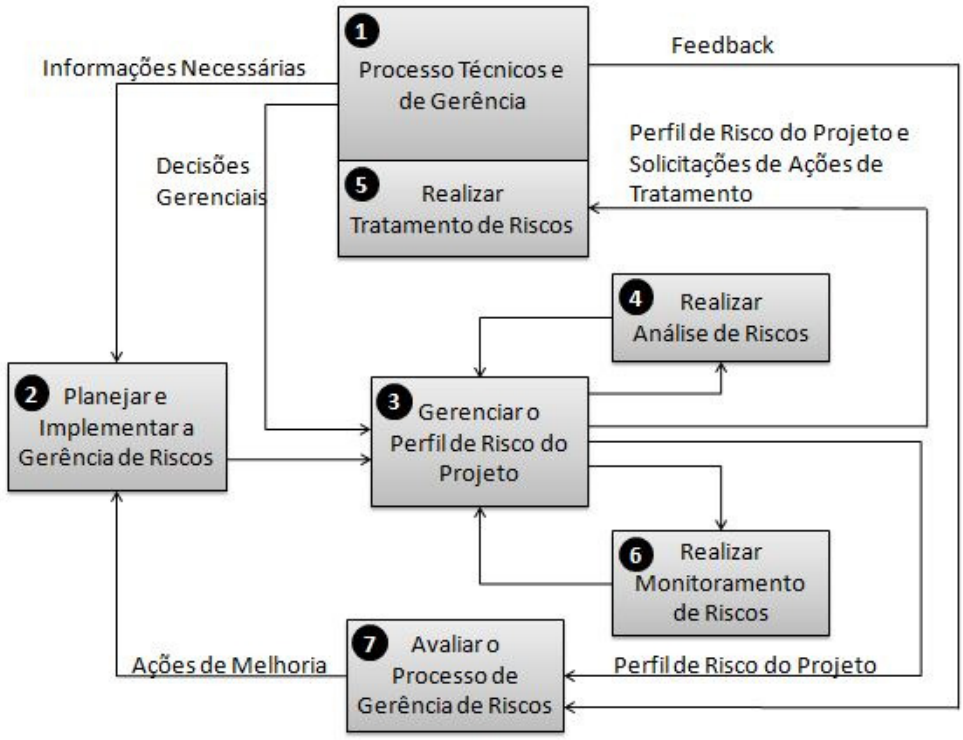

Figura 2.7 Processo para gerenciamento de riscos sugerido pelo padrão ISO/IEC 16085:2006 (IEEE, 2006)

2.3 Gerência de Riscos: Uma Visão Geral

Segundo o guia PMBOK, risco pode ser definido como a possibilidade de ocorrência de um evento ou condição que pode ter efeito positivo ou negativo em um objetivo de um projeto (PMI, 2014).

Charette (1989) define que um risco está relacionado a três aspectos: (i) um risco refere-se a aspectos futuros, uma vez que ontem e hoje não constituem uma preocupação, no sentido de que se está colhendo os resultados de nossas ações; (ii) risco envolve mudanças, que podem ser de opinião, ações, lugares, etc.; e (iii) riscos envolvem escolhas e as incertezas que as próprias escolhas trazem.

O instituto ISO possui uma norma específica para tratar princípios, terminologias e diretrizes relacionadas ao gerenciamento de risco, a norma ISO 31000:2009 (ABNT, 2009b), que define risco como um efeito da incerteza nos objetivos de um projeto, sendo que o efeito é um desvio em relação ao esperado (positivo ou negativo). Logo a gestão de riscos são atividades coordenadas para dirigir e controlar uma organização, no que se refere a riscos.

Ropponen e Lyytinen (2000) definem gerência de riscos como uma abordagem

que tenta formalizar práticas de sucesso orientadas a riscos em um conjunto de princípios e práticas prontamente aplicáveis. Enquanto que Chapman e Ward (2003) definem que o propósito da gerência de riscos é de melhorar a performance do projeto, através da identificação e da avaliação sistemática dos riscos, desenvolvendo estratégias para reduzi-los ou evitá-los, minimizando perdas e maximizando o sucesso do desenvolvimento do software.

Segundo Boehm (1991), a gerência de riscos pode ser dividida em oito principais passos: identificação, análise, priorização, gerência, planejamento, mitigação, resolução e monitoramento de riscos. Avdoshin e Pesotskaya (2011) identificaram que estudos mais recentes sintetizaram estes passos em cinco características:

a) **Identificação de riscos:** entendimento dos problemas comuns aos projetos que podem afetar o alcance dos objetivos;
b) **Análise de riscos:** definição da probabilidade de ocorrência, os possíveis impactos que causaria, e ordenamento de todos os riscos por grau de importância baseado nesses fatores;
c) **Planejamento de respostas aos riscos:** analisar as alternativas de avaliação dos riscos e modificar o plano do projeto para minimização de impacto ou probabilidade dos riscos;
d) **Monitoramento de riscos:** ao longo do projeto continuar a reavaliar as mudanças nos riscos identificados, identificar possíveis novos riscos e atualizar planejamentos após tomadas de ações;
e) **Documentação de lições aprendidas:** registro de informações relacionadas às etapas do gerenciamento de riscos para orientar melhorias do processo e planejamento de futuros projetos.

Para alcançar uma gestão de riscos eficaz, Willians *et al.*(1999), através de um relatório do SEI, recomendam a busca por alguns princípios, que envolvem: manter uma perspectiva global dos problemas; ter uma visão antecipada, estabelecendo planos de mitigação e contingência; estimular uma comunicação aberta e que estimule todos os interessados a sugerirem riscos a qualquer instante; integração da gestão de riscos à gestão de qualidade; enfatizar a melhoria contínua, aprimorando identificação e categorização dos riscos; desenvolver uma visão compartilhada e uniforme do produto entre todos os interessados; e estimular o trabalho em equipe.

Existem duas abordagem para lidar com riscos, segundo Pressman (2011). Uma delas é reativa, que espera que os riscos ocorram para terem que lidar com problemas, sendo menos recomendada e no melhor dos casos apenas identifica riscos e reserva recursos para tratá-los após a sua ocorrência. A outra forma, mais alinhada ao gerenciamento de riscos eficaz, é a proativa, que se inicia muito antes do trabalho técnico começar e tem como objetivo primário evitar a ocorrência do risco. Entretanto, como nem todos os riscos podem ser evitados, são desenvolvidos planos de contingência para permitir respostas de maneira controlada e eficaz.

O PMBOK (PMI, 2014) define quatro estratégias para planejamento de respostas aos riscos negativos:

a) **Eliminar:** engloba a alteração do plano de gerenciamento para remover totalmente a ameaça, podendo isolar os objetivos do projeto do impacto do risco ou alterar o objetivo que está em perigo, por exemplo estendendo o cronograma ou reduzindo o escopo;
b) **Transferir:** exige a mudança de alguns ou todos os impactos negativos de uma ameaça, incluindo a responsabilidade da resposta, para um terceiro. A transferência de um risco simplesmente passa a responsabilidade pelo gerenciamento para outra parte, mas não o elimina. É mais eficaz ao lidar com a exposição de riscos financeiros, e geralmente envolve o pagamento de um prêmio à parte que está assumindo o risco, podendo ser usados recursos, como por exemplo seguros, seguros-desempenho, garantias, fianças, etc.;
c) **Mitigar:** implica em focar na redução da probabilidade e/ou impacto de um risco para dentro dos limites considerados aceitáveis no projeto. A ação proativa de antecipar o risco, reduzindo probabilidade e/ou impacto, é em geral mais eficaz que tentar reparar os danos depois do risco ter ocorrido. Alguns exemplos de ações de mitigação são a adoção de processos menos complexos, fazer mais testes ou escolher um fornecedor mais estável;
d) **Aceitar:** raramente é possível ter recursos para tratar todos os riscos de um projeto, eliminando todas as ameaças, logo a aceitação de um risco indica que a equipe do projeto decidiu não alterar o plano de gerenciamento para lidar com o risco. Pode ser passiva ou ativa. A aceitação passiva não necessita de nenhuma ação, exceto a documentação da estratégia, deixando que a equipe trate os problemas, caso o risco ocorra. A estratégia de aceitação ativa mais comum é

estabelecer reservas para contingências, que podem ser na forma de tempo, dinheiro ou recursos para lidar com a ocorrência do risco.

Para Tianyin (2011), a gerência de riscos na indústria de software ainda carece de uma teoria completa, apesar de possuir uma documentação relevante, principalmente quando se trata da identificação e da análise de riscos em projetos. Isso ocorre primeiramente porque a indústria de desenvolvimento de software ainda é emergente, e as pessoas têm menos experiência acumulada que em outras áreas, e também devido a gerência de riscos ainda ser pouco abordada comparada às outras áreas do conhecimento em projetos de software, mesmo que muitos pesquisadores já tenham proposto vários modelos e práticas.

2.3.1 A Gerência de Riscos no Contexto de Normas, Modelos e Guias

As normas, modelos e guias relacionados a este trabalho (e descritos na seção 2.2 deste capítulo) possuem em seu conteúdo recomendações para a implantação da gerência de riscos, que podem ser na forma de modelo de processo, objetivos, práticas, técnicas, documentos ou ferramentas relacionados à área.

A norma ISO/IEC 12207 define um processo de gerência de riscos contendo seis atividades:

- Planejamento da gerência de riscos: suas tarefas envolvem a definição de políticas de gestão para riscos, documentação do processo que deverá ser implementado, definição de responsabilidades, fornecimento de recursos adequados aos responsáveis e descrição do processo de melhoria e avaliação do processo de gestão de riscos.
- Gerenciamento dos perfis de riscos: possui tarefas que orientam à definição do contexto da gerência de riscos, documentação dos limites do risco, estabelecimento do perfil de risco e comunicação periódica do perfil aos *stakeholders.*
- Análise de riscos: envolve tarefas que recomendam a identificação de riscos em categorias pré-estabelecidas, estimativa da probabilidade e consequência de cada risco, avaliação de prioridades de acordo com os limiares estabelecidos para cada risco, desenvolvimento de estratégias de tratamento aos riscos e definição de métricas para monitoramento dos

riscos durante a execução do processo.

- Tratamento de riscos: possui tarefas que indicam o fornecimento de alternativas aos tratamentos de riscos para os *stakeholders*, implementação da alternativa de tratamento selecionada, monitoramento e avaliação de riscos que estão sendo tratados.
- Monitoramento de riscos: recomenda a implementação de tarefas para monitorar todos os riscos e contextos estabelecidos, implementação e monitoramento de métricas para avaliar a efetividade do tratamento dos riscos, e procurar novos riscos e fontes de riscos durante o monitoramento do projeto.
- Avaliação do processo de gerência de riscos: suas tarefas envolvem a coleta de informações durante todo o ciclo de vida do projeto, a revisão do processo de maneira periódica, e revisão dos riscos identificados, para detectar novos riscos organizacionais.

O gerenciamento de riscos no CMMI-DEV é tratado no nível 3 de maturidade, segundo nível a ser avaliado no modelo, e possui três objetivos específicos, distribuídos em sete práticas específicas relacionadas ao planejamento da gestão de riscos, identificação, análise e mitigação de riscos.

A seguir são listados os objetivos específicos (SG - *Specific Goals*) relacionados às suas práticas (SP - *Specific Practices*) no guia referente ao modelo CMMI-DEV:

- SG 1 Preparar-se para Gestão de Riscos
  - SP 1.1 Determinar Fontes e Categorias de Riscos
  - SP 1.2 Definir Parâmetros para Riscos
  - SP 1.3 Estabelecer uma Estratégia para Gestão de Riscos
- SG 2 Identificar e Analisar Riscos
  - SP 2.1 Identificar Riscos
  - SP 2.2 Avaliar, Categorizar e Priorizar Riscos
- SG 3 Mitigar Riscos
  - SP 3.1 Elaborar Planos de Mitigação de Riscos
  - SP 3.2 Executar Planos de Mitigação de Riscos

O modelo MR-MPS-SW também possui um processo que aborda a gerência de riscos através de nove resultados esperados. Este processo, situado no nível C

(SOFTEX, 2013), tem como propósito a identificação, análise, tratamento, monitoramento e redução contínua dos riscos em nível organizacional e de projeto.

Os resultados esperados do processo de gerência de riscos do MR-MPS-SW estão relacionados abaixo:

- GRI1 - O Escopo da gerência de riscos é determinado
- GRI2 - As origens e as categorias de riscos são determinadas e os parâmetros usados para analisar riscos, categorizá-los e controlar o esforço da gerência de riscos são definidos
- GRI3 - As estratégias apropriadas para a gerência de riscos são definidas e implementadas
- GRI4 - Os riscos do projeto são identificados e documentados, incluindo seu contexto, condições e possíveis consequências para o projeto e as partes interessadas
- GRI5 - Os riscos são priorizados, estimados e classificados de acordo com as categorias e os parâmetros definidos
- GRI6 - Planos para a mitigação de riscos são desenvolvidos
- GRI7 - Os riscos são analisados e a prioridade de aplicação dos recursos para o monitoramento desses riscos é determinada
- GRI8 - Os riscos são analisados e a prioridade de aplicação dos recursos para o monitoramento desses riscos é determinada
- GRI9 - Ações apropriadas são executadas para corrigir ou evitar o impacto do risco, baseadas na sua prioridade, probabilidade, consequência ou outros parâmetros definidos.

O Guia PMBOK possui um grupo de processos voltados para o gerenciamento de riscos, que atuam nas fases de planejamento e monitoramento e controle. São processos que envolvem planejamento da gerência de riscos, identificação, análise quantitativa e qualitativa, planejamento das respostas e controle de riscos.

Os seis processos que compõem a abordagem do PMBOK para tratamento de riscos, abordados na Seção 11 do guia oficial (PMI, 2014), são os seguintes:

- 11.1 - Planejar a Gerência de Riscos
- 11.2 - Identificar Riscos
- 11.3 - Realizar Análise Qualitativa dos Riscos
- 11.4 - Realizar Análise Quantitativa dos Riscos

- 11.5 - Planejar Respostas aos Riscos
- 11.6 - Controlar Riscos

O padrão internacional ISO/IEC 16085:2006, como citado na seção 2.2.5, trata exclusivamente do gerenciamento de riscos em toda sua extensão, e além das atividades relacionadas ao gerenciamento de riscos em um ciclo de vida de um projeto, também relaciona atividades ao planejamento e avaliação do processo. Suas atividades e tarefas, que possuem estrutura semelhante à norma ISO/IEC 12207, são as seguintes de acordo com o documento original:

- *Plan and implement risk management*
  - *Establish risk management policies*
  - *Establish the risk management process*
  - *Establish responsibility*
  - *Assign resources*
  - *Establish the risk management process evaluation*
- *Manage the project risk profile*
  - *Define the risk management context*
  - *Establish risk thresholds*
  - *Establish and maintain the project risk profile*
  - *Communicate risk status*
- *Perform risk analysis*
  - *Risk identification*
  - *Risk estimation*
  - *Risk evaluation*
- *Perform risk treatment*
  - *Selecting risk treatment*
  - *Risk treatment planning and implementation*
- *Perform risk monitoring*
  - *Monitor risk*
  - *Monitor risk treatment*
  - *Seek new risks*
- *Evaluate the risk management process*
  - *Capture risk management information*
  - *Assess and improve the risk management process*

- *Generate lessons learned*

2.4 Trabalhos Relacionados

Através de uma revisão na literatura, foram analisados diversos trabalhos relacionados ao gerenciamento de riscos, porém não foram identificados muitos trabalhos sobre o mapeamento conjunto entre modelos de qualidade e metodologias em gerenciamento de riscos. Algumas propostas assemelham-se, porém não englobam práticas de diversos modelos de qualidade, ou não utilizam o modelo nacional MR-MPS-SW como referencial, que é mais abrangente que o modelo CMMI-DEV, como pode ser observado através do mapeamento abordado na Seção 3.1 deste trabalho.

A pesquisa de Raz e Hillson (2005) apresenta uma comparação entre os principais padrões internacionais para o gerenciamento de riscos, com o objetivo de identificar quais etapas são similares em cada padrão. Por ser um estudo um pouco mais antigo, pode ser considerado desatualizado, pois atualmente existem novas versões para alguns dos padrões abordados, também não é realizada uma análise de padrões voltados especificamente para o desenvolvimento de software.

Outros trabalhos mais recentes apresentaram mapeamentos entre modelos de qualidade de software. Von Wangenheim *et al.* (2010) realizam um mapeamento entre o modelo CMMI-DEV v1.2 e o Guia de Gerência de Projetos PMBOK 4ª edição, porém contempla apenas atividades relacionadas diretamente ao gerenciamento de projetos do guia CMMI-DEV, além de utilizar como base versões anteriores dos guias (PP - *Project Planning*, PMC - *Project Monitoring and Control*, SAM - *Supplier Agreement Management*).

Rout e Tuffley (2007) realizaram um mapeamento entre a norma ISO/IEC 15504 e o modelo CMMI-DEV, abordando também superficialmente a norma ISO/IEC 12207, não especificando de forma detalhada em quais atividades da norma há a aderência entre os modelos.

Mutafelija e Stromberg (2009) realizaram um mapeamento entre o modelo CMMI e as diversas normas ISO (9001:2000; 20000:2005; 15288:2008; 12207:2008) através de uma relação binária entre o modelo CMMI e as normas ISO, porém este trabalho não envolve práticas de outros modelos e guias de qualidade, como o MR-

MPS-SW ou o PMBOK.

Alguns trabalhos relacionados têm foco na definição de uma ferramenta para apoio à gerência de riscos. A Ferramenta TRIMS (TRIMS, 2014) foi desenvolvida pelo BMP – *Best Manufacturing Practices Center of Excellence*, como parte de uma suíte de produtos do PMWS – *Program Manager's Workstation*, sendo propriedade da marinha do governo dos Estados Unidos. Outra ferramenta, CRAMM (Yazar, 2002), foi desenvolvida pelo *British* CCTA – *Central Communication and Telecommunication Agency*, do governo do Reino Unido. No âmbito nacional, há a ferramenta *Riskfree* (Knob, 2006), desenvolvida na PUC-RS, baseada nas boas práticas do PMBOK e aderente ao modelo CMMI.

A tese de doutorado de Islam (2011) apresenta um *framework* para gerenciamento de riscos orientado a objetivos. O *framework*, denominado GSRM possui quatro níveis de abstração: (1) primeiramente define os objetivos dos projetos; em seguida (2) identifica os obstáculos que podem impedir que o projeto atinja seus objetivos (fatores de riscos ou perfil dos riscos); depois, (3) para cada fator de risco, identifica suas conseqüências (definição dos riscos); e finalmente (4) define como deve ser realizado o tratamento e o monitoramento dos riscos. O foco deste trabalho, porém é relatar um estudo de caso, realizado com a implementação deste *framework*, no qual é apresentada a forma de avaliação e de coleta de dados, o detalhamento do estudo de caso com as atividades realizadas, e uma discussão sobre resultados e conclusões obtidas após a finalização do experimento. A realidade apresentada no estudo de caso pode ser apenas local (Europa), podendo haver grande diferença, caso haja aplicação do *framework* em outros contextos. Além disso, todo o processo poderia ser sistematizado, facilitando sua implementação, que inclusive segundo autor, pode ser complexa, caso hajam inúmeros objetivos em um projeto.

Em seu trabalho, Tianyin (2011) apresenta uma visão geral sobre a gerência de riscos e cita alguns modelos de processos de gerenciamento de riscos. Há uma descrição de padrões, modelos e normas relacionados ao gerenciamento de riscos desde os anos 80, citando os principais conceitos e técnicas definidas na área. Apesar da lista de modelos de processos apresentada ser bastante diversificada, não há um detalhamento, também não são apresentados mapeamentos entre os modelos, a fim de concluir quais vantagens e desvantagens de cada.

Pereira (2005) apresenta um processo de Gerenciamento de Riscos para projeto

de software baseado em versões anteriores de modelos de qualidade, utilizando o *framework* do RUP – *Rational Unified Process*, assim como um relato da implantação deste processo em uma organização. No entanto, este estudo define um processo rígido, com tarefas e artefatos definidos, que dificultam a adaptação para a implementação em outras organizações com culturas diferentes. Apesar de utilizar como base diversos modelos de qualidade, o modelo nacional MR-MPS-SW foi desconsiderado, deixando de fora práticas exclusivas a este modelo, no qual tratando-se de Gerência de Riscos é mais abrangente que o CMMI-DEV utilizado como referência (SOFTEX, 2012b).

Gonçalves (2006) apresentou em sua dissertação um modelo de processo de gerenciamento de riscos (GRisk-Model) e uma ferramenta (GRisk-Tool). O GRisk-Model foi desenvolvido com base na literatura da área e a partir da experiência de diretores, gerentes e analistas de sistemas seniores de fábricas de software brasileiras, enquanto a ferramenta implementa o modelo de gerenciamento de risco fornecendo condições para que a base de conhecimento produzida durante a execução dos projetos possa ser atualizada e acrescida de informações de riscos de outros projetos.

Os diferenciais da pesquisa aqui apresentada em relação aos trabalhos relacionados encontram-se na definição de uma metodologia para o gerenciamento de riscos, que se baseia nas boas práticas sugeridas pelos modelos, normas e guias de qualidade mais citados na literatura técnica. Além disso, o modelo pretende fornecer um conjunto de formas de implementação para cada atividade descrita, permitindo ao gerente escolher a opção que mais se adéqua à realidade da sua organização. Outra observação destacada é o fato de haver muitas pesquisas relacionadas ao modelo de maturidade CMMI-DEV, porém uma carência de estudos de mapeamentos relacionados ao modelo de maturidade nacional MR-MPS-SW, que possui mais objetivos a serem atingidos no gerenciamento de ricos, que o modelo CMMI-DEV.

2.5 Considerações Finais

A definição de um processo de software é importante, pois a busca pela qualidade de processo pode levar a um aumento na qualidade do produto gerado,

evitando que seja entregue ao cliente um software que não esteja alinhado às expectativas e requisitos estabelecidos pelo usuário.

Os modelos, normas e guias descritos neste capítulo, buscam reunir um conjunto de práticas, consideradas pela indústria como boas soluções para as diversas fases de um ciclo de vida do software, os mesmos também têm o intuito de definir conceitos comuns a cada área do conhecimento que pode envolver o desenvolvimento de software eficaz.

Uma importante área do conhecimento relacionada entre os modelos normas e guias envolvidos neste trabalho é a gerência de riscos, que pretende amenizar as consequências envolvidas em uma atividade tão complexa quanto o gerenciamento de projetos de software.

As consequências danosas aos projetos de software podem afetar escopo, cronograma e consequentemente custos previamente estabelecidos. Logo, adotar práticas recomendadas por entidades nacionais e internacionais para gerenciar riscos é um forte indicador de um processo eficaz, que resulta em um produto de qualidade e não provoca excesso de custos ou grandes disparidades entre cronograma ou escopo planejados, em relação aos resultados.

3 A METODOLOGIA DO PROCESSO DE GERÊNCIA DE RISCOS EM PROJETOS DE SOFTWARE

Este capítulo aborda o principal resultado da pesquisa apresentada nesta dissertação, que se trata da proposta de uma metodologia para orientar o gerenciamento de riscos em projetos de software, baseada nos principais modelos, normas e guias de qualidade existentes na literatura especializada. A metodologia originou-se a partir de um conjunto de boas práticas, retiradas do mapeamento entre os documentos de referência destes modelos, normais e guias.

O mapeamento consistiu em identificar pontos em comum e distintos entre os modelos e normas, e analisar quais sugestões de implementações abordadas nos guias de qualidade poderiam ser aderentes aos objetivos propostos. O ponto de interseção definido para o mapeamento foi o modelo de qualidade MR-MPS-SW, visto que há uma carência do foco neste guia entre os trabalhos relacionados abordados no Capítulo 2, ou seja, o modelo de referência do MPS.BR foi utilizado como comparação entre todos os outros modelos, normas e guias envolvidos neste estudo.

A coleção de boas práticas, juntamente com o mapeamento, têm o intuito de orientar o trabalho dos implementadores de processo de software na realização de uma implementação integrada, e dar liberdade para definirem quais práticas desejam adotar de acordo com quais modelos, normas ou guias foram escolhidos para serem aplicados na organização.

A metodologia proposta está definida em fases, que consistem em um conjunto de tarefas orientadas por um fluxo. Cada tarefa contém orientações de passos, sugestões de informações de entradas, saídas e de papéis envolvidos, para que possam ser utilizados na implementação do processo de gerência de riscos.

Ainda, este capítulo aborda os diferenciais da proposta em relação a trabalhos semelhantes, e o relato da avaliação da metodologia através de uma avaliação realizada por um especialista.

3.1 O Mapeamento entre Modelos de Qualidade

Para mapear todas as boas práticas foi tomado como base o modelo MR-MPS-SW, visto que este é mais utilizado no âmbito nacional, e há menor ocorrência de pesquisas envolvendo este modelo com mapeamentos.

Inicialmente foi realizada uma análise comparativa entre os resultados esperados do processo de Gerência de Riscos do guia de implementação do MR-MPS-SW parte 11, e as tarefas do processo de Gestão de Risco da norma ISO/IEC 12207 (ABNT, 2008), resultando em uma tabela que agregou itens dos dois modelos. O guia de implementação parte 11 (SOFTEX, 2012b) realiza um mapeamento entre os resultados esperados dos processos do MR-MPS-SW, com as práticas específicas dos processos do CMMI-DEV 1.3.

Posteriormente, o guia de implementação parte 11 foi analisado em conjunto com a área de conhecimento de Gerenciamento de Riscos do guia PMBOK - 5ª edição (PMI, 2014), através do mapeamento de resultados esperados com as entradas, as ferramentas e técnicas, e as saídas de cada processo definido para esta área.

Além disso, foi realizado um mapeamento semelhante com o padrão internacional ISO/IEC 16085:2006 (IEEE, 2006), que trata sobre a implementação de gerência de riscos. Estes estudos resultaram em uma tabela comparativa entre os resultados esperados e as orientações de implementação contidas nestes modelos de qualidade.

Logo há dois tipos de mapeamentos: (i) o mapeamento entre o MR-MPS-SW, o CMMI-DEV e a norma ISO/IEC 12207, que visa identificar a possibilidade de um processo aderente a ambos, através de resultados esperados e tarefas em comum; e (ii) o mapeamento entre MR-MPS-SW e as recomendações presentes nos padrões PMBOK e ISO/IEC 16085, que visa agrupar um conjunto de sugestões de implementação do processo de gerência de riscos.

A formação do mapeamento foi realizada através da definição de quais elementos foram selecionados para comparação, sendo divididos em macrocomponentes, que encapsulam microcomponentes (vide Quadro 3.1). A busca por

aderência deu-se a partir da procura de quaisquer microcomponentes que possam ser equivalentes entre todos os macrocomponentes relacionados.

Quadro 3.1 Equivalência entre componentes das referências

	MR-MPS-SW	**CMMI-DEV**	**ISO/IEC 12007**	**PMBOK**	**ISO/IEC 16085**
Macro Componentes	Processo	Área de Processo	Processo	Área de Conhecimento	*Risk Management Process*
Micro Componentes	Resultados Esperados	Práticas Específicas	Tarefas	Entradas, Ferramentas e Técnicas e Saídas	*Tasks*

Para categorizar a análise conjunta de forma mais clara, cada mapeamento realizado entre o guia MR-MPS-SW e os outros modelos recebeu uma classificação relacionada ao grau de mapeamento. Esta classificação é baseada na classificação que o guia de implementação parte 11 (SOFTEX, 2012b) realiza entre os modelos MR-MPS-SW e CMMI-DEV, dividindo-se nas seguintes categorias:

- Equivalente (EQU): as exigências do MR-MPS-SW e da ISO/IEC 12207 são exatamente as mesmas; e/ou uma sugestão de implementação do PMBOK ou da ISO/IEC 16085 atendem às necessidades do resultado esperado do MR-MPS-SW em sua totalidade;
- Equivalente em conjunto (EQU+): as exigências do MR-MPS-SW e da ISO/IEC 12207 são exatamente as mesmas quando complementadas com mais de um resultado esperado ou tarefa; e/ou duas ou mais sugestões de implementação do PMBOK ou da ISO/IEC 16085 atendem às necessidades do resultado esperado do MR-MPS-SW;
- Não Equivalente (NEQ): as exigências do MR-MPS-SW e da ISO/IEC 12207 não são exatamente as mesmas; e/ou uma sugestão de implementação do PMBOK ou da ISO/IEC 16085 não atende totalmente ao resultado esperado do MR-MPS-SW, nem possui complementação para ser atendida em conjunto;
- Inexistente (INE): não existe resultado esperado do MR-MPS-SW na ISO/IEC 12207 ou vice e versa; e/ou não existe sugestão de implementação no PMBOK ou na ISO/IEC 16085 que atenda ao resultado esperado, ou vice e versa.

O resultado dos estudos comparados apresentam-se da seguinte forma: cada resultado esperado no MR-MPS-SW será apresentado com uma breve descrição e análise relacionada à implantação em conjunto com o modelo CMMI-DEV e com a norma ISO/IEC 12207; em seguida serão relacionadas as orientações de implementação presentes no Guia PMBOK e no padrão internacional ISO/IEC 16085, mapeadas a este resultado esperado.

Cada subseção a seguir apresenta um resultado esperado do processo de Gerência de Riscos (GRI) do MR-MPS-SW juntamente com os resultados obtidos no estudo. O primeiro resultado esperado possui o acrônimo de GRI1, o segundo de GRI2 e assim sucessivamente.

Os microcomponentes (resultados esperados, práticas específicas, tarefas, entradas, ferramentas e técnicas, saídas e *tasks*) constantes nos modelos de qualidade que não possuem uma prática equivalente no modelo MR-MPS-SW, são apresentados na Subseção 3.1.10 deste segmento do trabalho.

3.1.1 GRI1 - O escopo da gerência de riscos é determinado

Este resultado esperado exige que seja definida claramente a abrangência da aplicação do processo de gerência de riscos na organização e dentro do âmbito de projetos. Segundo o guia de implementação 11 do MR-MPS-SW, existe uma relação do tipo NEQ com a prática específica (*Specific Practices*) SP1.3 da área de processo de Gestão de Riscos do CMMI-DEV, pois a prática do CMMI-DEV refere-se apenas ao escopo em projetos.

No mapeamento com a norma ISO/IEC 12207 apresentado no Quadro 3.2, foi identificada uma relação do tipo EQU+ com duas tarefas da norma, são elas: a tarefa 6.3.4.3.1.1, que está alinhada ao GRI1 por exigir o tratamento da gerência de riscos no contexto da organização através de uma política de gestão; e a tarefa 6.3.4.3.2.1, que define que devem ser descritas as perspectivas das partes interessadas, as categorias de riscos e uma descrição de objetivos técnicos e gerenciais, além de suposições e limitações. Este detalhamento pode estar incluso em uma política organizacional para o tratamento do risco, e em cada Plano de Risco individual de um projeto.

Quadro 3.2 Mapeamento entre o resultado esperado GRI1 e as tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa da Norma ISO/IEC 12207	Grau de Mapeamento
GRI1 - O escopo da gerência de riscos é determinado.	6.3.4.3.1.1 - As políticas de gestão de risco que descrevem as diretrizes sob as quais a gestão de risco será executada devem ser definidas.	EQU+
	6.3.4.3.2.1 - O contexto do Processo de Gestão de Risco deve ser definido e documentado	EQU+

As orientações de implementação deste resultado esperado, segundo o PMBOK, sugerem que sejam utilizadas as entradas, as ferramentas e técnicas, e as saídas referentes ao processo 11.1 - Planejar o Gerenciamento de Riscos, que determina a realização de reuniões e a análise de planejamento para definir o escopo de um projeto. Como entradas podem ser utilizados a declaração do escopo do projeto, os planos de gerenciamento de custos, cronograma, comunicações e alguns ativos de processos organizacionais, como categorias de riscos, formatos da declaração de riscos, papéis e responsabilidades, entre outros. A saída do processo 11.1 que equivale ao GRI1 é implementada no item metodologia do plano de gerenciamento de riscos, porém apenas no que diz respeito ao âmbito de um projeto, por isso possui classificação (NEQ).

O padrão internacional ISO/IEC 16085 recomenda, em seu item 5.1.1.1 - *Establish risk management policies*, que devem ser estabelecidas políticas de gestão de riscos descrevendo: como a gerência de riscos deve ser implementada, administrada e apoiada pela gerência e funcionários; como deve ser obtido e mantido o compromisso contínuo das partes interessadas; como o processo de gerenciamento de riscos deve ser coordenado; como orientações e treinamentos a respeito de gerenciamento de riscos devem ser conduzidos; como informações sobre riscos são comunicadas e realizadas pelas partes interessadas. Em um plano de projeto, esta política deve ser referenciada e detalhados apenas os pormenores específicos ao projeto. Possui grau de mapeamento EQU+ atendido em conjunto com o item 5.1.2.1 - *Establish the risk management process* do padrão.

Outro item equivalente, descrito no tópico 5.1.2.1 do padrão proposto pela ISO/IEC, descreve acerca da definição e documentação do contexto do gerenciamento de riscos, no qual deve conter uma descrição técnica e gerencial dos objetivos, suposições e restrições, entre outras informações relevantes que surgirem.

3.1.2 GRI2 - As origens e as categorias de riscos são determinadas e os parâmetros usados para analisar riscos, categorizá-los e controlar o esforço da gerência de riscos são definidos

Este resultado esperado exige que seja definida uma classificação e critérios para a determinação da probabilidade e severidade dos riscos no âmbito organizacional. O guia de implementação parte 11 sugere que o GRI2 seja atendido em conjunto pelas práticas específicas 1.1 e 1.2 da área de processo de Gerência de Riscos do CMMI-DEV, que exigem a determinação das fontes e categorias de riscos (SP 1.1) e parâmetros para definição, categorização e controle dos riscos (SP 1.2).

O mapeamento do GRI2 com a norma ISO/IEC 12207 acontece em três tarefas, são elas: 6.3.4.3.2.2 e 6.3.4.3.2.3 na categoria EQU+, pois as tarefas descrevem, respectivamente, sobre um perfil de risco, que seriam as categorias de riscos organizacionais, e os limites destes riscos, que é a realização de cálculos para determinar quando um risco é aceitável; também foi identificado um mapeamento na categoria NEQ com a tarefa 6.3.4.3.2.4, que determina, após priorizados, estimados e classificados, que os perfis dos riscos devem ser comunicados aos interessados, comunicação esta não mencionada pelo MR-MPS-SW. Estas informações estão resumidas no Quadro3.3.

