



**FUNDAÇÃO EDSON QUEIROZ**

**UNIVERSIDADE DE FORTALEZA – UNIFOR**

Pascale Correia Rocha Pereira

**UM PROCESSO DE GERENCIAMENTO DE RISCOS PARA  
PROJETOS DE SOFTWARE**

**Fortaleza**

**2005**



**FUNDAÇÃO EDSON QUEIROZ**

**UNIVERSIDADE DE FORTALEZA – UNIFOR**

Pascale Correia Rocha Pereira

**UM PROCESSO DE GERENCIAMENTO DE RISCOS PARA  
PROJETOS DE SOFTWARE**

Dissertação apresentada ao Curso de Mestrado em Informática Aplicada (MIA) da Universidade de Fortaleza (UNIFOR), como requisito parcial para obtenção do título de Mestre em Informática.

Orientador: Prof. Dr. Arnaldo Dias Belchior

Fortaleza

2005

**Pascale Correia Rocha Pereira**

**UM PROCESSO DE GERENCIAMENTO DE RISCOS PARA  
PROJETOS DE SOFTWARE**

Data de Aprovação: 25/11/2005

Banca Examinadora:

---

Prof. Arnaldo Dias Belchior, D.Sc.  
(Presidente da Banca)

---

Prof. Manoel Gomes de Mendonça Neto, Ph.D. (UNIFACS)

---

Prof. Pedro Porfírio Muniz Farias, D.Sc. (UNIFOR)

## FICHA DE CATALOGAÇÃO

PEREIRA, Pascale Correia Rocha. **Um Processo de Gerenciamento de Riscos para Projetos de Software.** 2005. 220f. Dissertação (Mestrado em Informática Aplicada) – Universidade de Fortaleza (UNIFOR). Fortaleza, 2005.

Perfil do Autor: Graduada em Informática pela Universidade de Fortaleza (UNIFOR). Consultora de Tecnologia da Informação da Célula de Qualidade, Testes e Homologação do Ambiente de Sistemas da Informação do Banco do Nordeste do Brasil.

### RESUMO:

O desenvolvimento de software é uma atividade complexa, envolvendo inúmeros fatores, muitas vezes imprevisíveis e difíceis de ser controlados. Essa complexidade faz com que grande parte dos projetos de software exceda o prazo e o orçamento previstos, além de não atender às expectativas de seus clientes em termos de funcionalidade e qualidade. Como a incerteza é inerente a esse tipo de projeto, o gerenciamento de riscos torna-se cada vez mais relevante, pois conduz a organização a sistematicamente planejar, antecipar e tratar os riscos, para proativamente eliminar ou minimizar seus impactos no projeto. Este trabalho propõe um processo de gerenciamento de riscos para projetos de software, fundamentando-se principalmente nas abordagens de riscos do PMBOK (2004), da AS/NZS 4360 (2004), do padrão IEEE STD 1540 (2001), do CMMI (2002) e do RUP (2003). Em seguida, apresenta a implantação desse processo em uma organização de software, objetivando implementar a área de processo de Gerenciamento de Riscos do CMMI, nível 3, dessa organização.

### PALAVRAS-CHAVE:

1) RUP; 2) PMBOK; 3) CMMI; 4) IEEE STD 1540-2001; 5) AS/NZS 4360; 5) Gerenciamento de Riscos.

# DEDICATÓRIA

Dedico este trabalho à minha família por sempre me apoiar e dar provas de amor, carinho e dedicação.

## AGRADECIMENTOS

Agradeço a Deus, pelos desafios que tem colocado diante de mim e por me dar forças para superá-los.

Ao orientador e amigo professor Arnaldo Dias Belchior, pela sua inestimável orientação, estando sempre disponível e efetivamente comprometido com a qualidade deste trabalho.

Aos professores Manoel Mendonça e Pedro Porfírio, pela participação na banca examinadora.

Às minhas filhas, Ramayana e Camille, pelo amor, carinho, apoio e compreensão nos momentos de ausência, que não foram poucos durante a realização deste trabalho.

Ao meu marido, Carlos Henrique, pelos incentivos e por compreender os momentos de ausência, demonstrando companheirismo, paciência e carinho.

À minha mãe, Francisca, e aos meus irmãos, Elvice e Júnior, também pelos incentivos e conselhos nos momentos difíceis.

Aos amigos do mestrado, em especial à Lívia, à Dorotéia, à Rejane, ao Sales e ao Frank, pelo companheirismo, pelo apoio e pelo aprendizado que me proporcionaram.

Aos demais professores do mestrado, pela constante presença e contribuições indiretas.

À Tânia, secretária do MIA, pela atenção, paciência e presteza sempre imediatas.

Ao Instituto Atlântico, por ter me propiciado a aplicação prática deste trabalho, em especial ao Carlo Giovano, à Márcia e à Tatiana.

Ao Banco do Nordeste, pelo apoio financeiro.

Por fim, agradeço aos demais amigos aqui não citados, mas que certamente foram importantes para a conclusão deste trabalho.

## **RESUMO**

O desenvolvimento de software é uma atividade complexa, envolvendo inúmeros fatores, muitas vezes imprevisíveis e difíceis de ser controlados. Essa complexidade faz com que grande parte dos projetos de software exceda o prazo e o orçamento previstos, além de não atender às expectativas de seus clientes em termos de funcionalidade e qualidade. Como a incerteza é inerente a esse tipo de projeto, o gerenciamento de riscos torna-se cada vez mais relevante, pois conduz a organização a sistematicamente planejar, antecipar e tratar os riscos, para proativamente eliminar ou minimizar seus impactos no projeto. Este trabalho propõe um processo de gerenciamento de riscos para projetos de software, fundamentando-se principalmente nas abordagens de riscos do PMBOK (2004), da AS/NZS 4360 (2004), do padrão IEEE STD 1540 (2001), do CMMI (2002) e do RUP (2003). Em seguida, apresenta a implantação desse processo em uma organização de software, objetivando implementar a área de processo de Gerenciamento de Riscos do CMMI, nível 3, dessa organização.

**PALAVRAS-CHAVE:** RUP; PMBOK; CMMI; IEEE STD 1540-2001; AS/NZS 4360; Gerenciamento de Riscos.

## ABSTRACT

*Software development is a complex activity, involving several factors, which are sometimes unpredictable and hard to control. This complexity causes schedule delays, cost overruns, quality problems and missing functionality. As uncertainty is inherent to these types of projects, risk management has become more notable as it leads the organization to systematically plan, anticipate, and mitigate risks to proactively eliminate or minimize their impact on the project. This work proposes a software risk management process based on the risk approaches of PMBOK (2004), AS/NZS 4360 (2004), IEEE STD 1540-2001, CMMI-SW (2002), and on concepts of RUP (2003). It then presents its specialization and implementation in an organization, aiming to follow CMMI level 3 requirements for risk management.*

Keywords: *RUP; PMBOK; CMMI; IEEE STD 1540-2001; AS/NZS 4360; Risk Management.*



# LISTAS DE ILUSTRAÇÕES

## LISTA DE FIGURAS

Figura 2.1 – Visão geral do gerenciamento de riscos do projeto	9
Figura 2.2 – AS/NZS 4360:2004 – Processo de Gerenciamento de Riscos	30
Figura 2.3 – Processo de Tratamento de Riscos	41
Figura 3.1 – Modelo do processo de gerenciamento de riscos do padrão IEEE (2001)	50
Figura 3.2 – Componente do CMMI (2002)	60
Figura 3.3 – Diagrama do contexto do gerenciamento de riscos	63
Figura 3.4 – Arquitetura geral do RUP	79
Figura 3.5 – Fluxo da disciplina <i>Gerenciamento de Projetos</i>	82
Figura 3.6 – Fluxo <i>Conceber Novo Projeto</i>	83
Figura 3.7 – Fluxo <i>Avaliar escopo e riscos do projeto</i>	89
Figura 3.8 – Fluxo <i>Elaborar plano de desenvolvimento de software</i>	91
Figura 3.9 – Fluxo <i>Monitorar e controlar o projeto</i>	93
Figura 4.1 – Fluxo do <i>Processo de gerenciamento de riscos de software</i>	105
Figura 4.2 – Macroatividade <i>Planejar o gerenciamento de riscos</i>	108
Figuras 4.3 – Estrutura Analítica de Riscos	113
Figuras 4.4 – Definição de escalas de impacto para quatro objetivos do projeto	116
Figuras 4.5 – Matriz de probabilidade e impacto	117
Figura 4.6 – Macroatividade <i>Identificar riscos</i>	126
Figura 4.7 – Macroatividade <i>Analisar riscos</i>	130
Figura 4.8 – Macroatividade <i>Tratar riscos</i>	137
Figura 4.9 – Macroatividade <i>Monitorar e controlar riscos</i>	146
Figura 4.10 – Macroatividade <i>Avaliar o processo de gerenciamento de riscos</i>	152
Figura 5.1 – Estrutura de trabalho do Instituto Atlântico	158
Figura 5.2 – Fluxo principal do <i>Processo especializado de gestão de riscos</i>	164
Figura 5.3 – Planejar gestão de riscos	165
Figura 5.4 – Identificar e analisar riscos	166
Figura 5.5 – Planejar respostas aos riscos	169
Figura 5.6 – Monitorar e controlar riscos	170

## LISTA DE QUADROS

Quadro 4.1 – Atividade <i>Determinar fontes e categorias de riscos</i>	110
Quadro 4.2 – Atividade <i>Definir parâmetros para os riscos</i>	114
Quadro 4.3 – Atividade <i>Estabelecer estratégia</i>	121
Quadro 4.4 - Atividade <i>Identificar riscos potenciais</i>	127
Quadro 4.5 - Atividade <i>Estabelecer o contexto dos riscos</i>	129
Quadro 4.6 - Atividade <i>Categorizar os riscos</i>	131
Quadro 4.7 - Atividade <i>Avaliar impacto e probabilidade</i>	132
Quadro 4.8 - Atividade <i>Priorizar riscos</i>	134
Quadro 4.9 - Atividade <i>Analisar quantitativamente os riscos</i>	135
Quadro 4.10 - Atividade <i>Selecionar estratégias</i>	138
Quadro 4.11 - Atividade <i>Definir e selecionar respostas aos riscos</i>	143
Quadro 4.12 - Atividade <i>Monitorar e controlar riscos</i>	147
Quadro 4.13 - Atividade <i>Reportar os estados dos riscos</i>	150
Quadro 4.14 - Atividade <i>Monitorar e controlar o processo</i>	153

## LISTA DE TABELAS

Tabela 3.1 – Gerenciamento de riscos do CMMI (2002)	62
Tabela 3.2 – Fases do RUP (2003)	81
Tabela 3.3 – Mapeamento do gerenciamento de riscos	97
Tabela 4.1 – Detalhamento do fluxo <i>Processo de gerenciamento de riscos</i>	106
Tabela 4.2 – Critério para seleção de estratégia	118
Tabela 4.3 – Classificação de projetos de acordo com os respectivos portes	122
Tabela 5.1 – Macroatividade <i>Planejar o gerenciamento de riscos</i>	166
Tabela 5.2 – Macroatividade <i>Identificar riscos</i>	167
Tabela 5.3 – Macroatividade <i>Analisar riscos</i>	167
Tabela 5.4 – Macroatividade <i>Tratar riscos</i>	169
Tabela 5.5 – Macroatividade <i>Monitorar e controlar riscos</i>	171
Tabela 5.6 – Macroatividade <i>Avaliar o processo de gerenciamento de riscos</i>	171

## LISTA DE ABREVIATURAS E SIGLAS

AS/NZS 4360	<i>Australian and New Zealand Standard for Risk Management 4360</i>
CMM	<i>Capability Maturity Model</i>
CMMI	<i>Capability Maturity Model Integration</i>
CMMI-SW	<i>Capability Maturity Model Integration for Software</i>
EJB	<i>Enterprise Java Beans</i>
EMV	<i>Expected Monetary Value</i>
EPG	<i>Engineering Process Group</i>
IEEE	<i>Institute of Electrical and Eletronics Engineers</i>
IHC	<i>Interação Humano-Computador</i>
ISO	<i>International Standards Organization</i>
IEEE	<i>International Electronical and Electric Engineering</i>
ISO/IEC	<i>International Standardization Organization / International Engineering Committee</i>
J2EE	<i>Java 2 Platform, Enterprise Edition</i>
J2SE	<i>Java 2 Platform, Standard Edition</i>
PA	<i>Process Area ou Área de Processo</i>
PMBOK	<i>Project Management Body of Knowledge</i>
PMI	<i>Project Management Institute</i>
PMP	<i>Project Management Professional</i>
PRA	<i>Project Review Authority</i>
RBS	<i>Risk Breakdown Structure</i>
RUP	<i>Rational Unified Process ou Processo Unificado Rational</i>
SCAMPI	<i>Standard CMMI Appraisal Method for Process Improvement ou Método de Avaliação do padrão CMMI para melhoria de processos</i>
SPICE	<i>Software Process Improvement Capability Evaluation</i>
SQA	<i>Software Quality Assurance ou Garantia de Qualidade de Software</i>
SWOT	<i>Strengths, Weaknesses, Opportunities and Threats</i>
UP	<i>Unified Process ou Processo Unificado</i>
UML	<i>Unified Modeling Language ou Linguagem de Modelagem Unificada</i>
WBS	<i>Work Breakdown Structure</i>

# SUMÁRIO

Resumo	vii
Abstract	viii
Lista de Ilustrações	ix
Lista de Abreviaturas e Siglas	xii
<b>Cap 1 – Introdução</b>	<b>1</b>
1.1. Motivação	1
1.2. Objetivo	4
1.3. Organização do Trabalho	5
<b>Cap 2 – Gerenciamento de Riscos</b>	<b>7</b>
2.1. Gerenciamento de Riscos no PMBOK	7
2.1.1. Planejamento do Gerenciamento de Riscos	10
2.1.1.1. Entradas	11
2.1.1.2. Ferramentas e Técnicas	11
2.1.1.3. Saídas	11
2.1.2. Identificação de Riscos	13
2.1.2.1. Entradas	13
2.1.2.2. Ferramentas e Técnicas	14
2.1.2.3. Saídas	14
2.1.3. Análise Qualitativa de Riscos	15
2.1.3.1. Entradas	15
2.1.3.2. Ferramentas e Técnicas	16
2.1.3.3. Saídas	17
2.1.4. Análise Quantitativa de Riscos	18
2.1.4.1. Entradas	18
2.1.4.2. Ferramentas e Técnicas	18
2.1.4.3. Saídas	20
2.1.5. Planejamento de Respostas aos Riscos	20
2.1.5.1. Entradas	21
2.1.5.2. Ferramentas e Técnicas	21
2.1.5.3. Saídas	23
2.1.6. Monitoramento e Controle de Riscos	24
2.1.6.1. Entradas	25
2.1.6.2. Ferramentas e Técnicas	25
2.1.6.3. Saídas	26
2.2. Gerenciamento de Riscos no Padrão AS/NZS 4360	27
2.2.1. Comunicar e Orientar	29
2.2.2. Estabelecer o Contexto	31
2.2.2.1. Estabelecer o Contexto Externo	31
2.2.2.2. Estabelecer o Contexto Interno	31
2.2.2.3. Estabelecer o Contexto do Gerenciamento de Riscos	32
2.2.2.4. Desenvolver Critérios para Riscos	32
2.2.2.5. Definir Estrutura para o Processo	33
2.2.3. Identificar Riscos	33
2.2.3.1. Identificar Fontes de Riscos	33
2.2.3.2. Considerar as Causas e Cenários	33