Quadro 3.3 Mapeamento entre o resultado esperado GRI2 e as tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa da Norma ISO/IEC 12207	Grau de Mapeamento
GRI2 - As origens e as categorias de riscos são determinadas e os parâmetros usados para analisar riscos, categorizá-los e controlar o esforço da gerência de riscos são definidos	6.3.4.3.2.2 - Os limites de risco que definem as condições sob as quais um nível de risco pode ser aceitável, deve ser documentado.	EQU+
	6.3.4.3.2.3 - Um perfil de risco deve ser estabelecido e mantido	EQU+
	6.3.4.3.2.4 - O perfil de risco relevante deve ser comunicado periodicamente para as partes interessadas com base em suas necessidades.	NEQ

As orientações de implementação presentes no Guia PMBOK recomendam que para atingir este resultado esperado, é possível utilizar a ferramenta e técnica constante no item 11.3.2 - Categorização dos riscos, do processo Realizar a Análise Qualitativa dos Riscos. Durante a realização da categorização de riscos, é possível utilizar a EAR

(Estrutura Analítica de Riscos), contendo as categorias de riscos organizacionais, com severidade e probabilidade de ocorrência.

O resultado do mapeamento com o padrão ISO/IEC 16085 identificou as sugestões de implementação contidas: no item 5.1.2.2 - *Establish risk thresholds*, definindo que os limites de riscos identificados podem ser medidos para custo, cronograma, fatores técnicos ou outros fatores relevantes; e no item 5.1.2.3 - *Establish and maintain the project risk profile*, que sugere que um perfil de risco deve ser estabelecido e mantido, onde este perfil de risco pode conter, pelo menos o contexto da gerência de risco, um registro de cada categoria de risco, incluindo probabilidade, consequência e limite de risco, a prioridade de cada categoria de risco, e as ações recomendadas para tratamento de cada risco; também podem ser utilizadas as orientações de implementação constante no item 5.1.2.4 - *Communicate risk status*, que sugere que os riscos acima do limite determinado devem ser comunicados, de forma periódica às partes interessadas baseado em suas necessidades, direcionando apenas as informações de riscos necessárias a cada.

3.1.3 GRI3 - As estratégias apropriadas para a gerência de riscos são definidas e implementadas

O resultado esperado GRI3 determina que em um projeto devem ser relacionados aspectos como: escopo, ferramentas, métodos, a serem utilizados na identificação, análise, mitigação, monitoração dos riscos, entre outros. Estas informações podem ser agregadas em um plano de gerência de riscos. O mapeamento com o CMMI-DEV identificou que existe uma prática específica totalmente equivalente a este resultado esperado, o SP1.3 - Estabelecer e manter a estratégia a ser utilizada para a gestão de riscos.

O mapeamento com a norma ISO/IEC 12207, demonstrado no Quadro 3.4, identificou relação entre este resultado esperado e quatro tarefas da norma, de forma que,ao serem agregadas, são equivalentes ao GRI3. As tarefas 6.3.4.3.1.2, 6.3.4.3.1.3, 6.3.4.3.1.4 e 6.3.4.3.1.5 determinam etapas da estratégia da gerência de risco, analogamente, cada tarefa representa um tópico no plano de gerenciamento de riscos resultante do GRI3, como o detalhamento de todo processo de gestão de riscos, a definição das partes interessadas com seus papéis e responsabilidades, e a forma de

acesso aos recursos, além da forma como a gestão de riscos será avaliada e monitorada.

Quadro 3.4 Mapeamento entre o resultado esperado GRI3 e as tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa da Norma ISO/IEC 12207	Grau de Mapeamento
GRI3 - As estratégias apropriadas para a gerência de riscos são definidas e implementadas	6.3.4.3.1.2 - A descrição do Processo de Gestão de Risco a ser implementado deve ser documentada.	EQU+
	6.3.4.3.1.3 - As partes responsáveis em realizar a Gestão de Risco, seus papéis e responsabilidades devem ser identificados.	EQU+
	6.3.4.3.1.4 - As partes responsáveis devem ter acesso aos recursos adequados para a realização do processo de Gestão de Risco.	EQU+
	6.3.4.3.1.5 - Uma descrição do processo para avaliar e melhorar o Processo de Gestão de Risco deve ser fornecida.	EQU+

Segundo o PMBOK, este resultado esperado, sendo totalmente equivalente (EQU) ao processo 11.1 - Planejar o Gerenciamento de Riscos, todas as entradas, as ferramentas e técnicas, e as saídas sugeridas são aplicáveis para atingir o resultado. O principal artefato deste processo do PMBOK é o plano de gerenciamento de riscos, que pode conter: a metodologia de trabalho relacionado a riscos durante o ciclo de vida do projeto; os papéis e responsabilidades; o orçamento atribuído ao tratamento e mitigação de riscos; os prazos; a categoria de riscos do projeto; as definições de probabilidade e impacto; a matriz de probabilidade e impacto; as tolerâncias revisadas das partes interessadas; os formatos dos relatórios; o acompanhamento de riscos.

As orientações de implementação deste resultado esperado, segundo o padrão ISO/IEC 16085, determinam que deve ser estabelecido um processo de gerenciamento de riscos (item 5.1.1.2 - *Establish the risk management process*), no qual devem-se descrever: a frequência com que cada risco será analisado novamente e monitorado; o tipo de análise de risco necessário (quantitativo ou qualitativo); as escalas de probabilidade e consequências dos riscos; os tipos de limites de riscos; os tipos de medidas utilizadas para monitorar os riscos; como os riscos são priorizados para tratamento; as fontes de riscos e as categorias de riscos. Outros itens relacionados à implementação deste resultado esperado, são 5.1.1.3 - *Establish responsibility* e 5.1.1.4- *Assing resources*, que determinam que as partes responsáveis pelo gerenciamento de

riscos devem ser explicitamente identificadas, e os recursos necessários para aplicar o gerenciamento de riscos devem ser devidamente fornecidos. Além disso, o item 5.1.1.4 determina que deve ser estabelecido um processo de avaliação do gerenciamento de riscos, identificando como as métricas serão capturadas para futuras lições aprendidas.

3.1.4 GRI4 - Os riscos do projeto são identificados e documentados, incluindo seu contexto, condições e possíveis consequências para o projeto e as partes interessadas

O resultado esperado GRI4 determina que os riscos potenciais para um projeto devem ser identificados, assim como o contexto e as prováveis causas do risco, além de suas decorrentes consequências. Este resultado esperado é categorizado como NEQ com a prática específica SP 2.1 da área de processo Gerência de Riscos do CMMI-DEV, pois ambos os modelos exigem a identificação de riscos, porém o guia MR-MPS-SW é mais abrangente, obrigando a menção do contexto, condições e consequências.

Este resultado esperado é mapeado de forma totalmente equivalente com a tarefa 6.3.4.3.3.1 da norma ISO/IEC 12207, que exige que os riscos devem ser identificados nas categorias descritas no contexto de gestão de riscos. O Quadro 3.5 apresenta o resumo das informações do mapeamento deste resultado esperado.

Quadro 3.5 Mapeamento entre o resultado esperado GRI4 e tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa da Norma ISO/IEC 12207	Grau de Mapeamento
GRI4 - Os riscos do projeto são identificados e documentados, incluindo seu contexto, condições e possíveis consequências para o projeto e as partes interessadas	6.3.4.3.3.1 - Os riscos devem ser identificados nas categorias descritas no contexto de gestão de riscos	EQU

O GRI4 é totalmente equivalente (EQU) ao processo 11.2 do guia PMBOK, logo todas suas entradas, saídas, e ferramentas e técnicas podem ser aplicadas para atender este resultado esperado. Como sugestão de implementação, para coletar a lista de riscos, identifica-se: a revisão de documentação de projetos anteriores; as técnicas de coletas de informações, como *brainstormings*, técnica Delphi, entrevistas e análise de causa raiz; a análise de *checklists* de riscos; a análise de premissas; as técnicas de diagramas (de

causa e efeito, fluxograma, de influência); a análise de matriz SWOT. As sugestões de artefato que atendem a este resultado esperado é uma lista de riscos, contendo a identificação, o impacto, a causa, o efeito e os responsáveis, além da lista de potenciais respostas para cada risco identificado.

O padrão ISO/IEC 16085 sugere várias abordagens para a implementação deste resultado esperado no item 5.1.3.1 - *Risk identification*. Estas abordagens podem incluir o uso de questionários, *brainstormings*, análise de cenários, lições aprendidas, prototipação, entre outras. É importante ressaltar que riscos não identificados são automaticamente considerados implicitamente como aceitos. Este item também sugere que os riscos precisam ser categorizados de forma a relacioná-los combinadamente, facilitando análise, monitoramento, tratamento e comunicação com as partes interessadas.

3.1.5 GRI5 - Os riscos são priorizados, estimados e classificados de acordo com as categorias e os parâmetros definidos

O resultado esperado GRI5 determina que cada risco identificado deve ser priorizado, estimado e classificado, para que sejam direcionados recursos de tratamento de riscos aos mais prioritários. O guia de implementação parte 11 sugere que este resultado esperado seja totalmente equivalente (EQU) à prática SP 2.2 - Avaliar e categorizar cada risco identificado utilizando as categorias e os parâmetros definidos para riscos, e determinar suas prioridades relativas, pois possuem as mesmas exigências.

O GRI5 está alinhado com a norma ISO/IEC 12207 através de duas tarefas, 6.3.4.3.3.2 e 6.3.4.3.3.3, que em conjunto atingem as necessidades exigidas pelo MR-MPS-SW. Estas tarefas determinam, respectivamente, que a probabilidade de cada risco devem ser estimadas, e que cada risco deve ser avaliado se está acima do limite, ou seja, acima dos parâmetros definidos. Este mapeamento está resumido no Quadro 3.6.

Este resultado esperado possui o grau de mapeamento EQU com o processo 11.3 do guia PMBOK, portanto suas recomendações são totalmente aplicáveis para atingir os objetivos exigidos pelo MR-MPS-SW. Logo, como orientação de implementação deste resultado esperado, sugere-se a realização de: avaliação de probabilidade e impacto de riscos; utilização de matriz de probabilidade e impacto; avaliação da qualidade dos dados sobre os riscos; categorização de riscos; avaliação da urgência de riscos; e

sugestão de opinião especializada. A sugestão de artefato alinhado ao GRI5 é a atualização da lista de riscos priorizada e categorizada, mencionando a causa dos riscos, uma lista de riscos que requerem respostas a curto prazo, uma lista de observação de riscos de baixa prioridade e a tendência nos resultados da análise qualitativa dos riscos

Quadro 3.6 Mapeamento entre o resultado esperado GRI5 e as tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa da Norma ISO/IEC 12207	Grau de Mapeamento
GRI5 - Os riscos são priorizados, estimados e classificados de acordo com as categorias e os parâmetros definidos	6.3.4.3.3.2 - A probabilidade de ocorrência e as consequências de cada risco identificado devem ser estimadas.	EQU+
	6.3.4.3.3.3 - Cada risco deve ser avaliado em comparação com seu limite.	EQU+

O GRI5 tem como sugestão de implementação no padrão ISO/IEC 16085: o item 5.1.3.2 - *Risk estimation*, que especifica que a estimativa de riscos pode ser qualitativa ou quantitativa, as partes interessadas devem definir quais riscos já priorizados serão avaliados detalhadamente; e o item 5.1.3.3 - *Risk evaluation*, que detalha a avaliação de riscos de forma comparada aos seus limites, através de árvores de decisão, planejamento de cenários e análise probabilística.

3.1.6 GRI6 - Planos para a mitigação de riscos são desenvolvidos

Este resultado esperado determina a criação de planos de mitigação e contingência, que têm como objetivo diminuir a probabilidade de ocorrência do risco ou atenuar seus possíveis efeitos, antes que o risco ocorra (mitigação), ou depois (contingência). O guia de implementação parte 11 (SOFTEX, 2012b) sugere que este resultado esperado seja totalmente equivalente (EQU) à prática SP 3.1 - Elaborar um plano de mitigação de riscos conforme a estratégia para gestão de riscos, pois possuem as mesmas exigências.

O GRI6 está alinhado com a norma ISO/IEC 12207 através de duas tarefas, 6.3.4.3.3.4 e 6.3.4.3.4.1, que em conjunto atingem as necessidades exigidas pelo MR-MPS-SW. Estas tarefas determinam, respectivamente, que: (1) para riscos acima do

limite definido, ou seja prioritários, devem ser definidas estratégias de tratamento dos riscos através de planos de mitigação e contingência; e (2) após a priorização e desenvolvimento dos planos, todas as informações devem ser reportadas às partes interessadas, para serem tomadas decisões relativas ao tratamento ou aceitação dos riscos. O mapeamento deste resultado esperado possui equivalência em conjunto (EQU+) e está resumido no Quadro 3.7.

Quadro 3.7 Mapeamento entre o resultado esperado GRI6 e tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa da Norma ISO/IEC 12207	Grau de Mapeamento
GRI6 - Planos para a mitigação de riscos são desenvolvidos	6.3.4.3.3.4 - Para cada risco que esteja acima do limite definido, estratégias recomendadas para tratamento devem ser definidas e documentadas. As medições que indicam a eficácia das opções de tratamento também devem ser definidas e documentadas.	EQU+
	6.3.4.3.4.1 - As partes interessadas devem ter acesso às opções recomendadas para o tratamento de risco e as ações solicitadas	EQU+

O GRI6 é totalmente equivalente (EQU) ao processo 11.5 do guia PMBOK, logo todas suas entradas, saídas, e ferramentas e técnicas podem ser aplicadas para atender este resultado esperado. Como sugestão de implementação deste resultado, podem ser adotadas as seguintes estratégias para tratamento de riscos negativos: eliminação, transferência, mitigação ou aceitação. Para riscos positivos, é possível adotar a estratégia de explorar, compartilhar, melhorar e aceitar. Os artefatos recomendados pelo guia para a saída deste processo são os próprios planos de tratamento dos riscos e decisões contratuais relacionadas à transferência de riscos.

O GRI6 tem como sugestão de implementação no padrão ISO/IEC 16085: o item 5.1.3.3 - *Risk evaluation*, que sugere um modelo de requisição de ação de risco, agregando informações de escopo, assunto, originador da solicitação, perspectiva da parte interessada, categorias do risco, limites do risco, descrição detalhada do risco, com probabilidade e consequência, alternativas para o tratamento de risco com justificativas e disposição das ações a serem tomadas; e o item 5.1.4.1 - *Selecting risk treatment*, o qual determina que as alternativas de tratamento de riscos devem ser avaliadas pelas partes interessadas, podendo aceitar riscos que excederam o limite estipulado, em situações em que o custo de mitigação seja demasiadamente alto, porém estes riscos

devem ser considerados de alta prioridade e serem continuamente monitorados. As partes interessadas podem, também, solicitar novas alternativas para os tratamentos apresentados, nestes casos, o risco deve ser reanalisado pela equipe responsável.

3.1.7 GRI7 - Os riscos analisados e a prioridade de aplicação dos recursos para o monitoramento desses riscos é determinada

Este resultado esperado determina a priorização de aplicação dos recursos no monitoramento dos riscos. Devido às ações de gerenciamento de riscos serem custosas, faz-se necessária a otimização dos recursos materiais e humanos para otimizar esta tarefa. No modelo CMMI-DEV não há prática específica equivalente a este resultado esperado.

O GRI7 possui uma relação do tipo NEQ com a tarefa 6.3.4.3.4, apresentado no Quadro 3.8, que determina que os riscos que as partes interessadas aceitaram estão acima do limite, deverão ser tratados como mais alta prioridade para deslocamento de recursos em seu monitoramento. Porém estes itens não podem ser totalmente equivalentes, pois a norma ISO/IEC 12207 não especifica como priorizar recursos em projetos que não há riscos no qual as partes interessadas não aceitaram estar acima do limite estabelecido.

Quadro 3.8 Mapeamento entre o resultado esperado GRI7 e as tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa da Norma ISO/IEC 12207	Grau de Mapeamento
GRI7 - Os riscos são analisados e a prioridade de aplicação dos recursos para o monitoramento desses riscos é determinada	6.3.4.3.4.3 - Se as partes interessadas aceitarem um risco que exceda seu limite, ele deve ser considerado um caso de alta prioridade e monitorado continuamente, a fim de determinar se outras ações de tratamento são necessárias no futuro.	NEQ

O resultado esperado deste tópico possui grau de mapeamento inexistente com o guia PMBOK, portanto não possui orientações de implementação.

O padrão ISO/IEC 16085 não possui recomendação de implementação alinhada às exigências de GRI7.

3.1.8 GRI8 - Os riscos são avaliados e monitorados para determinar mudanças em sua situação e no progresso das atividades para seu tratamento

O resultado esperado GRI8 exige que seja determinada a periodicidade para reavaliar e monitorar riscos, planos de mitigação e contingência, e o processo de gerência de riscos como um todo, podendo também serem identificados novos riscos. Este risco atende parcialmente à prática do CMMI-DEV SP 3.2 - Monitorar periodicamente o *status* de cada risco e executar o plano de mitigação quando apropriado, sendo complementado com o GRI9 para obter o grau de mapeamento EQU+ a esta prática.

Este resultado esperado está alinhado a sete tarefas da norma ISO/IEC 12207, são elas: (1) 6.3.4.3.4.3, que determina que os riscos selecionados previamente devem ser monitorados como alta prioridade, caso as partes interessadas aceitem que o risco exceda seu limite; (2) 6.3.4.3.5.1, que determina que riscos devem ser monitorados, além de estender este monitoramento para o contexto da gestão de riscos; (3) 6.3.4.3.5.2, o qual determina que durante o monitoramento, as medições devem ser realizadas, de forma a existir dados concretos a respeito desta etapa; (4) 6.3.4.3.5.3, determinando que durante o monitoramento poderá ocorrer a identificação de um novo risco, devendo este ser classificado e priorizado como os demais; (5) 6.3.4.3.6.1, o qual exige que durante o monitoramento devem ser coletadas informações que possam gerar lições aprendidas; (6) 6.3.4.3.6.2, que determina que todo o processo de gestão de riscos seja verificado periodicamente; (7) 6.3.4.3.6.3, que exige que cada risco coletado seja revisado periodicamente, afim de identificar possíveis riscos organizacionais. O Quadro 3.9 apresenta o resumo deste mapeamento, identificando também o grau de equivalente em conjunto (EQU+).

O GRI8 é totalmente equivalente (EQU) ao processo 11.6 do guia PMBOK, logo todas suas entradas, saídas, ferramentas e técnicas podem ser aplicadas para atender este resultado esperado. Como sugestão de implementação deste resultado, sugere-se realizar: reavaliação de riscos; auditoria de riscos; análise de variação e tendências; medição de desempenho técnico; análise de reservas e reuniões de andamento. Artefatos que estão alinhados às exigências do resultado esperado são: lista de riscos atualizadas, contendo o resultado das reavaliações e solicitações de mudanças na forma de ações corretivas e ações preventivas.

Quadro 3.9 Mapeamento entre o resultado esperado GRI8 e tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa da Norma ISO/IEC 12207	Grau de Mapeamento
GRI8 - Os riscos são avaliados e monitorados para determinar mudanças em sua situação e no progresso das atividades para seu tratamento	6.3.4.3.4.3 - Se as partes interessadas aceitarem um risco que exceda seu limite, ele deve ser considerado um caso de alta prioridade e monitorado continuamente, a fim de determinar se outras ações de tratamento são necessárias no futuro.	EQU+
	6.3.4.3.5.1 - Todos os riscos e o contexto de gestão de risco devem ser constantemente monitorados para verificação de alterações. Os riscos cujos níveis tenham sido alterados devem passar por uma avaliação de risco	EQU+
	6.3.4.3.5.2 - Medições devem ser implementadas e monitoradas para avaliar a eficácia dos tratamentos de riscos	EQU+
	6.3.4.3.5.3 - O projeto deve monitorar de forma continua os novos riscos e fontes de risco durante todo o ciclo de vida	EQU+
	6.3.4.3.6.1 - Informações devem ser coletadas durante o ciclo de vida do projeto, a fim de melhorar o Processo de Gestão de Risco e gerar lições aprendidas	EQU+
	6.3.4.3.6.2 - O Processo de Gestão de Risco deve ser periodicamente revisado para verificação de eficácia e eficiência	EQU+
	6.3.4.3.6.3 - As informações sobre os riscos identificados, seus tratamentos e o sucesso de seus tratamentos devem ser revisados periodicamente, a fim de identificar sistematicamente os riscos organizacionais do projeto	EQU+

O resultado do mapeamento com o padrão ISO/IEC 16085, identificou seis sugestões de implementação: (1) item 5.1.5.1 - *Monitor risk*, que especifica que os riscos devem ser monitorados, inclusive o contexto da gestão de risco e da ordem de prioridade de monitoramento; (2) item 5.1.5.2 - *Monitor risk treatment*, que determina que medidas devem ser implementadas e monitoradas para avaliar a eficácia do tratamento dos riscos, podendo identificar e reparar tratamentos ineficazes; (3) item 5.1.5.3 - *Seek new risks*, o qual especifica que novos riscos e fontes de riscos devem ser buscados, e caso encontrados, deve ser realizada análise e comunicada às partes interessadas; (4) item 5.1.6.1 - *Capture risk management information*, que determina que informações acerca de riscos identificados, suas fontes, causas e tratamentos devem ser coletados e comunicados durante o ciclo de vida do projeto, para melhorar

procedimentos, processos e políticas da gestão de riscos; (5) item 5.1.6.2 - *Assess and improve therisk management process*, o qual sugere que o processo de gerenciamento de riscos, como um todo, deve ser avaliado, afim de identificar oportunidades de melhoria, onde a periodicidade desta avaliação deve ser determinada pelas partes interessadas; (6) item 5.1.6.3 - *Generate lessons learned*, que determina que os dados coletados durante a revisão do processo de gerenciamento de riscos, devem ser gerados na forma de lições aprendida.

3.1.9 GRI9 - Ações apropriadas são executadas para corrigir ou evitar o impacto do risco, baseadas na sua prioridade, probabilidade, consequência ou outros parâmetros

Este resultado esperado exige que sejam realizadas ações de mitigação e/ou contingência para os riscos, de acordo com as necessidades e com o planejado, estas ações devem ser executadas até sua conclusão. Assim como o GRI8, o GRI9 é agregado para atender de forma conjunta a prática específica SP 3.2 da área de processo Gerência de Riscos do modelo CMMI-DEV.

O GRI9 está alinhado com a norma ISO/IEC 12207 através de duas tarefas, apresentadas no Quadro 3.10, sendo: (1) a tarefa 6.3.4.3.4.2 totalmente equivalente (EQU), pois determina que as ações para minimizar ou corrigir riscos, planejadas anteriormente, devem ser executadas, quando necessário; e a (2) tarefa 6.3.4.3.4.4, categorizada com o grau NEQ, pois detalha ações de gestão de problemas sem correspondentes no processo de gestão de riscos do MR-MPS-SW.

Quadro 3.10 Mapeamento entre o resultado esperado GRI9 e as tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa da Norma ISO/IEC 12207	Grau de Mapeamento
GRI9 - Ações apropriadas são executadas para corrigir ou evitar o impacto do risco, baseadas na sua prioridade, probabilidade, consequência ou outros parâmetros definidos	6.3.4.3.4.2 - Se as partes interessadas determinarem que ações deveriam ser tomadas para tornar um risco aceitável, então uma opção de tratamento deve ser implementada	EQU
	6.3.4.3.4.4. Assim que o tratamento for selecionado, ele deve receber as mesmas ações de gestão que os problemas recebem, de acordo com as atividades de avaliação e controle da subseção 6.3.2 desta norma, ou da norma ISO/IEC 15288:2008	NEQ

As orientações de implementação presentes no Guia PMBOK, recomendam que para atingir este resultado esperado, é possível utilizar como artefato as solicitações de mudanças, que são uma das saídas do processo 11.6.3 - Controlar riscos, comprovando que ações corretivas e/ou preventivas recomendadas foram executadas corretamente.

O padrão ISO/IEC 16085 possui o item 5.1.4.2 - *Risk treatment planning and implementation*, como recomendação de implementação alinhada a este resultado esperado, possuindo duas alternativas: (1) o tratamento de riscos utilizando auxílio da norma ISO/IEC 15288:2002, o qual uma vez que um tratamento de risco é selecionado, o mesmo deve receber as mesmas ações de correção de problemas da norma 15288; e (2) quando uma alternativa de tratamento de risco é aceita, as partes interessadas devem definir um plano de tratamento detalhado, especificando responsáveis pelo plano, tarefas a serem realizadas, cronograma de tratamento, alocação de recursos para o tratamento, medidas de controle de tratamento, custos, métodos de comunicação entre os envolvidos e ambiente e infraestrutura necessária.

3.1.10 Práticas dos modelos de qualidade não relacionadas com nenhum resultado esperado do modelo MR-MPS-SW

Cada prática identificada no guia PMBOK e no CMMI-DEV possui um mapeamento com práticas abordadas no modelo MR-MPS-SW, porém a norma ISO/IEC 12207 possui algumas recomendações com equivalência parcial ao modelo brasileiro. As exigências do MR-MPS-SW são menos abrangentes que as exigências na norma, logo existem mapeamentos de tarefas que são totalmente equivalentes a resultados esperados, porém possuem mais diretrizes alinhadas à exigência internacional.

Essas tarefas geraram boas práticas e, consequentemente, tarefas no modelo de processo, por isso possuem também importância no mapeamento realizado neste estudo.

As tarefas 6.3.4.3.1.2 e 6.3.4.3.1.5 da norma ISO/IEC 12207 determinam, respectivamente, que deve haver uma descrição do processo implementado, e deve haver diretrizes para posterior avaliação e melhoria do processo descrito. Estas tarefas dão origem à boa prática "Planejar a Gestão de Riscos", sem vínculo direto com algum resultado esperado do processo de gerência de riscos do MR-MPS-SW.

Também as tarefas 6.3.4.3.6.2 e 6.3.4.3.6.3 da norma ISO/IEC 12207, relacionadas à avaliação da execução do processo, deram origem à boa prática "Avaliar a execução da Gestão de Riscos". Isso se deve ao fato de além do monitoramento exigido em resultados esperados do MR-MPS-SW, a norma exige a periodicidade de revisão das atividades planejadas e executadas, assim como a revisão de riscos identificados ao final de um projeto, para orientar futuros projetos.

3.2 As Boas Práticas Coletadas

A partir do mapeamento identificado entre os modelos de qualidade, foram catalogadas as boas práticas com suas respectivas recomendações. Práticas semelhantes foram agrupadas com o intuito de evitar repetições.

O Quadro 3.11 reúne informações coletadas a respeito do mapeamento entre modelos de qualidade. Cada boa prática possui: identificador, nome, descrição, a identificação em qual modelo ou norma de qualidade (MPS.BR, CMMI ou ISO/IEC 12207) é apresentada e a forma de implementar esta prática de acordo com os modelos de qualidade que sugerem implementação (ISO/IEC 16085 e PMBOK).

As boas práticas serviram como insumo para a elaboração da metodologia do processo de gerenciamento de riscos de software sugerido neste trabalho. Ao todo foram coletadas quatorze boas práticas distintas dos modelos de qualidade.

Quadro 3.11 Boas Práticas identificadas a partir do mapeamento de modelos de qualidade

ID	Nome	Descrição	Identificada no(s) modelos(s) e norma	Formas de Implementar esta prática
BP01	Definir o Escopo da Gerência de Riscos em uma organização	Definição da abrangência da aplicação da gerência de riscos na organização em relação à sua estrutura organizacional e de processos	MSP.BR (GRI1), CMMI (SP 1.3), ISO/IEC 12207 (6.3.4.3.1.1 e 6.3.4.3.2.1)	Política Organizacional: Descrição técnica e gerencial dos objetivos, suposições e restrições, entre outras informações

ID	Nome	Descrição	Identificada no(s) modelos(s) e norma	Formas de Implementar esta prática
BP02	Identificar papeis e responsáveis pelo gerenciamento de risco	Identificar e documentar os envolvidos no gerenciamento de riscos, para ser realizada a comunicação durante o ciclo de vida do projeto	ISO/IEC 12207 (6.3.4.3.1.3 e 6.3.4.3.1.4)	Política organizacional contemplando papeis e responsabilidades; Plano de projeto contemplando alocação de recursos humanos para cada um dos papeis definidos.
BP03	Definir Categorias de Riscos	Definir categorias de riscos, parâmetros para esta categorização e as possíveis origens de riscos de cada categoria	MPS.BR (GRI2), CMMI (SP 1.1), ISO/IEC 12207 (6.3.4.3.2.2, 6.3.4.3.2.3 e 6.3.4.3.2.4)	Estrutura Analítica de Riscos: riscos organizacionais, contendo severidade e probabilidade de ocorrência de cada categoria
BP04	Definir parâmetros para análise de riscos	É importante padronizar o modo como a organização determina parâmetros utilizados na análise de riscos identificados (como a probabilidade e a severidade)	MPS.BR (GRI2), CMMI (SP 1.2), ISO/IEC 12207 (6.3.4.3.2.3)	Estimativas qualitativas, definindo valores numéricos para variáveis subjetivas: muito alto (9-10); alto (8-9); médio(4-7); e baixo (0-3) para cada parâmetro que será utilizado. No caso de probabilidade e severidade, pode ser obtido o grau de exposição através da multiplicação dos valores numéricos para os dois parâmetros.
BP05	Definir Estratégias para a gerência de riscos	devem ser relacionados aspectos da gerência de riscos em um projeto, como escopo, métodos e ferramentas a serem utilizados, técnicas de mitigação, periodicidade, responsáveis.	MPS.BR (GRI3), CMMI (SP 1.3)	Plano de Gerenciamento de Riscos: metodologia de trabalho durante o ciclo de vida do projeto, orçamento atribuído ao tratamento e mitigação de riscos, prazos, categorias de riscos, definições de probabilidade e impacto, entre outros.
BP06	Identificar e Documentar Riscos	Todos os riscos identificados devem ser registrados, juntamente com informações adicionais, como contexto, condições associadas e conseqüências	MPS.BR (GRI 4), CMMI (SP 2.1), ISO/IEC 12207 (6.3.4.3.3.1)	Revisão de documentação de projetos anteriores; Técnicas de coletas de informações: brainstorming, checklists, análise de matriz SWOT, entre outros.

ID	Nome	Descrição	Identificada no(s) modelos(s) e norma	Formas de Implementar esta prática
BP07	Classificar Riscos	Riscos identificados devem ser detalhados de forma que possam ser melhor organizados para monitoramento e reutilizados da melhor maneira em projetos futuros. (grau de exposição e categorização)	MPS.BR (GRI 5), CMMI (SP 2.2), ISO/IEC 12207 (6.3.4.3.3.2)	Estimativa quantitativa ou qualitativa; matriz de probabilidade e impacto; sugestão de opinião especializada
BP08	Priorizar Riscos	É importante priorizá-los para definir quais riscos merecem maior atenção durante o monitoramento.	MPS.BR (GRI 5), CMMI (SP 2.2)	Comparação do grau de exposição (probabilidade x impacto) dos riscos identificados
BP09	Escolher estratégia de ação e definir respostas aos riscos	Estabelecer planos de ação para os riscos (mitigação e/ou contingência para tratar riscos) prioritários afim de reduzir alguma característica, como impacto ou probabilidade de ocorrência	MPS.BR (GRI 6), CMMI (SP 3.1), ISO/IEC 12207 (6.3.4.3.4.*)	Adotar uma das seguintes estratégias: eliminação, transferência, mitigação, aceitação; Plano de mitigação do risco: conseqüências, alternativas para tratamento, justificativa e ações a serem tomadas
BP10	Definir prioridade para aplicação de recursos em riscos	É importante definir quais riscos serão prioritários no recebimento de recursos para mitigação e monitoramento, devido à necessidade de otimização de recursos materiais e humanos.	MPS.BR (GRI 7)	Atividades de gerenciamento de riscos especificadas no cronograma
BP11	Monitorar (e reavaliar) riscos	realizar o monitoramento e avaliação de riscos em um determinada freqüência. Também durante o monitoramento, podem ser identificados novos riscos	MPS.BR (GRI 8), CMMI (SP 3.2), ISO/IEC 12207 (6.3.4.3.5.*)	auditoria de riscos, análise de variação e tendências, reuniões de andamento, checklists.
BP12	Realizar ações para reduzir impacto do risco	realizar ações de contingência e mitigação durante o monitoramento de riscos, com o objetivo de minimizar ou anular o impacto dos riscos	MPS.BR (GRI 9), CMMI (SP 3,2)	Execução do plano de ação do risco

ID	Nome	Descrição	Identificada no(s) modelos(s) e norma	Formas de Implementar esta prática
BP13	Planejar a Gestão de Riscos	A Gestão de riscos deve possuir um processo implementado e documentado. Assim como deve haver uma descrição do processo para avaliar e melhorar a execução das atividades planejadas	ISO/IEC 12207 (6.3.4.3.1.5)	Definir previamente um processo sequenciando as atividades de gerência de risco em um projeto de software, e garantir que todos possuam conhecimento e executem o que foi planejado.
BP14	Avaliar a execução da Gestão de Riscos	O processo de Gestão de riscos deve ser periodicamente revisado, assim como as informações sobre riscos identificados, seu tratamento e o sucesso desses tratamentos.	ISO/IEC 12207 (6.3.4.3.6.2 e 6.3.4.3.6.3)	Ao término de um projeto, avaliar execução e comparar com o planejamento, para alinhar novas diretrizes em futuros projetos.

As boas práticas identificadas nortearam o desenvolvimento da metodologia proposta neste trabalho, gerando uma ou mais tarefas no fluxo sugerido.

3.3 Detalhamento da Metodologia Proposta

O objetivo da metodologia proposta é auxiliar futuras implementações da gerência de riscos em organizações que desejam desenvolver software de maneira aderente ao MR-MPS-SW, CMMI, PMBOK, ISO/IEC 12207 e/ou ISO/IEC 16085 de forma conjunta, ou apenas utilizarem as sugestões de implementação de um subconjunto das boas práticas aqui apresentadas.

A metodologia apresentada possui algumas limitações com relação ao seu detalhamento, pois tem como principal foco nortear implementações nas mais diversas organizações, sem a necessidade de delimitar de forma rígida papéis, ferramentas e procedimentos de maneira extremamente detalhada, tornando mais simples sua adaptação ao processo padrão da organização.

Para realizar o detalhamento do fluxo foi utilizada a ferramenta Spider-PM (Barros e Oliveira, 2010), que permite a especificação da metodologia em fases, e para cada fase um conjunto de tarefas.