2.2.3.3. Informação para a Identificação de Riscos	34
2.2.3.4. Abordagens para a Identificação de Riscos	34
2.2.4. Analisar Riscos	34
2.2.4.1. Avaliar Controles Existentes	35
2.2.4.2. Avaliar Conseqüências e Probabilidades	35
2.2.4.3. Tipos de Análise	36
2.2.4.3.1. Análise Qualitativa	36
2.2.4.3.2. Análise Semi-quantitativa	37
2.2.4.3.3. Análise Quantitativa	37
2.2.5. Avaliar Riscos	37
2.2.5.1. Tipos de Critério de Avaliação	38
2.2.5.2. Avaliação a Partir da Análise Qualitativa	38
2.2.5.3. Risco Tolerável	39
2.2.5.4. Julgamento Implícito em Critérios	39
2.2.5.5. Critérios de Avaliação e Eventos Históricos	39
2.2.6. Tratar Riscos	40
2.2.6.1. Identificar Opções de Tratamento	41
2.2.6.1.1. Identificar Opções de Tratamento para Riscos Positivos	41
2.2.6.1.2. Identificar Opções de Tratamento para Riscos Negativos	42
2.2.6.2. Avaliar Opções de Tratamento	42
2.2.6.3. Selecionar Opções de Tratamento	43
2.2.6.4. Preparar e Implementar Planos de Tratamento	43
2.2.6.5. Riscos Residuais	44
2.2.7. Monitorar e Revisar	44
2.2.7.1. Mudanças no Contexto e nos Riscos	44
2.2.7.2. Monitoração e Garantia do Processo	45
2.2.7.3. Medida de Desempenho do Gerenciamento de Riscos	45
2.2.7.4. Análise após o Evento	46
2.2.8. Conclusão	46
<b>Cap 3 – Gerenciamento de Riscos de Software</b>	<b>47</b>
3.1. IEEE STD 1540-2001	48
3.1.1. Planejar e Implementar o Gerenciamento de Riscos	50
3.1.1.1. Estabelecer Políticas de Gerenciamento de Riscos	51
3.1.1.2. Estabelecer o Processo de Gerenciamento de Riscos	51
3.1.1.3. Estabelecer Responsabilidades	52
3.1.1.4. Designar Recursos	52
3.1.1.5. Estabelecer a Avaliação do Processo de Gerenciamento de Riscos	51
3.1.2. Gerenciar o Perfil de Riscos do Projeto	52
3.1.2.1. Definir o Contexto do Gerenciamento de Riscos	52
3.1.2.2. Estabelecer Limites para os Riscos	53
3.1.2.3. Estabelecer Manter o Perfil de Risco do Projeto	53
3.1.2.4. Comunicar o Status dos Riscos	54
3.1.3. Executar a Análise dos Riscos	54
3.1.3.1. Identificação dos Riscos	54
3.1.3.2. Estimativas dos Riscos	54
3.1.3.3. Avaliação dos Riscos	55
3.1.4. Executar o Tratamento dos Riscos	55
3.1.4.1. Selecionar Tratamento dos Riscos	56
3.1.4.2. Planejar e Implementar o Tratamento dos Riscos	56

3.1.5. Executar a Monitoração dos Riscos	57
3.1.5.1. Monitorar Riscos	56
3.1.5.2. Monitorar o Tratamento dos Riscos	57
3.1.5.3. Procurar Novos Riscos	58
3.1.6. Avaliar o Processo de Gerenciamento de Riscos	58
3.1.6.1. Capturar Informações sobre o Gerenciamento de Riscos	58
3.1.6.2. Avaliar e Melhorar o Processo de Gerenciamento de Riscos	59
3.1.6.3. Gerar Lições Aprendidas	59
3.2. Gerenciamento de Riscos no CMMI	59
3.2.1. Preparar o Gerenciamento de Riscos (SG 1)	64
3.2.1.1. Determinar Fontes e Categorias de Riscos (SP 1.1)	64
3.2.1.2. Definir Parâmetros para Riscos (SP 1.2)	65
3.2.1.3. Estabelecer a Estratégia de Gerenciamento de Riscos (SP 1.3)	67
3.2.2. Identificar e Analisar Riscos (SG 2)	68
3.2.2.1. Identificar Riscos (SP 2.1)	68
3.2.2.2. Avaliar, Categorizar e Priorizar Riscos (SP 2.2)	71
3.2.3. Mitigar Riscos (SG2)	73
3.2.3.1. Desenvolver Plano de Mitigação de Riscos (SP 3.1)	73
3.2.3.2. Implementar Planos de Mitigação de Riscos (SP 3.2)	76
3.3. Gerenciamento de Riscos no RUP	78
3.3.1. Fluxo <i>Conceber Novo Projeto</i>	82
3.3.1.1. Atividade <i>Identificar e Avaliar Riscos</i>	84
3.3.2. Fluxo <i>Avaliar Escopo e Riscos do Projeto</i>	88
3.3.3. Fluxo <i>Elaborar Plano de Desenvolvimento de Software</i>	89
3.3.3.1. Atividade <i>Desenvolver Plano de Gerenciamento de Riscos</i>	91
3.3.4. Fluxo <i>Monitorar e Controlar o Projeto</i>	93
3.3.4.1. Atividade <i>Monitorar o Status do Projeto</i>	94
3.3.4.2. Atividade <i>Reportar Status</i>	95
3.4. Mapeamento do Gerenciamento de Riscos	95
3.4.1. Planejar o Gerenciamento de Riscos	95
3.4.2. Identificar Riscos	98
3.4.3. Analisar Riscos	99
3.4.4. Tratar Riscos	100
3.4.5. Tratar Riscos	101
3.4.6. Avaliar o Processo de Gerenciamento de Riscos	102
3.5. Conclusão	103
<b>Cap 4 – Processo de Gerenciamento de Riscos de Software</b>	<b>104</b>
4.1. Macroatividade <i>Planejar o Gerenciamento de Riscos</i>	108
4.1.1. Atividade <i>Determinar Fontes e Categorias de Riscos</i>	110
4.1.1.1. Determinar as Fontes de Riscos	110
4.1.1.2. Determinar as Categorias de Riscos	110
4.1.2. Atividade <i>Definir Parâmetros para os Riscos</i>	110
4.1.2.1. Definir Critérios para a Análise dos Riscos	110
4.1.2.2. Definir Critérios para o Tratamento dos Riscos	110
4.1.2.3. Definir Métricas	118
4.1.2.4. Definir Limites para cada Categoria de Riscos	119
4.1.2.5. Definir Indicadores para Avaliação do Processo	119
4.1.3. Atividade <i>Estabelecer Estratégia</i>	121
4.1.3.1. Adaptar o Processo ao Projeto	121

4.1.3.2. Definir Metodologia	122
4.1.3.3. Atribuir Papéis e Responsabilidades	123
4.1.3.4. Definir Periodicidade	124
4.1.3.5. Planejar Comunicação	124
4.1.3.6. Definir a Avaliação do Processo	125
4.2. Macroatividade <i>Identificar Riscos</i>	125
4.2.1. Atividade <i>Identificar Riscos Potenciais</i>	126
4.2.1.1. Identificar os Riscos Associados às Fontes e Categorias	127
4.2.1.2. Revisar a Documentação do Projeto	128
4.2.1.3. Revisar Informações Históricas	128
4.2.2. Atividade <i>Estabelecer o Contexto dos Riscos</i>	129
4.2.2.1. Detectar as Circunstâncias ou Condições dos Riscos	129
4.2.2.2. Identificar Possíveis Consequências dos Riscos	130
4.3. Macroatividade <i>Analisar Riscos</i>	130
4.3.1. Atividade <i>Categorizar Riscos</i>	131
4.3.1.1. Agrupar os Riscos de Acordo com as Categorias	132
4.3.2. Atividade <i>Avaliar Impacto e Probabilidade</i>	132
4.3.2.1. Avaliar o Impacto dos Riscos	133
4.3.2.2. Avaliar a Probabilidade de Ocorrência dos Riscos	133
4.3.2.3. Determinar a Exposição aos Riscos	133
4.3.3. Atividade <i>Priorizar Riscos</i>	134
4.3.3.1. Determinar a Prioridade Relativa dos Riscos	134
4.3.4. Atividade <i>Analisar Quantitativamente os Riscos</i>	135
4.3.4.1. Analisar Quantitativamente os Riscos	135
4.4. Macroatividade <i>Tratar Riscos</i>	137
4.4.1. Atividade <i>Selecionar Estratégias</i>	138
4.4.1.1. Definir Limites	139
4.4.1.2. Selecionar Estratégias para Ameaças	139
4.4.1.3. Selecionar Estratégias para Oportunidades	141
4.4.1.4. Selecionar os Riscos que Serão Aceitos	142
4.4.2. Atividade <i>Definir e Selecionar Respostas aos Riscos</i>	142
4.4.2.1. Definir Ações de Resposta aos Riscos	143
4.4.2.2. Avaliar e Selecionar as Ações	143
4.4.2.3. Definir Plano de Contingências	144
4.4.2.4. Associar Gatilhos aos Riscos	145
4.4.2.5. Designar Proprietário e Envolvidos	146
4.5. Macroatividade <i>Monitorar e Controlar Riscos</i>	146
4.5.1. Atividade <i>Monitorar e Controlar Riscos</i>	147
4.5.1.1. Acompanhar os Estados Atuais dos Riscos	148
4.5.1.2. Executar o Plano de Tratamento dos Riscos	149
4.5.1.3. Acompanhar o Plano de Tratamento dos Riscos	148
4.5.2. Atividade <i>Reportar os Estados dos Riscos</i>	149
4.5.2.1. Revisar a Documentação dos Riscos	150
4.5.2.2. Comunicar os Estados dos Riscos	151
4.6. Macroatividade <i>Avaliar o Processo de Gerenciamento de Riscos</i>	152
4.6.1. Atividade <i>Avaliar o Processo de Gerenciamento de Riscos</i>	152
4.6.1.1. Capturar Informações sobre o Processo	153
4.6.1.2. Avaliar e Melhorar o Processo	153
4.6.1.3. Gerar Lições Aprendidas	154



4.7. <i>Guidelines</i> para Implantação do Processo Proposto	155
4.8. Conclusão	156
<b>Cap 5 – Aplicação do Processo de Gerenciamento de Riscos</b>	<b>157</b>
5.1. Perfil do Instituto Atlântico	157
5.2. Especialização do Processo para o Instituto Atlântico	160
5.2.1. Planejar a Gestão de Riscos	164
5.2.2. Identificar e Analisar Riscos	166
5.2.3. Planejar Respostas aos Riscos	168
5.2.4. Monitorar e Controlar Riscos	170
5.2.5. Avaliar o Processo de Gerenciamento de Riscos	171
5.3. Implantação do Processo de Gerenciamento de Riscos	160
5.3.1. Aplicação do Processo em Projetos	174
5.3.1.1. Projeto A	174
5.3.1.2. Projeto B	175
5.3.1.3. Projeto C	176
5.4. Implantação do Processo na Organização X	176
5.4.1. Caracterização da Organização X	177
5.4.2. Estratégia de Implantação do Processo na Organização X	178
5.5. Conclusão	178
<b>Cap 6 – Conclusão</b>	<b>179</b>
6.1. Contribuições deste Trabalho	181
6.2. Perspectivas Futuras	182
<b>Glossário</b>	<b>183</b>
<b>Referências Bibliográficas</b>	<b>185</b>
<b>Anexo A</b>	<b>191</b>
<b>Apêndices</b>	<b>194</b>
Apêndice A – Procedimento para a Gestão de Riscos	194
Apêndice B – Plano de Gerenciamento de Riscos	206
Apêndice C – Registro de Riscos	211
Apêndice D - Plano de Gerenciamento de Riscos – Projeto A	216

# Capítulo 1

## INTRODUÇÃO

---

*O presente capítulo apresenta a motivação deste trabalho, seus objetivos e sua organização.*

### 1.1 MOTIVAÇÃO

O desenvolvimento de software é uma atividade complexa (FUGETTA, 2000), envolvendo inúmeros fatores que, não raro, são imprevisíveis e de difícil controle, como as inovações tecnológicas, a imaturidade nos processos, as freqüentes mudanças nos requisitos do cliente, dentre muitos outros. Essa complexidade faz com que grande parte dos projetos de desenvolvimento de software exceda o prazo e o orçamento previstos, além de não atender às expectativas do cliente em termos de funcionalidade e qualidade.

As organizações têm aumentando sua dependência tecnológica, buscando eficiência para conseguir sobreviver em um mercado cada vez mais competitivo e globalizado. Isso requer sistemas cada vez mais complexos, o que faz com que as variáveis envolvidas no processo de desenvolvimento desses produtos de software tenham um nível de complexidade crescente (BARTIÉ, 2002).

Fuller (2001) afirma que o desenvolvimento de software atualmente envolve mais e maiores riscos do que em qualquer outra época. Isso ocorre devido às mudanças na natureza dos produtos desenvolvidos, com o advento das aplicações WEB e, principalmente, pelo fato de a maior parte dos produtos de software atualmente ser desenvolvida por pequenas e médias empresas. Como os processos de software são elaborados para grandes empresas, isso introduz um conjunto de riscos adicionais referentes à necessidade de adaptação desses processos, que foram desenvolvidos sem se levar em conta as restrições enfrentadas por empresas menores.

Diante do cenário ora exposto, um gerenciamento eficaz tem-se evidenciado como de alta relevância para o sucesso de projetos de software. Nesse tipo de projeto, devido ao

baixo nível de previsibilidade, muitas premissas do gerenciamento de um projeto “normal” podem não funcionar. Portanto, o gerenciamento de riscos torna-se essencial. Charette (1996) afirma que o gerenciamento de projetos aplicado a projetos de software de grande porte consiste no gerenciamento de riscos.

O gerenciamento de riscos trabalha justamente com a incerteza, visando à identificação de problemas e oportunidades potenciais antes que ocorram, com o objetivo de se eliminar ou reduzir a probabilidade de ocorrência e/ou o impacto de eventos negativos para os objetivos do projeto, além de potencializar os efeitos da efetivação de eventos positivos.

O gerenciamento de riscos em projetos de software é uma área relativamente recente. De certa maneira, foi introduzida de forma sistemática por meio do tutorial de Boehm (1989). Desde então, muitos pesquisadores têm abordado o gerenciamento de riscos para software (CHARETTE, 1989; HALL, 1998 apud JALOTE, 2003). Para alguns, o gerenciamento de riscos é uma das atividades mais importantes do gerenciamento de projetos (BROWN, 1996; OSMUNDSON, 2002; SOMMERVILLE, 2003).

O gerenciamento de riscos tem sido abordado por vários modelos e padrões relevantes, dentre os quais o PMBOK (2004), o CMMI (2002), a AS/NZS 4360 (2004), o RUP (2003) e o IEEE Std 1540 (2001). O PMBOK (*A Guide to the Project Management Body of Knowledge*) trata do gerenciamento de projetos de uma forma ampla, não sendo específico para software. O CMMI (*Capability Maturity Model Integration*) provê um *framework* para a implantação e melhoria do processo de software em organizações. O RUP (*Rational Unified Process*) é um processo baseado em melhores práticas de engenharia de software, e enfatiza a importância da gerência de riscos. O Padrão IEEE Std 1540-2001 (*IEEE Standard for Software Life Cycle Processes – Risk Management*) é um processo contínuo de gerenciamento de riscos aplicável às disciplinas de engenharia de software e de gerenciamento. A AS/NZS 4360 (*Australian and New Zealand Standard for Risk Management*) provê um *framework* genérico para o gerenciamento de riscos, tendo sido desenvolvida na Austrália e na Nova Zelândia.