As subseções seguintes apresentam as fases, papéis e tarefas da metodologia sugerida, além disso, cada tarefa possui seu próprio detalhamento, especificando

artefatos que podem ser utilizados, papéis que podem realizá-la, quais boas práticas do mapeamento estão relacionadas, e as formas de implementação segundo os padrões de qualidade envolvidos. Todas essas informações relacionadas ao detalhamento de cada tarefa estão especificadas no Apêndice A deste trabalho.

3.3.1 Fases Propostas

A Figura 3.1 apresenta uma visão macro do processo, que possui três fases: Planejamento, Execução e Avaliação. Cada uma das fases possui um fluxo, detalhando quais tarefas são recomendadas para cumprir seus objetivos.

Figura 3.1 Fases da metodologia proposta para gerenciamento de riscos

A fase de Planejamento é responsável pela definição inicial de como será trabalhada a gerência de riscos na organização, incluindo a delimitação de onde e quando ocorrerá a atuação para tratamento de riscos.

A segunda fase, Execução, define tarefas diretamente relacionadas ao gerenciamento de riscos durante o ciclo de vida de um projeto, do planejamento ao encerramento.

A fase final, Avaliação, é realizada após o fim de um projeto, sendo responsável por tarefas relacionadas a mudanças no processo e registro de dados históricos para orientar futuros projetos.

3.3.2 Papéis Sugeridos

A metodologia proposta sugere alguns papéis que podem ser assumidos por colaboradores do projeto durante a realização das tarefas. Algumas tarefas possuem mais de um papel sugerido, pois necessita ser realizada em conjunto entre diferentes perfis.

As responsabilidades de cada papel foram definidas a partir das tarefas especificadas na metodologia, consequentemente baseada no mapeamento realizado. Existem cinco diferentes papéis utilizados no detalhamento da metodologia (Apêndice A):

- **Alta Administração:** papel que deve ser representado por um colaborador de nível estratégico da organização, possui responsabilidades nas fases de planejamento e avaliação do processo, tomando decisões relacionadas à definição do escopo da gerência de riscos, categorias de riscos organizacionais e alterações para melhoria do processo;
- **Gerente de Riscos:** responsável por administrar e coordenar as ações relacionadas a riscos durante todo o ciclo de vida do projeto. Atua principalmente na fase de Execução em sua totalidade, porém participa de tarefas em outras fases, reportando análises de projetos anteriores para a tomada de decisão da alta administração;
- **Gerente de Projetos:** responsável por coordenar ações do projeto como um todo e manter todos os envolvidos informados das mudanças ocorridas durante seu ciclo de vida. Em muitas organizações, devido a escassez de recursos, torna-se proibitivo ter um gerente exclusivo para gerenciar riscos, neste caso o gerente de projetos assume as responsabilidades cabidas;
- **Equipe de Gerência de Riscos:** é importante que os demais responsáveis por atividades no projeto tenham um envolvimento com a gerência de riscos, logo a equipe de gerência de riscos deve ser formada por um conjunto de integrantes do projeto, podendo ser alguns membros selecionados em caso de projetos de grande porte ou toda a equipe, caso seja reduzida e permita fácil comunicação. Possui responsabilidades que envolvem principalmente a fase de execução da metodologia, envolvendo identificação, análise, priorização, monitoramento, mitigação e contingência, mas também participam da avaliação ao final do projeto, auxiliando a identificar pontos fortes, pontos fracos e oportunidades de melhoria.

3.3.3 Descrição das Tarefas Propostas

A fase de Planejamento, apresentada na Figura 3.2, possui três tarefas. A primeira tarefa, denominada "Determinar Escopo da Gerência de Riscos", deve ser responsável por gerar um artefato que especifique a abrangência da gerência de riscos, tanto no âmbito de cada projeto individualmente, quanto na organização como um todo. Esta tarefa pode ser atendida através da elaboração de uma política organizacional, por exemplo, que deve conter informações acerca das possíveis partes interessadas em riscos, as categorias de riscos, uma breve descrição de quais objetivos técnicos e gerenciais devem ser alcançados, assim como suposições e limitações deste gerência. Esta tarefa foi desenvolvida para atender a boa prática BP01: "Definir o Escopo da Gerência de Riscos em uma organização".

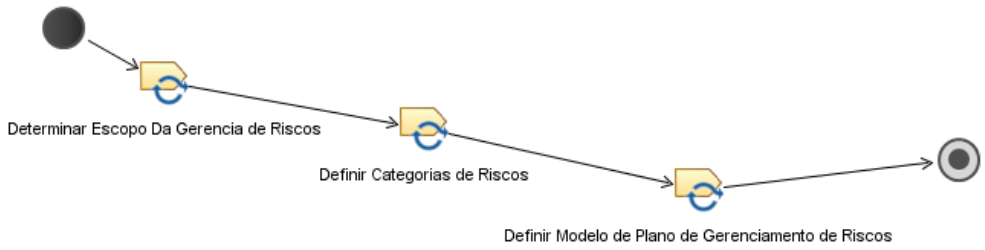

Figura 3.2. Tarefas da fase de Planejamento

A segunda tarefa da fase de Planejamento, "Definir Categorias de Riscos", é responsável por gerar uma lista com as categorias de riscos que podem ser encontrados durante a execução de um projeto de software. Devem ser disponibilizadas informações a respeito das possíveis origens do risco, além de um conjunto de critérios para a determinação da probabilidade de ocorrência e sua severidade. Outra forma eficiente de organizar as categorias de riscos, é através de uma estrutura analítica de riscos (EAR), que de forma hierárquica permite o arranjo de riscos em categorias e subcategorias, como pode ser observado na Figura 3.3. Esta tarefa está relacionada à boa prática BP03: "Definir Categorias de Riscos".

A terceira tarefa da fase de Planejamento baseia-se na boa pratica BP05: "Definir Estratégias para a gerência de riscos" e na boa prática BP04: "Definir parâmetros para análise de riscos", e é denominada "Definir Modelo de Plano de Gerenciamento de Riscos". Esta tarefa é responsável por analisar e definir quais informações relacionadas aos riscos serão importantes para serem monitoradas durante a execução do projeto. Ao final desta tarefa deve ser gerado um artefato com os tópicos

que um plano de gerenciamento de riscos desta organização deve possuir. É importante que um plano de gerenciamento de riscos possua um detalhamento de itens como: metodologia, definindo abordagens e ferramentas utilizadas para identificação e monitoramento dos risos; papéis e responsabilidades, definindo o líder e membros da equipe de gerenciamento de riscos; orçamento; prazos; categorias de riscos, que podem ser exatamente as mesmas categorias definidas no âmbito organizacional na tarefa anterior, ou uma instanciação da mesma, reaproveitando apenas uma parcela; definições de probabilidade e impacto dos riscos, relacionando estas informações às mudanças em custo, tempo escopo e qualidade do projeto; formatos de relatórios que serão utilizados durante a execução do projeto.

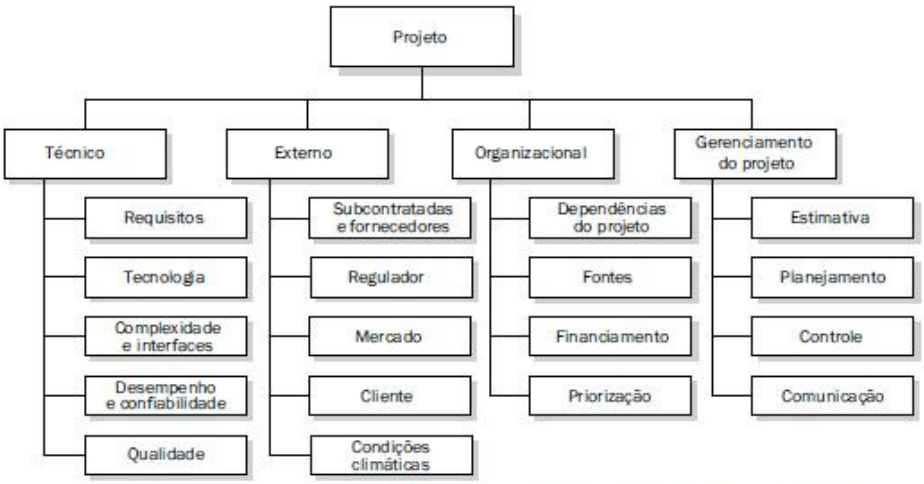

Figura 3.3 Exemplo de uma EAR (PMI, 2014)

A fase de Execução possui sete tarefas distintas que, como pode ser observado na Figura 4, segue um fluxo linear até a tarefa relacionada à avaliação e monitoramento de riscos, no qual (1) um novo risco pode ser identificado ou um existente alterado, necessitando ajustes no detalhamento e prioridades de riscos, ou (2) pode ocorrer a necessidade de execução de um plano de mitigação ou contingência anteriormente especificado. Ambos os fluxos retornam novamente à tarefa de avaliação e monitoramento de riscos, que deve ser executada até o fim do projeto.

A primeira tarefa desta fase é "Definir o Plano de Gerenciamento de Riscos", que deve utilizar o modelo de plano de gerenciamento de riscos gerado na fase anterior e preenchê-lo com as informações relevantes para o projeto. É importante que esta

tarefa seja executada pelo responsável pela gerência de riscos, porém em conjunto com a sua equipe e com outros gerentes, caso haja, uma vez que será necessário especificar informações a respeito do cronograma e orçamento do projeto. Esta tarefa também baseia-se na boa prática BP05: "Definir Estratégias para a gerência de riscos", e na boa prática BP02: "Identificar papeis e responsáveis pelo gerenciamento de risco".

Em seguida deve ser realizada a tarefa "Identificar os Riscos", que deve documentar os riscos deste projeto, especificando o contexto, as prováveis causas do risco e suas decorrentes consequências. Estas informações podem estar incorporadas no plano de gerenciamento de riscos. A boa prática BP06: "Identificar e Documentar Riscos" originou a criação desta tarefa. Para realizar a identificação de riscos podem ser utilizadas técnicas como a utilização de *checklists* pré-definidos, reuniões e *brainstorming*; análise de cenário de projetos anteriores; técnica Delphi; análise de causa-raiz; ou análise de forças, fraquezas, oportunidades e ameaças, através da matriz SWOT (*Strengths, Weaknesses, Opportunities And Threats*).

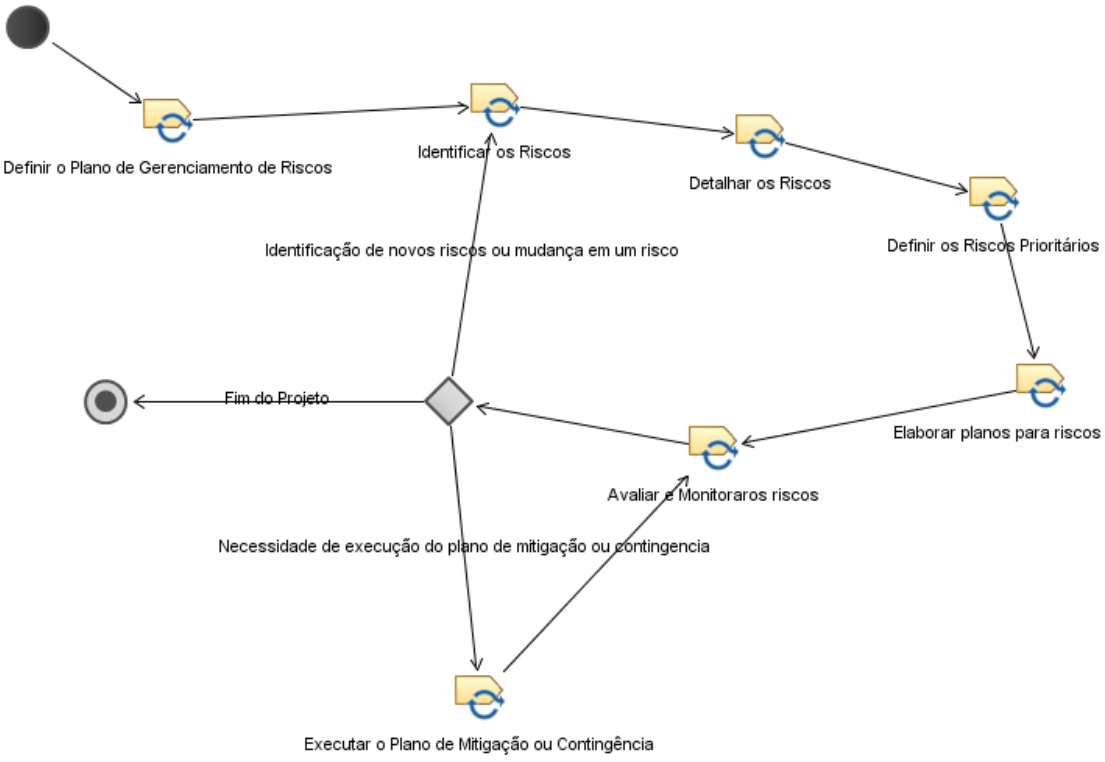

Figura 3.4 Tarefas da fase de Execução

Cada risco anteriormente identificado, deve ser priorizado, estimado e classificado na tarefa "Detalhar os Riscos". A inclusão destas informações resultam em uma atualização na lista de riscos. De acordo com a categorização de cada risco, podem ser utilizadas informações contidas na EAR para auxiliar no detalhamento,

especialmente na quantificação de probabilidade e impacto. Ao final desta tarefa o artefato com a lista de riscos deve estar detalhado e priorizado a partir dos riscos de maior grau de exposição (produto entre probabilidade e impacto), e esta atualização deve ser comunicada aos interessados definidos no plano de gerenciamento de riscos. Esta tarefa também baseia-se na boa prática BP06: "Identificar e Documentar Riscos, e na boa prática BP07: "Classificar Riscos".

A próxima tarefa da fase de Execução, denominada "Definir os Riscos Prioritários", originada pelas boas práticas BP08: "Priorizar Riscos e BP10: "Definir prioridade para aplicação de recursos em riscos", pode ser executada, por exemplo, através de uma reunião entre os responsáveis pelo gerenciamento de riscos e pelo projeto como um todo. O artefato contendo a lista de riscos priorizada e detalhada deve ser analisado para definir quais riscos terão maior visibilidade e receberão maior atenção durante a execução do projeto, seja por causar grande impacto, caso ocorra, ou devido sua grande probabilidade de ocorrência. Esta tarefa é importante, pois devido a limitações de tempo e orçamento, muitas vezes não é possível o monitoramento de todos os riscos identificados.

Após a definição de quais riscos são prioritários, cada um destes riscos selecionados deve possuir um plano de mitigação e um plano de contingência, de acordo com a boa prática BP09: "Escolher estratégia de ação e definir respostas aos riscos".

Estes planos são realizados durante a execução da tarefa seguinte, "Elaborar planos para riscos prioritários". Um plano de mitigação diz respeito à necessidade de reduzir o grau de exposição, ou seja, deve ser reduzida a probabilidade, o impacto ou ambos, antes que um risco ocorra. Enquanto o plano de contingência deve ser executado após a constatação de ocorrência do risco, com o intuito de contornar possíveis prejuízos causados. Para cada risco, é possível adotar estratégias de: eliminação, quando a ameaça é removida por completo; transferência, no qual a responsabilidade sobre um risco é direcionada a um terceiro; mitigação, que é a redução do grau de exposição de um risco; e aceitação, para riscos poucos prováveis, no qual não é detalhada a abordagem para superação da ocorrência.

A tarefa seguinte da fase de Execução é denominada "Avaliar e Monitorar os riscos", a qual define que todos os riscos devem ser monitorados e reavaliados em uma periodicidade, que pode ser definida no plano de gerenciamento de riscos. Podem ser

adotadas diferentes estratégias de monitoramento para cada categoria ou gravidade de riscos, assim como devem ser revisadas também a prioridade e os planos de mitigação e contingência dos riscos. Esta tarefa originou-se a partir da boa prática BP11: "Monitorar (e reavaliar) riscos".

A tarefa "Executar o Plano de Mitigação ou Contingência", originada a partir da boa prática BP12: "Realizar ações para reduzir impacto do risco", é executada apenas quando é detectada esta necessidade durante a avaliação e monitoramento dos riscos. Após a execução do planejado, as mudanças devem ser documentadas no próprio plano, relatando a evolução das medidas tomadas. Também deve haver uma preocupação em reavaliar se estas medidas geraram novos riscos ou afetaram riscos existentes, por isso faz-se necessária uma avaliação detalhada também dos riscos já documentados ao final do plano de mitigação ou contingência.

A fase final, Avaliação, apresentada na Figura 5, possui quatro tarefas, que serão executadas ao final de um projeto, com um intuito de avaliar o processo de gerência de riscos como um todo na organização e realizar ajustes necessários para sua otimização na execução em futuros projetos. Todas as tarefas desta fase baseiam-se na boa prática BP14: "Avaliar a execução da Gestão de Riscos".

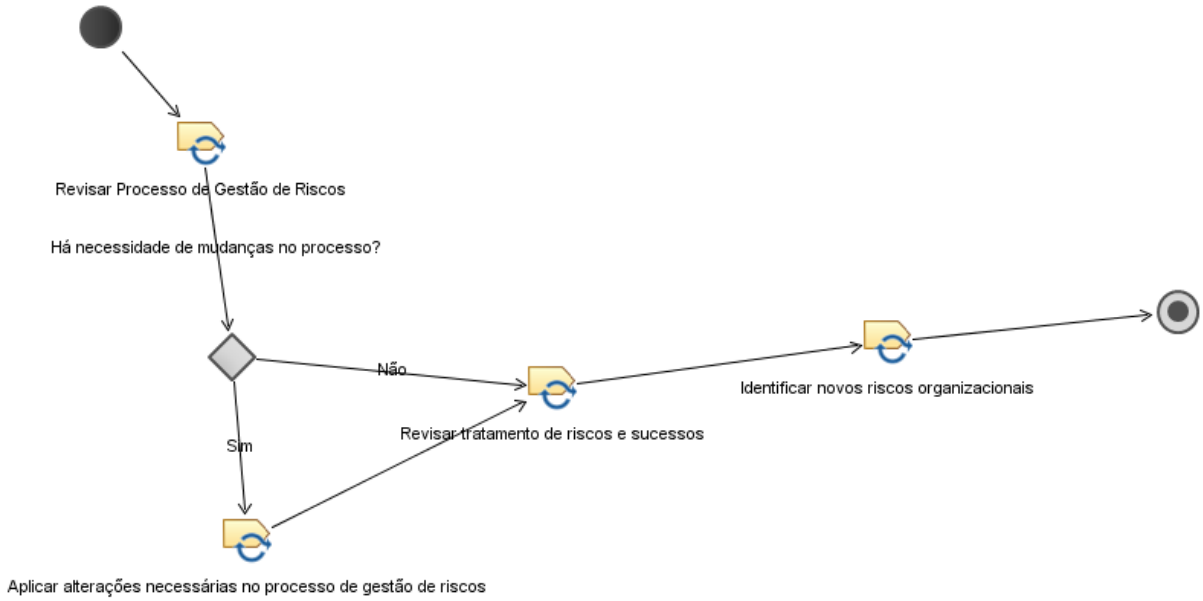

Figura 3.5Tarefas da fase de Avaliação

Inicialmente deve ser realizada a tarefa "Revisar Gestão de Riscos", que pode ser atendida através de uma reunião entre o responsável pela gerência de riscos e sua equipe. Nesta reunião devem ser identificados os pontos fracos encontrados durante a

execução do processo, para que possam ser ajustados. Outra alternativa eficiente é a elaboração de um *checklist* para a avaliação do processo. A forma como será realizada esta avaliação e como serão documentadas as necessidades de ajustes podem estar detalhadas na política organizacional, de forma que seja disponibilizada a todos.

Caso haja alterações, elas devem ser ajustadas na tarefa "Aplicar alterações necessárias no processo de gestão de riscos", que deve ser realizada em conjunto com o responsável pela definição do processo organizacional e, posteriormente, informado aos interessados a respeito das mudanças.

Em seguida, caso haja ou não necessidades de alterações, deve ser realizada a tarefa "Revisar tratamento de riscos e sucessos", responsável por identificar os pontos fortes durante a execução do projeto, armazenando informações para futuros projetos. Estas informações podem ser coletadas através de uma reunião, inclusive podendo ser a mesma reunião realizada na primeira tarefa da fase de Avaliação. Para cada ponto forte identificado no tratamento de riscos, deve haver detalhes de como foi realizado o tratamento, qual a categoria, prioridade e impacto do risco trabalhado e caso haja, quais técnicas para mitigação ou contingência foram utilizadas. Estas informações podem ser armazenadas em uma ferramenta de gerência de conhecimento, como uma *wiki*, por exemplo, de forma que esteja acessível a todos os integrantes da equipe de gerenciamento de riscos.

A tarefa final deste processo, "Identificar novos riscos organizacionais", também pode ser realizada durante uma reunião ao final do projeto, e está relacionada à necessidade de incluir novas categorias de riscos na EAR da organização, que foram identificados neste projeto e não estavam documentados anteriormente. Além de estar relacionada ao BP14, como mencionado anteriormente, esta tarefa relaciona-se também com a boa prática BP03: "Definir Categorias de Riscos".

3.4 Diferenciais da Proposta

O maior diferencial da metodologia para gerenciamento de riscos aqui proposta, em relação a trabalhos semelhantes, está no fato de sua definição ter sido embasada a partir de recomendações de modelos, normas e guias de qualidade, que envolvem o gerenciamento de riscos. Como existem inúmeras organizações interessadas na implementação de diferentes modelos, normas e guias, a adoção isolada de apenas um

destes reduz o conjunto de organizações que poderiam ser beneficiadas com as sugestões contidas neste trabalho.

Esta proposta objetivou também não apenas determinar equivalências de boas práticas entre os modelos MR-MPS-SW, CMMI-DEV e a norma ISO/IEC 12207, mas também sugerir diferentes formas de alcançar os objetivos do processo de gerenciamento de riscos em software através das propostas identificadas no guia PMBOK e no padrão ISO/IEC 16085, dando maior liberdade para o implementador que utilizar esta metodologia escolher qual se aproxima mais à cultura da organização.

Para auxiliar a implementação, com o intuito de reduzir tempo e custos, também foi desenvolvida uma ferramenta de apoio ao processo de gerenciamento e riscos, sistematizando as tarefas aqui descritas, centralizando informações estratégicas relacionadas a riscos e apoiando a aprendizagem por parte dos envolvidos. Esta ferramenta será detalhada no Capítulo 4 deste trabalho.

3.5 A Avaliação da Metodologia Proposta

Após a definição da metodologia, foi realizada uma avaliação da mesma juntamente com a lista de boas práticas, com o objetivo de avaliar os critérios utilizados para a definição de tarefas e verificar se há alinhamento com os modelos de qualidade, e se as considerações feitas esclarecem suas atribuições (Pavan, 2007).

A escolha do revisor foi definida a partir do grupo de implementadores e avaliadores do MPS.BR, de acordo com a sua disponibilidade, considerando também que o especialista possui qualificação em tal função. Algumas das características que influenciaram a escolha do avaliador/especialista foram: experiência com gerenciamento de riscos, experiência em pelo menos um dos modelos ou normas, conhecimento dos métodos de avaliação presentes nos modelos e normas, certificação em pelo menos um dos modelos, e mais de cinco anos de experiência em gerenciamento de projetos.

O questionário (detalhado no Apêndice B) foi composto por 14 questões objetivas, agrupadas em 2 conjuntos distintos: (i) Perfil do Revisor, que tem o intuito de esclarecer o nível de conhecimento do entrevistado em relação ao gerenciamento de projetos, gerenciamento de riscos, implementação de modelos para melhoria de processo, e métodos de avaliação constantes nos modelos; (ii) Apresentação da

Proposta, com o objetivo de conhecer a percepção do avaliador em relação ao trabalho apresentado, avaliando corretude e completude da proposta, e se a metodologia pode ser utilizada como referencial no gerenciamento de riscos.

Como anexo ao questionário, foi solicitada uma avaliação subjetiva para revisão do material enviado, baseado em (Mello *et al.*, 2012) e (Brito Neto, 2014), no qual era permitido o registro de comentários através de uma tabela a ser preenchida pelo avaliador contendo a identificação do comentário, sua categoria, o item a qual se corresponde (podendo ser relativo a uma fase, tarefa ou em geral da metodologia), o texto do comentário em si, e uma sugestão com a proposta do revisor para contornar o problema. As categorias definidas para os comentários foram:

- **TA (Técnico Alto)**, indicando que foi encontrado um problema em um item que, se não for alterado, comprometerá as considerações;
- **TB (Técnico Baixo)**, indicando que foi encontrado um problema em um item que seria conveniente alterar;
- **E (Editorial)**, indicando que foi encontrado um erro de português ou que o texto pode ser melhorado;
- **Q (Questionamento)**, indicando que houve dúvidas quanto ao conteúdo das considerações;
- **G (Geral)**, indicando que o comentário é geral em relação às considerações;
- **BP (Boas Práticas)**, indicando que o comentário está relacionado à lista de boas práticas.

O material de avaliação e a metodologia definida foram enviados ao revisor selecionado através de contato por e-mail e após conferência realizada para explicar a metodologia de avaliação, também descrita no documento, foi aguardado o retorno da avaliação realizada.

Os *feedbacks* recebidos após a avaliação foram bastante proveitosos e favoráveis para o aprimoramento da metodologia e serão descritos a seguir, junto ao perfil do avaliador.

Com relação ao perfil do especialista que enviou a avaliação realizada no dia 29 de setembro de 2014, o próprio revisor considera que possui conhecimento médio em gerenciamento de riscos, inclusive implantando esta área do conhecimento em diversas organizações em um tempo de dois a cinco anos. também possui mais de cinco anos de

experiência em gerenciamento de projetos de software. Além disso, ele considerou que possui alta experiência com métodos de avaliação constantes em modelos para melhoria de processo de software, possuindo certificação como implementador e avaliador MPS.BR, com tempo de experiência entre dois e cinco anos tanto em implementação quanto em avaliação de processos de gerência de riscos.

Relacionado às questões objetivas, o avaliador considerou que a metodologia, à época da revisão, necessitava de alguns ajustes sobre a completude com relação aos detalhamentos das fases e à proposta em geral, porém também considerou de grande valia o material apresentado, podendo ser usado mesmo que parcialmente como um referencial para a implantação do processo de melhoria da gerência de riscos.

As observações da avaliação subjetiva renderam três itens relacionados à proposta de metodologia em geral, descritos a seguir.

O comentário considerado mais grave pelo revisor, adequado à categoria TB (Técnico Baixo), foi a discussão se a sugestão apresentada era na realidade um *framework* ou uma metodologia. Inicialmente, a sugestão proposta era tratada como um *framework*, porém o revisor questionou que não foram encontrados pontos de adaptação ou escolha. Também, de acordo com Tomhave (2005), a proposta define melhores práticas e regras que devem ser seguidas para a aplicação de um modelo, logo estaria mais próxima de uma metodologia. Após consulta a outros pesquisadores com experiência em implementação e avaliação de processo de software, foi definido que seria adotada a terminologia metodologia para a proposta definida neste trabalho.

Outro comentário está relacionada à generalidade da proposta, que, segundo o revisor, pode dificultar sua aplicação no dia-a-dia da empresa para quem não possui conhecimento aprofundado da área. Foi sugerida a contextualização da proposta incluindo mais exemplos práticos e detalhados. A solução encontrada para aperfeiçoar a metodologia foi através da sua sistematização em uma ferramenta de software, que durante a descrição de suas funcionalidades são citados exemplos práticos e quais tarefas definidas na metodologia são realizadas em cada uma das funcionalidades.

Por fim, o terceiro comentário foi relacionado à carência de visões ou considerações em como aplicar a metodologia de acordo com o porte da organização e o processo utilizado (ágil ou tradicional). Porém o escopo desta pesquisa é justamente abranger o máximo de organizações possível sem delimitar alguns tipos. No entanto, a

sugestão é bastante perspicaz, no sentido que seria um excelente trabalho futuro instanciar a metodologia proposta para alguns cenários um pouco mais específicos, como métodos ágeis ou desenvolvimento distribuído de software.

3.6 Considerações Finais

Este capítulo apresentou a metodologia proposta para gerenciar riscos em uma organização, através das recomendações de modelos, normas e guias de qualidade, com o intuito de facilitar a aprendizagem e entendimento da gerência de riscos e reduzir custos e tempo na implantação de um processo capaz de auxiliar na melhoria dos processos e consequentemente de produtos.

A base para a definição da metodologia foi o mapeamento entre modelos, normas e guias de qualidade, que concebeu uma lista de boas práticas no gerenciamento de riscos, ambos também apresentados neste capítulo.

A metodologia foi avaliada através de revisão realizada por um especialista e após as sugestões fornecidas e aprimoramento da proposta, este trabalho está apto para ser utilizado em organizações que necessitam gerenciar riscos aderente aos padrões de qualidade envolvidos no mapeamento.

4 A FERRAMENTA SPIDER-RM

Este capítulo aborda os aspectos gerais que envolvem a ferramenta Spider-RM, desenvolvida para auxiliar a implementação do processo de gerência de riscos através da sistematização das tarefas descritas na metodologia apresentada no Capítulo 3. Portanto, serão abordados o contexto que a ferramenta está inserida, as particularidades relacionadas ao seu projeto técnico e as suas funcionalidades, apresentando telas e detalhando seu funcionamento e sua operação.

4.1 O Objetivo da Ferramenta Spider-RM

A ferramenta Spider-RM (Mendes e Oliveira, 2014) possui licença *General Public License* - GPL (GNU, 2015),e foi concebida para apoiar a metodologia de implantação da gerência de riscos em organizações desenvolvedoras de software, apresentada no Capítulo 3. A Spider-RM é subprojeto do Projeto SPIDER – *Software Process Improvement: DEvelopment and Research* (Oliveira, 2011), que pretende criar um conjunto de abordagens baseadas em software livre aderentes aos resultados esperados do modelo MR-MPS-SW, com o objetivo de reduzir custos de implementação de cada processo abordado.

A elaboração da ferramenta deu-se a partir da necessidade de sistematizar práticas abordadas na metodologia, com o objetivo de reduzir custos e tempo ao implementar da gerência de riscos nas organizações, facilitando o aprendizagem dos envolvidos em conceitos e técnicas relacionados à área. Sua utilização permite a aderência às necessidades solicitadas pelas normas, modelos e guias de qualidade envolvidos neste trabalho, pois suas funcionalidades foram baseadas na lista de boas práticas obtidas a partir do mapeamento entre os documentos de referência em qualidade.

O uso da ferramenta pode ser aplicado em diversas organizações que tenham como produto software e serviços correlatos, independente do porte da mesma, encontrando-se disponível no endereço eletrônico *http://www.spider.ufpa.br* no menu *Downloads*.

4.2 Projeto Técnico da Ferramenta Spider-RM

Nesta seção será apresentado o projeto técnico de construção da ferramenta Spider-RM, abordando a arquitetura adotada, os casos de uso definidos após análises das boas práticas em gerência de riscos e quais tecnologias estão envolvidas na execução da mesma.

4.2.1 Arquitetura da Ferramenta

A ferramenta foi construída para ser utilizada em modo *desktop* e em princípio dá suporte a um usuário, que pode ser por exemplo Gerente de Projeto, Líder de Projeto ou Gerente de Riscos. A escolha dessa abordagem inicial deu-se em razão da equipe envolvida no desenvolvimento da Spider-RM já possuir conhecimento prévio em desenvolvimento de aplicações *desktop* e devido ao tempo reduzido para a conclusão desta pesquisa, seria difícil consumir muito tempo com a aprendizagem de uma nova abordagem.

Além disso, a execução do processo de gerenciamento de risco, na maioria de suas atividades, é comumente realizada apenas por um envolvido no projeto, que assume, entre outros papeis, o papel de gerente de riscos. Entretanto, sua arquitetura foi desenvolvida de modo a facilitar constantes evoluções, podendo ser adaptada futuramente ao ambiente web e multiusuário ou integração com outras ferramentas de gerência de projeto, facilitando a comunicação com a equipe e promovendo uma melhor sincronia entre as diversas tarefas envolvidas em um projeto.

A arquitetura do Spider-RM foi baseada em uma combinação entre a arquitetura em três camadas e o modelo MVC (*Model-View-Controller*). Deste modo, os eventos ocorridos são gerenciados por controladores, que são intermediários entre a interface com o usuário e as entidades modeladas do banco de dados. Assim, o principal ganho

com essa abordagem é a facilidade de manutenção e de adição de novos recursos que podem surgir, como a mudança das interfaces com o usuário ou do banco de dados nativo.

Também foram adotados padrões de projetos Façade e DAO (Gamma *et al*. 2000), isolando a camada de negócio das camadas de visualização e persistência, para manter o código de maneira mais legível possível, padronizar o entendimento da equipe de desenvolvimento e reduzir custos de futuras manutenções.

A Figura 4.1 apresenta uma visão geral da arquitetura, que foi simplificada propositalmente para melhor entendimento de todos os membros da equipe de desenvolvimento. A camada mais acima, Visualização, é responsável pela interação direta com o usuário. A camada Negócio preocupa-se em implementar as lógicas de negócio particulares à proposta da ferramenta e a camada Dados é responsável por manter as classes de entidades do banco de dados e as classes de acesso a dados, que estabelece uma interface com o SGBD - Sistema de Gerenciamento de Banco de Dados. A ferramenta utiliza-se de uma base de dados, que internamente pode ser dividida em um repositório de ativos organizacionais e um repositório de projetos.

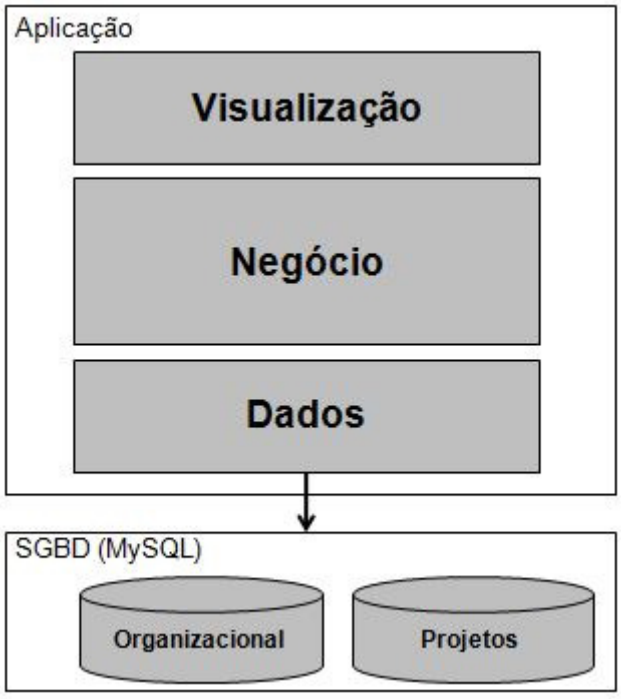

Figura 4.1 Visão geral da arquitetura da ferramenta Spider-RM

4.2.2 Casos de Uso da Ferramenta

Os casos de usos planejados para a ferramenta Spider-RM foram baseados a partir das tarefas definidas na metodologia sugerida e do conjunto de boas práticas coletadas após o mapeamento entre os modelos, as normas e os guias de qualidade relacionados neste trabalho, ambos apresentados no Capítulo 3.