Muitas outras abordagens têm sido elaboradas para tratar o gerenciamento de riscos em projetos de software. Machado (2002) propõe um método para identificação e

quantificação de riscos de atendimento ao prazo em projetos de desenvolvimento de software sob encomenda, do ponto de vista do gerente de projeto.

Farias (2002) define uma abordagem para o planejamento de riscos em projetos de software baseada na reutilização do conhecimento organizacional sobre riscos acumulado pelos gerentes de projetos.

Leopoldino (2004) avalia riscos vivenciados no desenvolvimento de software em projetos brasileiros, com base na experiência de gerentes de projetos e desenvolvedores.

Webster (2005) propõe uma taxonomia que visa auxiliar o processo de identificação de riscos em projetos de manutenção de software.

Pinho (2005) realiza uma análise do tratamento de riscos em projetos de desenvolvimento de software no SERPRO (Serviço Federal de Processamento de Dados), e estrutura os passos realizados em uma metodologia de maneira a poder ser aplicada em outras organizações.

Apesar da relevância cada vez maior dada pela literatura ao gerenciamento de riscos e da constatação prática dos seus benefícios, por meio de muitos relatórios individuais de sucessos em desenvolvimento de software, a indústria de software como um todo parece ainda não aplicar esses métodos ativamente e sistematicamente (GUSMÃO, 2004).

Uma avaliação de melhoria de processos realizada na Austrália em 1999 constatou que o gerenciamento de riscos era executado de forma planejada e com acompanhamento em somente 12% das empresas daquele país, sendo que 48% o executavam de maneira informal e 40% simplesmente não o executavam (KWAC, 2003). No Brasil, uma pesquisa da Secretaria de Planejamento em Informática demonstrou que somente 11,4% das 446 empresas pesquisadas executam o processo de gerenciamento de riscos (SEPIN, 2002 apud PRIKLADNICKI, 2005).

De acordo com pesquisa de campo realizada por Branco (2001), com o objetivo de avaliar a qualidade dos processos gerenciais de software em empresas brasileiras, o gerenciamento de riscos foi considerado o de menor importância para o grupo de gerentes de projetos de software e especialistas em computação entrevistados.

Em uma pesquisa realizada por Lima (2004), com o propósito de caracterizar os conhecimentos mencionados na literatura técnica de engenharia de software, do ponto de vista de programadores, analistas, gerentes de projetos e diretores, verificou-se que os participantes dessa pesquisa geralmente não atribuíram grande importância aos conhecimentos referentes à gerência de riscos.

## 1.2 OBJETIVO

Este trabalho analisa um conjunto de normas e padrões que tratam do gerenciamento de riscos, sendo bastante referenciado *urbi et orbi*. A partir dessa análise, propõe-se um processo para o gerenciamento de riscos em projetos de software.

A definição de um processo é importante, porquanto possibilita uma melhor comunicação, ajuda as equipes a definir exatamente o que precisa ser feito e os critérios a serem utilizados. Conduz também a uma maior consistência dos artefatos produzidos e, finalmente, possibilita a melhoria do processo, a partir da identificação de falhas e fraquezas (KRUCHTEN, 2001).

O processo proposto visa auxiliar no gerenciamento de riscos em projetos de software, objetivando contribuir para o processo decisório durante o ciclo de vida do projeto. Objetiva-se que esse processo venha a ser utilizado diretamente em organizações de software, ou seja, especializado para essas organizações e, posteriormente, instanciado para projetos de software, independentemente dos portes respectivos. Para projetos de pequeno porte, por exemplo, pode ser executado apenas um subconjunto das atividades desse processo, o que deve ser previamente definido no planejamento do gerenciamento de riscos desses projetos.

O formato de apresentação do processo proposto usou a estrutura do RUP (2003), porquanto esse formato é amigável e tem sido utilizado em muitas organizações. Essa estrutura descreve o modelo de processo especificando o “como”, isto é, as atividades que devem ser executadas e os relacionamentos entre elas, os artefatos que devem ser gerados e os papéis a serem desempenhados. Entretanto, esse processo não teve por objetivo atender ou estender conceitos do RUP.

Por fim, esse processo foi especializado para utilização em uma organização de software cujos processos foram definidos com base na estrutura do RUP (2003), visando atender aos requisitos de gerenciamento de riscos do CMMI-SW nível 3.

### 1.3 ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado em seis capítulos, inclusive esta introdução como Capítulo 1, trazendo ainda um anexo e cinco apêndices, consoante resumidamente descrito a seguir.

No Capítulo 2 – **Gerenciamento de Riscos**, apresentam-se duas abordagens de gerenciamento de riscos, aplicáveis a projetos de qualquer natureza: a área de conhecimento *Gerenciamento de Riscos* do PMBOK (2004) e o padrão AS/NZS 4360 (2004).

No Capítulo 3 – **Gerenciamento de Riscos de Software**, são apresentadas três abordagens de gerenciamento de riscos específicas para software: o padrão IEEE STD 1540-2001, as áreas de processo do CMMI (2002) e as atividades da disciplina *Gerenciamento de Projetos* do RUP (2003).

No Capítulo 4 – **Processo de Gerenciamento de Riscos de Software**, aborda-se o processo proposto para o gerenciamento de riscos em projetos de software, baseado nos modelos apresentados nos capítulos 2 e 3.

No Capítulo 5 – **Aplicação do Processo de Gerenciamento de Riscos**, o processo proposto é validado por meio de estudos de caso, envolvendo basicamente a especialização desse processo para uma organização de software e a sua aplicação em três projetos-piloto.

No Capítulo 6 – **Conclusão**, são apresentadas as conclusões e as contribuições deste trabalho, bem como suas perspectivas futuras.

No Anexo A, são mostradas algumas técnicas de identificação de riscos, citadas na literatura.

O Apêndice A discute o procedimento para gerenciamento de riscos elaborado a partir do processo proposto em uma organização desenvolvedora de software.

No Apêndice B, apresenta-se um *template* do Plano de Gerenciamento de Riscos, elaborado de acordo com o processo proposto.

O Apêndice C consigna um *template* do Registro de Riscos, elaborado de acordo com o processo proposto.

No Apêndice D, é apresentada a aplicação do Plano de Gerenciamento de Riscos em um projeto real, utilizando-se o modelo proposto no Apêndice B.

O Apêndice E explica a aplicação do Registro de Riscos em um projeto real, a partir do modelo proposto no Apêndice C.

## Capítulo 2

# GERENCIAMENTO DE RISCOS

---

*Este capítulo apresenta duas abordagens de gerenciamento de riscos para projetos em geral.*

O presente capítulo apresenta duas abordagens de gerenciamento de riscos, que podem ser aplicadas a qualquer área do conhecimento: a área de conhecimento em Gerenciamento de Riscos do PMBOK (2004) e o padrão AS/NZS 4360 (2004). O PMBOK tem foco no projeto, enquanto o padrão AS/NZS objetiva fornecer um guia para se estabelecer e implementar os processos de gerenciamento de riscos no âmbito organizacional.

Inicialmente, aborda-se o PMBOK (2004), que descreve o conhecimento e as melhores práticas em gerenciamento de projetos, por meio de nove áreas de conhecimento: Gerenciamento de Integração, Gerenciamento do Escopo, Gerenciamento de Tempo, Gerenciamento de Custo, Gerenciamento da Qualidade, Gerenciamento de Recursos Humanos, Gerenciamento das Comunicações, Gerenciamento de Riscos e Gerenciamento de Aquisições.

Em seguida, é apresentado o padrão AS/NZS 4360 – *Australian and New Zealand Standard for Risk Management* – que fornece diretrizes para a estruturação e implementação de uma estratégia efetiva para o gerenciamento de riscos. Esse padrão enfatiza que sua estruturação varia de acordo com as necessidades da organização, seus objetivos específicos, seus produtos e serviços, bem como suas práticas e processos. Sua finalidade é definir um *framework* genérico para o estabelecimento do contexto da gerência de riscos e para a identificação, a análise, a avaliação, o tratamento, a monitoração e a comunicação dos riscos na organização.

### 2.1 GERENCIAMENTO DE RISCOS NO PMBOK



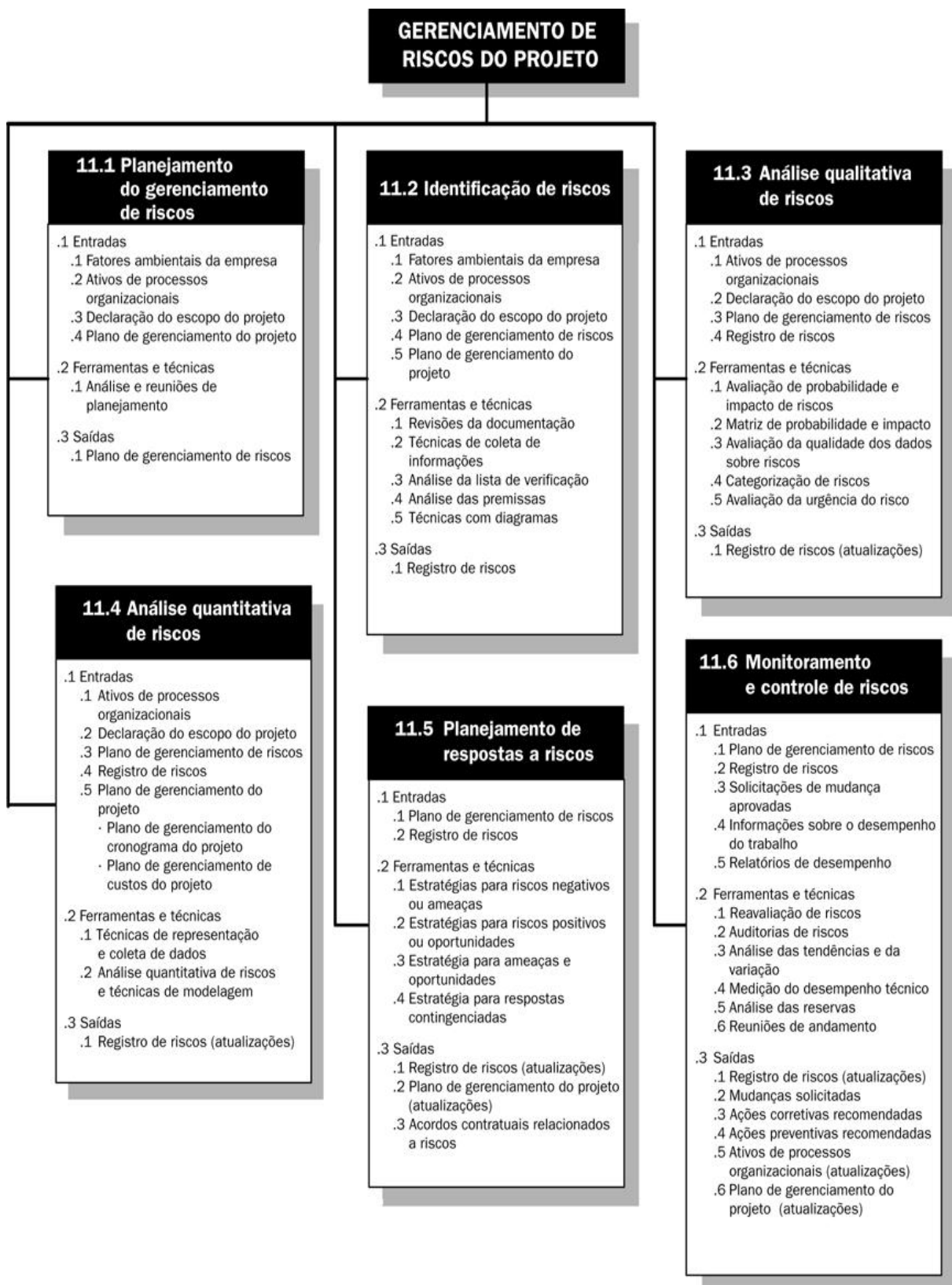
O PMI (*Project Management Institute*) define como uma prática essencial da gerência de projetos a execução do processo de gerenciamento de riscos. Para o PMBOK, riscos de projeto são eventos ou condições incertas que, se ocorrerem, têm um efeito positivo ou negativo em pelo menos um objetivo do projeto. Os riscos positivos relacionam-se às oportunidades de aumentar as possibilidades de sucesso do projeto, enquanto os negativos dizem respeito às ameaças ao sucesso do projeto. Os riscos que correspondem a ameaças ao projeto podem ser aceitos, se estiverem balanceados com compensações que possam representar ganhos pela aceitação do risco.

Um risco pode ter uma ou mais causas e, se ocorrer, um ou mais impactos nos objetivos do projeto, como no custo, no cronograma ou no desempenho do projeto. Condições de risco podem incluir aspectos do ambiente do projeto ou do ambiente organizacional, tal como práticas de gerenciamento de projetos pobres, falta de sistemas de gerência integrados, projetos múltiplos simultâneos ou a dependência de participantes externos que não podem ser controlados.

Os riscos podem ser conhecidos ou desconhecidos. Os conhecidos são aqueles que foram identificados e analisados, podendo-se fazer um planejamento para eles. Os riscos desconhecidos não podem ser gerenciados proativamente, e uma resposta prudente da equipe do projeto seria alocar uma contingência genérica para tais riscos, assim como para todos os riscos conhecidos para os quais não seja viável ou possível desenvolver uma resposta proativa. Para cada projeto, deve ser desenvolvida uma abordagem consistente e proativa que atenda aos requisitos da organização. A comunicação dos riscos e a elaboração das respostas devem ser abertas e transparentes.

O gerenciamento de riscos do projeto inclui os processos referentes ao planejamento do gerenciamento de riscos, à identificação, à análise, ao planejamento das respostas e à monitoração e controle dos riscos. Esses processos interagem entre si e com os processos das demais áreas de conhecimento.

Dentre os objetivos do gerenciamento de riscos, destacam-se: (1) aumentar a probabilidade de ocorrência e os impactos de eventos positivos; e (2) diminuir a probabilidade e os impactos dos eventos contrários aos objetivos do projeto. O gerenciamento de riscos em um projeto efetiva-se mediante implementação de seis processos (PMBOK,



**Figura 2.1 – Visão geral do gerenciamento de riscos do projeto. Fonte: PMBOK (2004)**

2004): planejamento do gerenciamento de riscos, identificação de riscos, análise qualitativa de riscos, análise quantitativa de riscos, planejamento de respostas a riscos e monitoramento e controle de riscos. A Figura 2.1 destaca, para cada um dos processos citados, as respectivas entradas, as ferramentas e técnicas utilizadas e as saídas.

- *Planejamento do gerenciamento de riscos*: planejamento das atividades de gerenciamento de riscos que serão realizadas no projeto.
- *Identificação de riscos*: identificação dos riscos que podem afetar o projeto e a documentação das suas características.
- *Análise qualitativa de riscos*: avaliação e combinação do impacto e probabilidade, priorizando os riscos para efeito de análise ou ação adicional.
- *Análise quantitativa dos riscos*: mensuração da probabilidade de ocorrência dos riscos e das suas conseqüências por meio de análise numérica.
- *Planejamento de respostas aos riscos*: desenvolvimento de opções para tratamento dos riscos por meio de ações voltadas para aumentar as oportunidades e reduzir as ameaças aos objetivos do projeto.
- *Monitoramento e controle dos riscos*: acompanhamento dos riscos identificados; monitoramento dos riscos residuais e identificação de novos riscos; execução dos planos de respostas aos riscos; e avaliação da sua eficácia durante todo o ciclo de vida do projeto.