A apresentação dos casos de uso está organizada de acordo com as fases definidas na metodologia (Planejamento, Execução e Avaliação), além disso nem todas as tarefas sugeridas possuem componentes equivalentes na ferramenta, seja por motivo de ser uma tarefa administrativa ou por ser uma funcionalidade menos prioritária, que pode ser desenvolvida futuramente.

O Apêndice C desta dissertação apresenta a rastreabilidade entre os casos de uso e as tarefas da metodologia, identificando a correspondência entre eles e consequentemente quais boas práticas e quais modelos, normas ou guias de qualidade originaram cada funcionalidade da ferramenta.

Por ser um software monousuário, o único ator envolvido em todos os casos de uso é o papel de Gerente de Riscos, apresentado na Seção 3.3.2, porém as funcionalidades da ferramenta também podem ser executadas por outros perfis, como um Gerente de Projetos, por exemplo.

Os diagramas desenvolvidos foram validados por um consultor com experiência em implementação e avaliação do modelo MR-MPS-SW, certificado pela SOFTEX.

A fase de planejamento definida na metodologia sugerida pretende planejar e definir estratégias para tratamento de riscos em nível organizacional. Suas tarefas envolvem a delimitação do escopo para o gerenciamento de riscos na organização, a institucionalização das categorias de riscos comuns aos projetos anteriores e a definição das estratégias que serão utilizadas para lidar com riscos durante a execução dos projetos.

Por possuir tarefas mais relacionadas à administração, a fase de planejamento não teve todas suas tarefas mapeadas para a ferramenta, gerando apenas dois casos de uso apresentados na Figura 4.2 e definidos abaixo:

- **Definir Política Organizacional para Riscos:**armazenar informações a respeito de como a organização lida com riscos em um âmbito geral e dentro do escopo

de um projeto, determinando diretrizes, especificando abrangência e identificando artefatos e técnicas;

- **Gerenciar Estrutura Analítica de Riscos Organizacional:**permitir cadastro, edição e exclusão de categorias na estrutura analítica de riscos organizacional, permitindo o agrupamento de categorias e apontando atributos relacionadas a cada uma delas, como possíveis origens e critérios para análise.

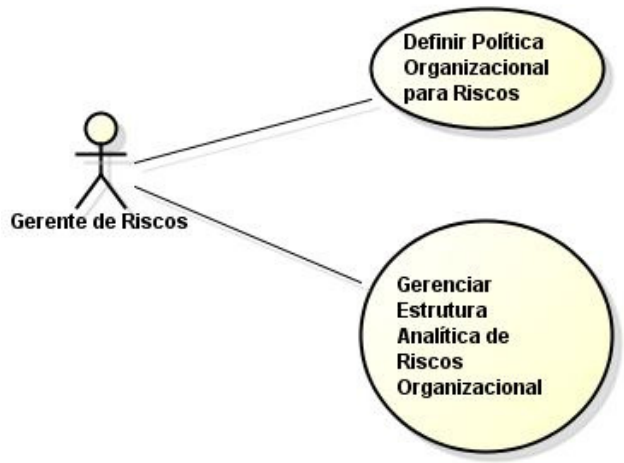

Figura 4.2 Casos de Uso relacionados à fase de planejamento da metodologia sugerida

A segunda fase, Execução, encarrega-se de lidar com riscos durante o ciclo de vida de um projeto, portanto envolve atividades relacionadas ao planejamento, identificação, detalhamento, priorização, monitoramento, mitigação e contingência de riscos dos projeto.

Esta fase concebeu o maior quantitativo de casos de uso, pois é onde encontra-se o maior foco da gerência de riscos de acordo com os modelos, as normas e os guias de qualidade relacionados ao trabalho. A Figura 4.3 apresenta graficamente os casos de uso descritos abaixo:

- **Gerenciar Projeto**: cadastrar, editar informações, armazenar e excluir um projeto de software;
- **Definir Estrutura Analítica de Riscos do Projeto**: de forma semelhante à tarefa que envolve a estrutura analítica de riscos na fase anterior, deve ser possível cadastrar, editar, excluir e manter categorias de riscos desta estrutura,

que inicialmente deve ser uma instância idêntica às categorias institucionalizadas;

- **Definir Plano de Gerenciamento de Riscos:** armazenar informações de como os riscos serão tratados durante o ciclo de vida do projeto, identificando os envolvidos e detalhando técnicas e outras ferramentas que podem ser utilizadas para gerenciar os riscos;
- **Gerenciar Marcos e Pontos de Controle do Projeto:** definir datas importantes durante o projeto, compondo informações como data, descrição e tipo (marco ou ponto de controle), para os riscos serem reavaliados e possíveis ações possam ser tomadas;
- **Identificar Riscos:** cadastrar, editar, excluir e recuperar informações básicas a respeito dos riscos, como nome, descrição e categoria;
- **Analisar Riscos:** detalhar os riscos identificados, coletando mais informações que serão úteis para a priorização e o monitoramento dos riscos, como probabilidade, impacto e dependências entre riscos;
- **Priorizar Riscos:** definir a ordem de prioridade dos riscos, que pode ser determinada automaticamente pela própria ferramenta a partir das informações de probabilidade e impacto, ou pode ser editada manualmente pelo próprio usuário;
- **Desenvolver Plano de Mitigação:** cadastrar, editar, excluir e recuperar informações importantes de tarefas a serem realizadas para a redução da probabilidade, impacto ou ambos em riscos identificados;
- **Desenvolver Plano de Contingência:** cadastrar, editar, excluir e recuperar informações importantes de tarefas a serem realizadas e decisões a serem tomadas após a determinação de que um riscos ocorreu;
- **Monitorar Riscos:** registrar a realização de inspeções periódicas nos riscos identificados para identificar se houve mudança de *status* ou em seus atributos, levando a uma nova análise do mesmo;
- **Deliberar Ocorrência de Riscos:** registrar informações relacionadas à ocorrência de um risco, identificando a data que o mesmo ocorreu;
- **Executar Plano de Mitigação:** registrar data e outras informações importantes, que identifiquem que um plano de mitigação previamente cadastrado foi executado;

- **Executar Plano de Contingência:** registrar data e outras informações importantes, que identifiquem que um plano de contingência foi executado após a deliberação de sua ocorrência.

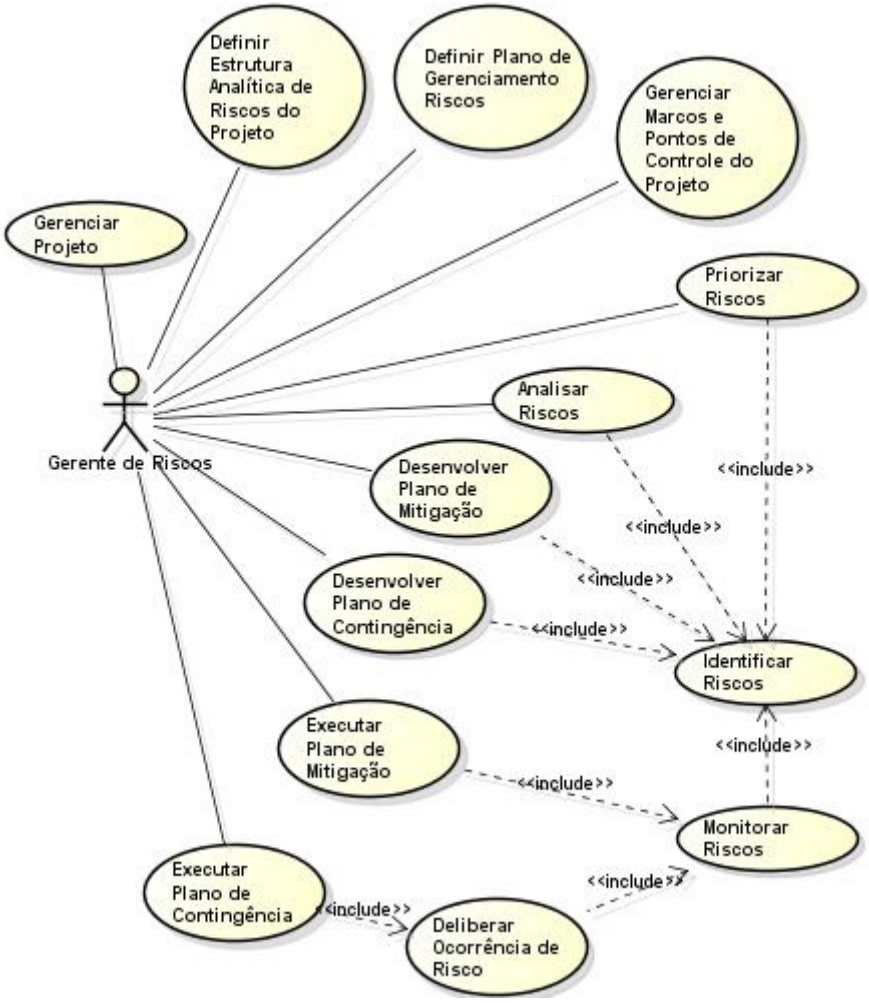

Figura 4.3 Casos de Uso relacionados à fase de execução da metodologia sugerida

Finalmente, a fase de Avaliação tem o objetivo de analisar informações de um projeto concluído e coletar aprendizados, que possam nortear a melhoria do processo de gerência de riscos da organização e orientar futuros projetos, por isso envolve tarefas relacionadas à revisão e à alteração do processo, bem como a revisão das abordagens utilizadas no tratamento dos riscos e na categorização da estrutura analítica de riscos institucionalizada.

A Figura 4.4 apresenta os casos de uso dessa fase, que necessitam primeiramente que um projeto esteja concluído, para enfim realizar a avaliação do projeto ou de novas categorias identificadas. A descrição destes casos de uso estão elucidadas abaixo:

- **Concluir Projeto:** registrar que um projeto cadastrado previamente foi concluído, armazenando a data de ocorrência;
- **Avaliar projeto:** coletar pontos fortes, pontos fracos, oportunidades de melhoria entre outras informações de um projeto concluído com o intuito de orientar melhorias no processo e o gerenciamento de riscos durante o ciclo de vida de futuros projetos;
- **Avaliar Novas Categorias Definidas em um Projeto:** destacar categorias criadas em um projeto que não constam na estrutura analítica de riscos organizacional, para que possam ser analisadas, e em seguida realizada a definição caso seja decidida pela sua institucionalização.

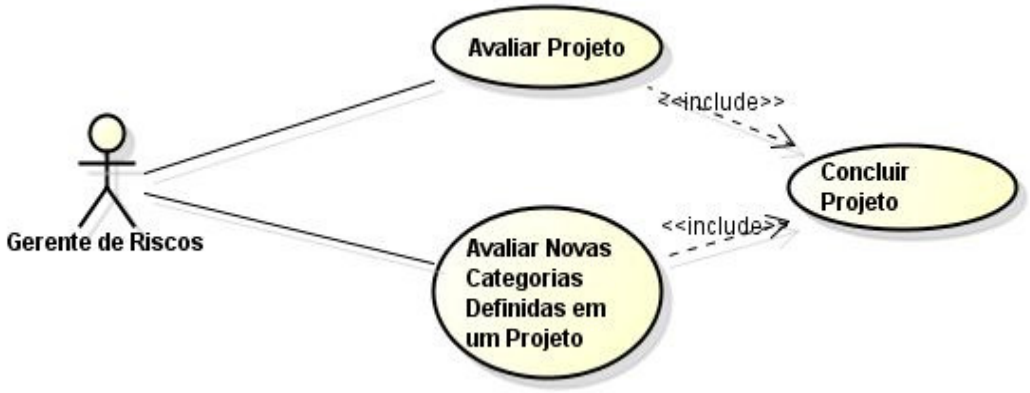

Figura 4.4 Casos de Uso relacionados à fase de avaliação da metodologia sugerida

4.2.3 Tecnologias utilizadas na Ferramenta

O desenvolvimento da Spider-RM foi pautado no uso de ferramentas de software livre, sendo implementada utilizando a tecnologia Java (Java SE) para *desktop*, pois através destes recursos seria possível um desenvolvimento célere, devido à experiência prévia da equipe com essa tecnologia e por ser disponibilizado gratuitamente através de licença GPL.

Quanto ao armazenamento dos dados, optou-se pela implementação através do sistema de gerenciamento de banco de dados MySQL, que é uma solução simples e ágil, adequada às necessidades da ferramenta. Também foi utilizado de forma associada o *framework* Hibernate Annotation com JPA (Java *Persistence Annotation*) para gerenciar a interface entre a aplicação e o SGBD.

4.3 As Funcionalidades da Ferramenta Spider-RM

Como mencionado anteriormente, a ferramenta Spider-RM possui licença GPL, logo é gratuita e de código aberto, possuindo as seguintes características como destaque:

- **Baseada em Normas Modelos e Guias:** é aderente aos resultados esperados do processo de gerência de riscos do MR-MPS-SW, às práticas específicas do processo de gestão de riscos do CMMI-DEV, às tarefas definidas na ISO/IEC 12207 e implementa práticas recomendadas no PMBOK e na ISO/IEC 16085, garantido por meio do mapeamento apresentado no Capítulo 3;
- **Fornece Evidências**: a ferramenta permite registro histórico das informações relacionadas ao gerenciamento de riscos, logo os dados podem ser consultados tanto em futuros projetos, quanto em possíveis avaliações oficiais realizadas pelas instituições mantenedoras dos modelos citados acima;
- **Estrutura Analítica de Riscos:** a ferramenta permite a criação e a manutenção de uma EAR, possibilitando um melhor gerenciamento de riscos semelhantes, quando agrupados em uma mesma categoria. Uma EAR é importante para auxiliar durante a identificação de riscos em um projeto, principalmente quando os envolvidos ainda não possuem muita experiência prática com a área;
- **Gerência de Planos de Mitigação e Contingência:** possibilita a criação, acompanhamento e encerramento de planos de mitigação e contingência para os riscos, de forma que as informações relacionadas à gerência de riscos ficam concentradas em apenas um lugar e podem ser facilmente consultadas em ocasiões futuras.

A ferramenta está dividida em dois módulos: (i) o Organizacional, que possui funcionalidades relacionadas à gerência de riscos no âmbito de toda a organização, independentemente de projeto, como controle do portfólio, estrutura analítica de riscos institucionalizada, política organizacional e algumas configurações básicas; e o (ii) de Escopo de Projeto, que realiza atividades de gerenciamento de riscos dentro do ciclo de vida de um projeto, como identificação, análise, priorização, monitoramento, mitigação e contingência de riscos.

4.3.1 Visão Geral

A Figura 4.5 apresenta a tela inicial da ferramenta Spider-RM, que possui uma barra superior com algumas funções relacionadas a configurações, como endereços onde os artefatos utilizados serão armazenados, opção para criar um novo projeto, ou editar a estrutura analítica de riscos organizacional. Também há um menu do tipo *combobox* para selecionar o projeto atual que deverá ser consultado nas demais funcionalidades.

Por ser monousuário, a ferramenta não necessita de cadastro de *login* e senha, porém possui a opção de editar informações relacionadas à organização e aos gerentes de cada projeto.

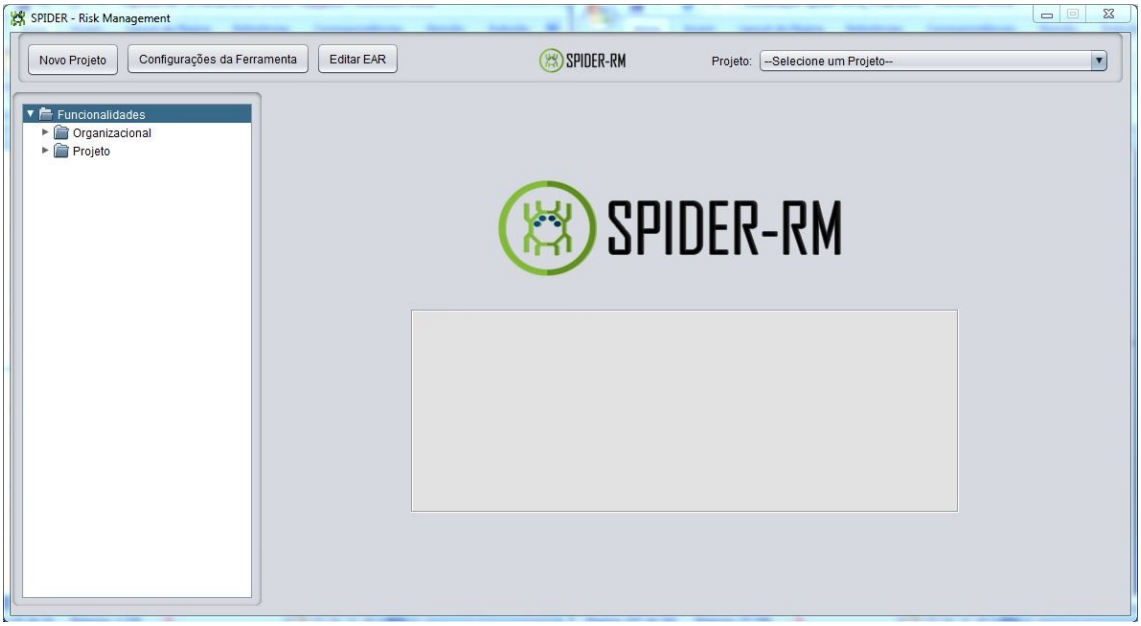

Figura 4.5 Tela Principal da Spider-RM

No menu à esquerda estão as funções principais que o gerente de risco poderá realizar, e estão divididas em dois grupos organizacional e projeto, que serão detalhados nas subseções seguintes.

4.3.2 Módulo Organizacional

As funcionalidades relacionadas à organização estão agregadas no menu à esquerda denominado Organizacional e possui três principais funcionalidades: Política Organizacional, Estrutura Analítica de Riscos e Portfólio.

a) Política Organizacional

A organização deverá definir uma política para o gerenciamento de riscos. Esta funcionalidade está relacionada com as tarefas da metodologia "Determinar Escopo da Gerência de Riscos" e "Definir Modelo de Plano do Gerenciamento de Riscos", onde devem ser definidas as diretrizes do gerenciamento de projetos na organização e de forma genérica a todos os projetos.

A Figura 4.6 apresenta a tela desta funcionalidade, que deve armazenar o conteúdo da política organizacional através da importação de um arquivo, ou através da inserção manual de texto.

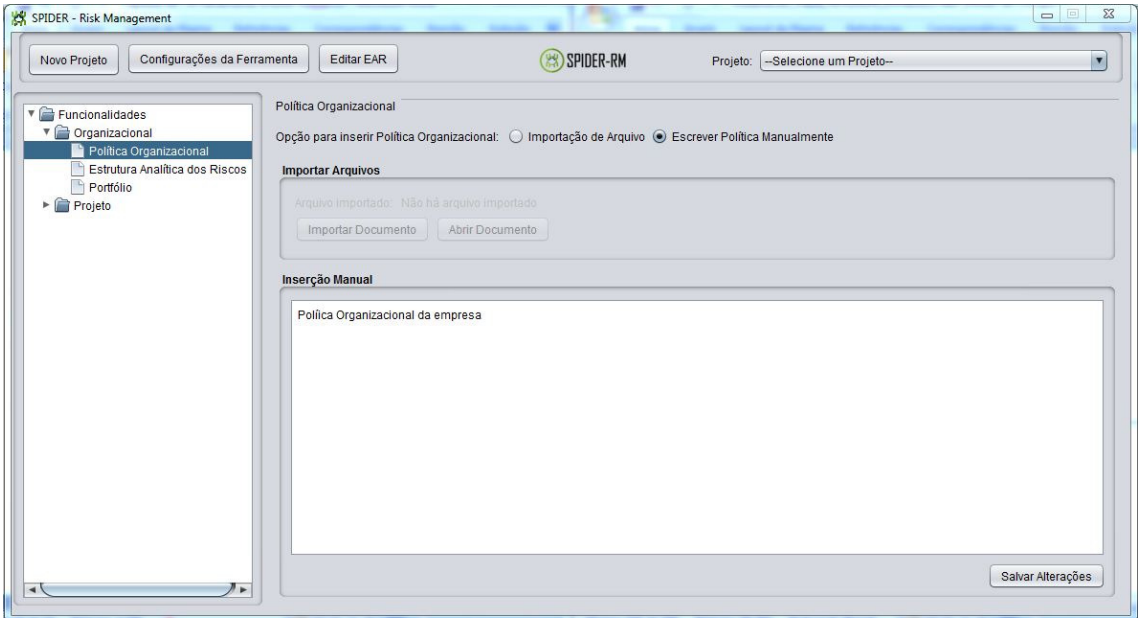

Figura 4.6 Tela de Política Organizacional

b) Estrutura Analítica de Riscos

Esta funcionalidade relaciona-se com a tarefa "Definir Categoria de Riscos", também da fase de planejamento da metodologia sugerida, e com a tarefa "Identificar Novos Riscos Organizacionais" da fase de Avaliação. Como pode ser observado na Figura 4.7, é possível adicionar e remover itens utilizados em outros projetos à estrutura organizacional, além de consultar informações relacionadas a cada categoria, como descrição, possíveis origens, critérios para determinação de probabilidade e critérios para determinação de impacto.

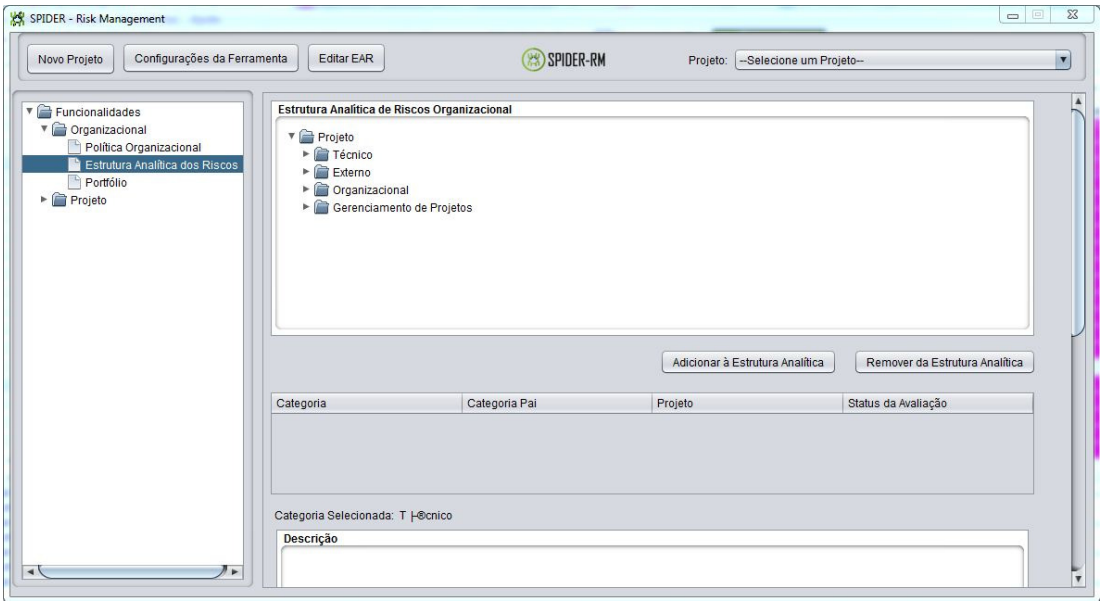

Figura 4.7 Tela de Estrutura Analítica de Riscos Organizacional

c) Portfólio

Originou-se a partir das tarefas "Revisar Processo de gestão de Riscos", "Revisar tratamento de Riscos e sucessos" e "Identificar novos riscos organizacionais", todas da fase de Avaliação da metodologia. A Figura 4.8 apresenta a tela de Portfólio, no qual resume os projetos cadastrados na ferramenta, identificando quais foram concluídos e podem ser avaliados.

A avaliação realizada nesta tela dá-se de duas formas, representadas pelas abas. A primeira refere-se à avaliação do projeto, que registra informações dos pontos fortes, pontos fracos, oportunidades de melhoria e outras informações adicionais que forem convenientes. Outra avaliação são das categorias adicionadas ao projeto que não constam na EAR institucionalizada, no qual também são registradas as mesmas informações que a avaliação do projeto, para orientar a tomada de decisão na tarefa "Identificar Novos Riscos Organizacionais".

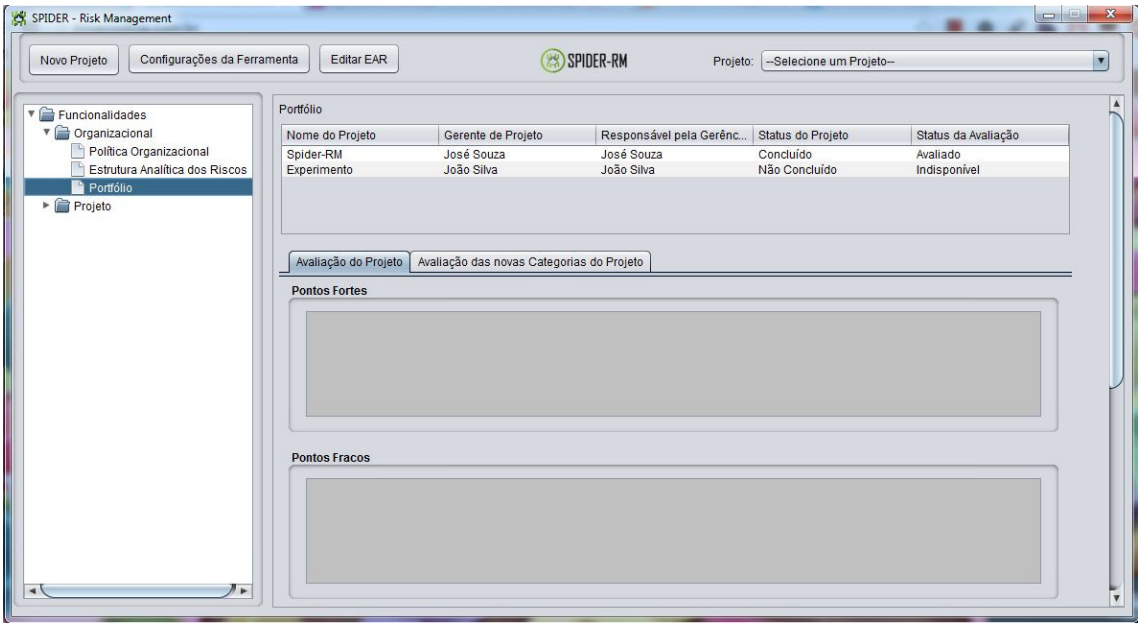

Figura 4.8 Tela de Portfólio

4.3.3 Módulo de Escopo de Projetos

As demais funcionalidades estão agrupadas no submenu Projeto. Para acessar estas opções faz-se necessária a seleção de um projeto no menu *combobox* detalhado na visão geral da ferramenta. Estas funções podem ser separadas em três categorias: (i) as que são referentes ao planejamento, ou seja, as fases iniciais do projeto, que são Plano de Risco, Estrutura Analítica de Riscos do Projeto e Calendário; (ii) as funções relacionadas ao gerenciamento de riscos, que são Gerenciar Riscos, Priorizar Riscos e Riscos Ocorridos; e (iii) as funções que dizem respeito ao monitoramento de riscos, que são Analisar Riscos, Planos Pendentes e Planos Realizados.

a) Plano de Risco

Esta funcionalidade está alinhada à tarefa "Definição do Plano de Gerenciamento de Riscos" da metodologia e, de forma semelhante à política organizacional, tem o intuito de registrar informações a respeito das ações que serão tomadas para administrar os riscos durante o projeto, podendo ser armazenada em um arquivo de qualquer formato que deverá ser importado para a ferramenta ou através de texto diretamente no campo identificado para inserção manual. A Figura 4.9 apresenta esta tela.

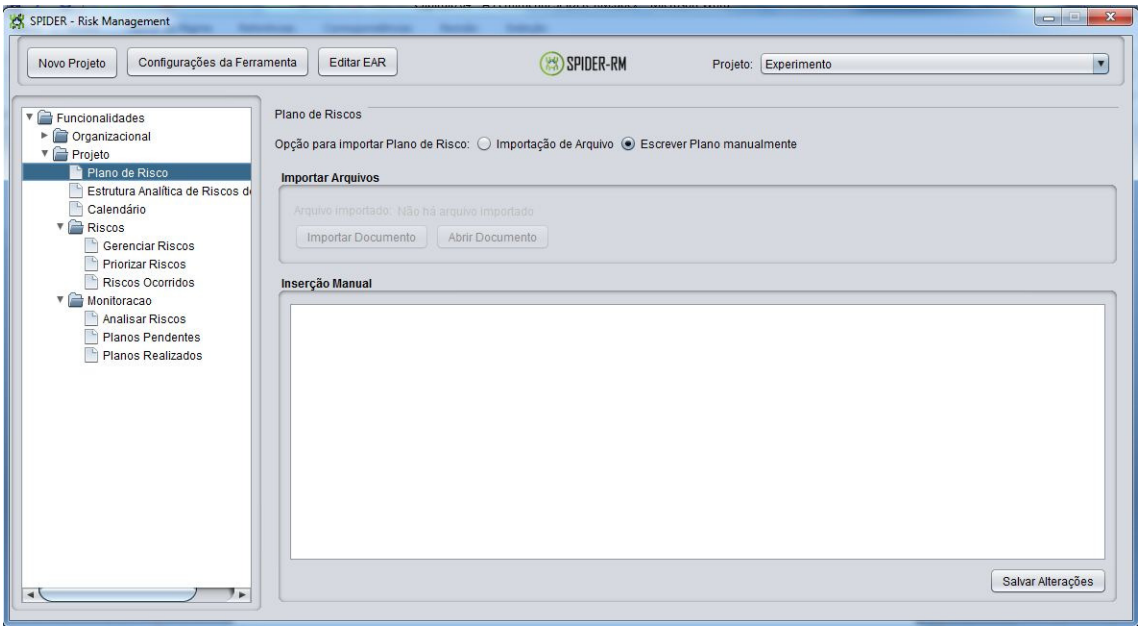

Figura 4.9 Tela de Plano de Risco

b) Estrutura Analítica de Riscos do Projeto

Associada também à tarefa "Definir Categorias de Riscos", esta funcionalidade permite gerenciar a EAR instanciada de um projeto. Ao ser criado um novo projeto, automaticamente é feita uma cópia da EAR organizacional para do projeto, que tornam-se então independentes. Esta tela, observada na Figura 4.10, assemelha-se com a tela de Estrutura Analítica de Riscos do módulo organizacional, porém possui duas abas específicas: uma para adicionar um nova categoria avulsa não institucionalizada; e outra para adicionar novamente uma categoria da EAR organizacional que havia sido apagada após a instância da mesma.

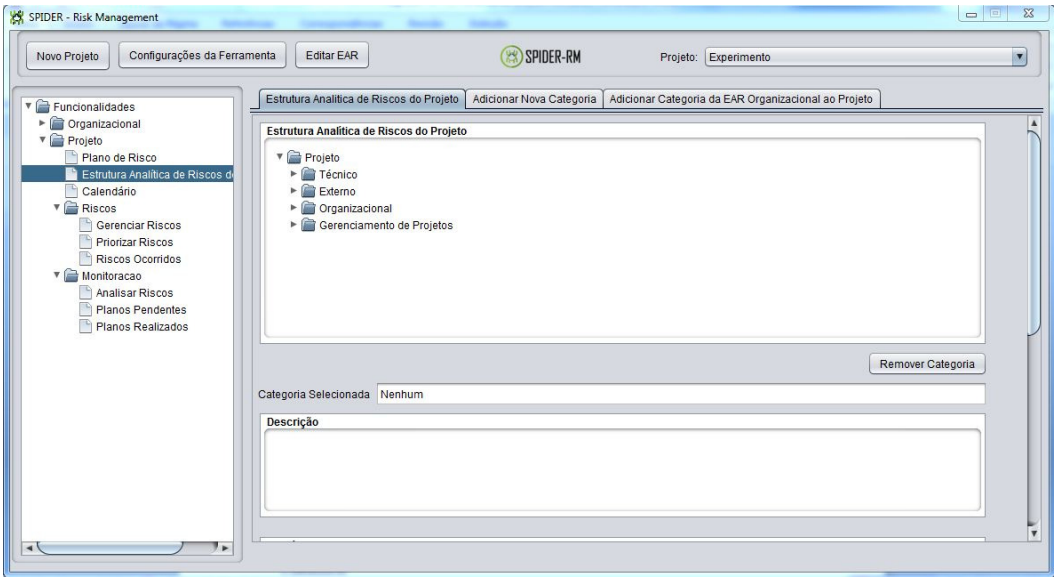

Figura 4.10 Tela de Estrutura Analítica de Riscos do Projeto

c) Calendário

Esta funcionalidade não possui relação direta com alguma tarefa da metodologia, porém foi necessária sua inclusão para estratégias de monitoramento de forma mais clara, registrando assim *deadlines* para avaliar mudanças nos riscos ou executar os planos de mitigação. A Figura 4.11 exibe esta tela, que possui um calendário marcando as datas importantes (Marcos ou Pontos de Controle cadastrados) e um formulário para registro, alteração, exclusão e consulta de Marcos ou Pontos de Controle.