A seguir, são detalhados os seis processos da área de gerenciamento de riscos, com suas respectivas entradas, ferramentas e técnicas e saídas, consoante ilustrado na Figura 2.1.

### **2.1.1 PLANEJAMENTO DO GERENCIAMENTO DE RISCOS**

Consiste no processo de decisão quanto à forma de abordar e conduzir as atividades de gerenciamento de riscos para um projeto. O nível, o tipo e a visibilidade do gerenciamento de riscos devem ser proporcionais ao risco e à importância do projeto para a organização. Em função desses aspectos, são definidos os recursos e o tempo necessários para as atividades de gerenciamento de riscos, estabelecendo-se uma base para a avaliação dos riscos. Esse processo deve ser concluído no início do planejamento do projeto, pois é fundamental para a bem-sucedida execução dos outros processos de gerenciamento de riscos.

### **2.1.1.1 ENTRADAS**

- *Fatores ambientais da empresa:* políticas e atitudes relacionadas a riscos e à tolerância a riscos das organizações e indivíduos envolvidos com o projeto.
- *Ativos de processos organizacionais:* abordagens predefinidas para o gerenciamento de riscos na organização, como categorias de riscos, definições comuns de conceitos e termos, modelos, papéis e responsabilidades e níveis de autoridade para o processo decisório.
- *Declaração de escopo do projeto:* descrição detalhada compreendendo as entregas do projeto, o esforço necessário para completá-las, os principais objetivos do projeto, requisitos, restrições, premissas e riscos iniciais conhecidos.
- *Plano de gerenciamento do projeto:* definição de como o projeto será executado, monitorado, controlado e encerrado, especificando o conjunto de saídas do grupo de processos de planejamento em um só documento ou em documentos distintos (planos auxiliares e outros componentes).

### **2.1.1.2 FERRAMENTAS E TÉCNICAS**

As técnicas utilizadas são a análise e as reuniões de planejamento, que deve contar com a presença do gerente do projeto, de membros da equipe especialmente selecionados, partes interessadas, o responsável pelo gerenciamento das atividades de execução e planejamento de riscos, e de outras pessoas, caso se mostre necessário. Nas reuniões, discute-se o planejamento das atividades de gerenciamento de riscos do projeto.

### **2.1.1.3 SAÍDAS**

A principal saída desse processo é o Plano de Gerenciamento de Riscos, que integra o Plano de Gerenciamento do Projeto, o qual descreve como o gerenciamento será estruturado e executado no projeto, devendo conter:

- *Metodologia:* abordagem, ferramentas e fontes de dados que podem ser utilizados para executar o gerenciamento de riscos do projeto.

- *Funções e responsabilidades*: definição da liderança, suporte e membros da equipe de gerenciamento de riscos, com designação de pessoas para essas funções e definição das respectivas responsabilidades.
- *Orçamento*: definição dos recursos necessários e estimativa do custo das atividades de gerenciamento de riscos do projeto, para inclusão na base de custos.
- *Tempo*: definição da frequência de execução do processo de gerenciamento de riscos durante todo o ciclo de vida do projeto e das atividades que serão incluídas no cronograma do projeto.
- *Categorias de riscos*: definição de uma estrutura de organização para os riscos do projeto, que pode ser previamente definida pela organização e revisada para utilização no projeto. Uma maneira de representar as categorias é a Estrutura Analítica de Riscos (WBS), que mostra as categorias e subcategorias nas quais os riscos podem surgir em um projeto típico.
- *Definição de impacto e probabilidade dos riscos*: adaptação dos níveis de impacto e probabilidade para o projeto, com base nas definições gerais da organização.
- *Matriz de probabilidade e impacto dos riscos*: revisão e adaptação da matriz definida pela organização para o projeto. A matriz é uma abordagem para priorização dos riscos de acordo com suas eventuais implicações para o atendimento dos objetivos do projeto, sendo definidas as combinações de probabilidade e impacto que podem fazer com que um risco seja classificado como de importância “alta”, “moderada” ou “baixa”.
- *Tolerância*: revisão da tolerância das partes interessadas para o projeto específico.
- *Formatos de relatórios*: descrição do conteúdo e formato do registro de riscos, bem como de qualquer outro relatório necessário, onde serão documentados, analisados e comunicados os resultados do processo de gerenciamento de riscos.
- *Acompanhamento*: documentação registrando os benefícios que as atividades de gerenciamento de riscos poderão trazer para o projeto corrente, suas futuras necessidades e as lições aprendidas. Documenta, também, como os processos de riscos serão auditados.

Entre as mudanças introduzidas no PMBOK (2004), destaca-se a introdução das categorias de riscos e sua representação por meio da RBS, das definições de probabilidade e impacto e da matriz de probabilidade e impacto já no planejamento, definindo-se como os riscos serão priorizados no projeto.

### **2.1.2 IDENTIFICAÇÃO DE RISCOS**

Consiste em (1) identificar os riscos que podem afetar o projeto e (2) documentar suas características. Isso deve ocorrer de forma iterativa, porquanto novos riscos podem surgir durante todo o ciclo de vida do projeto. A frequência das iterações e quem deve participar de cada ciclo variam caso a caso.

Na identificação de riscos, é fundamental a participação do gerente do projeto, dos membros da equipe do projeto, da equipe de gerenciamento de riscos (se houver), de especialistas no assunto de fora da equipe do projeto, clientes, usuários, partes interessadas, outros gerentes de projetos e especialistas em riscos. É importante que a equipe do projeto esteja envolvida de maneira a desenvolver um senso de responsabilidade pelos riscos e ações de respostas associadas.

#### **2.1.2.1 ENTRADAS**

- *Fatores ambientais da empresa*: informações publicadas (estudos acadêmicos, *benchmarking*, bancos de dados comerciais) que possam ser úteis na identificação dos riscos do projeto.
- *Ativos de processos organizacionais*: informações sobre projetos anteriores, incluindo dados reais e lições aprendidas.
- *Declaração de escopo do projeto*: premissas do projeto, cuja indefinição pode ser uma causa potencial de riscos.
- *Plano de gerenciamento de riscos*: atribuição de funções e responsabilidades, provisão para as atividades de gerenciamento de riscos no cronograma e no orçamento e as categorias de riscos.
- *Plano de gerenciamento do projeto*: entendimento do plano de gerenciamento do cronograma, de custos e da qualidade, além de revisão de outros documentos do projeto, com o objetivo de identificar riscos.

### 2.1.2.2 FERRAMENTAS E TÉCNICAS

- *Revisões de documentação:* revisão estruturada da documentação do projeto, incluindo planos do projeto, premissas, arquivos de projetos anteriores e outras informações. A qualidade e a consistência entre os planos e com os requisitos e as premissas do projeto podem ser indicadores de riscos.
- *Técnicas de coleta de informações:* técnica *delphi*, *brainstorming*, entrevistas, identificação de causas-base, análise das forças, fraquezas, oportunidades e ameaças (SWOT).
- *Listas de verificação:* essas listas podem ser desenvolvidas com base em informações históricas e na experiência acumulada de projetos anteriores semelhantes. O nível mais baixo da WBS pode ser usado também como *checklist*.
- *Análise de premissas:* explora a validade das premissas aplicadas ao projeto, objetivando identificar riscos oriundos de falta de exatidão e consistência nas premissas, além de premissas incompletas.
- *Técnicas com diagramas:* são diagramas de causa e efeito (espinha de peixe), fluxogramas e diagramas de influência.

### 2.1.2.3 SAÍDAS

As principais saídas desse processo compõem o início da preparação do Registro de Riscos, que se torna um componente do Plano de Gerenciamento do Projeto e, nesse ponto, contém as seguintes informações:

- *Lista de riscos identificados:* descrição dos riscos identificados, incluindo suas causas e as premissas incertas do projeto.
- *Lista de respostas possíveis:* sugestões de respostas que foram identificadas e poderão ser úteis como entradas do processo do Planejamento de Respostas aos Riscos.
- *Causas-base do risco:* condições ou eventos fundamentais que podem causar o risco identificado.

- *Categorias de riscos atualizadas*: adição de novas categorias de riscos à lista de categorias de riscos, o que poderá causar modificações na RBS desenvolvida no Planejamento do Gerenciamento de Riscos.

A principal mudança na versão 2004 foi a introdução do Registro de Riscos no lugar de uma simples lista dos riscos identificados. O Registro de Riscos contém os riscos identificados, suas causas-base, as possíveis respostas e a atualização das categorias de riscos nesse processo, quando necessário.

### **2.1.3 ANÁLISE QUALITATIVA DE RISCOS**

Consiste no processo de avaliação da prioridade dos riscos identificados, usando-se sua probabilidade de ocorrência, o impacto correspondente nos objetivos do projeto, se os riscos ocorrerem, além de outros fatores como o prazo, a tolerância a riscos dos envolvidos e as restrições de custo, cronograma, escopo e qualidade do projeto.

Geralmente, é uma maneira rápida e econômica de estabelecer prioridades para o planejamento de respostas aos riscos, além de estabelecer a base para a análise quantitativa do risco, caso esta seja necessária. Essa análise deve ser revisada durante o ciclo de vida do projeto, para possibilitar o acompanhamento das mudanças nos riscos do projeto.

#### **2.1.3.1 ENTRADAS**

- *Ativos de processos organizacionais*: informações sobre riscos de projetos anteriores, incluindo dados reais e lições aprendidas.
- *Declaração de escopo do projeto*: verificar se o projeto é inovador ou corriqueiro. Neste último caso, seus riscos são bem compreendidos. Projetos que usam tecnologia inovadora ou que são altamente complexos tendem a gerar mais incertezas.
- *Plano de gerenciamento de riscos*: atribuição de funções e responsabilidades, orçamento e cronograma para as atividades de gerenciamento de riscos, categorias de riscos, definição de probabilidade e impacto, matriz de probabilidade e impacto, revisão das tolerâncias a riscos das partes interessadas e fatores ambientais da empresa.
- *Registro de riscos*: riscos identificados.



### 2.1.3.2 FERRAMENTAS E TÉCNICAS

- *Avaliação da probabilidade e impacto dos riscos:* avaliar a probabilidade de ocorrência de cada risco identificado (ameaças ou oportunidades) e seu impacto para os objetivos do projeto, como prazo, custo, escopo e qualidade. Essa avaliação pode ocorrer por meio de entrevistas ou reuniões com os participantes do projeto, selecionados pela sua familiaridade com as categorias de riscos em questão, podendo também ser incluídos especialistas de fora do projeto. A opinião de especialistas é necessária quando há pouca informação sobre riscos na base de dados referentes a projetos anteriores da organização. Um facilitador experiente poderá conduzir a discussão, caso os participantes tenham pouca experiência com avaliação de riscos. Devem ser registrados também os detalhes da explanação, incluindo premissas, justificando os níveis atribuídos. Os riscos com probabilidade e impacto baixos podem ser apenas incluídos em uma lista de observação, para ser monitorados. Essa avaliação deve ser realizada de acordo com o que foi estabelecido no Plano de Gerenciamento de Riscos.
- *Matriz de probabilidade e impacto:* deve-se utilizar a matriz definida ou adaptada no planejamento do gerenciamento de riscos para classificar os riscos de acordo com a sua prioridade (alta, moderada ou baixa). A pontuação do risco ajuda a orientar as respostas aos riscos. Por exemplo: se ocorrerem os riscos que geram impacto negativo nos objetivos (ameaças), e estiverem na zona de alto risco da matriz, podem exigir agressivas estratégias de resposta e priorização das ações. As ameaças classificadas como de baixo risco podem não requerer uma ação proativa da gerência, além de sua inclusão em uma lista para observação ou da sua adição a uma reserva para contingências.
- *Avaliação da qualidade dos dados sobre riscos:* avalia-se o grau de utilidade dos dados sobre riscos disponíveis para o gerenciamento de riscos, examinando-se o grau em que o risco é compreendido, a exatidão, a qualidade, a confiabilidade e a integridade desses dados. O uso de dados de baixa qualidade pode conduzir a uma análise qualitativa de pouca utilidade para o projeto, sendo necessário recolher dados melhores, o que frequentemente é difícil e consome mais tempo e recursos do que o originalmente planejado.
- *Categorização dos riscos:* categorizar os riscos por fontes, pela área do projeto afetada (por exemplo, usando a WBS) ou outra categoria útil (por exemplo, fase do

projeto), para determinar as áreas do projeto mais expostas aos efeitos da incerteza. O agrupamento de riscos segundo causas-base comuns pode conduzir ao desenvolvimento de respostas mais eficazes aos riscos.

- *Avaliação da urgência do risco*: riscos que requerem respostas a curto prazo podem ser considerados mais urgentes. Os indicadores de prioridade podem incluir o tempo para dar uma resposta ao risco, sintomas, sinais de advertência e avaliação de risco.

### 2.1.3.3 SAÍDAS

As principais saídas desse processo consistem nas seguintes atualizações no Registro de Riscos, que passam a compor o Plano de Gerenciamento do Projeto:

- *Lista de riscos priorizados*: riscos priorizados, por exemplo, com base na matriz de probabilidade e impacto. O resultado dessa priorização será útil para que o gerente de projeto possa focalizar a atenção nos riscos de maior significado e cujas respostas possam conduzir a melhores resultados para o projeto. Os riscos podem ser priorizados separadamente para custo, tempo, escopo e qualidade, pois a organização pode valorizar mais um objetivo do que outro.
- *Riscos agrupados por categoria*: riscos categorizados para descobrir causas comuns ou áreas do projeto que requerem atenção particular, com o objetivo de melhorar a eficácia das respostas aos riscos.
- *Lista de riscos que exigem resposta a curto prazo*: riscos agrupados em função da urgência da resposta, compreendendo os que exigem resposta urgente e os que podem ser tratados em data posterior.
- *Lista dos riscos para análise e resposta adicionais*: riscos que podem precisar de análise adicional, inclusive a análise quantitativa do risco, assim como ação de resposta.
- *Listas de observação de riscos de baixa prioridade*: riscos que não foram considerados importantes podem ficar numa lista de observação, para ser continuamente monitorados.
- *Tendências dos resultados da análise qualitativa do risco*: tendência a riscos específicos evidenciada por meio da repetição do processo de análise.

Na versão do PMBOK (2004), as mudanças mais representativas relacionam-se à introdução das técnicas de categorização dos riscos e de avaliação da urgência do risco, que não estavam presentes na versão anterior (de 2000).

## **2.1.4 ANÁLISE QUANTITATIVA DE RISCOS**

Consiste no processo de análise numérica da probabilidade de ocorrência de cada risco identificado e sua conseqüência para os objetivos do projeto, e apresenta uma abordagem quantitativa, para subsidiar decisões na presença da incerteza. Esse processo geralmente segue o processo de análise qualitativa dos riscos, embora gerentes de risco mais experientes às vezes o executem diretamente após a identificação do risco.

Esse processo nem sempre é fundamental para o desenvolvimento de respostas eficazes ao risco. A disponibilidade de tempo e de orçamento e a necessidade de declarações qualitativas ou quantitativas do risco e seus impactos determinarão os métodos que serão utilizados em um projeto específico.