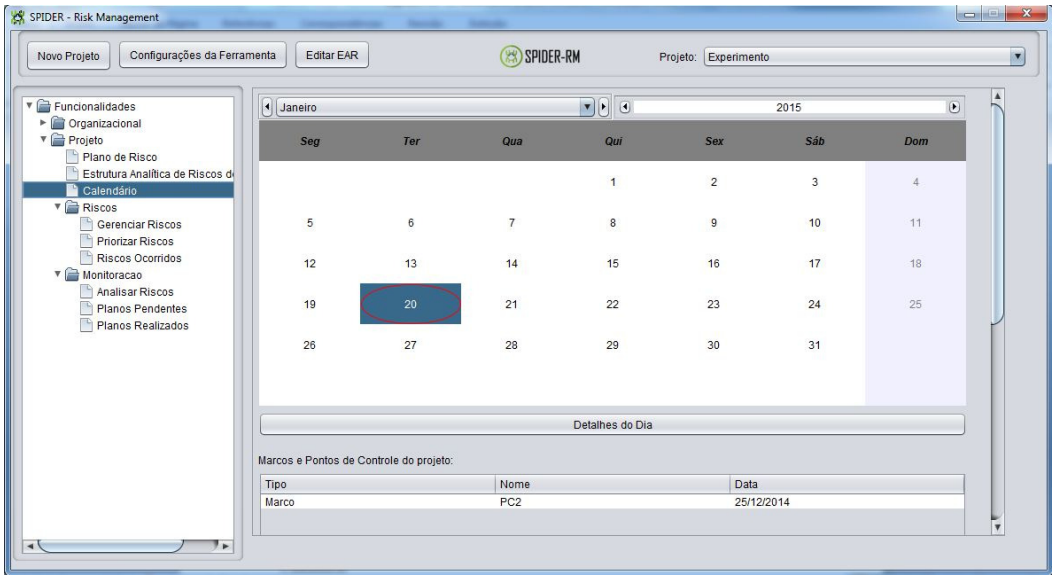

Figura 4.11 Tela de Calendário

d) Gerenciar Riscos

A Figura 4.12 apresenta esta tela, que foi baseada nas tarefas "Identificação dos Riscos","Detalhamento de Riscos" e "Elaboração de Planos para Riscos Prioritários", sendo responsável tanto pelo registro básico do risco, contendo identificação, descrição e categoria, quanto pelos dados relacionados à análise de riscos, evidenciados não somente pela combinação de probabilidade e impacto, mas também pelas relações entre riscos, pelas condições de ocorrência do risco, e pelo desenvolvimento de planos de mitigação e contingência, dispostos nas demais abas desta tela.

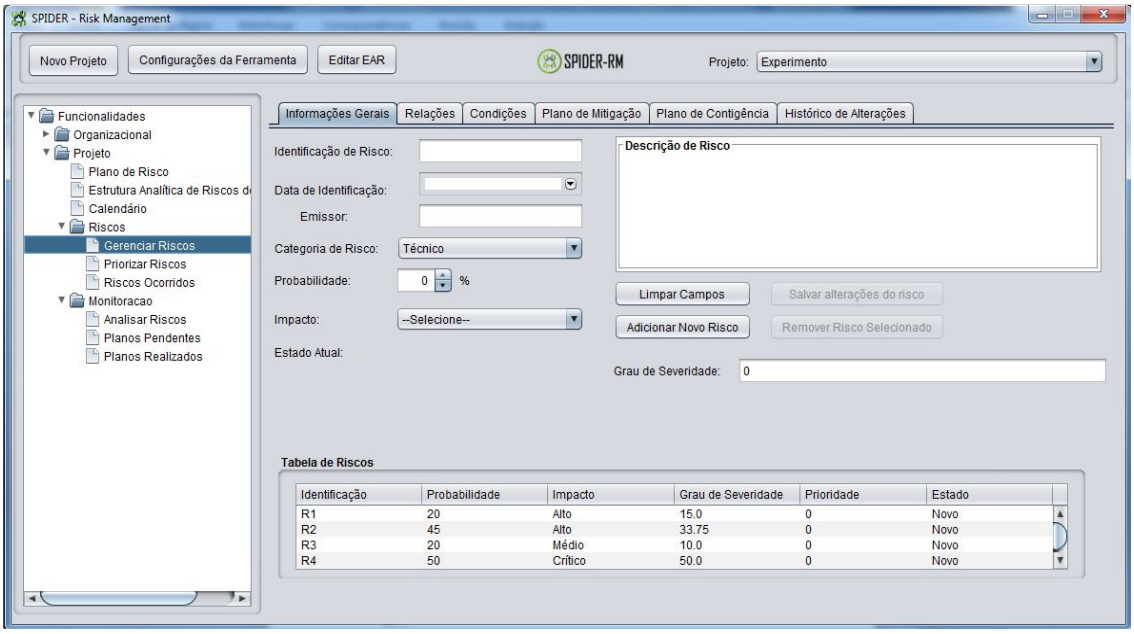

Figura 4.12 Tela de Gerenciar Riscos

e) Priorizar Riscos

A priorização de riscos baseia-se na tarefa da metodologia denominada "Definição de Riscos Prioritários", e como pode ser visto na Figura 4.13, sua tela dispõe de uma lista de riscos cadastrados, ordenados pelo grau de severidade calculado automaticamente, através do produto entre impacto e probabilidade. Caso seja conveniente para o usuário é possível alterar a ordem de prioridade manualmente.

Na tela responsável pela priorização, também há uma funcionalidade para selecionar quais destes riscos serão monitorados, uma vez que os recursos dos projetos são limitados e pode ser inviável o monitoramento de todos os riscos de forma simultânea. Ao apertar o botão "Selecionar risco para monitorar" surge uma caixa de diálogo apresentada na Figura 4.14, que permite ao usuário marcar quais riscos serão

monitorados durante o projeto, desde que já possuam um plano de mitigação definido. A qualquer momento durante o projeto ambas as telas podem ser acessadas para repensar a priorização e consequentemente reavaliar os riscos que necessitam ser monitorados.

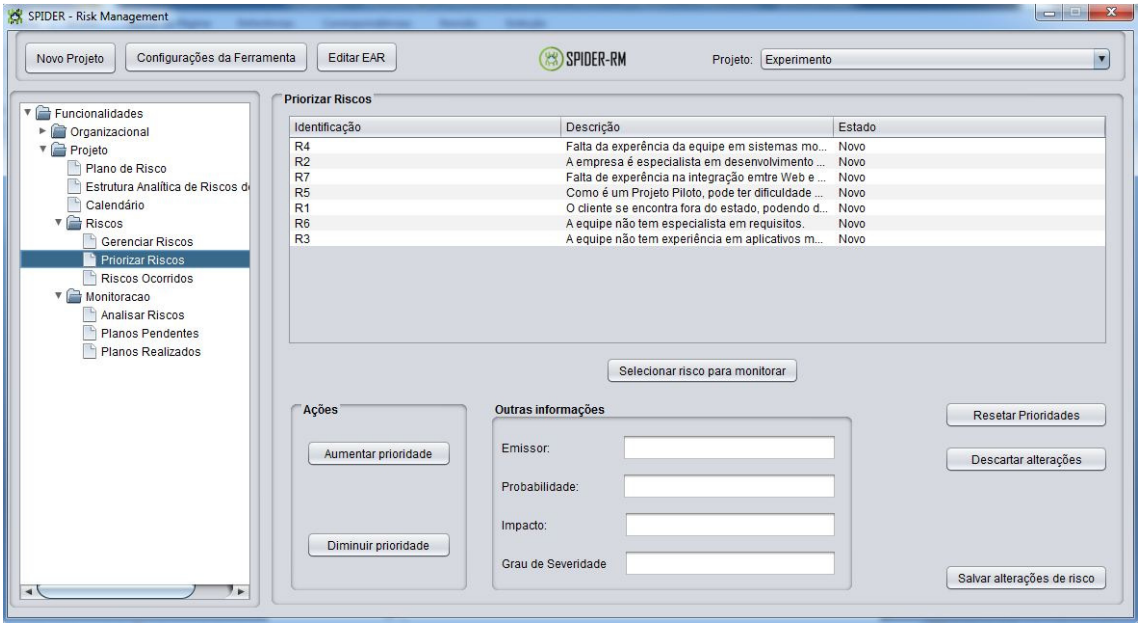

Figura 4.13 Tela de Priorizar Riscos

Os riscos que foram selecionados para monitoramento passam a ter seu *status* alterado para "Mitigando". Todo risco, após ser cadastrado, passa a ter seu *status* definido como "Novo", e a primeira alteração deste valor ocorre na situação aqui especificada.

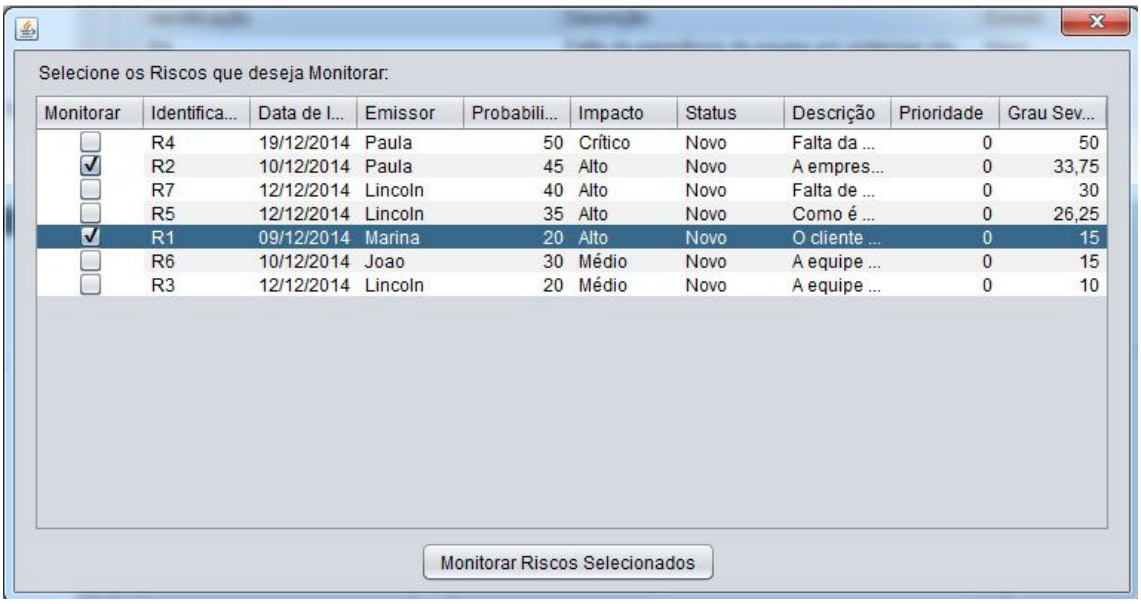

Figura 4.14 Tela da Seleção de Riscos para Monitoramento

f) Riscos Ocorridos

A tela de Riscos Ocorridos, apresentada na Figura 4.15, é basicamente uma tela para consulta de riscos que tiveram sua ocorrência deliberada durante o projeto, gerando assim um relatório de fácil acesso às suas informações.

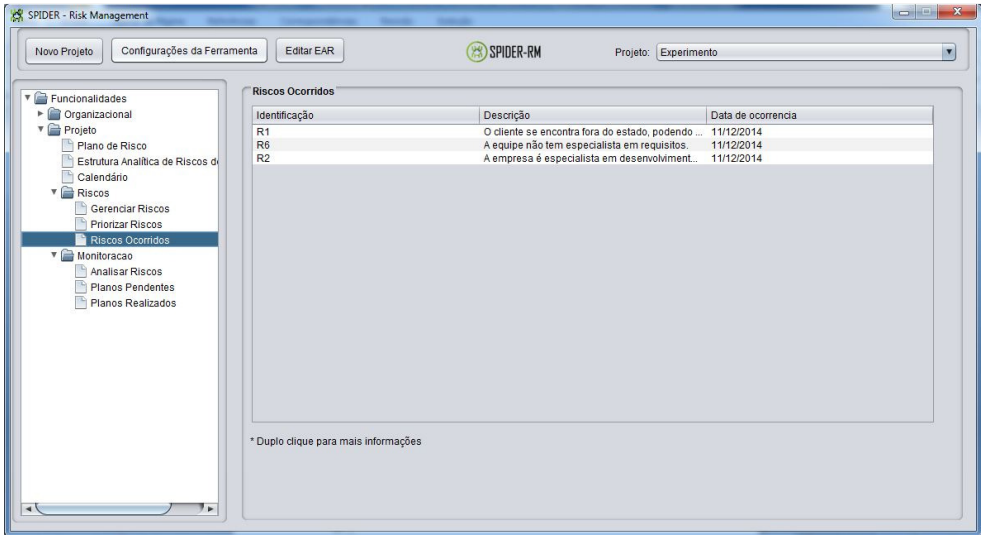

Figura 4.15 Tela de Apresentação de Riscos Ocorridos

g) Analisar Riscos

A Figura 4.16 exibe a tela de Seleção de Risco para Análise, onde os riscos selecionados para monitoramento ficam pendentes até que sejam analisados antes do marco ou ponto de controle ao qual foi definido. Esta funcionalidade está relacionada à tarefa "Avaliação e Monitoramento de riscos" da metodologia sugerida.

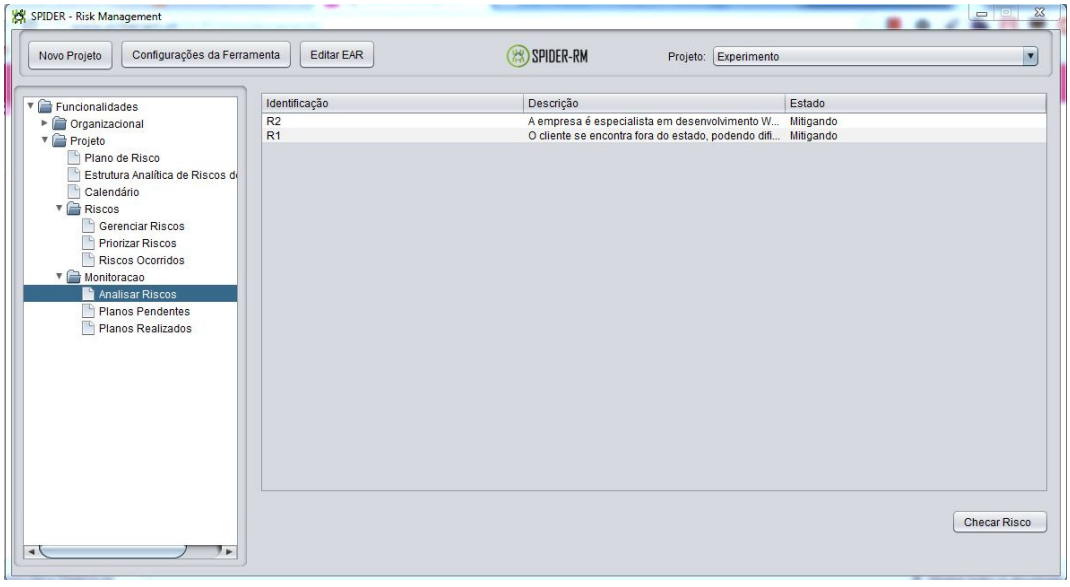

Figura 4.16 Tela de Seleção de Risco para Análise

Após selecionado o risco a ser analisado e o botão "Checar Risco" ser pressionado, é aberta uma caixa de diálogo especificada na Figura 4.17, que apresenta dados importantes a respeito do risco envolvido, e é onde é registrado o monitoramento do risco. Nesta tela é possível alterar novamente o *status* do risco que neste momento está com o valor "Mitigando". As opções para alteração são os valores "Contingenciando", quando o risco ocorreu, ou "Novo", quando o risco não ocorreu. Neste último caso o risco volta a ficar aguardando ser selecionado novamente para um novo monitoramento.

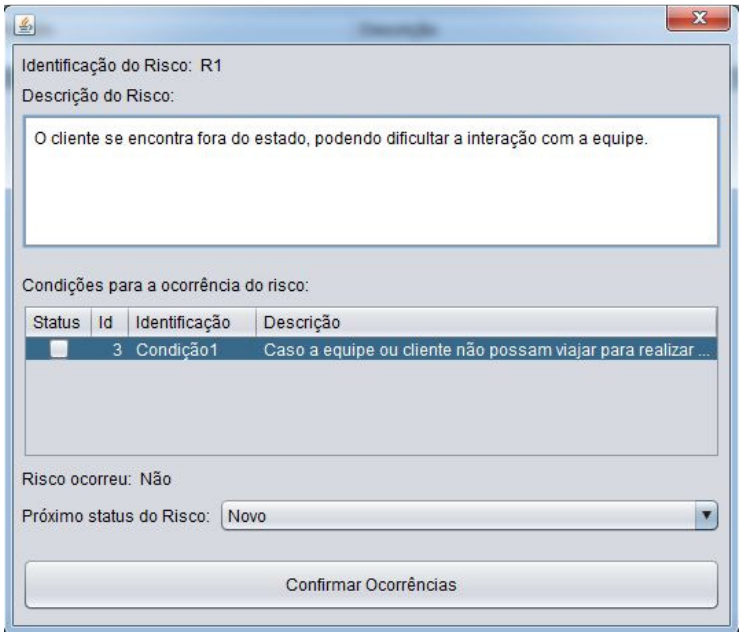

Figura 4.17 Tela da Análise de Risco

h) Planos Pendentes

A tela de Execução de planos pendentes (Figura 4.18) está relacionada com a tarefa "Execução do Plano de Mitigação ou Contingência" e apresenta uma lista de planos que precisam ser executados antes da data limite especificada. Após a mudança de *status* de um risco um plano é acionado, de Mitigação, caso o *status* seja "Mitigando" ou de Contingência, caso seja "Contingenciando".

Ao ser selecionado um plano, abrirá uma caixa de diálogo com os detalhes cadastrados dos planos, identificando entre outras informações, como deverá ser realizado.

Os planos executados devem ser marcados na coluna "Realizar" da tela, e em seguida deve ser pressionado o botão "Salvar realização de planos", para que as alterações sejam registradas e o plano selecionado seja omitido da lista.

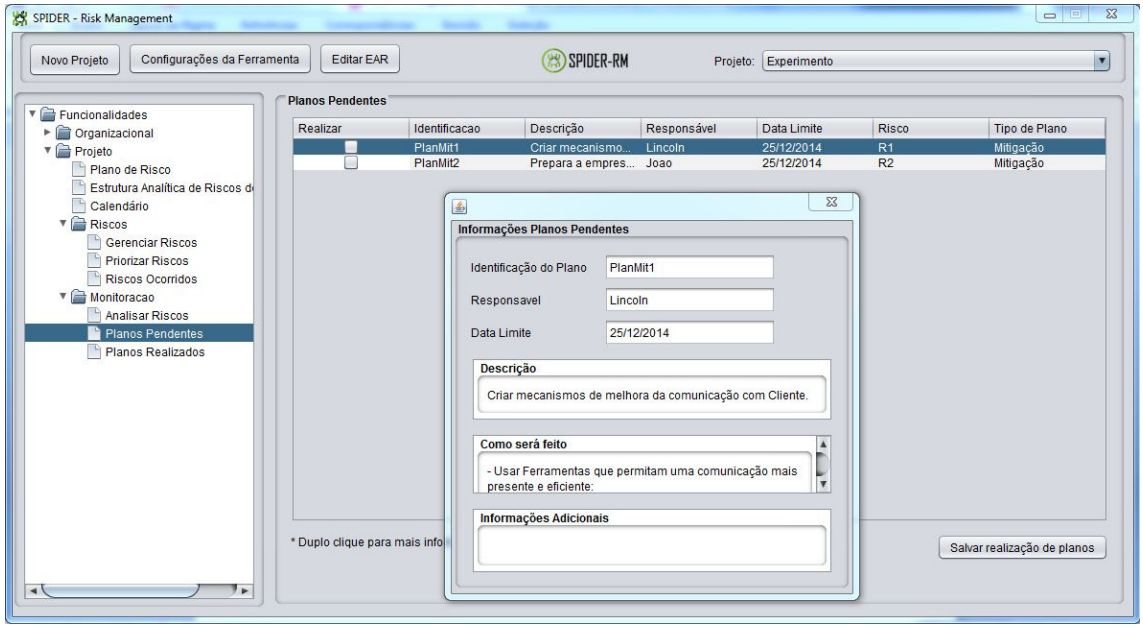

Figura 4.18 Tela da Execução de Planos Pendentes

i) Planos Realizados

A tela de Planos Realizados, apresentada na Figura 4.19, é basicamente uma tela para consulta dos planos já executados e omitidos da tela anterior, gerando assim um relatório de fácil acesso às suas informações.

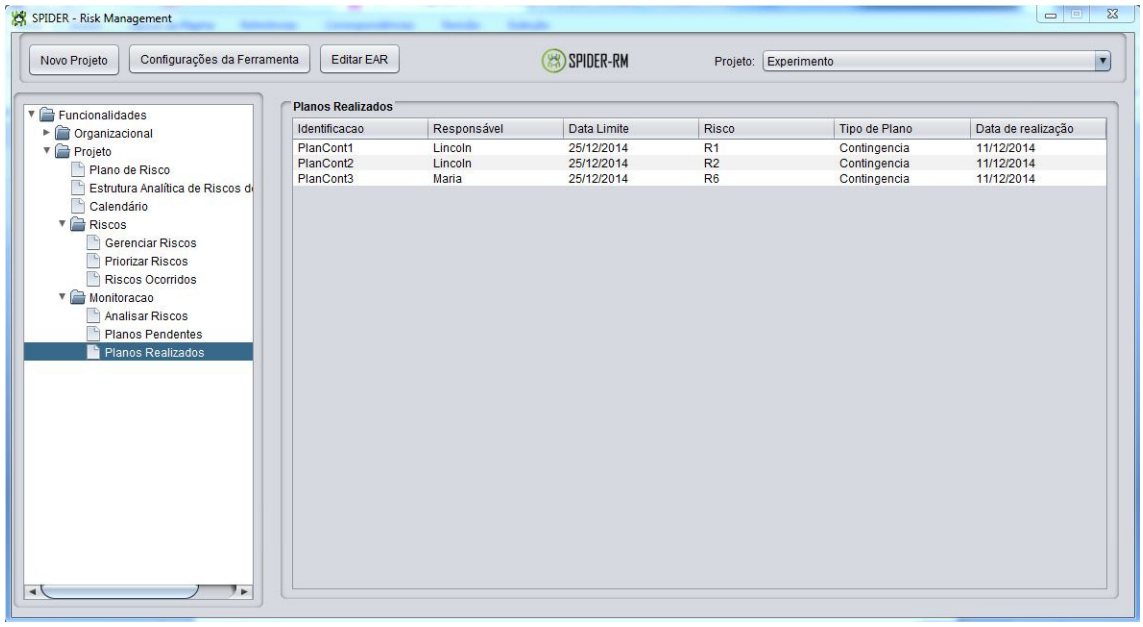

Figura 4.19 Tela da Apresentação dos Planos Realizados

4.4 Diferenciais da Ferramenta

Os principais diferenciais da ferramenta Spider-RM aos trabalhos relacionados, que desenvolvem uma ferramenta de apoio ao processo de gerência de riscos são: o embasamento em modelos de qualidade de processo de software; a possibilidade de definição e personalização da Estrutura Analítica de Riscos; a priorização de riscos; a identificação de condições para ocorrência de riscos; e elaboração de planos de mitigação e contingência para o monitoramento dos riscos. Para mais detalhes, o Quadro 4.1 compara funcionalidades entre as ferramentas TRIMS (TRIMS,2014), CRAMM (Yazar, 2002), RiskFree (Knob, 2006) e Spider-RM.

Foi realizado um agrupamento de funcionalidades em categorias semelhantes, recebendo cada ferramenta a informação: "S", caso possua a funcionalidade; "P", caso realize a funcionalidade parcialmente, ou seja, com restrições; "N", caso não exista tal funcionalidade; e "D", caso a referência analisada sobre a ferramenta não identifique esta informação.

Quadro 4.1. Comparativo entre as principais funcionalidades da ferramenta Spider-RM e outras ferramentas mencionadas em trabalhos relacionados.

Categorias de Funcionalidades	Funcionalidades	TRIMS	CRAMM	RiskFree	Spider-RM
Organizacional	Permite fácil acesso à Política Organizacional	N	N	N	S
	Avaliação de Projeto Concluído	N	N	P	S
	Avaliação de Categorias de Risco Adicionadas	N	N	N	S
	Gerenciamento de vários Projetos Simultaneamente	S	D	S	S
Planejamento para a Gerência de Riscos	Inserção do Plano de Gerência de Riscos para Fácil Acesso	N	N	S	S
	Definir e Personalizar a Estrutura Analítica de Riscos (Categorias de Risco)	S	D	N	S
	Definir Marcos e Pontos de Controle	N	N	N	S
Análise de Riscos	Inserção e Controle de Plano de Mitigação	S	P	S	S
	Inserção e Controle de Plano de Contingência	N	N	S	S

Categorias de Funcionalidades	Funcionalidades	TRIMS	CRAMM	RiskFree	Spider-RM
	Identificar Subcondições para Monitorar Ocorrência dos Riscos	P	N	N	S
	Identificação de Relações entre Riscos	N	N	N	S
	Flexibilidade para Priorização de Riscos	N	N	N	S
	Cálculo do Grau de Severidade de um Risco	S	S	S	S
	Personalização do Grau de Severidade de um Risco	P	N	N	S
Monitoração de Riscos	Acompanhamento de Mudanças em Riscos durante o Projeto	S	P	S	S
	Identificação de Risco Ocorrido	S	D	S	S
	Permite Escolha Livre dos Riscos a serem Monitorados	N	N	N	S
	Histórico de Ocorrência de Risco	S	N	D	S
	Histórico de Ocorrência geral no Projeto	N	D	D	S
	Histórico de Alterações nos Riscos	N	N	N	S
Gerenciamento de tarefas	Apresentação de Tarefas Pendentes	P	D	N	S
	Histórico de Tarefas Realizadas	N	D	S	S
	Apresentação de Tarefas a serem Realizadas em Ponto de Controle ou Marco do Projeto	N	N	N	S

4.5 Considerações Finais

A ferramenta Spider-RM tem o intuito de auxiliar a implementação de um processo de gerenciamento de riscos em uma organização desenvolvedora de software, tendo como base, objetivos e práticas recomendadas por modelos, normas e guias de qualidade.

A motivação para o desenvolvimento da ferramenta originou-se do pressuposto que o gerenciamento de riscos pode ser facilitado significativamente ao se utilizar

recursos ferramentais sistematizados ou automatizados, pois é possível a redução de custos relacionado a tempo e recursos financeiros.

Com a aplicação da Spider-RM espera-se que a mesma permita um melhor acompanhamento dos riscos de uma organização, de maneira geral ou durante um projeto de software, integrando e centralizando as informações coletadas em um só lugar de maneira que facilite a manipulação dos documentos e a geração dos resultados para os modelos de referência MR-MPS-SW e CMMI-DEV.

É importante ressaltar que cada passo do desenvolvimento da ferramenta foi supervisionado por um consultor de implementação e avaliador MPS.BR certificado pela SOFTEX, como forma de garantir que a ferramenta esteja alinhada às necessidades dos modelos de qualidade e à metodologia sugerida neste trabalho.

5 AVALIAÇÃO QUALITATIVA

Este capítulo discute sobre a avaliação qualitativa realizada na metodologia sugerida para gerenciamento de riscos e na ferramenta de apoio desenvolvida, com o principal foco de identificar se a utilização de ambos, ferramenta e metodologia, usados de forma combinada podem auxiliar na aprendizagem de práticas relacionadas ao processo de gerência de riscos.

A avaliação sucedeu-se através de um experimento controlado com alunos de pós-graduação, que preencheram questionários objetivos e um grupo de questões subjetivas para avaliar o conhecimento relacionado ao gerenciamento de riscos.

5.1 Abordagem da Avaliação

Para realizar a avaliação aqui pretendida, Travassos (2002) recomenda que seja elaborada em um cenário mais próximo possível da realidade, de preferência que o contexto e o cenário sejam uma situação real. No entanto, existem algumas limitações para efetivar tal validação dentro de uma organização, em um projeto que gerará um produto de software, principalmente porque os resultados obtidos tratam-se de um trabalho acadêmico ainda em processo de aceitação, e o tempo estimado para implantação e validação do processo de gerenciamento de riscos extrapolam o período programado para esta pesquisa.

Esta avaliação qualitativa baseou-se nas estruturas definidas pelos trabalhos feitos nas dissertações de Teles (2011) e Alho (2012), e teve como abordagem a avaliação através de um experimento com pessoas que possuíssem alguma experiência em gerenciamento de projetos, melhoria do processo de software e/ou gerência de riscos.

O objetivo definido para a experimentação é definir se a ferramenta Spider-RM,

utilizada em conjunto com a metodologia definida, podem fornecer apoio à aprendizagem do processo de gerenciamento de riscos em projetos de software. As métricas foram obtidas através de questionários objetivos e subjetivos preenchidos pelos participantes.

A utilização dos questionários pretendeu identificar aspectos como o perfil do participante, a percepção dos mesmos com relação à ferramenta Spider-RM e seu grau de conhecimento relacionado às atividades de gerenciamento de riscos.

Com relação ao perfil do entrevistado foram abordadas questões objetivas relacionadas ao tempo de experiência em projetos de software, e em modelos de qualidade, assim como se possuem alguma certificação relacionada aos modelos e o nível de conhecimento e experiência com gerenciamento de riscos. Deste forma, é possível assegurar que os participantes possuem algum conhecimento em gerenciamento de projetos, melhoria de processo e/ou gerenciamento de riscos.

No que diz respeito ao questionário de avaliação da ferramenta, foram solicitadas percepções objetivas referentes à usabilidade, desempenho, funcionalidades e aderência ao modelo MR-MPS-SW, logicamente, na medida do possível de acordo com o nível de conhecimento do participante. Também foi elaborada uma questão discursiva a respeito da ferramenta, convidando o participante a definir pontos fortes, pontos fracos e oportunidades de melhoria identificados durante a execução do experimento.

Os questionários de perfil do entrevistado e de avaliação da ferramenta utilizados encontram-se em sua íntegra no documento: Questionário de Perfil e Avaliação da Spider-RM,disponíveis o Apêndice E deste trabalho.

Outro questionário subjetivo aplicado durante o experimento está detalhado no Apêndice F. Trata-se do Questionário de Avaliação do Conhecimento, contendo cinco questões relacionadas ao gerenciamento de riscos para a avaliação do grau de conhecimento dos participantes a respeito da área. Estas perguntas foram aplicadas duas vezes, a primeira antes do experimento e a segunda após o experimento, para posteriormente ser realizada a análise de ambas e identificar se houve aperfeiçoamento nas respostas.

A avaliação qualitativa foi realizada em cinco fases distintas embasadas no trabalho de Rouiller *et al.* (2006):

1. **Fase 1 - Apresentação do Projeto:** foi inicialmente solicitado aos participantes o preenchimento do questionário relacionado ao seu perfil e à avaliação do conhecimento, para que seja identificado o grau de entendimento da gerência de riscos antes do experimento. Em seguida, foi ministrada uma aula sobre o processo, suas definições em modelos de qualidade e sobre as funcionalidades da ferramenta Spider-RM;
2. **Fase 2 - Formação das Equipes, Diagnósticos e Planejamento:** foram analisados os questionários de perfil dos participantes, para identificar se todos possuíam o perfil necessário para a realização das próximas etapas do experimento, com o mínimo de conhecimento em gerenciamento de projetos de software ou em modelos de qualidade. Com relação à formação das equipes, foi estabelecido que cada participante executaria as atividades individualmente;
3. **Fase 3 - Gestão da Ferramenta:**foi apresentada a metodologia aos participantes, que em seguida foram apresentados a um cenário inicial (especificado no Apêndice D) e fizeram, individualmente, uso das funcionalidades da ferramenta Spider-RM, para gerenciar os possíveis riscos em diversos pontos de controle do ciclo de vida do projeto, ocorrendo pequenas variações no cenário expostas verbalmente;
4. **Fase 4 - Maturação do Processo:** os participantes preencheram o questionário de avaliação da ferramenta com base nas atividades realizadas e nos conhecimentos obtidos, e novamente, o questionário relacionado à avaliação do conhecimento;
5. **Fase 5 - Encerramento:** foi realizada a análise dos dados fornecidos pelos participantes e um comparativo entre os questionários de avaliação do conhecimento preenchidos antes e depois do experimento, seguida pela interpretação das informações.

As atividades que dependiam dos voluntários foi realizada em um período de oito horas totais de duração durante uma disciplina da pós-graduação do PPGCC-UFPA, logo o perfil dos participantes é essencialmente de alunos. No entanto, como pode ser observado na análise dos resultados, todos possuíam conhecimento mínimo necessário para a execução das tarefas planejadas. O plano de execução das fases descritas, juntamente com os responsáveis por cada tarefa e a quantidade de horas

utilizadas para execução estão detalhados no Quadro 5.1.

Quadro 5.1 Plano de Realização das Fases

Fase	***Tarefa***	***Responsável***	***Carga horária***
Apresentação do projeto	Preenchimento do "questionário do perfil do participante"	Alunos da disciplina	0,5 hora
	Avaliação do conhecimento, a partir do preenchimento do "formulário de avaliação"	Alunos da disciplina	1 hora
	Apresentar o que é gerência de riscos	Gerente do projeto do estudo	2 horas
	Apresentar sobre gerência de riscos no mps.br/cmmi-dev		
	Apresentação da ferramenta		
Formação das equipes, diagnósticos e planejamento	Análise de perfil dos participantes para identificar se todos enquadram-se nas necessidades do experimento	Gerente do projeto do estudo	0,5 hora
	Entendimento do plano de execução das tarefas de gerenciamento de riscos	Gerente do projeto do estudo e alunos da disciplina	0,5 hora
Gestão da Ferramenta	Uso da ferramenta	Gerente do projeto do estudo e alunos da disciplina	2,5 horas
Maturação dos projetos	Avaliação do conhecimento, a partir do preenchimento do "formulário de avaliação"	Alunos da disciplina	1 horas
	Preenchimento do "questionário de avaliação da ferramenta"	Alunos da disciplina	0,5 hora
Encerramento	Análise dos resultados obtidos	Gerente do projeto do estudo	12 horas
	Interpretação	Gerente do projeto do estudo	6 horas

A metodologia utilizada mostrou-se bastante eficiente em sua execução, já que contou com o comprometimento dos participantes, que estavam focados nas realizações das tarefas planejadas e trouxeram resultados relevantes. Apesar disso, pode ser pouco satisfatória se comparada com uma auditoria real, no qual a ferramenta e a metodologia seriam inseridas na organização em um projeto executado pela mesma.

5.2 Análise dos Resultados Obtidos

Nesta seção serão apresentados os resultados obtidos dos questionários utilizados durante o experimento, que envolveu seis participantes com conhecimentos distintos em gerência de projeto, modelos de qualidade de software e gerência de riscos.