### **2.1.4.1 ENTRADAS**

- *Ativos de processos organizacionais*: informações sobre projetos anteriores similares já concluídos, estudos de projetos similares, feitos por especialistas em riscos, e bases de dados de riscos que podem estar disponíveis comercialmente ou a partir de fontes proprietárias.
- *Declaração de escopo do projeto*: objetivos, requisitos, entregas, restrições, premissas, estimativas de custos, riscos conhecidos e outras informações sobre o projeto.
- *Plano de gerenciamento de riscos*: funções e responsabilidades para conduzir o gerenciamento de riscos, orçamentos e atividades no cronograma para o gerenciamento de riscos, categorias de riscos, a RBS e a revisão de tolerância ao risco das partes interessadas.
- *Registro de riscos*: riscos identificados, priorizados e agrupados por categoria.
- *Plano de gerenciamento do projeto*: o plano de gerenciamento do cronograma do projeto e o plano de gerenciamento de custos do projeto.

### **2.1.4.2 FERRAMENTAS E TÉCNICAS**

Como técnicas de coleta e representação de dados, podemos ter:

- *Entrevistas*: utilizar essa técnica para quantificar a probabilidade e os impactos dos riscos para os objetivos do projeto, coletando informações de acordo com o tipo de distribuição de probabilidade que será utilizado. A documentação da análise lógica das faixas de risco é fundamental, porque pode fornecer informações sobre a confiabilidade e a credibilidade da análise.
- *Distribuições de probabilidades*: utilizar as distribuições contínuas de probabilidade para representar a incerteza nos valores, tais como duração de atividades do cronograma e custos de componentes do projeto. As distribuições discretas podem ser usadas para representar eventos incertos, tal como o resultado de um teste ou de um cenário possível em uma árvore de decisão.
- *Opinião especializada*: validação dos dados e das técnicas por especialistas internos ou externos à organização, como engenheiros e estatísticos.

Como técnicas de modelagem, podemos ter:

- *Análise de sensibilidade*: examina a extensão em que a incerteza de cada elemento do projeto afeta o objetivo sob exame, quando todos os elementos incertos restantes são fixados em seus valores de linha de base, objetivando determinar os riscos de maior impacto potencial para o projeto.
- *Análise do valor monetário esperado (EMV)*: calcula o resultado médio quando o futuro inclui cenários passíveis de acontecer. A EMV é calculada multiplicando-se o valor de cada resultado possível pela sua probabilidade de ocorrência, e adicionando os dois. Um uso comum desse tipo de análise está na análise da árvore de decisão.
- *Análise da árvore de decisão*: geralmente é estruturada usando o diagrama da árvore de decisão, que apresenta uma situação sob consideração e as implicações de cada uma das escolhas e cenários possíveis, incorporando o custo de cada escolha disponível, as probabilidades de cada cenário possível e o retorno de cada trajeto lógico alternativo. A resolução da árvore de decisão indica a decisão que produz a EMV (ou outra medida útil à organização) para cada alternativa, quando todas as premiações e decisões subseqüentes estiverem quantificadas.

- *Modelagem e simulação*: utiliza um modelo que traduz as incertezas especificadas em um nível detalhado do projeto, em seu impacto potencial nos objetivos do projeto. Geralmente, as simulações são executadas utilizando-se a técnica de Monte Carlo

#### **2.1.4.3 SAÍDAS**

Os registro de riscos ou atualizações podem ser dos tipos:

- *Análise probabilística do projeto*: estimativa de possíveis resultados de cronograma e custo para o projeto, listando-se as datas de conclusão e os custos possíveis, com os níveis de confiança associados. Essas saídas, geralmente expressas como distribuições cumulativas, são usadas juntamente com a tolerância ao risco das partes interessadas, para possibilitar a quantificação das reservas de contingência de custo e tempo necessárias, evitando-se que o risco atinja os objetivos do projeto, permanecendo em um nível aceitável para a organização.
- *Probabilidade de realização dos objetivos de custo e tempo*: estimativa da probabilidade de atingir os objetivos do projeto, de acordo com o plano vigente e com o nível de conhecimento atual sobre os riscos que afetam o projeto.
- *Lista priorizada de riscos quantificados*: riscos que representam a maior ameaça ou oferecem a maior oportunidade para o projeto, incluindo aqueles que requerem a maior contingência de custo e aqueles com maior probabilidade de influenciar o caminho crítico.
- *Tendências nos resultados da análise quantitativa dos riscos*: tendência nos resultados observada à medida que a análise é repetida e leva a conclusões que afetam as respostas ao risco.

Esse processo é executado quando se identifica a necessidade de uma análise adicional por meio da análise qualitativa dos riscos, ou imediatamente após a identificação dos riscos, quando executado por um gerente experiente. As saídas desses dois processos mostram com que o projeto deve se preocupar e conduzem ao planejamento das respostas aos riscos, que vai conduzir as ações que podem ser tomadas para evitar a concretização dos riscos.

#### **2.1.5 PLANEJAMENTO DE RESPOSTAS AOS RISCOS**

Consiste no desenvolvimento de opções e na determinação de ações para ampliar as oportunidades e reduzir as ameaças aos objetivos do projeto. É executado após a análise qualitativa dos riscos, ou após a análise quantitativa dos riscos, quando esta ocorrer.

O planejamento das respostas aos riscos aborda os riscos de acordo com sua prioridade, inserindo-se recursos e atividades no orçamento, no cronograma e no Plano de Gerenciamento do Projeto, se necessário. Inclui, também, a identificação e a atribuição da função de “proprietário do risco” a indivíduos ou grupos, que serão responsáveis por cada resposta ao risco acordada e financiada.

As respostas aos riscos planejadas devem ser apropriadas à gravidade dos riscos, devem pesar os custos com relação aos desafios enfrentados, considerar a probabilidade de êxito, ser realísticas no contexto do projeto e ser aceitas por todas as partes envolvidas, delegando-se cada resposta a um “proprietário” específico. Frequentemente, torna-se necessário selecionar a melhor resposta aos riscos de diversas opções disponíveis.

#### **2.1.5.1 ENTRADAS**

- *Plano de gerenciamento de riscos*: funções e responsabilidades para conduzir o gerenciamento de riscos, definições da análise de riscos, limites para riscos baixos, moderados e altos, e o tempo e o orçamento necessários para condução do gerenciamento de riscos no projeto.
- *Registro de riscos*: riscos identificados, categorizados e priorizados, riscos que requerem resposta imediata, lista de riscos de baixa prioridade, causas dos riscos, tendências nos resultados da análise qualitativa dos riscos, lista de respostas potenciais, proprietários dos riscos, sintomas e sinais de alerta no desenvolvimento das respostas aos riscos.

#### **2.1.5.2 FERRAMENTAS E TÉCNICAS**

Deve ser selecionada a estratégia ou o conjunto de estratégias com maior probabilidade de ser eficaz para cada risco, utilizando-se, por exemplo, ferramentas de decisão tais como a análise da árvore de decisão. Em seguida, devem ser desenvolvidas ações específicas para implementá-la. Pode ser desenvolvido um plano de contingências a ser executado se a estratégia selecionada não for eficaz ou se um risco aceito vier a ocorrer. Esse plano envolve a identificação

das condições, que poderão provocar sua execução e a alocação de reservas de custo e prazo. Seguem as descrições das estratégias para ameaças e oportunidades:

- Estratégias para riscos negativos ou ameaças
  - *Prevenir*: mudar o Plano de Gerenciamento do Projeto para eliminar ameaças, com vistas a proteger os objetivos do projeto de seu impacto, ou para flexibilizar o objetivo sob ameaça, como, por exemplo, estender o cronograma ou reduzir o escopo.
  - *Transferir*: passar o impacto negativo de um risco, assim como sua responsabilidade, a um terceiro, apenas mudando a responsabilidade de seu gerenciamento para outra parte, sem, no entanto, eliminá-lo.
  - *Mitigar*: reduzir a probabilidade e/ou o impacto de um evento adverso de risco a um limite aceitável. Quando não for possível reduzir a probabilidade de ocorrência, uma resposta de mitigação pode atacar o impacto do risco, concentrando-se nos elementos que determinam a gravidade.
- Estratégias para riscos positivos ou oportunidades
  - *Explorar*: assegurar que a oportunidade seja concretizada por meio da eliminação da incerteza, associada a um risco em particular.
  - *Compartilhar*: atribuir a propriedade a terceiros que possam capturar melhor a oportunidade para o benefício do projeto.
  - *Melhorar*: aumentar a probabilidade e/ou os impactos positivos da oportunidade, por meio da identificação e maximização dos principais acionadores desses riscos de impacto positivo. Procurar facilitar ou fortalecer a causa da oportunidade e reforçar as condições de acionamento para aumentar a probabilidade e direcionar os acionadores do impacto, procurando-se aumentar a suscetibilidade do projeto à oportunidade.
- Estratégias para ameaças e oportunidades
  - *Aceitação*: aceitar os riscos com relação aos quais a equipe de projeto decidiu não mudar o plano do projeto para tratá-los ou é incapaz de identificar outra estratégia de resposta adequada. A aceitação pode ser

passiva ou ativa. A primeira não exige nenhuma ação, deixando a equipe do projeto reagir aos riscos à medida que eles ocorrem, enquanto a segunda consiste em estabelecer uma reserva para contingências.

- *Estratégia para respostas de contingência*: fazer um plano de respostas para ser executado somente em certas condições predefinidas. As condições de alerta que provocam a resposta de contingência devem ser acompanhadas.

### **2.1.5.3 SAÍDAS**

Como principais saídas, temos: o Registro de Riscos, o Plano de Gerenciamento do Projeto, e acordos contratuais relacionados a riscos.

O Registro de Riscos é atualizado por meio da inclusão das respostas escolhidas e acordadas. O documento contém os seguintes componentes:

- Riscos identificados: os riscos, suas descrições, as áreas do projeto afetada (por exemplo, elemento de WBS), suas causas e como podem afetar os objetivos do projeto.
- Proprietários do risco e responsabilidades a eles atribuídas.
- Resultados dos processos de análise qualitativa e quantitativa dos riscos, incluindo a lista priorizada dos riscos e a análise probabilística do projeto.
- Estratégias de respostas acordadas.
- Ações específicas para implementação da estratégia de resposta escolhida.
- O nível do risco residual esperado como remanescente, depois que as ações forem executadas.
- Sintomas e sinais de alerta da ocorrência do risco.
- Orçamento e atividades no cronograma necessários para se implementar as respostas selecionadas.
- Reservas para contingências de prazo e custos, determinadas para atender à tolerância a riscos das partes interessadas.



- Planos de contingência e gatilhos que acionam sua execução.
- Planos alternativos para ser utilizados como uma reação a um risco que ocorreu, e cuja resposta principal foi inadequada.
- Riscos residuais esperados como remanescentes após a realização das respostas planejadas, além daqueles que foram aceitos deliberadamente.
- Riscos secundários que surgem como resultado direto da implementação de uma resposta a riscos.
- Reservas para contingências que são calculadas com base na análise quantitativa dos limites de riscos do projeto e da organização.

O Plano de Gerenciamento do Projeto é atualizado por meio da adição das ações de resposta aos riscos acordadas, objetivando-se assegurar sua implementação e monitoramento, como parte do projeto em andamento. O planejamento de respostas aos riscos deve sensibilizar os processos adequados de outras áreas de conhecimento, como o orçamento e o cronograma do projeto.

Os acordos contratuais relacionados a riscos são dos tipos contrato de seguro, serviços e outros itens, que podem ser preparados para especificar a responsabilidade de uma das partes por riscos específicos, se vierem a ocorrer.

No PMBOK (2004), as estratégias para responder aos riscos foram separadas em estratégias para riscos negativos ou ameaças e estratégias para riscos positivos ou oportunidades, dando-se maior destaque a este último tipo de risco.

### **2.1.6 MONITORAMENTO E CONTROLE DE RISCOS**

O monitoramento e controle dos riscos consiste no processo de identificar, analisar e planejar novos riscos que surgem no decorrer do projeto e acompanhar os riscos identificados e residuais, monitorando-se as condições de acionamento dos planos de contingência e garantindo-se a execução das respostas aos riscos, além de avaliar sua eficácia. As respostas aos riscos planejadas, que são incluídas no Plano de Gerenciamento do Projeto, são executadas durante o ciclo de vida do projeto, e o trabalho do projeto deve ser continuamente monitorado, para identificação de novos riscos e mudanças nos riscos.

Esse processo aplica técnicas tal como a análise das tendências e da variação, que requerem o uso de dados de desempenho gerados durante a execução do projeto, a fim de verificar a ocorrência de mudanças no estado dos riscos.

O proprietário do risco deve informar periodicamente ao gerente de projeto acerca da eficácia do plano, assim como qualquer efeito inesperado e correções necessárias ao longo do projeto, para responder apropriadamente ao risco. Esse processo pode envolver a escolha de estratégias alternativas, a implementação de um plano de contingência ou emergência, a implementação de ações corretivas ou a modificação do Plano de Gerenciamento do Projeto. Inclui também a atualização dos Ativos de processos organizacionais, inclusive das bases de dados de lições aprendidas e dos modelos de gerenciamento de riscos, para benefício de projetos futuros.

#### **2.1.6.1 ENTRADAS**

- *Plano de gerenciamento de riscos*: inclui a alocação de pessoas, proprietários dos riscos, o tempo e outros recursos para conduzir o gerenciamento de riscos no projeto.
- *Registro de riscos*: envolve riscos identificados e seus proprietários, respostas acordadas, ações de implementação, sintomas e sinais de alerta, riscos secundários e residuais, riscos de baixa prioridade e que fazem parte da lista de observação e reservas de contingência de custo e prazo.
- *Solicitações de mudanças aprovadas*: envolvem modificações tais como métodos de trabalho, termos contratuais, escopo e cronograma que foram aprovadas e possam gerar riscos ou mudanças em riscos identificados, sendo necessária sua análise em relação aos efeitos no Registro dos Riscos, no Plano de Respostas a Riscos ou no Plano de Gerenciamento de Riscos. Todas as mudanças devem ser formalmente documentadas.
- *Informação sobre o desempenho do trabalho*: situação das entregas do projeto, ações corretivas e relatórios de desempenho.
- *Relatórios de desempenho*: desempenho do trabalho do projeto, como uma análise que pode influenciar os processos de gerenciamento de riscos.

#### **2.1.6.2 FERRAMENTAS E TÉCNICAS**

- *Reavaliação dos riscos*: reavaliar os riscos do projeto regularmente nas reuniões sobre o andamento do projeto. A quantidade e os detalhes de repetição apropriados dependem de como o projeto progride com relação aos seus objetivos, levando-se em conta o surgimento de novos riscos e a inadequação do impacto esperado ou da resposta planejada para determinados riscos.
- *Auditorias de riscos*: examinar e documentar a eficácia das respostas aos riscos identificados e suas causas, assim como a eficácia do processo de gerenciamento de riscos.
- *Análise das variações e tendências*: revisar as tendências da execução do projeto por meio dos dados do desempenho do projeto, podendo ser utilizada a análise de valor agregado ou outros métodos de análise das variações e tendências do projeto. Os resultados dessas análises podem prever os eventuais desvios de custo e cronograma ao final do projeto em relação à linha de base, os quais podem indicar o impacto potencial de ameaças e oportunidades.
- *Medição do desempenho técnico*: comparar as realizações técnicas durante a execução do projeto, com o que foi previsto no cronograma do projeto; os desvios encontrados podem representar riscos para a realização do escopo do projeto.
- *Análise das reservas*: comparar a quantidade restante das reservas para contingências com a quantidade restante de riscos em dado momento do projeto, a fim de determinar se a reserva restante está adequada.
- *Reuniões de andamento*: o acompanhamento dos riscos do projeto pode integrar as pautas das reuniões periódicas de andamento do projeto.

### 2.1.6.3 SAÍDAS

- *Registro de riscos*: atualização por meio da inclusão dos resultados das reavaliações dos riscos, auditorias e revisões periódicas, podendo incluir atualizações do *status*, de probabilidades, impactos, prioridades, planos de respostas, propriedades e outros elementos. Essas informações serão utilizadas no encerramento do projeto.

- *Mudanças solicitadas*: a implementação do plano de contingências ou plano de soluções alternativas frequentemente resulta em uma requisição de mudança no Plano de Gerenciamento do Projeto, para responder aos riscos.
- *Ações corretivas recomendadas*: incluem os planos de contingência e os planos de soluções alternativas, que são respostas não planejadas inicialmente, porém necessárias para tratar riscos emergentes não previamente identificados, ou aceitos passivamente. Essas soluções devem ser adequadamente documentadas.
- *Ações preventivas recomendadas*: destinadas a assegurar a conformidade com o Plano de Gerenciamento do Projeto.
- *Ativos de processos organizacionais*: atualização por meio de inclusão das informações do projeto que poderão ser úteis a outros projetos, como lições aprendidas, versão final do Registro dos Riscos, matriz de impacto e probabilidade, listas de verificações e RBSs do Plano de Gerenciamento de Riscos. Além disso, pode ser necessário alterar os modelos do Plano de Gerenciamento de Riscos, da matriz de probabilidade e impacto e do Registro dos Riscos.
- *Plano de gerenciamento do projeto*: atualização por meio da inclusão das solicitações de mudanças aprovadas e que venham a gerar impacto no plano.

Na versão 2004, foi dada uma maior visibilidade da interação desse processo com outros da área de conhecimento Integração do Gerenciamento de Projetos.

## **2.2 GERENCIAMENTO DE RISCOS NO PADRÃO AS/NZS 4360**

O *Australian and New Zealand Standard for Risk Management 4360:2004* é um padrão internacional para o gerenciamento de riscos, que fornece diretrizes para a estruturação e implementação de uma estratégia efetiva para o gerenciamento de riscos (AS/NZS 4360: 2004). Enfatiza que essa estruturação varia de acordo com as necessidades da organização, seus objetivos específicos, seus produtos e serviços, bem como suas práticas e seus processos.

A primeira edição desse padrão foi publicada em 1995, tendo sido desenvolvida para atender à necessidade de um apoio prático para a aplicação do gerenciamento de riscos no setor público e em organizações do setor privado. Essa foi a primeira norma de âmbito

mundial sobre sistemas de gerenciamento de riscos. Em 1999, foi publicada a segunda versão, e em 2004, a terceira. Esta última versão incorpora o aprendizado adquirido por meio da aplicação da versão de 1999 e o pensamento atual sobre o gerenciamento de riscos, destacando-se maior ênfase à inclusão de práticas de gerenciamento de riscos na cultura e nos processos organizacionais, e também no gerenciamento de ganhos potenciais, assim como de perdas potenciais. Além disso, os exemplos indicativos foram expandidos e transformados no manual *Risk Management Guidelines* (HB 4360, 2004).

Para esse padrão, o gerenciamento de riscos consiste em atingir o equilíbrio apropriado entre realizar as oportunidades para obter ganhos e minimizar perdas. É um processo iterativo, constituído de passos bem definidos, que, quando executados, conduzem à melhoria contínua no processo decisório e no desempenho, por meio de uma melhor compreensão dos riscos e dos seus impactos.

A finalidade desse padrão é definir um *framework* genérico para o estabelecimento do contexto da gerência de riscos e para a identificação, a análise, a avaliação, o tratamento, a monitoração e a comunicação dos riscos na organização. A norma dá ênfase à importância da difusão da cultura de gerenciamento de riscos em toda a organização e seus processos, e pode ser aplicada em qualquer organização, independentemente do tipo de indústria ou do setor econômico. O processo de gerenciamento de riscos será influenciado pelas necessidades da organização, seus objetivos, seus produtos e serviços, processos e práticas.

O objetivo desse padrão é prover um guia para que as organizações consigam:

- Uma base mais confiável e rigorosa para o processo decisório e para o planejamento;
- Uma melhor identificação de oportunidades e ameaças;
- Agregar valor a partir da incerteza e da variedade;
- Um gerenciamento proativo, em vez de reativo;
- Reduzir a perda decorrente do risco e do custo;
- Maior confiança por parte dos *stakeholders*;
- Maior conformidade com a legislação;
- Melhor governança corporativa.

Os principais elementos do gerenciamento de riscos são ilustrados na Figura 2.2.

- *Comunicar e orientar*: facilitar a comunicação entre os envolvidos internos e externos, conforme seja apropriado, em cada estágio do processo de gerenciamento de riscos e de acordo com o processo como um todo.
- *Estabelecer o contexto*: definir o contexto em que está inserido o gerenciamento de riscos, definindo os critérios de avaliação e a estrutura de análise dos riscos.
- *Identificar riscos*: identificar os eventos incertos, que envolvem o projeto, e quando, onde, porque e como podem afetá-lo.
- *Analisar riscos*: analisar os riscos, considerando suas fontes, conseqüências positivas e negativas, probabilidade de ocorrência e nível de risco.
- *Avaliar riscos*: comparar os níveis de risco com os critérios preestabelecidos para tomar decisões sobre a extensão e natureza do tratamento requerido e sobre as prioridades.
- *Tratar riscos*: desenvolver e implementar estratégias e planos de ação para ampliar os possíveis benefícios e reduzir os prejuízos decorrentes dos riscos.
- *Monitorar e revisar*: monitorar a efetividade de todos os passos do processo para a melhoria contínua, e monitorar os riscos e a efetividade do tratamento.

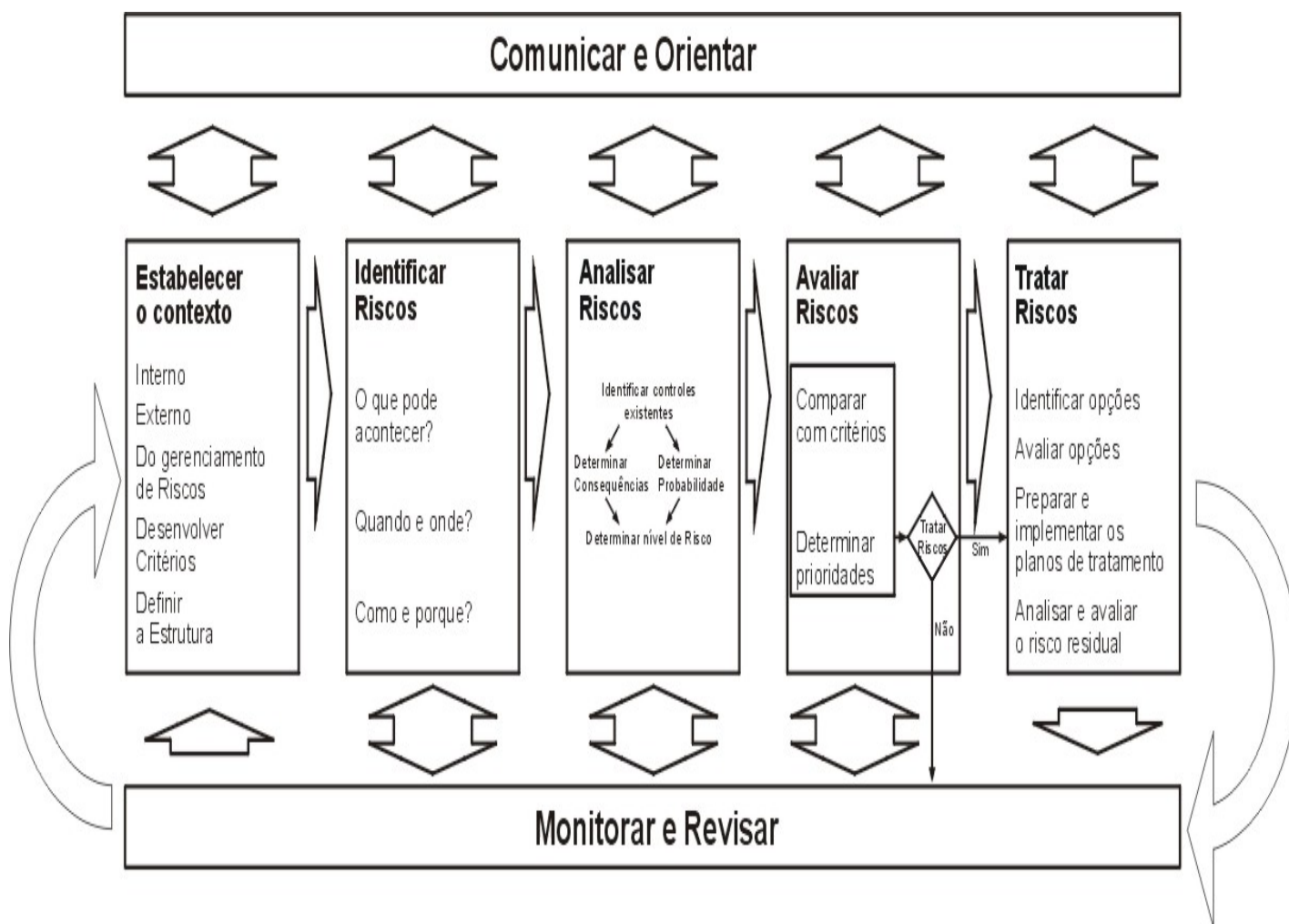
A seguir são detalhados os principais elementos que compõem o processo de gerenciamento de riscos do padrão AS/NZS 4360:2004.

### **2.2.1 COMUNICAR E ORIENTAR**

É importante desenvolver um plano de comunicação entre os *stakeholders* internos e externos em um estágio inicial do processo, contendo questões relacionadas ao risco em si e ao processo para gerenciá-lo. Esse plano deve especificar a finalidade ou o objetivo da comunicação e quem deve ser consultado, por quem, quando e como.

Em uma organização, uma boa comunicação é essencial para se desenvolver uma cultura em que as dimensões positivas e negativas dos riscos sejam reconhecidas e avaliadas, possibilitando o estabelecimento de uma atitude com relação a riscos. Além disso, a comunicação é importante para que os envolvidos no processo de gerenciamento de riscos compreendam as bases sobre as quais as decisões estão sendo tomadas e a

necessidade de determinadas ações. Uma comunicação inapropriada pode conduzir à quebra de confiança ou a um pobre gerenciamento de riscos.



**Figura 2.2 – AS/NZS 4360:2004 – Processo de Gerenciamento de Riscos**

Uma abordagem de consultoria é útil para ajudar a definir o contexto apropriadamente, de maneira a assegurar que os riscos sejam eficazmente identificados, para trazer diversos especialistas com vistas a auxiliar na análise dos riscos, e assegurar que diferentes pontos de vista estejam sendo considerados na avaliação dos riscos, propiciando um adequado gerenciamento de mudanças durante o tratamento dos riscos.

Os elementos essenciais de um plano de comunicação e consultoria são:

- os objetivos da comunicação;
- os participantes, por exemplo, *stakeholders* (grupos ou indivíduos), especialistas ou time de comunicação;

- as perspectivas dos participantes que devem ser consideradas;
- os métodos de comunicação a ser utilizados;
- o processo de avaliação a ser utilizado.

## **2.2.2 ESTABELEECER O CONTEXTO**

Consiste na definição de parâmetros com base nos quais os riscos devem ser gerenciados, na preparação do escopo do processo de gerenciamento de riscos. É importante garantir que os objetivos definidos levem em consideração o ambiente organizacional e o ambiente externo. A seguir são detalhados os passos para a definição do contexto: (i) estabelecer o contexto externo; (ii) estabelecer o contexto interno; (iii) estabelecer o contexto do gerenciamento de riscos; (iv) desenvolver critérios para riscos; e (v) definir estrutura para o resto do processo.

### **2.2.2.1 ESTABELEECER O CONTEXTO EXTERNO**

Define o contexto externo no qual a organização atua, e o relacionamento entre a organização e o ambiente externo. São exemplos disso:

- o ambiente de negócios, o social, o competitivo, o financeiro e o político;
- as forças e fraquezas da organização e as oportunidades e ameaças;
- *stakeholders* externos;
- elementos-chave do negócio.

É particularmente importante levar em conta a percepção e os valores dos *stakeholders* externos, assim como garantir que seus objetivos sejam considerados no desenvolvimento dos critérios para o gerenciamento dos riscos, e que as ameaças e oportunidades externas sejam apropriadamente consideradas.

### **2.2.2.2 ESTABELEECER O CONTEXTO INTERNO**

Estabelecer o contexto interno consiste na compreensão da organização no tocante a:

- cultura;
- *stakeholders* internos;
- estrutura;



- capacidade em termos de recursos logísticos, como pessoas, sistemas, processos e capital;
- metas e objetivos, e as estratégias para atingi-los.

Os fatores acima são importantes porque:

- o gerenciamento de riscos acontece no contexto das metas e dos objetivos da organização;
- os principais riscos para algumas organizações se devem ao fato de que elas falham em atingir seus objetivos estratégicos, de negócios e de projetos;
- a política organizacional, os objetivos e interesses ajudam a definir a política de riscos;
- objetivos e critérios específicos de um projeto ou atividade devem ser considerados à luz dos objetivos da organização como um todo.

### **2.2.2.3 ESTABELEECER O CONTEXTO DO GERENCIAMENTO DE RISCOS**

Devem ser estabelecidos metas, objetivos, estratégias, escopo e parâmetros. O processo deve levar em conta as necessidades de balanceamento de custos, benefícios e oportunidades. Devem ser definidos os papéis e as responsabilidades das diversas partes no processo de gerenciamento de riscos. A definição da abrangência do processo de gerenciamento de riscos compreende:

- definir o processo organizacional e estabelecer suas metas e objetivos;
- especificar as naturezas das decisões que devem ser tomadas; e
- definir a abrangência das atividades de gerenciamento de riscos que devem ser executadas.

### **2.2.2.4 DESENVOLVER CRITÉRIOS PARA RISCOS**

Desenvolver critérios para riscos consiste em decidir os critérios sob os quais os riscos serão avaliados, refletindo o contexto citado nos itens anteriores. Os critérios gerais para o processo decisório são desenvolvidos como parte da definição do contexto, e podem ser refinados à medida que riscos específicos são identificados e as técnicas de análise são selecionadas. Vejamos alguns critérios a serem considerados:

- os tipos de consequência a ser considerados;

- como a probabilidade será definida;
- como será determinado se o risco está no nível que exigirá atividades de tratamento.

Os requisitos da organização e dos *stakeholders* relevantes podem ser usados para estabelecer um conjunto de medidas críticas de desempenho, que podem fornecer critérios específicos para avaliação dos riscos nos estágios mais adiantados.

#### **2.2.2.5 DEFINIR ESTRUTURA PARA O PROCESSO**

Uma estrutura deve compreender um conjunto de elementos ou passos que viabilize que os principais riscos sejam devidamente considerados. Essa estrutura depende da natureza dos riscos e do escopo do projeto, do processo ou da atividade.