A análise dos resultados está dividida em três subseções: na Subseção 5.2.1 será detalhado o perfil dos entrevistados; a Subseção 5.2.2 apresenta o resultado da avaliação da ferramenta (ambos podem ser consultados no Apêndice E); e a Subseção 5.2.3 realiza uma análise dos questionários de avaliação do conhecimento (Apêndice F) respondidos antes e após o experimento.

5.2.1 Perfil dos Participantes

As questões relacionadas ao perfil têm o objetivo de identificar o grau de conhecimento e experiência que os participantes possuem gerenciamento de projetos, modelos de qualidade e gerência de riscos.

Inicialmente foi perguntado aos participantes a respeito do tempo de experiência que possuíam em atividades de gerenciamento de projetos de software. A Figura 5.1 apresenta um gráfico detalhando as respostas, que foram bem distribuídas, sendo um participante com nenhuma experiência, um com menos de 1 ano de experiência, um tendo entre 1 e 2 anos de experiência, dois com experiência entre 2 e 5 anos e um com mais de 5 anos de experiência.

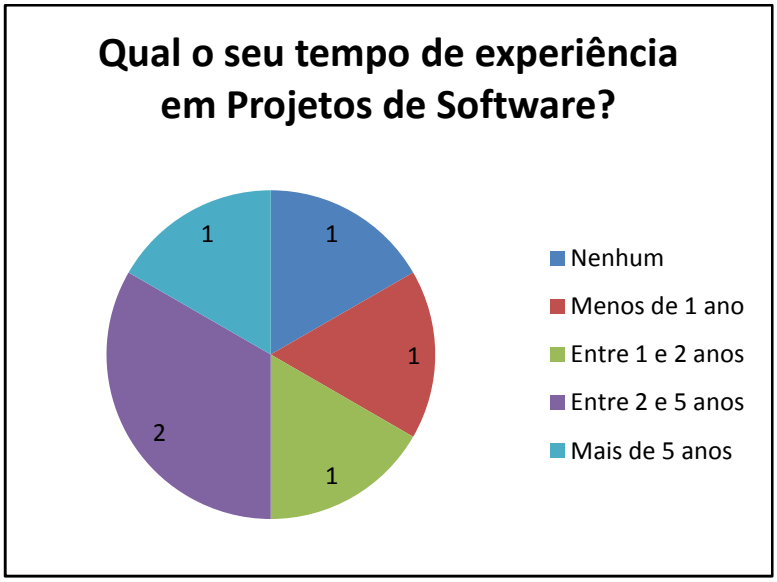

Figura 5.1 Tempo de experiência dos participantes do experimento em projetos de software

Outra questão refere-se ao nível de conhecimento em modelos de qualidade, no qual todos possuíam algum grau de compreensão, sendo dois indivíduos que se consideravam com baixo nível de conhecimento e quatro com conhecimento médio na temática, como pode ser observado na Figura 5.2.

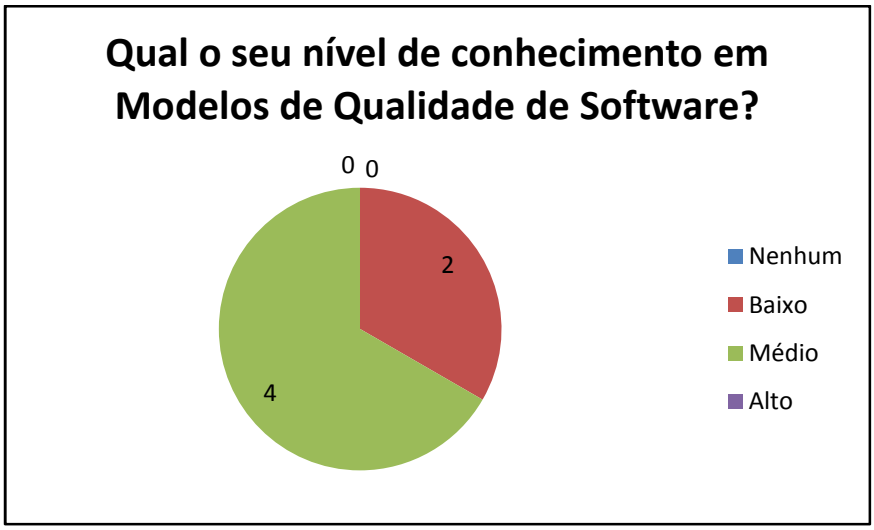

Figura 5.2 Nível de conhecimento em modelos de qualidade de software dos participantes do experimento

Também foi perguntado aos participantes o tempo que tinham de experiência com modelos de qualidade. A Figura 5.3 evidencia que dois participantes não possuíam experiência prática, enquanto que dois tinham entre 1 e 2 anos de experiência e outros dois participantes possuíam entre 2 e 5 anos.

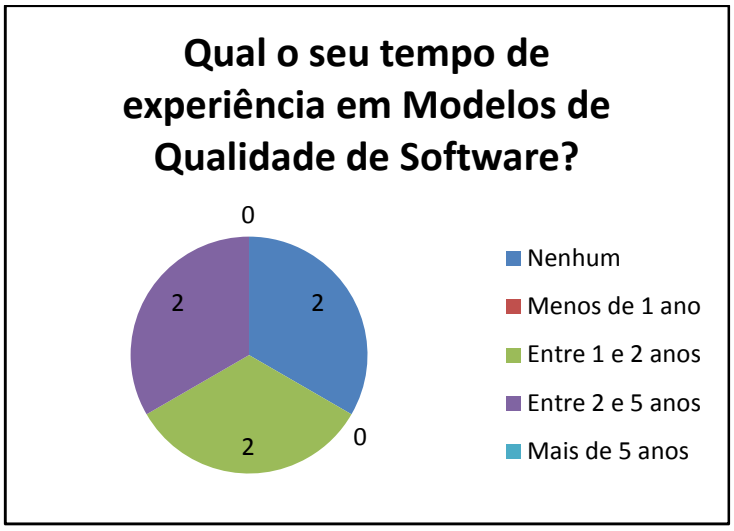

Figura 5.3 Tempo de experiência dos participantes do experimento em modelos de qualidade de software

Com relação à questão que identificava se os participantes possuíam alguma certificação relacionada a modelos de qualidade, como MPS.BR, CMMI entre

outras,houve quatro que afirmaram não possuir, e dois que haviam certificação (vide Figura 5.4), ambos com o curso C1 do programa MPS.BR para software.

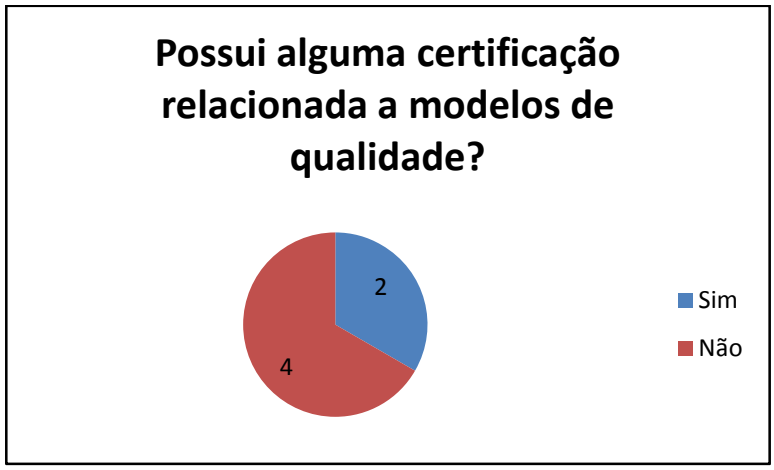

Figura 5.4 Identificação de quantos participantes possuem ou não alguma certificação em modelos de qualidade de software.

No que tange à gerência de riscos, foram realizadas duas perguntas para traçar o perfil dos participantes. A primeira foi relacionada ao nível de conhecimento na área, no qual houve quatro ocorrências no nível baixo e duas ocorrências de nível médio, como pode ser observado na Figura 5.5.

Figura 5.5 Nível de conhecimento em gerência de riscos dos participantes do experimento

Outra pergunta, apresentada graficamente na Figura 5.6, diz respeito ao tempo de experiência com gerenciamento de riscos, no qual houve quatro ocorrências com menos de 1 ano de experiência e duas de participantes com nenhuma experiência.

Figura 5.6 Tempo de experiência dos participantes do experimento em gerência de riscos

Em suma, o perfil dos participantes foi bem distribuído com relação ao conhecimento e à experiência em gerenciamento de projetos e em modelos de qualidade, fornecendo um conjunto relevante para as necessidades do experimento, quanto ao conhecimento e experiência em gerenciamento de riscos, todos indicaram ter pouca ou nenhuma familiaridade com a área, permitindo que seja realizada posterior análise se os envolvidos adquiriram conhecimento com as práticas realizadas.

5.2.2 Avaliação da Ferramenta

Após a realização das atividades do experimento, os participantes foram solicitados a responder o Questionário de Avaliação da Spider-RM, que tem o objetivo de capturar a percepção de cada um em relação às funcionalidades, à usabilidade e ao desempenho da ferramenta, de acordo com os conhecimentos prévios e adquiridos durante o experimento.

Primeiramente foi questionado se os envolvidos achavam relevante a sistematização do processo de gerenciamento de riscos através de uma ferramenta de software. Neste caso, as respostas obtidas foram unânimes em declarar a resposta com relevância importante, como pode ser observado na Figura 5.7.

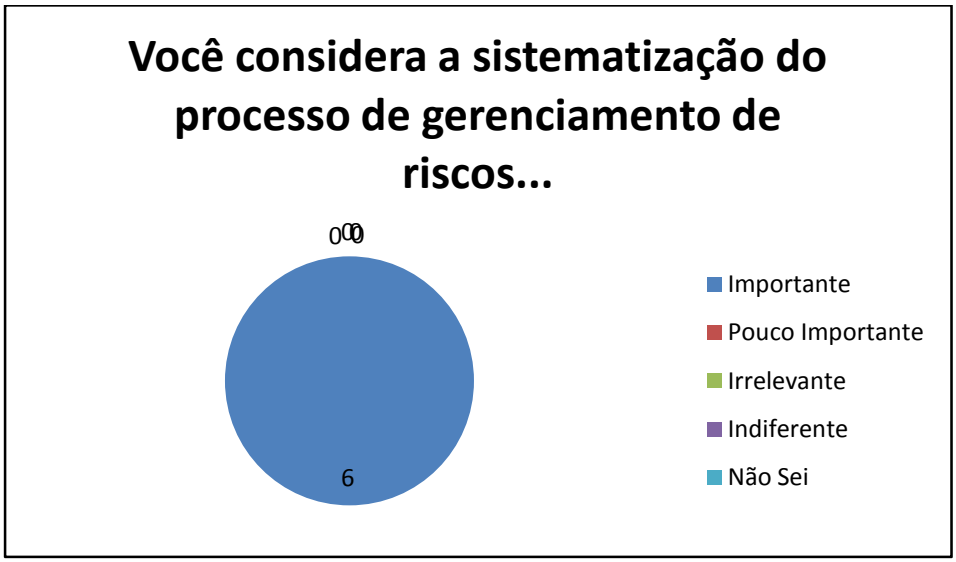

Figura 5.7 Percepção dos participantes com relação à importância da sistematização da gerência de riscos

Com relação às funcionalidades, fica menos provável tomar conclusões definitivas acerca dos resultados obtidos, uma vez que os participantes em suma não possuíam uma vasta experiência com gerenciamento de riscos, porém ainda assim é válido e viável obter as percepções dos mesmos. As questões feitas acerca das funcionalidades relacionam-se às etapas da gerência de riscos e foram divididas em identificação, análise, priorização, mitigação, monitoramento e contingência de riscos.

Quando questionados acerca do suporte que a ferramenta fornece à identificação dos riscos, os participantes responderam que acharam Ótimo (com três respostas) e Bom (também com três respostas), como pode ser observado na Figura 5.8.

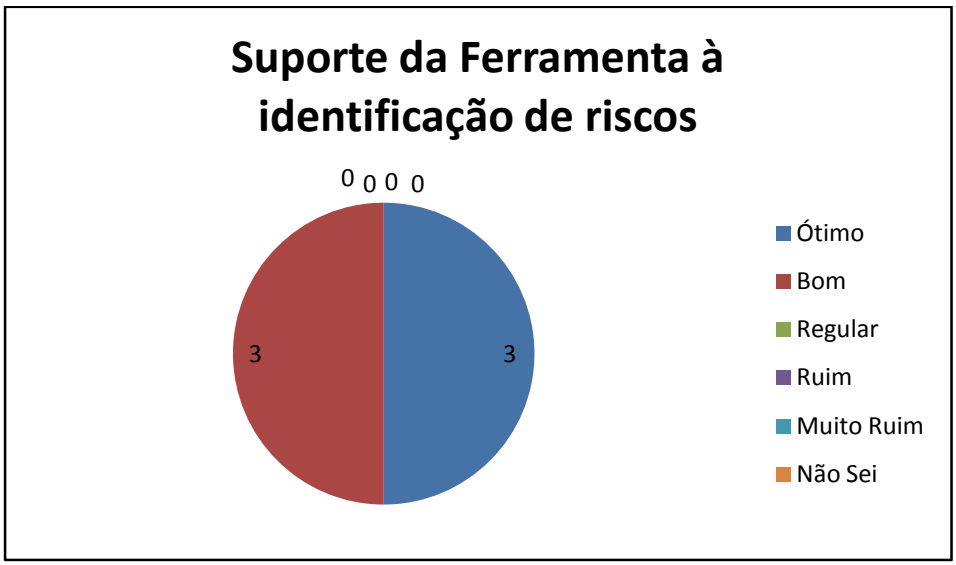

Figura 5.8 Respostas dos participantes quando perguntado se a ferramenta fornece suporte à identificação dos riscos

Na questão que procura identificar o grau de suporte à realização de análise de riscos,dois participantes consideraram Ótimo, enquanto quatro consideraram Bom(vide Figura 5.9).

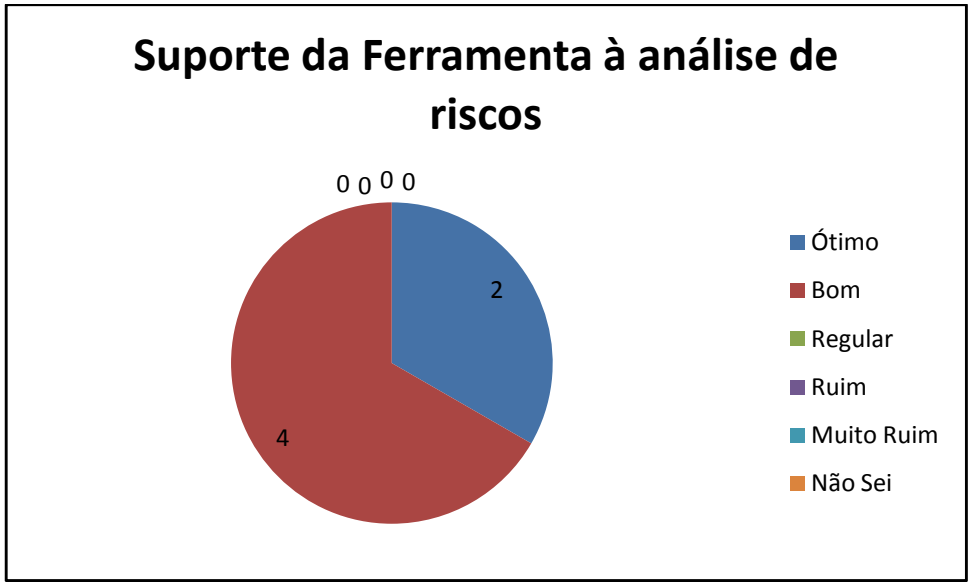

Figura 5.9 Respostas dos participantes quando perguntado se a ferramenta fornece suporte à análise de riscos

Acerca do suporte fornecido à priorização de riscos na ferramenta, os resultados foram mais distribuídos, se comparados aos anteriores. Duas respostas consideraram Ótimo, duas consideraram Bom e outras duas acreditam ser Regular. Estes resultados são apresentados graficamente na Figura 5.10

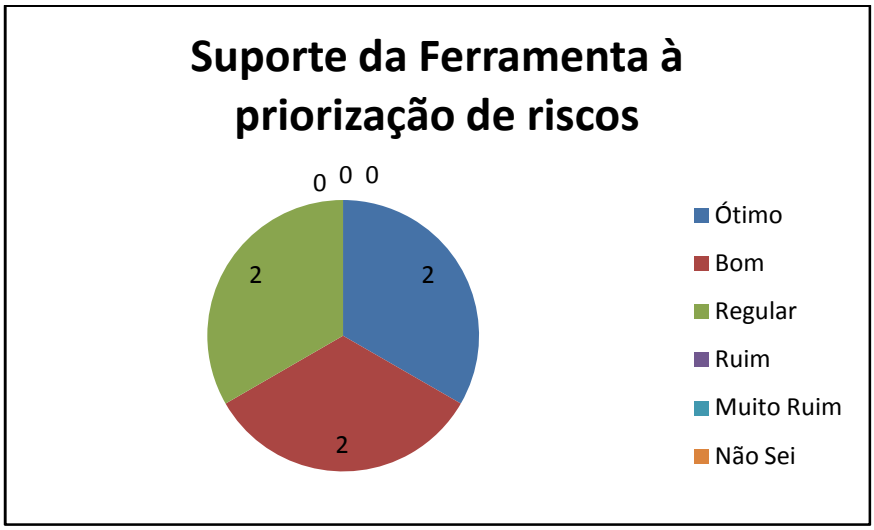

Figura 5.10 Respostas dos participantes quando perguntado se a ferramenta fornece suporte à priorização de riscos

A Figura 5.11 apresenta os resultados da perspectiva dos participantes com relação ao suporte da ferramenta à mitigação dos riscos, que foram cinco respostas conceituando como Bom e uma resposta considerando Regular.

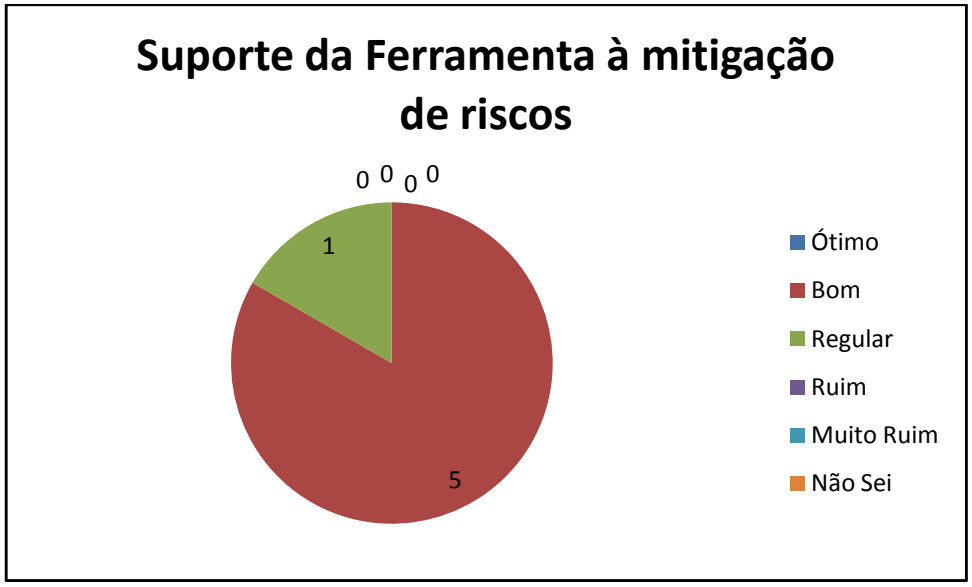

Figura 5.11 Respostas dos participantes quando perguntado se a ferramenta fornece suporte à mitigação de riscos

No que diz respeito ao suporte da ferramenta ao monitoramento de riscos, a Figura 5.12 apresenta o gráfico com as respostas, que foi uma ocorrência definida com grau Ótimo e cinco ocorrências para a resposta Bom.

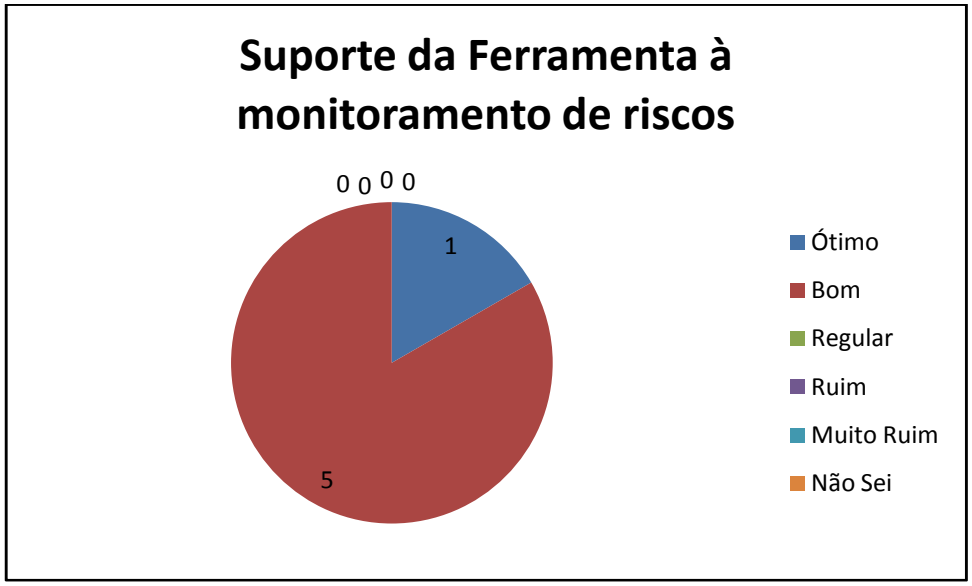

Figura 5.12 Respostas dos participantes quando perguntado se a ferramenta fornece suporte ao monitoramento de riscos

Para avaliar o grau de suporte da ferramenta à contingência de riscos, os participantes foram unânimes em considerar que há um Bom suporte da Spider-RM para esta etapa, observado na Figura 5.13.

Figura 5.13 Respostas dos participantes quando perguntado se a ferramenta fornece suporte à contingência dos riscos

Outro questionamento realizado neste formulário está relacionado à usabilidade da ferramenta, que visa identificar se a Spider-RM possui funcionalidades intuitivas e que não necessitam de muito esforço por parte do usuário. Para esta pergunta, cinco indivíduos consideraram a ferramenta com usabilidade Boa e uma considerou-a Regular (vide Figura 5.14).

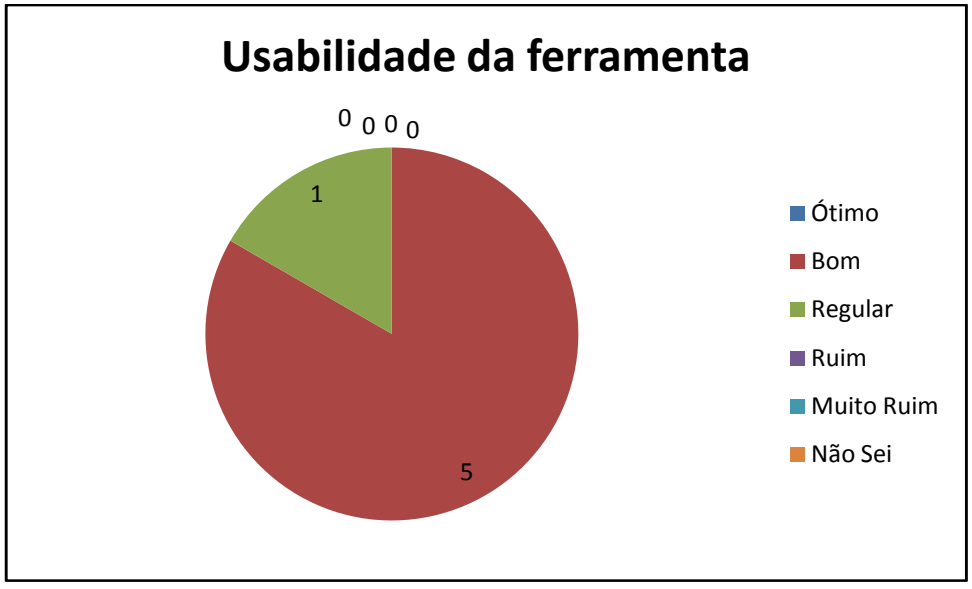

Figura 5.14 Respostas dos participantes quando perguntado se a ferramenta possui usabilidade adequada

Também foi questionado se os participantes consideravam a ferramenta Spider-RM adequada para auxiliar as atividades de gerenciamento de riscos em uma organização, de acordo com o aprendizado no experimento e de acordo com a experiência profissional prévia de cada. A Figura 5.15 apresenta as respostas obtidas, que foram cinco ocorrências considerando que sim, a ferramenta auxiliaria as organizações, e uma afirmando que não saberia responder.

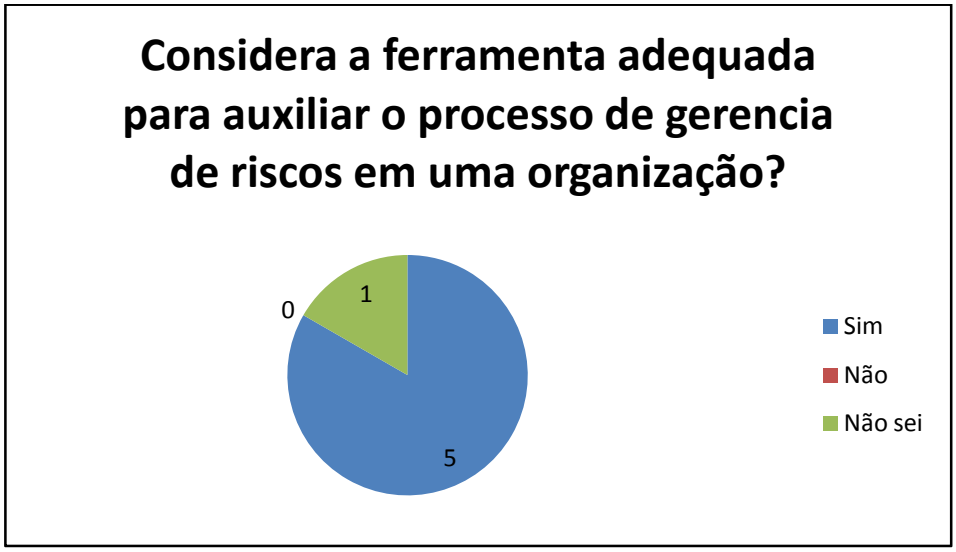

Figura 5.15 Respostas dos participantes quando perguntado se consideram a ferramenta adequada ao uso em uma organização

Com relação à percepção dos participantes ao desempenho da ferramenta, ou seja, se as tarefas executadas na Spider-RM possuem um tempo de resposta aceitável, foram coletadas quatro respostas considerando que a ferramenta possui um alto desempenho e duas respostas considerando moderado (vide Figura 5.16).

Figura 5.16 Percepção dos participantes com relação ao desempenho da ferramenta na execução de tarefas

Finalmente, foi solicitado aos participantes do experimento que analisassem se a ferramenta encontra-se aderente aos resultados esperados do processo de gerência de riscos do modelo MR-MPS-SW. Logicamente não é possível obter resultados conclusivos com este questionamento ao perfil dos participantes, porém pode indicar uma orientação, uma vez que entre os envolvidos há pessoas com grande tempo de experiência em gerenciamento de projetos e com conhecimento certificado no modelo de qualidade MR-MPS-SW. A Figura 5.17 apresenta graficamente as respostas, que foram cinco ocorrências considerando completamente aderente e uma considerando parcialmente.

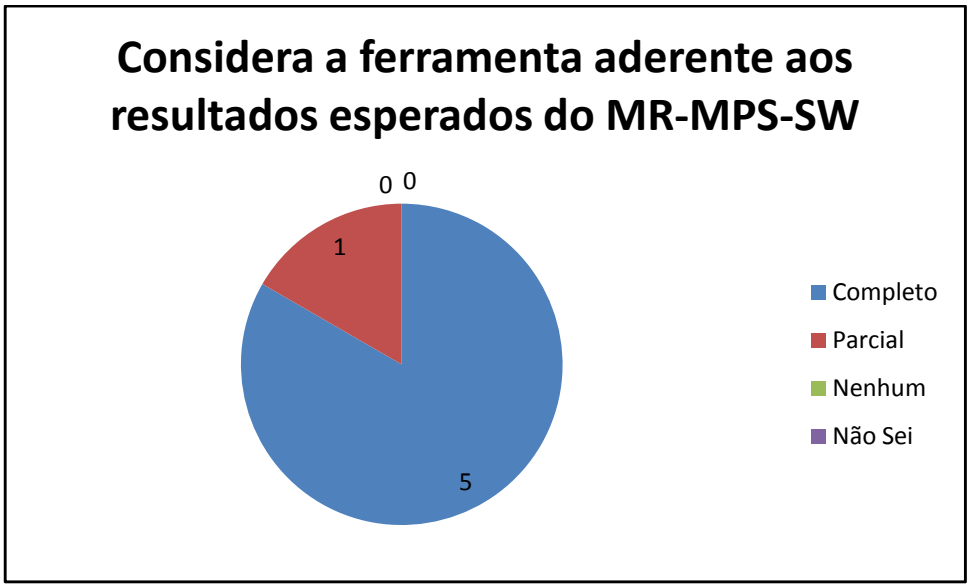

Figura 5.17 Percepção dos participantes com relação à aderência da ferramenta ao modelo MR-MPS-SW

O último campo do questionário de avaliação solicitava aos participantes que fornecessem suas opiniões e críticas que achavam relevantes, através da identificação de pontos fortes, pontos fracos e oportunidades de melhoria. Algumas sugestões foram observadas com a análise desse campo:

- Tentar fazer com que as informações fiquem visíveis a todos na organização. Considerando que a ferramenta é monousuário, poderia ser gerado um relatório que possa ser visualizado ou compartilhado em qualquer máquina;
- Alertas mais dinâmicos informando aos usuários quando há monitoramento ou execução de planos pendentes;

- Alguns ajustes relacionados à usabilidade, como melhorar o *feedback* do usuário em algumas telas ou apresentar dicas quando o usuário colocar o mouse em um campo a ser preenchido.

A avaliação realizada na ferramenta foi bastante relevante, pois permitiu analisar a percepção de possíveis usuários fazendo com que seja possível direcionar os futuros ajustes necessários. Também foi possível identificar quais funcionalidades foram consideradas menos alinhadas aos propósitos do gerenciamento de riscos, possibilitando priorizar futuros esforços onde necessita-se de maior atenção.

5.2.3 Análise do Apoio à Aprendizagem

Para avaliar se a metodologia sugerida e a ferramenta Spider-RM podem apoiar o processo de aprendizagem em gerenciamento de riscos, foram submetidos aos participantes dois questionários de avaliação subjetiva do conhecimento (ambos encontram-se definidos no Apêndice F).

Inicialmente, como forma de avaliar o conhecimento prévio dos indivíduos foi submetido o formulário,denominado pré-avaliação, antes de quaisquer outras atividades planejadas no experimento. O segundo formulário, denominado pós-avaliação, foi preenchido pelos participantes após a realização das atividades planejadas para o experimento.

O tempo de duração para o preenchimento de ambos os formulários foi o mesmo (uma hora de duração) e teve o intuito de complementar a avaliação, identificando se é possível utilizar os recursos deste trabalho na contribuição para a aprendizagem dos alunos em gerenciamento de riscos, tendo seu uso combinado às aulas tradicionais.

A análise das respostas comparadas identificou uma evolução nas notas obtidas após a correção dos questionários. A média inicial era de 4,5 pontos em uma escala de 1 a 10, enquanto que a média obtida pelos participantes na pós-avaliação foi de 6 pontos. Além disso foi observado que, após as práticas, as respostas foram menos prolixas e houve maior ocorrência de termos técnicos relacionados à área.

Logo, a partir das conclusões obtidas com a análise, é possível utilizar a estratégia aqui adotada como forma de familiarização ao gerenciamento de riscos para alunos ou colaboradores de um organização, desde que tenham conhecimento prévio de gerenciamento de projetos, modelos de qualidade e/ou possuam algum conhecimento básico em gerência de riscos.

5.3 Considerações Finais

A análise qualitativa abordada neste capítulo pretendeu identificar pontos fortes e possíveis pontos de melhoria na ferramenta e na metodologia aqui apresentados, através de um experimento controlado, utilizando um cenário fictício com alunos de pós-graduação. É importante salientar que a metodologia utilizada para executar o experimento possui algumas limitações, tendo em vista que o conjunto de participantes foi composto por alunos fora de um ambiente real.

A abordagem utilizada permitiu identificar quais funcionalidades críticas da ferramenta necessitam de maior priorização para futuros ajustes, e qual a percepção de possíveis usuários finais ao utilizarem-na em um determinado cenário.

Também a partir da avaliação do conhecimento dos participantes do experimento foi possível identificar que as práticas na ferramenta, associadas ao uso da metodologia, pode beneficiar a aprendizagem de indivíduos com pouco conhecimento sobre o gerenciamento de riscos.

6 CONCLUSÕES

Neste capítulo é abordada uma sumarização do trabalho apresentado através das principais conclusões, também são apresentadas as principais contribuições à área de gerência de riscos em projetos de software, algumas limitações identificadas, assim como trabalhos futuros a serem executados a partir do estudo realizado.

6.1 Considerações Finais

É certo que é pouco provável que se esgote um assunto tão complexo e delicado quanto a gerência de riscos no contexto da engenharia de software, por isso em nenhum momento houve esse pretensão durante o desenvolvimento desta dissertação, que almejou fornecer algumas contribuições à área e incentivar futuras discussões.

O objetivo maior do trabalho foi promover a otimização do tempo de implementação e aprendizagem do processo de gerência de riscos nas organizações, através da qualidade do produto baseada na qualidade do processo.

Sua execução teve como foco inicial a coleta de boas práticas e técnicas utilizadas para gerenciar riscos recomendadas pelos modelos MR-MPS -SW e CMMI-DEV, pela norma ISO/IEC 12207, pelo guia PMBOK e pelo padrão internacional ISO/IEC 16085. Essas boas práticas foram identificadas a partir de um mapeamento entre os documentos de qualidade envolvidos e focou em apontar os objetivos semelhantes e as técnicas para implementação equivalentes.

Apenas as boas práticas e o mapeamento entre os modelos, normas e guias já são uma contribuição valiosa para as organizações que pretendem melhorar seu processo de software, porém além disso, este trabalho baseou-se nestas práticas listadas para desenvolver uma metodologia de implantação da gerência de riscos, sugerindo fases, tarefas, papéis, artefatos e procedimentos, permitindo que as organizações possam adaptá-lo a sua realidade.