### **2.2.3 IDENTIFICAR RISCOS**

Identificar riscos consiste em reconhecer os riscos a serem gerenciados. Um processo de identificação bem estruturado é crítico, porque riscos não identificados nesse ponto podem ser excluídos de uma análise posterior. A identificação deve considerar os riscos independentemente de estarem ou não sob o controle da organização. A identificação deve utilizar os elementos definidos no estabelecimento do contexto do gerenciamento de riscos. A seguir são detalhados passos importantes na identificação dos riscos: (i) identificar fontes de riscos; (ii) considerar as causas e cenários; (iii) informação para identificação de riscos; e (iv) abordagens para identificação de riscos.

#### **2.2.3.1 IDENTIFICAR FONTES DE RISCOS**

O objetivo é gerar uma lista de fontes de riscos e eventos que podem gerar impacto sobre cada um dos objetivos identificados no contexto. O ponto de partida para a identificação dos riscos compreende a informação histórica disponível e a posterior discussão com os *stakeholders* sobre questões atuais e históricas. Deve ser produzido um registro dos riscos.

#### **2.2.3.2 CONSIDERAR AS CAUSAS E CENÁRIOS**

Há várias formas de ocorrência de um evento, e as causas importantes devem ser consideradas. Deve-se definir por que e como o risco pode ocorrer.

### **2.2.3.3 INFORMAÇÃO PARA A IDENTIFICAÇÃO DE RISCOS**

Informação de boa qualidade é essencial para a identificação dos riscos. O ponto de partida para a identificação dos riscos podem ser informações históricas, que devem ser discutidas com os *stakeholders*.

É necessário que as pessoas envolvidas na identificação dos riscos tenham conhecimento dos aspectos do problema em questão. Identificar riscos pode também requerer imaginação e experiência. O envolvimento dos *stakeholders* também ajuda a construir um compromisso com o processo, assim como a garantir que diferentes *stakeholders* sejam considerados, quando apropriado.

### **2.2.3.4 ABORDAGENS PARA A IDENTIFICAÇÃO DE RISCOS**

A abordagem ou conjunto de abordagens a serem utilizadas depende do contexto do gerenciamento de riscos. Podem ser consideradas as seguintes abordagens: *brainstorming*, técnicas estruturadas, análise de cenários e *checklist*.

## **2.2.4 ANALISAR RISCOS**

Analisar riscos consiste em estabelecer um entendimento do nível de riscos e de sua natureza, auxiliando a definir que riscos devem ser tratados e quais as estratégias mais apropriadas, levando-se em conta os custos respectivos. A análise dos riscos leva em conta suas fontes, as conseqüências positivas e negativas de sua ocorrência e a probabilidade de ocorrer tais conseqüências. Devem ser identificados os fatores que podem afetar a conseqüência e a probabilidade. O nível de riscos é determinado pela combinação da conseqüência com a probabilidade. As escalas apropriadas e os métodos para combiná-las devem ser consistentes com os critérios definidos ao se estabelecer o contexto. Para uma análise mais técnica, a natureza dos dados e as saídas necessárias ditarão os métodos a serem requeridos.

Geralmente, o processo de análise tem início com uma análise qualitativa para a obtenção de uma compreensão geral sobre os riscos. Quando necessário, será realizada a

análise quantitativa, para um maior nível de detalhe. Porém, não se deve supor que a análise quantitativa é superior à qualitativa. É mais apropriado escolher a abordagem mais adequada a cada situação. A seguir, são detalhados elementos importantes na análise dos riscos: (i) avaliar controles existentes; (ii) conseqüências e probabilidades; e (iii) tipos de análise.

#### **2.2.4.1 AVALIAR CONTROLES EXISTENTES**

Avaliar controles existentes significa identificar processos, dispositivos ou práticas que agem para minimizar os riscos negativos e aumentar a oportunidade dos riscos positivos e avaliar seus pontos fortes e fracos.

#### **2.2.4.2 AVALIAR CONSEQÜÊNCIAS E PROBABILIDADES**

O levantamento de conseqüências e probabilidades consiste na avaliação da extensão das conseqüências de um evento em relação aos objetivos do projeto, caso ele ocorra, e em sua probabilidade de ocorrer. Um evento pode acarretar múltiplas conseqüências e afetar diferentes objetivos. A conseqüência e a probabilidade devem ser estimadas, usando informações históricas de boa qualidade e, quando estas não estiverem disponíveis, devem ser feitas estimativas que venham a refletir o grau de crença de que determinado evento irá ocorrer. Informações e técnicas devem ser utilizadas para analisar esses dois atributos do risco. As fontes de informação podem incluir:

- registros passados;
- práticas e experiências;
- literatura publicada;
- pesquisas de mercado;
- resultados de consultorias;
- experimentos e protótipos;
- julgamento de especialistas.

As técnicas podem incluir:

- entrevistas estruturadas com especialistas experientes na área de interesse;
- uso de grupos multidisciplinares de especialistas;
- avaliações individuais, por meio de questionários;
- uso de modelos e simulações.

As formas de expressão da consequência e da probabilidade e de como esses fatores são combinados determinam o nível de risco, que varia de acordo com o tipo do risco e o propósito para o qual a avaliação do risco será utilizada. A incerteza e a variação da consequência e da probabilidade devem ser consideradas na análise, e efetivamente comunicadas.

### **2.2.4.3 TIPOS DE ANÁLISE**

A análise de risco pode ser do tipo qualitativa, semi-quantitativa ou quantitativa, ou uma combinação desses tipos. A escolha do método de análise depende do propósito e das informações, assim como dos dados e recursos disponíveis. A ordem de complexidade e custos é ascendente, da qualitativa para a quantitativa. Na prática, a análise qualitativa é primeiramente utilizada para obtenção de uma compreensão sobre o nível de riscos e sobre os principais riscos. A forma da análise deve ser consistente com os critérios estabelecidos como parte da definição do contexto.

#### **2.2.4.3.1 ANÁLISE QUALITATIVA**

A análise qualitativa utiliza palavras para descrever a magnitude das consequências, assim como da probabilidade de tais consequências ocorrerem. As escalas podem ser adaptadas ou ajustadas de acordo com as circunstâncias, e diferentes descrições podem ser utilizadas para diferentes riscos. A análise qualitativa pode ser utilizada nas seguintes situações:

- quando o nível de risco não justificar o tempo e os recursos necessários para uma análise numérica;
- como uma atividade inicial de seleção, para identificar os riscos que requeiram uma análise mais detalhada;
- quando esse tipo de análise for apropriado para o processo decisório;
- quando os dados numéricos e os recursos forem inadequados para o uso da análise quantitativa.

Seguem-se exemplos de métodos qualitativos:

- avaliação utilizando grupos multidisciplinares;
- julgamento de especialistas;
- entrevistas estruturadas e questionários.

#### **2.2.4.3.2 ANÁLISE SEMI-QUANTITATIVA**

Na análise semi-quantitativa, são atribuídos valores às escalas qualitativas, com o objetivo de se produzir uma escala maior do que a geralmente obtida na análise qualitativa, mas que não chega aos níveis de valores realísticos da análise quantitativa. Um valor alocado a cada descrição pode não representar um relacionamento exato com o valor real de suas conseqüências ou de sua probabilidade. Portanto, os valores somente devem ser combinados a partir de uma fórmula que reconheça as limitações dos tipos das escalas utilizadas. Deve-se ter cuidado com o uso da análise semi-quantitativa, pois as escalas escolhidas podem não refletir apropriadamente as relações, o que pode gerar inconsistências ou saídas inapropriadas.

#### **2.2.4.3.3 ANÁLISE QUANTITATIVA**

A análise quantitativa utiliza valores numéricos para conseqüências e probabilidade, usando dados de fontes variadas. A qualidade da análise depende da exatidão e integridade dos valores numéricos e da validade do modelo utilizado. As conseqüências podem ser determinadas por meio da modelagem dos resultados de um evento ou de um conjunto de eventos, ou pela dedução através de estudos experimentais ou dados passados. Essas conseqüências podem ser expressas em termos monetários, técnicos ou com base em qualquer outro critério estabelecido na definição do contexto. Seguem exemplos de métodos quantitativos:

- análise de conseqüências;
- análise estatística de dados históricos;
- diagramas de influência;
- análise de rede;
- análise de probabilidade;
- simulação e modelagem por computador.

#### **2.2.5 AVALIAR RISCOS**

Consiste em tomar decisões baseadas nos resultados da análise do risco, sobre quais riscos precisam de tratamento e qual será a ordem de prioridade para o tratamento. Envolve a comparação do nível de risco encontrado durante o processo de análise com os critérios

estabelecidos, no momento em que o contexto foi estabelecido. Devem ser considerados os objetivos da organização e a extensão da oportunidade, que poderá ser gerada.

Para a seleção entre as opções, devem ser feitas associações entre as perdas potenciais e os ganhos potenciais, sendo a escolha apropriada dependente do contexto da organização. As decisões devem considerar um contexto mais amplo do risco e levar em conta a tolerância ao risco das partes envolvidas. Em algumas circunstâncias, a avaliação do risco pode conduzir à decisão de empreender uma análise adicional.

A seguir são detalhados alguns elementos essenciais na avaliação dos riscos: (i) tipos de critério de avaliação; (ii) avaliação a partir da análise qualitativa; (iii) risco tolerável; (iv) julgamento implícito em critérios; e (v) critérios de avaliação e eventos históricos.

#### **2.2.5.1 TIPOS DE CRITÉRIO DE AVALIAÇÃO**

Os critérios utilizados para subsidiar decisões devem ser coerentes com o contexto do gerenciamento de riscos, e levar em conta os objetivos da organização, os objetivos do gerenciamento de riscos e a visão dos *stakeholders*. Esses critérios podem ser expressos quantitativa ou qualitativamente.

As decisões podem ser tomadas com base no nível de risco, mas também podem basear-se nos limites especificados em termos de:

- conseqüências especificadas;
- probabilidade de ocorrência de eventos específicos;
- efeito cumulativo de múltiplos eventos; e
- escala de incerteza para os níveis de risco, em um grau de segurança específico.

#### **2.2.5.2 AVALIAÇÃO A PARTIR DA ANÁLISE QUALITATIVA**

As organizações não dispõem de recursos ilimitados para tirar vantagens das oportunidades de lidar com os riscos adversos. Assim sendo, torna-se necessário definir prioridades. A análise qualitativa é usada para definir prioridade ou tratamento baseados no nível de risco. A prioridade também pode ser estabelecida com base na conseqüência isoladamente ou em qualquer outro critério de avaliação (item 2.2.5.1).

Os diferentes níveis de risco em uma matriz de riscos qualitativa são algumas vezes utilizados para definir ações requeridas, e sendo empregados como critério para os riscos. Entretanto, a decisão sobre consequência e probabilidade do risco, e entre os níveis qualitativos do risco é definida na matriz, para atender a circunstâncias particulares. Nesse contexto, matrizes desse tipo tornam-se ferramentas limitadas para subsidiar decisões.

### **2.2.5.3 RISCO TOLERÁVEL**

Torna-se necessário definir quais riscos precisam de tratamento e quais podem ser tolerados em determinadas circunstâncias. Uma abordagem comum consiste em dividir os riscos em três faixas:

- *Faixa superior*: riscos adversos são intoleráveis, medidas de redução do risco são essenciais, independentemente do seu custo.
- *Faixa média*: custos e benefícios são devidamente considerados, enquanto oportunidades são balanceadas em relação às potenciais consequências adversas.
- *Faixa inferior*: riscos positivos ou negativos são insignificantes, ou são tão pequenos que dispensam qualquer medida de tratamento.

### **2.2.5.4 JULGAMENTO IMPLÍCITO EM CRITÉRIOS**

O valor dos julgamentos está implícito em muitos critérios. Estes dependem da familiaridade de um indivíduo com o risco, sua confiança na eficácia dos controles implementados e sua percepção quanto aos riscos e aos benefícios da atividade.

O mesmo risco pode parecer insignificante para uma pessoa, e muito elevado para outra. Os critérios devem representar uma visão objetiva, levando em conta as necessidades de todas as partes afetadas. *A comunicação e a consultoria* podem referir-se a esses pontos (item 2.2.1).

### **2.2.5.5 CRITÉRIOS DE AVALIAÇÃO E EVENTOS HISTÓRICOS**

Os critérios para decisão sobre a necessidade de tratamento de um risco freqüentemente são ajustados com base em eventos similares, já ocorridos. Entretanto, os dados podem ser distorcidos por fatores como:

- grandes incidentes ou catástrofes;



- o declínio de um nível de risco devido ao aumento do controle, fazendo com que os dados históricos possam não ser adequados para controlar a situação;
- mudanças nas atividades ou nas circunstâncias atuais em comparação à situação passada.

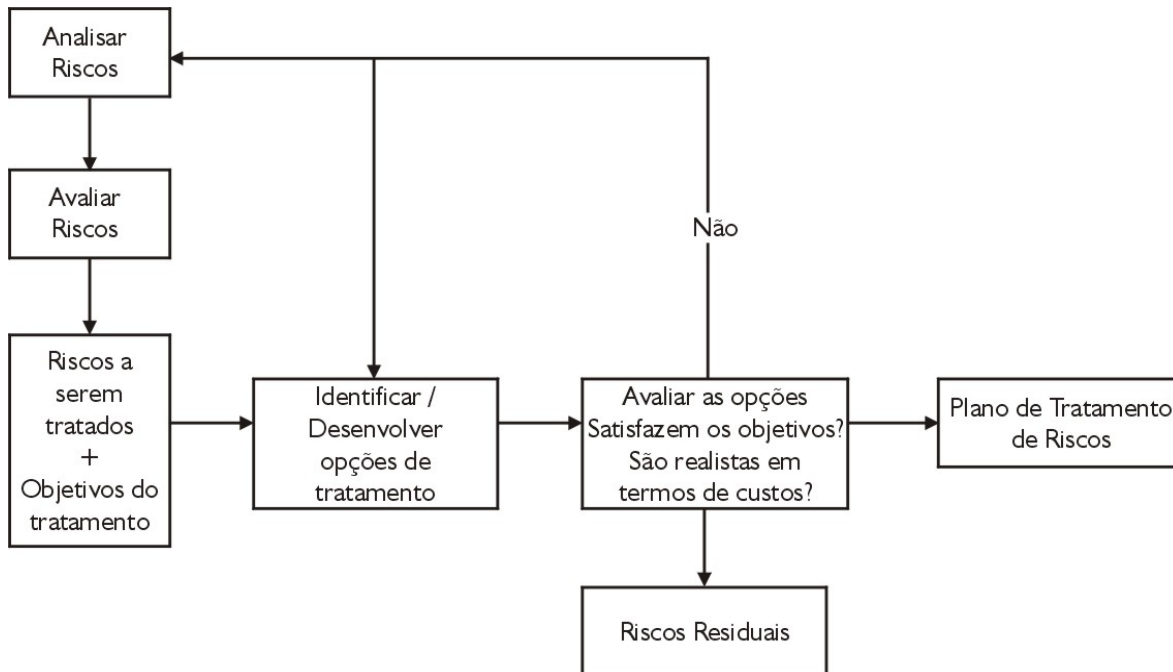
O ajuste dos critérios de avaliação por meio das estimativas históricas do risco pode acarretar os seguintes problemas:

- um risco pode precisar de tratamento em uma circunstância, mas dispensá-lo em outra;
- mesmo tendo sido aceito no passado, um risco pode não ser aceitável no momento atual, utilizando-se os métodos de análise atuais e fazendo-se o exame da tolerância ao risco no contexto atual;
- os riscos são diferentes em situações diferentes (por exemplo, em países diferentes), o que leva a se questionar até que ponto os critérios de avaliação devem ser adaptados à situação e não ser aplicados globalmente.