As metodologia sugerida pode ser considerada aderente às exigências dos modelos e normas pois se baseou no mapeamento entre os mesmos e foi avaliada por um especialista da área de gerência de riscos e certificado em melhoria de processo de software, com experiência em implementação e avaliação de processos.

A partir da revisão realizada pelo especialista, foi desenvolvida uma ferramenta de software, denominada Spider-RM, com o intuito de apoiar a metodologia sugerida e reduzir mais ainda possíveis entraves de custos e tempo para a implementação do processo de gerenciamento de riscos. Para avaliar o funcionamento da ferramenta e determinar se seria possível utilizá-la também como um apoio ao processo de aprendizagem da área, foi realizado um experimento com alunos de pós-graduação, que através de suas percepções foram realizadas análises, que comprovaram a adequação ao contexto proposto e ao apoio no processo de aprendizagem. Este momento foi a culminância do trabalho desenvolvido, com a aceitação positiva da ferramenta desenvolvida.

6.2 Contribuições

A seguir são apresentadas algumas contribuições obtidas durante o desenvolvimento deste trabalho:

- **Mapeamento e Boas Práticas**: o mapeamento realizado entre o MR-MPS-SW, o CMMI-DEV, a ISO/IEC 12207, o PMBOK e a ISO/IEC 16085 foi importante pois concede uma análise dos pontos relacionados entre modelos, normas e guias. A consolidação do mapeamento é apresentada na forma de uma lista de boas práticas, que identifica práticas semelhantes e distintas entre os modelos de qualidade envolvidos. Esta abordagem auxilia organizações que procuram implementações conjuntas de modelos ou utilizam as recomendações nos guias de qualidade;
- **Metodologia para gerência de riscos:** foi importante pois levou em consideração as boas práticas documentadas, que são consideradas referências no gerenciamento de riscos em projetos de software, tornando-a uma metodologia mais fácil de ser aceita, na medida que se baseia em referências aceitas pela comunidade. Além disso, esta aceitação é embasada pela avaliação realizada por especialista na área;

- **Ferramenta Spider-RM:** tem a importância de apoiar o processo de gerenciamento de riscos em projetos de software, pois sistematiza grande parte das tarefas da metodologia sugerida. Pode servir de apoio às organizações interessadas na aplicação da maturidade no desenvolvimento de produtos de software, centralizando informações a respeito dos riscos em apenas um lugar, facilitando a evolução do processo e por ser aderente às principais referências em qualidade de software;
- **Iniciação Científica**: o desenvolvimento da ferramenta contou com a colaboração de alunos de Iniciação Científica, que resultou na elaboração de relatórios científicos;
- **Experimento:** foi importante pois auxiliou na avaliação da ferramenta por possíveis usuários, obtendo através dos resultados fornecidos pelos participantes, um grau de adequação considerável ao contexto proposto. Também através do experimento realizado foi possível demonstrar que a ferramenta pode ser utilizada para apoiar o aprendizado do processo de gerência de riscos e consequentemente de processo de software;
- **Produção de trabalhos científicos:** houve a publicação de um artigo apresentando os objetivos e a metodologia de pesquisa deste trabalho (Mendes e Oliveira, 2014) no Workshop de Teses e Dissertações em Qualidade de Software (WTDQS), do Simpósio Brasileiro de Qualidade de Software (SBQS). Também foi publicado um segundo artigo, que trata da ferramenta Spider-RM (Mendes *et al.* 2014) na Sessão de Ferramentas do Congresso Brasileiro de Software: Teoria e Prática (CBSOFT). Há ainda um terceiro artigo tratando do mapeamento entre os modelos de qualidade, da lista de boas práticas e de uma visão geral sobre a metodologia, que foi aceito para publicação em 2015 no periódico Abakós mantido pela PUC-Minas.

6.3 Limitações

Uma das principais limitações deste trabalho é o fato da metodologia sugerida ter sido avaliada apenas por um especialista com conhecimentos tanto em melhoria de

processo software, quanto em gerenciamento de riscos. Isto ocorre devido a dificuldade de conseguir avaliadores experientes credenciados pela SOFTEX ou SEI com disponibilidade para auxiliar na pesquisa. Caso o número de avaliadores fosse maior, poderiam ser obtidas conclusões que permitiriam um maior aprimoramento do trabalho,reduzindo mais vieses existentes.

Outra limitação deu-se em razão da falta de tempo hábil para realização da avaliação qualitativa, que poderia ser realizada em uma organização, através de um estudo comparativo, no qual seriam coletadas informações de projetos atuais, em seguida seria implantada a metodologia sugerida com auxílio da ferramenta em um novo projeto, para após conclusão coletar novos dados e realizar comparações. Assim, a ferramenta e a metodologia poderiam ser avaliadas em um ambiente real.

Ainda com relação à avaliação qualitativa, há outra limitação com relação aos avaliadores, que foi um quantitativo limitado. Também, apesar de possuírem experiência com gerenciamento de projetos, estes avaliadores não possuíam conhecimentos comprovados em gerência de riscos para realizarem uma análise mais sucinta a respeito das funcionalidades da ferramenta. Logo, caso o tempo necessário para a conclusão do trabalho fosse maior, seria possível aplicar o experimento entre mais participantes, e que possuam experiência prática com a gerência de riscos.

6.4 Trabalhos Futuros

Espera-se que esta dissertação oriente novos trabalhos a respeito do mesmo tema. Assim, esta seção identifica sugestões de prosseguimentos do trabalho aqui apresentado, indicando possíveis evoluções que podem torná-lo mais completo e adequado para o gerenciamento de riscos.

6.4.1 Integração da metodologia com outras áreas de processos

Um projeto de software utiliza-se de abordagens em várias áreas de conhecimento, logo seria importante que a metodologia identificasse relacionamentos de suas tarefas com as tarefas destas outras áreas, como Gerência de Projetos, Gerência de Requisitos, Garantia da Qualidade, entre outros. A partir desta integração as tarefas

da metodologia poderiam apresentar uma maior completude, reduzindo a complexidade da sua implementação na prática.

6.4.2 Aprimoramento da metodologia para cenários específicos

A abordagem adotada neste trabalho para definir a metodologia de gerenciamento de riscos procurou abranger o maior número possível de organizações que queiram implementar, independente do porte ou do tipo de projeto, porém seria interessante evoluir a metodologia para sua aplicação em determinados cenários com características específicas, como em uma organização com um processo ágil, em equipes de projetos que trabalham com desenvolvimento distribuído de software, por exemplo.

6.4.3 Aprimoramento da ferramenta Spider-RM

A ferramenta poderia ser aprimorada para suportar múltiplos usuários, permitindo dar suporte ao gerenciamento da comunicação, importante para tomada de decisões que envolvem o gerenciamento de riscos. Além disso, pode ser interessante a integração da ferramenta com softwares que são responsáveis por outros processos especificados nos modelos de qualidade.

6.4.4 Estudo de caso em cenário real

Para avaliar o comportamento da metodologia sugerida neste trabalho e da ferramenta de apoio, seria interessante a realização de um estudo de caso contextualizado em um cenário real de uma organização. Desta forma, sua implementação seria acompanhada, sendo possível a identificação de resultados mais pontuais através da análise dos resultados alcançados, e posteriormente um novo aprimoramento da metodologia com as mudanças sugeridas.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT – Associação Brasileira de Normas e Técnicas. **NBR ISO/IEC 15504-1:2008 - Tecnologia da Informação - Avaliação de processo Parte 1: Conceitos e Vocabulário.** Rio de Janeiro. 2008.

ABNT – Associação Brasileira de Normas e Técnicas. **NBR ISO/IEC 12207:2009 – Engenharia de Sistemas de Software – Processos de Ciclo de Vida de Software**. Rio de Janeiro, Brasil, 2009a.

ABNT - Associação Brasileira de Normas e Técnicas. **NBR ISO 31000:2009 - Gestão de Riscos - Princípios e Diretrizes**. Rio de Janeiro. 2009b.

AHERN, D. M., CLOUSE, A. et al. **CMMI distilled**. Addison-Wesley. 2001.

ALHO, F. M. **Uma Abordagem de Sistematização do Processo de Gerência de Reutilização de Ativos de Software Aderente a Modelos e Normas de Qualidade**. 2012, 199 f. Dissertação (Mestrado em Ciência da Computação), Universidade Federal do Pará - UFPA. Belém, Brasil.

AVDOSHIN, S. M.; PESOTSKAYA, E. Y. **Software risk management**. 7th Central and Eastern European Software Engineering Conference (CEE-SECR), 2011.

AVISON, D. E.; SHAH, H. U.; WILSON, D. N. **Software quality standards in practice: the limitations of using ISO-9001 to support software development.** Software Quality Journal. v. 3. p.105-111. 1994

BARROS, R.; OLIVEIRA, S. **Spider-PM: Uma Ferramenta de Apoio à Modelagem de Processos de Software**. In: Anais do VIII Encontro Anual de Computação, 2010.

BOEHM, B. W. **Software risk management: principles and practices**. Software, IEEE. v.8, i. 1, p. 32-41, 1991.

BRITO NETO, O. **Uma Abordagem Metodológica para Implementação Multi-Modelos de Teste de Software Adotando o MPT.Br e o TMMi**, 2014, 156 f. Dissertação (Mestrado em Ciência da Computação), Universidade Federal do Pará - UFPA, Belém, Brasil.

BROOKS, Fred P. **No Silver Bullet — Essence and Accident in Software Engineering**. In: IFIP Tenth World Computing Conference, 1986, p. 1069–1076

CHAPMAN C.B.; WARD, S.C. **Project Risk Management, Processes, Techniques and Insights**, 2ª Edição. John Wiley. Chichester. Reino Unido. 2003.

CHARETTE, R. N. **Software Engineering Risk Analysis and Management**. McGraw-Hill, 1989.

CONRADI, R. **Software Process Improvement: Why We Need SPIQ**, Norwegian University of Science and Technology (NTNU). 1996.

FALBO, R. A.. **Integração de Conhecimento em um Ambiente de Desenvolvimento de Software**. 1998, 225 f. Tese (Doutorado em Ciências em Engenharia de Sistemas e Computação), COPPE/UFRJ, Rio de Janeiro.

FIORINI, S. T., VON STAA, A., BAPTISTA, R. M. **Engenharia de Software com CMM**, Brasport, 1998.

FUGGETA, A.. **Software process: a roadmap**. In Proceedings of the Conference on the Future of Software Engineering. ICSE '00. ACM, New York, NY, 25-34, 2000.

GAMMA, Erich et al. **Padrões de Projeto:** Soluções Reutilizáveis de Software Orientado a Objetos. Porto Alegre: Bookman, 2000.

GLASS, R. L. **Software Runaways: Monumental Software Disasters**, Prentice-Hall, 1998

GNU Project. **General Public License – GPL, Version 3.** Free Software Foundation , 2007. Disponível em: <http://www.gnu.org/licenses/gpl.html>. Acesso em Janeiro de 2015.

GONÇALVES, E. L. B. A. **Gerenciamento de risco de software: um modelo de processo e uma ferramenta**, 2006, 154 f. Dissertação (Mestrado em Ciência da Computação), Universidade Metodista de Piracicaba - UNIMEP, Piracicaba.

HUMPHREY, W., S. **Managing the Software Process, The SEI Series in Software Engineering**. Addison-Wesley, 1989.

IEEE - Institute of Electrical and Electronics Engineers. **ISO/IEC 16085 - IEEE Std 16085-2006 - Systems and software engineering - Life cycle processes - Risk management**. USA, 2006.

ISLAM, S. **Software development risk management model-a-goal-driven approach**, 2011, 195 f. Tese (Doutorado em Ciência da Computação), Institute für Informatik, Technische Universität München, Munique.

ISO/IEC – INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMISSION. **ISO/IEC 15504-1:** Information Technology - Process Assessment - Part 1: Concepts and Vocabulary, Geneva: 2004.

KOSCIANSKI, André; SOARES, Michel dos S. **Qualidade de Software. 2. ed**. São Paulo, Novatec, 2007.

MELLO, M.; A. R. C.; G. S. **Metodologia para Definição de Instrumentos de Apoio a Iniciativas de Melhoria de Processos de Software Multi-Modelos Baseadas nos Modelos MR-MPS e CMMI-DEV**. Simpósio Brasileiro de Qualidade de Software. 2012

MENDES, H. J. P. S.; OLIVEIRA, S. R. B. **Uma Proposta de Metodologia para Gerenciamento de Riscos em Projetos de Software aderente a Modelos e Normas de Qualidade de Processo de Software.** Simpósio Brasileiro de Qualidade de Software - SBQS. 2014

MENDES, H. J. P. S. *et al.* **Spider-RM: Uma ferramenta para Auxílio ao Gerenciamento de Riscos em Projetos de Software.** CBSOFT - Congresso Brasileiro de Software: Teoria e Prática. 2014.

MUTAFELIJA, Boris; STROMBERG, Harvey. **Process Improvement with CMMI v1.2 and ISO Standarts**.CRC Press, 2009.

OLIVEIRA, S. R. B. et al. **SPIDER – Uma Proposta de Solução Sistêmica de um SUITE de Ferramentas de Software Livre de Apoio à Implementação do Modelo MPS.BR.** Revista do Programa Brasileiro da Qualidade e Produtividade em Software. PBQP Software, SEPIN/MCT, 2011.

PAULK, M.C. **Surviving the Quagmire of Process Models, Integrated Models, and Standards**. Proceedings of the Annual Quality Congress. 2004.

PAVAN, C.; STUMPF, I. R. C. **Revistas Brasileiras de Ciência da Informação: procedimentos de avaliação pelos pares**. VIII ENANCIB – Encontro Nacional de Pesquisa em Ciência da Computação, 2007.

PEREIRA, P. C. R. **Um processo de gerenciamento de riscos para projetos de software**, 2005, 235 f. Dissertação (Mestrado em Informática Aplicada), Universidade de Fortaleza - UNIFOR, Fortaleza.

PMI. **Um Guia do Conhecimento em Gerenciamento de Projetos,** Quinta Edição, Editora Saraiva, São Paulo, 2014.

PRESSMAN, R. S. **Engenharia de Software: Uma Abordagem Profissional.** Mcgraw Hill. 2011.

RAZ, Tzvi; HILLSON, David. **A comparative review of risk management standarts**. Risk Management: An International Journal, v.7, n.4, p. 53-66, 2005.

ROPPONEN, J.; LYYTINEN, K. **Components of Software Development Risk: How to Address Them?** IEEE Transactions on Software Engineering, v. 26, p.98-111. 2000.

ROUILLER, A. C. et al. **Metodologia e Análise das Implantações MPS.BR realizadas pela SWQuality**, Revista ProQualiti – Qualidade na Produção de Software, vol. 2, n. 2, Recife, Brasil, 2006.

ROUT, Terence P.; TUFFLEY, Angela. **Harmonizing ISO/IEC 15504 and CMMI**. Software Process Improvement and Practice, 12, p. 361-371, 2007.

SEI - Software Engineering Institute. **Capability Maturity Model Integration (CMMI) for Development, Version 1.3**.Carnegie Mellon, USA, 2010.

SILVA, E. L. e MENEZES, E. M. **Metodologia da Pesquisa e Elaboração da Dissertação**. 3. ed. rev. Atual – Laboratório de Ensino a Distância da UFSC. Florianópolis, Brasil, 2001.

SOFTEX, **Melhoria do Processo de Software Brasileiro (MPS.BR) - Guia Geral 2012**, Brasil. 2012a.

SOFTEX, **Melhoria do Processo de Software Brasileiro (MPS.BR) - Guia de Implementação - Parte 11: Implementação e Avaliação do MR-MPS-SW em conjunto com o CMMI-DEV v1.3**. Brasil. 2012b.

SOFTEX, **Melhoria do Processo de Software Brasileiro (MPS.BR) - Guia de Implementação - Parte 5: Fundamentação para Implementação do Nível C do MR-MPS-SW:2012**. Brasil. 2013.

SOFTEX, **Avaliações MPS-SW (Software) Publicadas (prazo de validade: 3 anos)**. 2015. Disponível em < http://www.softex.br/wp-content/uploads/2013/07/2Avaliacoes-MPSSW-Publicadas_19.JAN_.2015_6122.pdf>. Acesso janeiro de 2015.

SOMMERVILLE, Ian. **Engenharia de Software. 8 ed**. São Paulo. Pearson Addison-Wesley. 2007.

SPINOLA, M. M., TONINI, A.C.; CARVALHO, M.M. **Contribuição dos modelos de qualidade e maturidade na melhoria dos processos de software**. EPUSP. Revista Produção, 2008.

TELES, M. P. **Spider-QA: Apoio à Implementação do Processo de Garantia de Qualidade no Contexto de Modelos e Normas de Qualidade**. 2011, 166 f. Dissertação (Mestrado em Ciência da Computação), Universidade Federal do Pará - UFPA, Belém, Brasil, 2011.

TIANYIN, P. **Development of software project risk management model review**. 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC). 2011.

TOMHAVE, Benjamin. L. **Alphabet Soup: Making Sense of Models, Frameworks, and Methodologies**. 2005. Disponível em < http://www.secureconsulting.net/Papers/Alphabet_Soup.pdf>. Acesso em 15 de janeiro de 2015.

TRAVASSOS, G. H. **O Modelo de Integração de Ferramentas da Estação TABA.** 1994, 243 f. Tese (Doutorado em Ciências em Engenharia de Sistemas e Computação), COPPE/UFRJ, Rio de Janeiro, Brasil.

TRAVASSOS, G. H. et al. **Introdução à Engenharia de Software Experimental**, Relatório Técnico RT-ES-590/02 do Programa de Engenharia de Sistemas e Computação, COPPE/UFRJ, Rio de Janeiro, Brasil, 2002.

VAN LAMSWEERDE, A. **Requirements Engineering: From System Goals to UML Models to Software Specifications**, Wiley, 2009.

VON WANGENHEIM, C. G.; DA SILVA, D. A.; BUGLIONE, L.; SCHEIDT, R.; PRIKLADNICKI, R. **Best practice fusion of CMMI-DEV v1.2 (PP, PMC, SAM) and PMBOK 2008**. Information and Software Technology, 52, p. 749-757, 2010

WILLIANS, R.; PANDELLOS, G. J.; BEHRENS, S. G. **Software Risk Evaluation SER Method Description**. Pittsburgh, 1999. Technical Report, version 2.0. CMU/SEI - 99- TR-029.

APÊNDICE A – DETALHAMENTO DAS TAREFAS DA METODOLOGIA

Este documento contém a especificação das atividades definidas para a metodologia de implantação do gerenciamento de riscos em projetos de software (com base nos modelos MR-MPS-SW, CMMI, na norma ISO/IEC 12207, no guia PMBOK e no padrão ISO/IEC 16085) , a indicação dos responsáveis envolvidos, e a análise de aderência às boas práticas apresentadas no Capítulo 3.

A metodologia é composta por um conjunto de tarefas, agrupadas em fases. Cada fase possui um objetivo que contribui para a definição, execução e melhoria de um processo de gerência de riscos. As tarefas são compostas por: objetivo que norteará sua execução, a sua correlação com as boas práticas e com os modelos de qualidade, sugestões de entradas e resultados, sugestões de passos a serem executados, técnicas de implementação recomendadas pelo PMBOK e ISO/IEC 16085 e sugestões de papéis envolvidos nesta tarefa.

A primeira fase, Planejamento, tem o objetivo de preparar a organização para executar adequadamente o gerenciamento de riscos durante um projeto, através da definição de padrões e técnicas a serem adotados. As tarefas desta fase estão relacionadas ao escopo organizacional.

A fase seguinte, Execução, é responsável pela implementação de tarefas diretamente relacionadas ao gerenciamento de riscos, ou seja, seu escopo engloba o ciclo de vida de um projeto, da concepção à conclusão. Esta fase tem o objetivo de identificar, analisar, priorizar, monitorar e mitigar riscos de um determinado projeto.

A última fase, Avaliação, tem o objetivo de analisar e avaliar o processo executado nas fases anteriores. Seu intuito é identificar pontos de melhoria e classificar informações obtidas, como sucessos ao realizar a mitigação e novas categorias de riscos, para orientar futuros projetos.

1) Fase Planejamento

A fase de Planejamento é composta pelas tarefas: "Determinar Escopo da Gerência de Riscos", "Definir Categorias de Riscos" e "Definir Modelo de Plano de Gerenciamento de Riscos" executadas de forma sequencial, respectivamente.

a. Determinar Escopo da Gerência de Riscos

Objetivo	
Determinar diretrizes para o gerenciamento de riscos tanto em um âmbito organizacional, quanto no escopo dos projetos especificando abrangência, modelos de artefatos, técnicas e papéis recomendados.	
Sobre o Item	
Boas Práticas	BP01 - Definir escopo da gerência de riscos BP04 - Definir parâmetros para análise de riscos
Entradas e Resultados Sugeridos	
Entradas	Ativos de Processos organizacionais (Escopo, Custo, Cronograma)
Resultados	Política Organizacional de Gerência de Riscos
Recomendações Segundo os Padrões	
[PMBOK] Não se aplica	
[ISO/IEC 16085] Descreve acerca da definição e documentação do contexto do gerenciamento de riscos, no qual deve conter uma descrição técnica e gerencial dos objetivos, suposições e restrições, entre outras informações relevantes que surgirem. Além disso, devem ser estabelecidas políticas de gestão de riscos, que devem descrever: • como a gerência de riscos deve ser implementada, administrada e apoiada pela gerência e funcionários; • como deve ser obtido e mantido o compromisso contínuo das partes interessadas; • como o processo de gerenciamento de riscos deve ser coordenado; como orientações e treinamentos a respeito de gerenciamento de riscos devem ser conduzidos; • como informações sobre riscos são comunicadas e realizadas pelas partes interessadas.	
Papéis	
Alta Administração | Gerentes de Riscos | Gerentes de Projetos	
Observações sobre o uso do item da Metodologia	
Uma vez definida a política organizacional, esta tarefa torna-se facultativa, visto que a fase de avaliação possui uma tarefa responsável pela revisão do processo.	

b. Definir Categorias de Riscos

Objetivo	
Organizar riscos que serão identificados através de agrupamentos com características semelhantes, de forma a favorecer a posterior análise.	
Sobre o Item	
Boas Práticas	BP03 - Definir categorias de riscos | BP06 - Identificar e documentar riscos
Entradas e Resultados Sugeridos	
Entradas	Ativos de Processos Organizacionais (registro de riscos em projetos anteriores)
Resultados	Estrutura analítica de riscos (EAR)
Recomendações Segundo os Padrões	
[PMBOK] sugere a realização de reuniões para a definição de uma Estrutura Analítica de Riscos, de forma a garantir uma estrutura abrangente, que auxilia na identificação sistemática de riscos em um nível de detalhe consistente contribuindo para eficácia e qualidade durante a identificação de riscos. A EAR é uma representação de riscos organizada hierarquicamente, ordenada por categoria e subcategoria de riscos, identificando as diversas áreas e causas de riscos.	
[ISO/IEC 16085] Determina que deve ser definido limites de riscos, definindo um nível ao qual o risco será aceito. Pode ser definido por valores máximos que um risco poderá aceitar em impactos no custo, cronograma, outras consequências relevantes ou pelo fator de exposição (cálculo relacionando impacto com probabilidade). Além disso, um perfil de risco deve ser mantido contendo o contexto de ocorrência do risco, uma categorização, probabilidade, consequência e o limite definido. As informações de um perfil de risco podem ser agrupadas por categorias, apresentando além das informações descritas anteriormente, possíveis origens e critérios para determinação de probabilidade e impacto. Os limites de risco são importantes, pois durante a análise e monitoramento, caso algum risco ultrapasse o limite aceitável, deve haver uma comunicação para responsáveis e/ou patrocinador do projeto tomarem uma decisão.	
Papéis	
Alta Administração | Gerentes de Riscos | Gerentes de Projetos	
Observações sobre o uso do item da Metodologia	
Caso a organização não possua previamente uma EAR, deve ser institucionalizada uma versão contendo as categorias de riscos comuns a todos os projetos. Cada novo projeto deve conter uma instância da EAR organizacional (institucionalizada), denominada EAR do projeto. Durante a evolução do processo, após a execução de alguns projetos, podem surgir novas categorias, que posteriormente em análise com a alta administração pode haver a necessidade de serem institucionalizadas junto às demais categorias da EAR organizacional.	

c. Definir Modelo Padrão do Plano de Gerenciamento de Riscos

Objetivo	
Institucionalizar elementos importantes relacionado aos riscos, que serão tratados durante o ciclo de vida de um projeto.	
Sobre o Item	
Boas Práticas Relacionadas	BP04 - Definir parâmetros para análise de riscos BP05 - Definir estratégias para a gerência de riscos
Entradas e Resultados Sugeridos	
Entradas	Estrutura Analítica de Riscos Ativos de processos organizacionais (registros de projetos anteriores, modelos padrão)
Resultados	Modelo do Plano de Gerenciamento de Riscos

Recomendações Segundo os Padrões

[PMBOK] A sugestão de modelo do plano de gerenciamento de riscos é composta por:

- Metodologia: definindo abordagens, ferramentas e fontes de dados usadas para gerenciamento de riscos
- Papéis e responsabilidades: definição de líder e membros da equipe responsável pelo gerenciamento de riscos, explicando suas responsabilidades
- Orçamento: recursos financeiros disponíveis para o gerenciamento dos riscos e aplicação das reservas de contingência.
- Prazos: Definição de quando e com que frequência serão realizadas tarefas de gerenciamento de riscos.
- Categorias de Riscos: Estrutura analítica de Riscos definida na tarefa anterior
- Definições de Probabilidade e Impacto dos Riscos: Escala de graduação para determinação de probabilidade e impacto dos riscos identificados
- Matriz de Probabilidade e Impacto: alguns autores denominam grau de exposição, que trata-se da correlação entre probabilidade e impacto, para posterior priorização de riscos.
- Formatos dos relatórios: como os resultados coletados serão apresentados durante e após a execução do projeto.
- Acompanhamento: Documenta como as atividades serão registradas e se haverá auditoria no gerenciamento de riscos, e de que forma.

[ISO/IEC 16085] Deve ser estabelecida uma descrição de como o gerenciamento de riscos será implementado, documentado e comunicado, incluindo os seguintes itens:

- A frequência com que riscos são reanalisados e monitorados
- Detalhamento do tipo de análise de riscos (qualitativo ou quantitativo). Para este trabalho será considerado apenas uma análise qualitativa dos riscos, por entendermos qu a análise quantitativa depende fortemente da implementação de outros processos constantes no programa de melhoria organizacional (Medição, Gerência Quantitativa de Projetos).
- As escalas para expressar probabilidade e impacto
- Os tipos de limites de riscos
- Tipos de medidas que serão utilizadas para monitorar riscos
- Como riscos serão priorizados para tratamento
- Quais perspectivas de *stakeholders* o gerenciamento de riscos apóia.

Também deve possibilitar a identificação de responsáveis, identificando explicitamente pessoas e papéis envolvidos.

Papéis
Alta Administração ǀ Gerentes de Riscos ǀ Gerentes de Projetos
Observações sobre o uso do item da Metodologia
O propósito desta tarefa é permitir que haja um planejamento e definição de quais elementos do gerenciamento de riscos são importantes no âmbito organizacional. Desta forma, os futuros projetos terão um grau considerável de similaridade em métricas e informações disponíveis, para posterior análise de melhorias. Outra justificativa para esta tarefa é a necessidade do processo ser flexível para diversas organizações, logo não é obrigatório que o modelo para plano de gerenciamento de riscos seja um documento extenso, detalhando cada item. O resultado desta tarefa também pode ser apresentado em outras formas, por exemplo, através de ferramentas de software, mapas mentais ou outro modelo que se adéquem mais à realidade da organização.

2) Fase Execução

A fase de Execução é composta pelas tarefas: "Definição do Plano de Gerenciamento de Riscos", "Identificação de Riscos", "Detalhamento de Riscos", "Definição de riscos prioritários" e "Elaboração de planos para riscos prioritários", que são executadas em sequência, e são equivalentes às etapas de identificação, análise e priorização de riscos.

Posteriormente, é executada a tarefa "Avaliação e Monitoramento de Risco", que se repete em marcos e pontos de controle durante todo o ciclo de vida do projeto, esta tarefa pode resultar em duas situações: (1) na identificação de um novo risco, ou uma mudança em um risco já identificado, direcionando o fluxo novamente para a tarefa "Identificação de Riscos", que seguirá a mesma sequência inicial até retornar à tarefa "Avaliação e Monitoramento de Riscos"; (2) ou na identificação da necessidade de executar um plano de mitigação ou contingência., que direcionará o fluxo para a tarefa: "Execução do Plano de Mitigação ou Contingência", que em seguida retornará para a tarefa "Avaliação e Monitoramento de Riscos".

d. Definir o Plano de Gerenciamento de Riscos

Objetivo	
Agregar informações relevantes para o gerenciamento de riscos do projeto	
Sobre o Item	
Boas Práticas Relacionadas	BP05 - Definir estratégias para a gerência de riscos BP02 - Identificar papéis e responsáveis pelo gerenciamento de riscos
Entradas e Resultados Sugeridos	
Entradas	Modelo do Plano de Gerenciamento de Riscos Plano(s) do Projeto (escopo, custos, cronograma, comunicações) Estrutura Analítica de Riscos Papéis e responsabilidades do Projeto Níveis de autoridades para tomada de decisões
Resultados	Plano de Gerenciamento de Riscos do Projeto

Recomendações Segundo os Padrões

[PMBOK]

Devem ser realizadas reuniões entre os papéis envolvidos, afim de desenvolver o plano do projeto a partir do modelo organizacional estabelecido na última tarefa da fase de anterior. Nesta etapa podem ser delineadas especificidades do projeto que não foram definidas anteriormente.

As reuniões devem ser conduzidas de forma a consolidar os planos de alto nível que nortearão as atividades de gerenciamento de riscos, avaliando custos e cronograma para serem sincronizados ao orçamento e cronograma globais do projeto.

Também podem ser atualizadas as abordagens para utilização de reservas de contingência e atribuídas as responsabilidades.

[ISO/IEC 16085]

As partes responsáveis por realizar o gerenciamento de riscos, incluindo papéis e responsabilidades devem ser explicitamente identificados, e os recursos devem ser disponibilizados de forma adequada para os envolvidos realizarem suas atividades.

Papéis

Gerente do Projeto
Gerente de Riscos do Projeto
Equipe de Gerência de Risco (Membros selecionados da equipe do projeto)

Observações sobre o uso do item da Metodologia

A partir do modelo de plano de riscos institucionalizado, devem ser preenchidas as informações específicas ao projeto. Também podem ser incluídos itens específicos para cada projeto, e ao final da execução avaliar a possibilidade de institucionalização junto ao Modelo Padrão do Plano de Gerenciamento de Riscos.

e. Identificar Riscos

Objetivo	
Determinar os riscos que podem afetar a execução do projeto e documentação das possíveis causas e consequências desses riscos para posterior análise.	
Sobre o Item	
Boas Práticas	BP06 - Identificar e documentar riscos
Entradas e Resultados Sugeridos	
Entradas	Estrutura Analítica de Riscos (EAR) Plano de Gerenciamento de Riscos do Projeto Estimativas (de custo e duração) das atividades Escopo do Projeto Ativos de Processos Organizacionais (projetos anteriores) Política Organizacional de Gerência de Riscos
Resultados	Lista de Riscos (identificados)

Recomendações Segundo os Padrões

[PMBOK]

- Revisões de documentação: realização de uma revisão estruturada de planos do projeto atual e arquivos de projetos anteriores.
- Técnicas de Coleta de Informações:
  - *Brainstorming*: A equipe do projeto realiza uma reunião, se possível, com especialistas multidisciplinares que não fazem parte do projeto, o objetivo é obter uma lista completa de riscos categorizados. As idéias devem ser fornecidas de forma livre pelos participantes, com a condução de um facilitador.
  - Técnica Delphi: Utilização de questionário pré-definido para solicitar idéias sobre riscos importantes do projeto a especialistas em riscos, que devem participar anonimamente. Em uma segunda etapa as respostas são resumidas e redistribuídas a especialistas para comentários adicionais, até se chegar a um consenso.
  - Entrevistas a membros mais experientes da equipe do projeto, a partes interessadas ou a especialistas no assunto identificados pelo gerente do projeto.
  - Análise de causa-raiz: São identificados problemas, que em seguida levam a identificação das causas subjacentes.
- *Checklist*: Desenvolvimento de *checklist* pré-definido, com base em informações históricas de projetos anteriores. Pode ser construído a partir do nível mais baixo da EAR. Deve ser utilizado como um suporte, pois apesar de ser rápido e simples, é impossível criar um *checklist* completo.
- Análise de Premissas: Os riscos identificados são concebidos a partir de um conjunto de hipóteses, cenários ou premissas. A análise explora a validade de cada premissa em relação ao projeto, que podem possuir caráter inexato, instável, inconsistente ou incompleto.
- Técnicas de Diagramas: Utilizadas principalmente para relacionar causalidade, pode ser feito uso dos diagramas de causa e efeito, fluxogramas, ou diagramas de influência.
- Análise de forças, fraquezas, oportunidades e ameaças (Matriz SWOT): Inicialmente, através de *brainstorming*, são identificadas as forças e fraquezas da organização, dando ênfase ao projeto. Em seguida são identificadas as oportunidades resultantes da forças e as ameaças resultantes das fraquezas da organização.

[ISO/IEC 16085] Diversas técnicas para identificação de riscos podem ser utilizadas, como a utilização de questionários de riscos, taxonomias de riscos (a partir da EAR), técnicas de *brainstorming*, análise de cenários, lições aprendidas em projetos anteriores, ou prototipação. Categorias de riscos devem ser usadas de forma consistente, para que a comunicação com *stakeholders* seja efetiva, e para reduzir a complexidade da análise, monitoramento e tratamento de riscos semelhantes.
Papéis
Gerente do Projeto Gerente de Riscos do Projeto Equipe de Gerência de Riscos Equipe do Projeto (membros selecionados)
Observações sobre o uso do item da Metodologia
É importante ressaltar que a identificação de riscos é uma tarefa iterativa. Inicialmente é necessário um esforço maior para documentação de riscos que possam afetar o projeto, porém durante a execução do projeto, podem ser identificados novos riscos, que devem ser registrados para posterior análise e comparação com riscos previamente identificados.

f. Detalhar Riscos

Objetivo	
Análise de riscos identificados em um maior grau de detalhamento, classificando e coletando mais informações dos riscos para posterior priorização, especialmente quanto à probabilidade e ao impacto.	
Sobre o Item	
Boas Práticas	BP 07 - Classificar riscos
Entradas e Resultados Sugeridos	
Entradas	Lista de Riscos (identificados) Estrutura Analítica de Riscos Plano de Gerenciamento de Riscos
Resultados	Lista de Riscos (analisados)
Recomendações Segundo os Padrões	

[PMBOK]

Devem ser determinados a probabilidade e o impacto dos riscos identificados, que podem ser realizados com auxílio de:

- Entrevistas ou reuniões com participantes selecionados de acordo com a familiaridade com as categorias de riscos, ou com pessoas experientes externas ao projeto. Além de probabilidade e impacto, devem ser registrado detalhes explicativos, como as premissas que justificam os níveis atribuídos.
- Uso da matriz de probabilidade e impacto, que especificam combinações entre probabilidade e impacto, resultando em uma classificação automática de riscos de acordo com a prioridade (baixa, moderada, alta).
- Avaliação da qualidade de riscos, pois para um risco ser detalhados é necessário um maior grau de compreensão do mesmo. Riscos que não possuem um bom grau de precisão, qualidade, confiabilidade e integridade de dados podem não possuir um bom grau de detalhamento necessário para o sucesso da gerência de riscos. Logo se a qualidade de dados for inaceitável, pode ser necessário coletar dados de qualidade maior.

[ISO/IEC 16085]

A probabilidade de ocorrência dos riscos devem ser estimadas e a escala utilizada para estimativas devem ser utilizadas de forma consistente ao descrito no plano de gerência de riscos.

Podem ser definidos individualmente para cada risco os limites de aceitação, relacionados a custo, cronograma ou outras consequências relevantes.

A avaliação de limites de aceitação de riscos pode ser realizada através de árvores de decisões, planejamento de cenários, teoria dos jogos, análise probabilística ou programação linear.

Papéis
Gerente de Riscos do Projeto | Equipe de Gerência de Riscos
Observações sobre o uso do item da Metodologia

É importante que, após a realização da tarefa, o máximo de informações a respeito dos riscos sejam coletadas, com destaque para a categorização e a combinação entre probabilidade e impacto dos riscos, aqui denominada grau de exposição.

A categorização pode ser definida nesta tarefa ou na tarefa anterior, como foi mencionado, sendo escolha do implementador a forma que melhor se adéque à realidade da organização.

g. Definir Riscos Prioritários

Objetivo	
Definir uma ordem de prioridade de riscos de acordo com o grau de exposição, e selecionar um conjunto de riscos com consequências que mais afetem o projeto, para receberem maior atenção e acompanhamento.	
Sobre o Item	
Boas Práticas Relacionadas	BP08 - Priorizar riscos BP10 - Definir prioridade para aplicação de recursos em riscos
Entradas e Resultados Sugeridos	
Entradas	Lista de Riscos (analisados)
Resultados	Lista de Riscos (priorizada)
Recomendações Segundo os Padrões	
[PMBOK] As recomendações contidas na tarefa anterior (Detalhar Riscos) , realizam a análise de risco em conjunto com a priorização, gerando uma lista de riscos já priorizada.	
[ISO/IEC 16085] Não se aplica.	
Papéis	
Gerente de Riscos do Projeto Equipe de Gerência de Riscos	
Observações sobre o uso do item da Metodologia	
Caso a organização opte por realizar a tarefa anterior (Detalhar Riscos) de acordo com as recomendações do PMBOK, então já existirá uma Lista de Riscos priorizada e analisada antes da realização desta tarefa, ficando facultada sua realização. É interessante ainda assim realizá-la para revalidar a lista de riscos priorizada, e destacar quais dos riscos priorizados serão monitorados durante a execução do projeto.	

h. Elaborar Planos para Riscos Prioritários

Objetivo	
A partir dos riscos prioritários e dos recursos disponíveis, definir as estratégias para evitar as consequências dos riscos mais prioritários, de forma proativa (mitigação) ou reativa (contingência).	
Sobre o Item	
Boas Práticas Relacionadas	BP09 - Escolher estratégia de ação e definir respostas aos riscos
Entradas e Resultados Sugeridos	
Entradas	Lista de Riscos (priorizada) Plano de Gerenciamento de Riscos
Resultados	Lista de Riscos (com respostas aos riscos detalhadas) Planos de Projeto atualizados (escopo, custos, cronograma, comunicações, recursos humanos, aquisições, qualidade)

Recomendações Segundo os Padrões

[PMBOK]

Devem ser observadas as estratégias de respostas ao riscos, e em seguida é necessário a seleção da estratégia ou mescla de estratégias com maior probabilidade de serem eficazes para cada risco, podendo também serem registradas estratégias alternativas que complementam ou substituem as principais em caso de insucesso. Entre as estratégias para riscos negativos sugerem-se adotar:

- Mitigação: implica na redução da probabilidade e/ou do impacto de um risco para dentro de limites aceitáveis, reduzindo assim seu grau de exposição. Em geral, adotar uma ação antecipada ao risco é mais eficaz que tentar reparar o dano após ter ocorrido.
- Eliminação: Alteração do plano de gerenciamento do projeto para remover totalmente uma ameaça, como por exemplo estender o cronograma ou reduzir o escopo
- Transferência: Mudança de responsabilidade pelo gerenciamento de riscos para um terceiro. Geralmente associada a riscos financeiros, é comumente utilizada na contratação de seguradoras para serem responsáveis por eventuais ocorrências de um risco. Transferir um risco simplesmente passa a responsabilidade para outra parte, mas não o elimina.
- Aceitação: raramente é possível eliminar ou mitigar todas as ameaças de um projeto, logo esses riscos devem ser aceitos. A aceitação pode ser passiva, que não envolve nenhuma ação a não ser documentar a estratégia, mas também pode ser uma aceitação ativa, que estabelece um plano de contingência, incluindo tempo, dinheiro e recursos para lidar com a ocorrência do risco.
- Contingência: para alguns riscos, mesmo mitigados, é apropriada a definição de um plano de resposta a sua ocorrência, que será executado somente sob certas condições predefinidas.

[ISO/IEC 16085]
Para cada riscos que está acima de seu limite de aceitação devem ser adotadas estratégias para redução ou eliminação dos riscos, que reduzem sua probabilidade e impacto, ou pode ser adotada uma estratégia de aceitação do risco.
Planos de contingência devem ser desenvolvidos para todos os riscos que estão acima do seu limite de aceitação, mesmo que já tenha sido realizada mitigação.
Os planos e estratégias abordados para cada risco devem ser comunicados aos *stakeholders* para aprovação, rejeição ou modificação. Caso seja aprovada, então a estratégia deve ser implementada, apoiada pelos recursos necessários e monitorada e coordenada como uma atividade do projeto.
Os *stakeholders* podem aceitar um limite mesmo que exceda o limite de aceitação e não possua uma estratégia proativa para redução do grau de exposição, nesse caso o risco deve ser considerado de alta prioridade e monitorado continuamente para determinar se algum tratamento futuro será necessário.
Os riscos que tiveram estratégias rejeitadas pelos *stakeholders*, devem ter novas estratégias determinadas, que serão novamente submetidas aos *stakeholders* para nova avaliação.

Papéis

Gerente de Riscos do Projeto
Equipe de Gerência de Riscos

Observações sobre o uso do item da Metodologia

É importante a definição de planos e estratégias para o maior número possível de riscos, porém como os recursos dos projetos são finitos, em algumas ocasiões não é possível a observação de todos os riscos identificados. A priorização realizada na tarefa anterior é importante, pois tornará mais claro quais riscos merecem um maior grau de atenção durante a execução de um projeto, e esses riscos devem possuir um maior nível de detalhamento, sendo especificados planos e estratégias abordados para terem suas consequências reduzidas.

Planos de mitigação aprovados devem ser definidos como tarefas no projeto, assim como riscos de alta prioridade devem ter monitoramento constante.

i. Avaliar e Monitorar Riscos

Objetivo	
Realizar acompanhamento de ameaças, com ênfase em riscos prioritários, durante toda a execução do projeto até sua conclusão.	
Sobre o Item	
Boas Práticas Relacionadas	BP11 - Monitorar (e reavaliar) riscos BP06 - Identificar e documentar riscos
Entradas e Resultados Sugeridos	
Entradas	Lista de Riscos (priorizada) Plano de Gerenciamento de Risco Plano de Projeto (escopo, custos, cronograma, comunicações, recursos humanos, aquisições, qualidade)
Resultados	Atualizações na Lista de Riscos Planos de Projeto atualizados (escopo, custos, cronograma, comunicações, recursos humanos, aquisições, qualidade)

Recomendações Segundo os Padrões

[PMBOK]

- Reavaliação de riscos programadas com regularidade. A quantidade e os detalhes de repetição que são apropriados dependem de como está o andamento do projeto em relação aos seus objetivos. Durante o processo de reavaliação podem ser identificados novos riscos relacionados aos que estão sendo monitorados.
- Realização de auditorias de riscos, para examinar e documentar a eficácia das respostas para lidar com os riscos identificados e suas causas-raiz, assim como a eficácia do processo de gerenciamento de riscos. As auditorias podem ser incluídas durante as reuniões rotineiras de revisões do projeto ou realizadas separadamente. O formato da auditoria e seus objetivos devem ser definidos previamente de forma clara.
- Utilização de análises de variação e tendências para comparar resultados planejados com os resultados atuais. A análise de valor agregado é um exemplo que pode ser utilizado para monitorar o desempenho geral do projeto. Os resultados das análises podem prever o desvio potencial do projeto no término em relação às metas de custos, cronograma e escopo.
- Utilização de medição e desempenho técnico, através da definição prévia de medidas quantificáveis e objetivas do desempenho técnico. Alguns exemplos de medidas são: prazos, números de defeitos entregues, etc. Qualquer desvio do planejado, como demonstrar mais ou menos funcionalidades em um marco, pode ajudar a prever o grau de sucesso para atingir o escopo do projeto e expor o grau de risco técnico que o projeto está enfrentando.
- Análise de reservas, para comparar a quantidade restante de reservas de contingências com a quantidade de riscos restante a qualquer momento no projeto, com a finalidade de determinar se as reservas restantes são adequadas.
- Reuniões periódicas de andamento do projeto, com discussões frequente sobre os riscos identificados, aumentando a probabilidade de identificação de novas estratégias.

[ISO/IEC 16085]

- Todos os riscos devem ser monitorados durante todo o ciclo de vida do projeto, para identificar mudanças em seu estado usando medidas documentada no Plano de Gerenciamento de Riscos. Riscos devem ser alocados em uma ordem de prioridade de monitoramento, baseado em critérios definidos pelos *stakeholders*. A ordem de prioridade de monitoramento deve ser revisada periodicamente para verificar se a ordem definida ainda é válida. Riscos de alta prioridade devem ser monitorados com frequência maior, e mudança de estado de um risco deve levar a uma nova análise, para um novo detalhamento deste risco.
- Medidas devem ser implementadas e monitoradas para avaliar a efetividade do tratamento de riscos. As causas de um tratamento ineficiente devem ser remediadas imediatamente. Critérios devem ser determinados pelos *stakeholders* para determinar quando um riscos não necessita mais ser monitorado para tratamento efetivo.
- Devem ser monitoradas as ocorrências de novos riscos durante o ciclo de vida do projeto. Novos riscos devem ser comunicados aos *stakeholders* após o detalhamento.

Papéis

Gerente de Riscos do Projeto
Equipe de Gerência de Riscos

Observações sobre o uso do item da Metodologia

A avaliação e monitoramento de riscos é uma tarefa contínua, que só é encerrada ao final do projeto. Recomenda-se a realização do monitoramento em uma periodicidade específica, para avaliar o estado dos riscos identificados e considerar a necessidade de mitigação ou a determinação de ocorrência, a partir das condições determinadas na análise do risco.

Caso seja identificada a ocorrência de um riscos, o plano de contingência deve ser executado de forma prioritária, o detalhamento destas ações está apresentado na tarefa "Executar Plano de Mitigação ou Contingência".

Durante o monitoramento pode ocorrer a identificação de um novo risco, logo é importante que esta ameaça seja documentada na Lista de Riscos, para posterior detalhamento e reavaliação da lista de prioridade de riscos. Caso o novo risco tenha prioridade relevante também é recomendável elaborar planos de mitigação e contingência, especificando a estratégia adotada.

j. Executar Plano de Mitigação ou Contingência

Objetivo	
Executar ações previamente planejadas, para que o risco tenha seu grau de severidade reduzido, ou que um risco ocorrido possa ser contingenciado, minimizando suas consequências	
Sobre o Item	
Boas Práticas Relacionadas	BP12 - Realizar ações para reduzir impacto do risco
Entradas e Resultados Sugeridos	
Entradas	Lista de Riscos (com respostas aos riscos detalhadas) Plano de Gerenciamento de Riscos
Resultados	Solicitações de mudanças Lista de Riscos (atualizada com respostas aos riscos detalhadas)

Recomendações Segundo os Padrões

[PMBOK]

A implementação das estratégias de resposta aos riscos pode resultar em uma solicitação de mudança, que podem incluir:

- Ações corretivas recomendadas: incluem planos de contingência e de contorno. Esses últimos foram respostas que não foram inicialmente planejadas, mas são necessárias para lidar com os riscos emergentes que não foram identificados anteriormente ou que foram aceitos passivamente
- Ações preventivas recomendadas: são usadas para manter a conformidade do projeto em relação ao plano de gerenciamento do projeto.

[ISO/IEC 16085]

Para implementação do padrão em conjunto com a norma ISO/IEC 12207, uma vez que a forma de tratamento de um risco é selecionado, ele deve receber as mesmas ações que um problema recebe de acordo com a execução e os controles das atividades no item 7.1.3.3 da norma ISO/IEC 12207:1995

Papéis

Gerente de Riscos do Projeto
Equipe de Gerência de Riscos

Observações sobre o uso do item da Metodologia

Os planos executados devem ser relatados junto às informações detalhadas sobre os riscos. Data de execução, responsável pela execução e observações devem ser documentadas para registro histórico e o estado de riscos que tiveram planos executados devem ser alterados para valores como "mitigado" ou "contingenciado".

3) Fase Avaliação

A fase de Avaliação é composta pelas tarefas: "Revisar Processo de Gestão de Riscos", "Aplicar Alterações Necessárias no Processo De Gestão De Riscos", "Revisar Tratamento de Riscos e Sucessos" e "Identificar Novos Riscos Organizacionais".

A tarefa inicial desta fase pode resultar em necessidade de mudanças, por isso há um controle de fluxo que, caso hajam mudanças, direcionará para a execução da tarefa "Aplicar Alterações Necessárias no Processo De Gestão De Riscos". As demais tarefas são executadas de forma sequencial até a finalização desta fase.

k. Revisar o Processo de Gestão de Riscos

Objetivo	
Avaliar processo implantado na organização e identificar pontos de melhoria	
Sobre o Item	
Boas Práticas	BP14 - Avaliar a execução da Gestão de Riscos
Entradas e Resultados Sugeridos	
Entradas	Plano de Gerenciamento de Riscos Lista de Riscos (atualizada com respostas aos riscos detalhadas)
Resultados	Sugestões de mudanças no processo de gerência de riscos
Recomendações Segundo os Padrões	
[PMBOK] Não se Aplica	
[ISO/IEC 16085] O processo de gerenciamento de riscos deve ser revisado periodicamente para aumentar eficácia e eficiência. Oportunidades de melhoria para evoluir o processo devem ser identificados, incluindo melhorias nas formas de reduzir ou eliminar a ocorrência de novos riscos. Se aplicável, também devem ser atualizados a política organizacional e o modelo de plano de gerenciamento de riscos.	
Papéis	
Alta Administração Gerentes de Riscos Gerentes de Projetos Equipe de Gerência de Riscos do Projeto	
Observações sobre o uso do item da Metodologia	
Esta tarefa pode ser realizada através de uma reunião entre o responsável pela gerência de riscos, sua equipe e a presença de alguns membros da alta administração e de outros gerentes de projetos. Nesta reunião devem ser identificados os pontos fracos encontrados durante a execução do processo, para que possam ser ajustados. Outra alternativa eficiente é a elaboração de um *checklist* para avaliação do processo. A forma como será realizada esta avaliação e como serão documentadas as necessidades de ajustes podem estar detalhadas na política organizacional, de forma que seja disponibilizada a todos.	

l. Aplicar Alterações Necessárias no Processo de Gestão de Riscos

Objetivo	
Aprimorar o processo de gerenciamento de riscos, através de mudanças no fluxo ou nos seus componentes.	
Sobre o Item	
Boas Práticas Relacionadas	BP14 - Avaliar a execução da Gestão de Riscos
Entradas e Resultados Sugeridos	
Entradas	Sugestões de mudanças no processo de gerência de riscos
Resultados	Registro de mudanças no processo de gerência de riscos
Recomendações Segundo os Padrões	
[PMBOK] Não se Aplica	
[ISO/IEC 16085] Não se Aplica	
Papéis	
Gerentes de Riscos	
Observações sobre o uso do item da Metodologia	
As sugestões de mudanças definidas para o processo devem ser institucionalizadas no processo padrão para serem executadas em futuros projetos. Os registros destas mudanças devem contar data de alteração, responsável pela alteração e identificação do documento de sugestão que a originou.	

m. Revisar Tratamento de Riscos e Sucessos

Objetivo	
Agrupar e documentar dados históricos relacionados à redução de impacto de riscos identificados, para orientar futuros projetos em lições aprendidas.	
Sobre o Item	
Boas Práticas Relacionadas	BP14 - Avaliar a execução da Gestão de Riscos
Entradas e Resultados Sugeridos	
Entradas	Lista de Riscos (atualizada com respostas aos riscos detalhadas) Plano de Gerenciamento de Riscos do Projeto Registro de Mudanças nos Planos do Projeto
Resultados	Lições Aprendidas
Recomendações Segundo os Padrões	
Segundo os Padrões:	**[PMBOK]** Não se Aplica
	[ISO/IEC 16085] Informações acerca dos riscos identificados, seu tratamento, e o sucesso do tratamento devem ser revisados periodicamente pelos *stakeholders* e outras partes com o propósito de auxiliar na identificação sistemática de riscos do projeto e organizacionais.
Papéis	
Gerente de Riscos do Projeto Equipe de Gerência de Riscos	
Observações sobre o uso do item da Metodologia	
É importante a identificação de pontos fortes no gerenciamento de riscos encontrados ao final da execução do projeto, armazenando informações para futuros projetos. Estas informações podem ser coletadas através de uma reunião, inclusive podendo ser a mesma reunião realizada na primeira tarefa da fase de Avaliação. Para cada ponto forte identificado no tratamento de riscos, devem haver detalhes de como foi realizado o tratamento, qual a categoria, prioridade e impacto do risco trabalhado e caso haja, quais técnicas para mitigação ou contingência foram utilizadas. Estas informações podem ser armazenadas em uma ferramenta de gerência de conhecimento, como uma *wiki*, por exemplo, de forma que esteja acessível a todos os integrantes da equipe de gerenciamento de riscos.	

n. Identificar Novos Riscos Organizacionais

Objetivo	
Institucionalizar mudanças na Estrutura Analítica de Riscos da organização, podendo ser alterações, novos registros ou exclusões.	
Sobre o Item	
Boas Práticas Relacionadas	BP14 - Avaliar a execução da Gestão de Riscos BP03 - Definir Categorias de Riscos
Entradas e Resultados Sugeridos	
Entradas	Estrutura Analítica de Riscos Lista de Riscos (atualizada com respostas aos riscos detalhadas) Plano de Gerenciamento de Riscos do Projeto
Resultados	Atualização na Estrutura Analítica de Riscos
Recomendações Segundo os Padrões	
[PMBOK] Não se Aplica	
[ISO/IEC 16085] Não se Aplica	
Papéis	
Alta Administração Gerentes de Riscos Gerentes de Projetos	
Observações sobre o uso do item da Metodologia	
Pode ser realizada durante uma reunião ao final do projeto, e está relacionada à necessidade de incluir novas categorias de riscos na EAR da organização, que foram identificados neste projeto e não estavam documentados anteriormente. A atualização da EAR organizacional proporcionará um aperfeiçoamento que orientará de uma melhor maneira a identificação de riscos em futuros projetos.	

APÊNDICE B – QUESTIONÁRIO DE AVALIAÇÃO DA METODOLOGIA POR UM ESPECIALISTA

1. Objetivo da Avaliação

Avaliar os critérios utilizados para a definição da metodologia; verificar a aderência entre boas práticas no gerenciamento de riscos e definição de tarefas da metodologia; e analisar se as considerações feitas esclarecem suas atribuições.

Devem ser revisados fases, fluxos, tarefas, artefatos, papéis e práticas relacionadas em relação às boas práticas em Gerência de Riscos utilizadas nos modelos de qualidade MR-MPS-BR, CMMI-DEV, PMBOK e ISO/IEC 12207**.**

2. Instruções para a Execução da Avaliação

a) Preencha a sua Identificação e o seu Perfil como especialista em gerência de riscos (Seções 3 e 4)

b) Leia o documento de especificação do framework e a lista de boas práticas (em anexo), analisando se os dados informados são válidos, com relação a clareza, requisitos técnicos, aderência a modelos de qualidade e ortografia. Avalie se as informações contribuem pra o gerenciamento de riscos em uma organização desenvolvedora de software.

c) Durante a leitura, identifique pontos do conteúdo das considerações para as quais você deseja registrar um comentário;

d) Utilize a Tabela constante no final deste documento (Seção 6) para registrar seus comentários:

- A coluna **ID** representa um campo autoincremental de considerações provenientes das Revisões;
- A coluna **Categoria** representa o tipo de consideração da Revisão. Estes tipos são melhor explicados na Seção 6 deste documento;
- A coluna **Item** representa o ativo (nome da Fase ou da Tarefa) constante no framework apresentado e que possui alguma consideração proveniente da Revisão;
- A coluna **Comentário com a Justificativa** representa a consideração do Revisor quanto à definição do framework;

- A coluna **Sugestão** representa a proposta do Revisor para contornar o problema, caso aplicável.

e) Após concluir a análise do documento em anexo preencha a avaliação objetiva da proposta (Seção 5)

f) Ao concluir a revisão, por favor, envie seu documento de revisão para o remetente deste anexo

3. Dados de Identificação do Revisor

Nome do Revisor:

Data da Revisão:

4. Perfil do Revisor do Framework

a) Qual seu nível de conhecimento em Gerenciamento de Riscos

( ) Alto ( ) Médio

( ) Baixo ( ) Nenhum

b) Já Trabalhou implantando Gerência de Riscos em uma organização?

( ) Sim. Qual(is): _____

( ) Não

c) Qual o seu tempo de experiência em gerenciamento de projetos de software?

( ) Mais de cinco anos ( ) Entre dois e cinco anos

( ) Entre um e dois anos ( ) Menos de um ano

( ) Nenhum

d) Qual o seu tempo de experiência em Implantação de Modelos para Melhoria do Processo de Gerência de Riscos?

( ) Mais de cinco anos ( ) Entre dois e cinco anos

( ) Entre um e dois anos ( ) Menos de um ano

( ) Nenhum

e) Possui certificação em algum Modelo para Melhoria do Processo de Software?

( ) Sim. Qual(is): _____

( ) Não

f) Qual o seu nível de conhecimento em Métodos de Avaliação constantes nos Modelos para Melhoria do Processo de Software?

( ) Alto ( ) Médio

( ) Baixo ( ) Nenhum

g) Caso você tenha algum nível de conhecimento em relação à questão anterior, por favor, cite em que método(s):_____

h) Qual o seu tempo de experiência em Avaliação de Processos de Gerencia de Riscos:

( ) Mais de cinco anos ( ) Entre dois e cinco anos

( ) Entre um e dois anos ( ) Menos de um ano

( ) Nenhum

5. Apresentação da proposta

i) Como você considera a proposta do *framework* para gerência de riscos (especificações, atividades, fluxo, etc.)?

( ) Completa
( ) Incompleta
( ) Inconsistente
( ) Não sei

Observações: _____

j) Como você considera a descrição do fluxo e das fases para o Modelo Geral (Macro-Fluxo) ?

( ) Completa
( ) Incompleta
( ) Inconsistente
( ) Não sei

Observações: _____

k) Como você considera a descrição das atividades para a fase “Planejamento da Gestão de Riscos”?

( ) Completa

( ) Incompleta

( ) Inconsistente

( ) Não sei

Observações: _____

l) Como você considera a descrição das atividades para a fase “Execução da Gestão de Riscos”?

( ) Completa

( ) Incompleta

( ) Inconsistente

( ) Não sei

Observações: _____

m) Como você considera a descrição das atividades para a fase “Avaliação da Gestão de Riscos”?

( ) Completa

( ) Incompleta

( ) Inconsistente

( ) Não sei

Observações: _____

n) Você considera que o *framework* pode ser um referencial para ser utilizado na Gerência de Riscos?

( ) Sim
( ) Parcialmente
( ) Não

Observações: _____

6. Revisão do Framework

Observação: A linha em amarelo na Tabela abaixo representa um exemplo de preenchimento das colunas descritas na Seção 2 deste documento.

Segue abaixo os itens utilizados para a coluna "**Categoria**"

- **TA (Técnico Alto)**, indicando que foi encontrado um problema em um item que, se não for alterado, comprometerá as considerações;
- **TB (Técnico Baixo)**, indicando que foi encontrado um problema em um item que seria conveniente alterar;
- **E (Editorial)**, indicando que foi encontrado um erro de português ou que o texto pode ser melhorado;
- **Q (Questionamento)**, indicando que houve dúvidas quanto ao conteúdo das considerações;
- **G (Geral)**, indicando que o comentário é geral em relação às considerações.
- **BP (Boas Práticas)**, indicando que o comentário está relacionado à lista de boas práticas.

ID	Categoria	Item	Comentário com a Justificativa	Sugestão
1	TA	Geral	Não foi contemplada nenhuma tarefa relacionada à priorização de riscos identificados	Inserção de nova tarefa no fluxo após identificação de riscos, detalhar tarefa com informações constantes no modelo de qualidade X que apresenta a priorização dos riscos como uma boa prática

APÊNDICE C – RASTREABILIDADE ENTRE METODOLOGIA E OS CASOS DE USO

Este documento contém a rastreabilidade entre as atividades da metodologia para gerenciamento de riscos e os casos de uso da ferramenta Spider-RM (ver subeção 4.2.2).

No quadro abaixo, as atividades da metodologia estão posicionadas na coluna à esquerda e para cada uma delas foi estabelecida a correspondência com um ou mais casos de uso elencado na coluna à direita.

Nem todas as atividades da metodologia possuem casos de uso correspondentes, pois: podem se tratar de atividades administrativas, ou por não haver possibilidade de sistematização através da ferramenta. Quando isso ocorre, a ausência de correspondência é representada por um hífen ("-"). Assim como alguns casos de uso foram necessários serem desenvolvidos, sem estarem diretamente relacionados a alguma tarefa da metodologia.

Atividade da Metodologia	**Caso de Uso**
Determinar Escopo da Gerência de Riscos	Definir Política Organizacional para Riscos
Definir Categorias de Riscos	Gerenciar Estrutura Analítica de Riscos
Definir Modelo de Plano de Gerenciamento de Riscos	-
Definir o Plano de Gerenciamento de Riscos	Definir Plano de Gerenciamento de Riscos
Identificar os Riscos	Identificar Riscos
Detalhar os Riscos	Analisar Riscos
Definir os Riscos Prioritários	Priorizar Riscos
Elaborar Planos para Riscos Prioritários	Desenvolver Plano de Contingência
	Desenvolver Plano de Mitigação
Avaliar e Monitorar os Riscos	Monitorar Riscos
	Deliberar Ocorrência de Riscos
Executar o Plano de Mitigação ou Contingência	Executar Plano de Mitigação
	Executar Plano de Contingência
Revisar o Processo de Gestão de Riscos	Avaliar Projeto
Revisar Tratamento de Riscos e Sucessos Aplicar	

Atividade da Metodologia	Caso de Uso
Alterações Necessárias no Processo de Gestão de Riscos	-
Identificar Novos Riscos Organizacionais	Avaliar Novas Categorias
-	Gerenciar Projeto
-	Definir Estrutura Analítica de Riscos do Projeto
-	Concluir Projeto

APÊNDICE D – CENÁRIO DO EXPERIMENTO

Este documento descreve o cenário proposto aos alunos de pós-graduação que participaram do experimento realizado com o uso da ferramenta Spuder-RM, detalhado no Capítulo 5.

Cenário

Imagine que você trabalha, como gerente de projetos, em uma organização especializada em desenvolvimento de software Web. Esta empresa possui um programa interno de melhoria de processo de software, e pretende implantar um processo baseado em boas práticas para o gerenciamento de riscos de acordo com o guia fornecido pelo programa MPS.BR.

Assim, é selecionado um projeto piloto para implantação da gerência de riscos e você e sua equipe serão os responsáveis pela gerência e execução. Porém o projeto selecionado foi uma demanda para desenvolvimento de um aplicativo *mobile* para um cliente localizado em outro Estado.

Você, sendo o gerente do projeto, dispõe de uma equipe formada 1 desenvolvedor sênior, 1 desenvolvedora *front*-end especialista em *mobile* e 1 desenvolvedor junior e 1 designer. Toda e qualquer mudança que possam gerar impacto em escopo, prazo e orçamento devem ser comunicadas à alta administração para ser tomada uma decisão, e o *feedback* do projeto deve ser comunicado ao cliente em uma periodicidade regular de no máximo 15 dias.

Com base nessa necessidade e nesses pré-requisitos, você deve seguir com o gerenciamento de riscos do projeto levando em consideração o Guia de Implementação do MPS.BR e possui à disposição uma ferramenta (Spider-RM) para auxiliar a execução do projeto, no qual devem ser registradas as informações relacionadas.

APÊNDICE E – QUESTIONÁRIO DE PERFIL E AVALIAÇÃO DA SPIDER-RM

Este documento contem os questionários utilizados para coletar informações objetivos dos participantes durante o experimento realizado, detalhado no Capítulo 5.

Perfil do Entrevistado

1) Qual o seu tempo de experiência em Projetos de Software?
( ) Mais de cinco anos
( ) Entre dois e cinco anos
( ) Entre um e dois anos
( ) Menos de um ano
( ) Nenhum

2) Qual o seu nível de conhecimento em Modelos de Qualidade de Software?
( ) Alto
( ) Médio
( ) Baixo
( ) Nenhum

3) Qual o seu tempo de experiência em Modelos de Qualidade de Software?
( ) Mais de cinco anos
( ) Entre dois e cinco anos
( ) Entre um e dois anos
( ) Menos de um ano
( ) Nenhum

4) Possui alguma certificação relacionada a modelos de qualidade? (MPS.BR, CMMI-DEV, PMBOK)?
( ) Sim Quais? _____
( ) Não

5) Qual o seu nível de conhecimento em Gerência de Riscos?
( ) Alto
( ) Médio
( ) Baixo
( ) Nenhum

6) Qual o seu tempo de experiência em Gerência de Riscos?
( ) Mais de cinco anos
( ) Entre dois e cinco anos
( ) Entre um e dois anos
( ) Menos de um ano
( ) Nenhum

Avaliação da Ferramenta

Nesta seção as questões estão relacionadas com a utilização da ferramenta que sistematiza a metodologia de gerencia de riscos integrada.

1) **Em relação à sistematização do processo de gerenciamento de riscos com uso de ferramenta, você considera:**

( ) Importante ( ) Pouco Importante ( ) Indiferente

( ) Irrelevante ( ) Não sei

2) **Em relação ao suporte que a ferramenta oferece:**
   a. **à identificação de riscos, pode-se dizer que é:**
      ( ) Ótimo ( ) Bom ( ) Regular
      ( ) Ruim ( ) Muito ruim ( ) Não sei

   b. **à análise de riscos, pode-se dizer que é:**
      ( ) Ótimo ( ) Bom ( ) Regular
      ( ) Ruim ( ) Muito ruim ( ) Não sei

   c. **à priorização de riscos, pode-se dizer que é:**
      ( ) Ótimo ( ) Bom ( ) Regular
      ( ) Ruim ( ) Muito ruim ( ) Não sei

   d. **à mitigação de riscos, pode-se dizer que é:**
      ( ) Ótimo ( ) Bom ( ) Regular
      ( ) Ruim ( ) Muito ruim ( ) Não sei

   e. **ao monitoramento, pode-se dizer que é:**
      ( ) Ótimo ( ) Bom ( ) Regular
      ( ) Ruim ( ) Muito ruim ( ) Não sei

   f. **à contingência de riscos, pode-se dizer que é:**
      ( ) Ótimo ( ) Bom ( ) Regular
      ( ) Ruim ( ) Muito ruim ( ) Não sei

3) **Em relação à usabilidade (facilidade de uso) da ferramenta, pode-se dizer que ela possui:**

( ) Ótima ( ) Boa ( ) Regular

( ) Ruim ( ) Muito ruim ( ) Não sei

4) Você acha que a ferramenta é adequada para ser utilizada em uma organização para auxiliar gerenciamento de riscos em projetos de software?

( ) Sim ( ) Não ( ) Parcialmente

( ) Não sei

5) Em relação ao desempenho das atividades do processo sistematizadas na ferramenta, pode-se dizer que ela possui:

( ) Alto desempenho ( ) Desempenho moderado ( ) Baixo desempenho

6) De acordo com o seu conhecimento, qual o grau de aderência que o processo apoiado na ferramenta encontra-se em relação às práticas do MPS.BR?

( ) Completo ( ) Parcial ( ) Nenhum

( ) Não sei

7) Quais os pontos fracos / fortes / melhorias que você identificou na ferramenta?

_____

_____

_____

_____

_____

_____

_____

_____

_____

APÊNDICE F – Questionário de avaliação do Conhecimento

Este documento apresenta o questionário de avaliação do conhecimento, aplicado durante o experimento detalhado no Capítulo 5. Estas perguntas foram entregues aos participantes, para serem respondidas em dois momentos: antes do uso da ferramenta e após seu uso, para, através de análise das respostas, avaliar se houve aquisição de conhecimento durante a execução do experimento.

1. Qual seu entendimento sobre a Gestão de Riscos? Quando e como deve ser realizado o Gerenciamento de Riscos?

2. Qual seu entendimento sobre as etapas de identificação, análise e priorização de riscos?

3. Qual seu entendimento sobre a etapa de monitoração de riscos?

4. Qual seu entendimento sobre a etapa de mitigação e contingência de riscos?

5. Qual a importância do Gerenciamento de Riscos no Escopo de uma Organização? E no Escopo individual dos projetos?