Em consequência de problemas como esses, devem ser aplicados julgamentos adicionais, além dos dados disponíveis sobre o risco.

### **2.2.6 TRATAR RISCOS**

O tratamento de riscos compreende etapas como (1) identificar as opções de tratamento, (2) avaliar essas opções e (3) preparar e executar planos de tratamento. Não se revela viável, em termos de custos, a implementação de todas as opções de tratamento. Assim sendo, deve ser selecionada a opção ou a combinação de opções mais apropriada. A Figura 2.3 representa o processo de tratamento de riscos e a natureza iterativa da escolha das ações que integrarão o Plano de Tratamento dos Riscos. A seguir são detalhados os principais elementos para a seleção das opções de tratamento dos riscos: (i) identificar opções de tratamento; (ii) avaliar opções de tratamento; (iii) selecionar opções de tratamento; (iv) preparar e implementar planos de tratamento; e (v) riscos residuais.



**Figura 2.3 Processo de Tratamento de Riscos (AS/NZS 4360, 2004)**

### 2.2.6.1 IDENTIFICAR OPÇÕES DE TRATAMENTO

Quando não há guias para o tratamento de um tipo específico de risco, devem ser desenvolvidas as opções de tratamento. Para isso é fundamental a compreensão das causas originais do risco, para que estas – e não apenas o sintoma – também recebam tratamento. A seguir são descritas opções de tratamento para oportunidades e para ameaças.

#### 2.2.6.1.1 IDENTIFICAR OPÇÕES DE TRATAMENTO PARA RISCOS POSITIVOS

Consiste na seleção de opções para o tratamento das oportunidades, conforme explicitado a seguir:

- procurar ativamente uma oportunidade através da decisão de iniciar ou continuar uma atividade que provavelmente irá criá-la ou mantê-la;
- mudar a probabilidade de ocorrência da oportunidade, para aumentar a probabilidade dos ganhos decorrentes;
- mudar as conseqüências, para aumentar a extensão dos ganhos;

- compartilhar a oportunidade, envolvendo uma outra parte, que irá prover capacidades adicionais ou recursos, para aumentar a probabilidade de ocorrência da oportunidade ou a extensão dos ganhos decorrentes; e
- reter a oportunidade residual.

#### **2.2.6.1.2 IDENTIFICAR OPÇÕES DE TRATAMENTO PARA RISCOS NEGATIVOS**

Consiste na seleção de opções para o tratamento de ameaças, que são conceitualmente similares àquelas indicadas para o tratamento das oportunidades, embora a interpretação e as implicações sejam bastante diferentes. As opções incluem:

- evitar o risco através da decisão de não iniciar ou continuar atividades que podem dar causa ao seu surgimento. Essa estratégia será inapropriada, se os indivíduos ou organizações são demasiadamente avessos a riscos;
- mudar a probabilidade de ocorrência do risco, para reduzir a probabilidade das perdas decorrentes;
- mudar as conseqüências, para reduzir a extensão das perdas;
- compartilhar o risco; e
- reter o risco residual.

#### **2.2.6.2 AVALIAR OPÇÕES DE TRATAMENTO**

Consiste em avaliar as opções de tratamento, com o objetivo de selecionar a mais apropriada, comparando os custos envolvidos na implementação de cada uma delas, com os benefícios derivados, porquanto os custos do controle dos riscos devem ser proporcionais aos benefícios obteníveis. É importante que se leve em conta o contexto, assim como a percepção do risco pelas partes interessadas. A seguir, são sugeridos alguns passos para a elaboração de opções de tratamento:

- revisar causas e controles, o que inclui rever a análise do risco, para garantir que ele foi compreendido;
- objetivos do tratamento;
- planejar ações;
- projetar revisões;

- comunicar e implementar.

### **2.2.6.3 SELECIONAR OPÇÕES DE TRATAMENTO**

Por ocasião da seleção das opções de tratamento, devem ser consideradas as seguintes questões:

- alguns benefícios decorrentes do tratamento podem ser mais importantes que outros;
- analisar benefícios quantificáveis e não-quantificáveis;
- considerar benefícios diretos e indiretos e custos associados com o tratamento do risco em diferentes períodos de tempo;
- considerar a incerteza envolvida nas estimativas de benefícios diretos e indiretos e de custos associados;
- a expectativa social, assim como as obrigações legais, pode guiar algumas ações de tratamento dos riscos;
- a análise qualitativa e quantitativa do custo *versus* benefícios.

### **2.2.6.4 PREPARAR E IMPLEMENTAR PLANOS DE TRATAMENTO**

Consiste em documentar como as opções de tratamento selecionadas serão implementadas, devendo incluir:

- ações propostas;
- como as opções selecionadas serão implementadas;
- recursos necessários;
- responsabilidades;
- cronograma;
- orçamento;
- medidas de desempenho;
- necessidade de monitoração e relato;
- mecanismos para monitorar e avaliar a efetividade do tratamento segundo os objetivos.

Os planos de tratamento devem estar integrados com os processos de gerenciamento da organização. O sucesso da implementação desse plano requer um gerenciamento efetivo, com especificação dos métodos escolhidos, atribuição de responsabilidades e a monitoração

de acordo com os critérios especificados. A comunicação é muito importante para a execução do plano de tratamento.

#### **2.2.6.5 RISCOS RESIDUAIS**

Os riscos residuais são aqueles que restam após a implementação do plano de tratamento. É importante que os *stakeholders* estejam cientes da natureza e extensão dos riscos residuais. Esses riscos devem ser documentados e submetidos a monitoração e revisão.

#### **2.2.7 MONITORAR E REVISAR**

Monitorar e revisar fundamenta-se no acompanhamento dos riscos, identificando-se mudanças em fatores que podem afetar a probabilidade e a consequência dos riscos, e comparando-se periodicamente a situação atual com o que foi previsto no Plano de Tratamento. É um dos passos mais importantes do gerenciamento de riscos, pois é necessário monitorar os riscos, a eficácia das estratégias selecionadas para o seu tratamento, e o sistema de gerenciamento utilizado para implementá-las. Além disso, o processo de gerenciamento de riscos como um todo deve ser monitorado, o que envolve a captura das lições aprendidas. Alguns aspectos importantes a serem considerados são: (i) mudanças no contexto e nos riscos; (ii) monitoração e garantia do processo; (iii) medida de desempenho do gerenciamento de riscos; e (iv) análise após o evento.

##### **2.2.7.1 MUDANÇAS NO CONTEXTO E NOS RISCOS**

O processo de gerenciamento de riscos deve guardar sintonia com os processos organizacionais. Revisões periódicas dos riscos e das estratégias de tratamento são particularmente úteis, quando associadas com o planejamento de negócios e com o planejamento estratégico. Quando mudanças organizacionais são planejadas, ou mudanças externas são percebidas, pode haver mudanças:

- no contexto organizacional (por exemplo: objetivos, ambiente externo ou interno ou critérios para os riscos);
- nos riscos e níveis de riscos;
- na efetividade das opções de tratamento selecionadas para os riscos.

### **2.2.7.2 MONITORAÇÃO E GARANTIA DO PROCESSO**

A monitoração e a garantia do processo dizem respeito a monitorar e revisar os riscos e o processo de gerenciamento de riscos, de acordo com uma cuidadosa seleção, já que essas atividades absorvem recursos escassos. Têm prioridade para monitoração:

- altos riscos;
- eventuais falhas nas estratégias de tratamento, especialmente quando podem resultar em conseqüências altas ou freqüentes;
- atividades relacionadas a riscos que têm alta incidência de mudanças;
- critérios de tolerância ao risco, especialmente onde isso resulta em um alto índice de riscos residuais;
- avanços tecnológicos que podem oferecer alternativas mais eficazes, ou de custo mais baixo, para o tratamento de determinado risco.

### **2.2.7.3 MEDIDA DE DESEMPENHO DO GERENCIAMENTO DE RISCOS**

Os indicadores do desempenho são medidas quantitativas do nível de desempenho de um item ou de uma atividade. Esses indicadores devem ser mensuráveis e apropriados às unidades de negócio individuais, fornecendo-se uma base para a melhoria contínua.

As organizações devem usar seus processos de planejamento com o propósito de gerar medidas de desempenho para o processo de gerenciamento de riscos. Esses indicadores devem refletir os objetivos organizacionais definidos, quando o contexto foi estabelecido no início do processo. Os indicadores de desempenho devem monitorar resultados (por exemplo: perdas específicas ou ganhos) ou processos (por exemplo: o desempenho consistente de procedimentos de tratamento do risco).

Na definição dos indicadores, deve ser levado em conta se:

- os indicadores podem ser medidos de maneira razoável;
- os indicadores são eficientes em termos de demanda de tempo, esforço e recursos;
- o processo de medição encoraja ou facilita comportamentos desejáveis e não motiva comportamentos indesejáveis (como a fabricação de dados);
- os envolvidos compreendem o processo de medição e os benefícios esperados;

- os resultados são capturados e relatados de uma maneira que irá facilitar o aprendizado e a melhoria do processo.

Alguns exemplos de indicadores de desempenho úteis para o gerenciamento de riscos:

- declínio no custo total dos riscos;
- progresso com relação a um objetivo organizacional específico;
- a extensão na qual estão sendo executadas as recomendações para o tratamento dos riscos.

#### **2.2.7.4 ANÁLISE APÓS O EVENTO**

A análise após o evento consiste na revisão dos eventos após sua ocorrência, sejam eventos de fracasso ou de sucesso. Esses eventos oferecem uma oportunidade para uma análise de como o processo de gerenciamento de riscos pode ser melhorado. A intenção deve ser adotar um processo sistemático, para se rever as causas dos sucessos e das falhas, para se aprender lições úteis para a organização. Seguem algumas questões a ser analisadas:

- Os riscos envolvidos foram previamente identificados e analisados?
- As causas reais foram especificadas na identificação dos riscos?
- Os riscos e os controles foram avaliados corretamente?
- Os controles funcionaram como esperado?
- Os planos de tratamento foram efetivos? Se não, que melhorias poderiam ser feitas?
- O processo de monitoração e revisão foi efetivo?
- Como o processo de gerenciamento de riscos como um todo poderia ser melhorado?
- Como disseminar essas experiências com as pessoas apropriadas?
- Como garantir que os eventos de falha não irão se repetir, mas os de sucesso irão?

#### **2.2.8 CONCLUSÃO**

Este capítulo apresentou duas abordagens para o gerenciamento de riscos, aplicáveis a qualquer área do conhecimento, não sendo específicas para projetos de desenvolvimento de *software*. O capítulo seguinte descreve abordagens de gerenciamento de riscos específicas para *software*.

## Capítulo 3

### GERENCIAMENTO DE RISCOS DE SOFTWARE

---

*O presente capítulo apresenta três abordagens de gerenciamento de riscos, desenvolvidas especificamente para projetos de software.*

Este capítulo apresenta três abordagens de gerenciamento de riscos, que foram desenvolvidas especificamente para *software*: (a) o padrão IEEE para Processos de Ciclo de Vida de Software – Gerenciamento de Riscos, (b) as áreas de processo do CMMI (2002) e (c) as atividades da disciplina *Gerenciamento de projetos* do RUP (2003) que tratam do gerenciamento de riscos.

Inicialmente, aborda-se o padrão IEEE para Processos de Ciclo de Vida de Software – Gerenciamento de Riscos. Esse padrão define um processo contínuo de gerenciamento de riscos aplicável às disciplinas de engenharia de *software* e de gerenciamento. O processo é definido para o gerenciamento de riscos de projetos de *software*, mas também pode ser útil para o gerenciamento de riscos em âmbito organizacional ou de sistema.

Em seguida, apresenta-se a representação por estágio do CMMI, com ênfase nas áreas de processo que abordam o gerenciamento de riscos. No nível 2, temos as áreas de processo *Planejamento do projeto* e *Monitoração e controle do projeto*. No nível 3, a área de processo *Gerenciamento de riscos*.

Na seqüência, são mostradas as atividades relacionadas ao gerenciamento de riscos do RUP, contidas na disciplina *Gerenciamento de projetos*.

Apresenta-se também um mapeamento das abordagens de gerenciamento de riscos apresentadas neste capítulo e no capítulo anterior e das macroatividades do processo proposto, abordadas no próximo capítulo.

Atualmente, há também a abordagem do MPS-BR (Melhoria de Processo do Software Brasileiro), que trata do Processo de Gerência de Riscos (GRI), no Nível C (Definido), que tem como propósito identificar, gerenciar e reduzir continuamente os



riscos em âmbito organizacional e de projeto. Os principais resultados esperados da aplicação desse processo de riscos são os seguintes (MPS-BR, 2006):

- O escopo da gerência de riscos é determinado.
- As origens e as categorias de riscos são determinadas, os parâmetros usados para quantificação da probabilidade e severidade são definidos, e são também definidas as ameaças e suas fronteiras para cada categoria de risco.
- São definidas e implementadas estratégias apropriadas para a gerência de riscos.
- Os riscos do projeto são identificados e documentados, incluindo seu contexto, condições e possíveis conseqüências para o projeto e as partes que serão afetadas.
- Os riscos são priorizados, estimados e classificados de acordo com as categorias e os parâmetros definidos.
- São desenvolvidos planos para a mitigação de riscos.
- Os riscos são analisados, e é determinada a prioridade de aplicação dos recursos para o monitoramento desses riscos.
- A situação de cada risco é periodicamente monitorada e, quando apropriado, é implementado o plano de mitigação de riscos.
- São coletadas as medições de desempenho nas atividades de tratamento de riscos.
- São executadas ações apropriadas para corrigir ou evitar o impacto dos riscos.

### **3.1 IEEE STD 1540-2001**

Esse padrão foi desenvolvido para ser adaptado a situações e necessidades de organizações e de projetos específicos (FARIAS, 2002), de modo a poder-se aplicá-lo junto com as normas da série ISO, ou independentemente. Para esse padrão, o objetivo do gerenciamento de riscos compreende identificar e mitigar os riscos de modo contínuo. Uma bem-sucedida implementação do gerenciamento de riscos gera os seguintes resultados (IEEE, 2001):

- escopo do gerenciamento de riscos bem definido;
- estratégias apropriadas de gerenciamento de riscos bem definidas e implementadas;

- riscos identificados durante a condução do projeto;
- riscos adequadamente analisados e priorizados, com a definição dos recursos a ser aplicados em sua monitoração;
- métricas de riscos definidas, aplicadas e avaliadas para determinar mudanças no *status* dos riscos e no progresso das atividades de monitoração;
- ações apropriadas postas em prática para reduzir ou evitar o impacto dos riscos.

O processo de gerenciamento de riscos é iterativo, compreendendo uma série de atividades, consoante seqüência demonstrada na Figura 3.1 e explicitada na seguinte discriminação:

- *Planejar e implementar o gerenciamento de riscos:* consiste em definir a política, os procedimentos e as técnicas específicas a serem utilizados no gerenciamento de riscos; atribuir os recursos; e determinar a forma de comunicar e coordenar os riscos e seu tratamento.
- *Gerenciar o perfil de riscos do projeto:* significa criar uma visão consistente dos riscos presentes durante o projeto, e do seu tratamento, incluindo o contexto da gerência de risco, o estado atual de todos os riscos do projeto e seu histórico.
- *Executar a análise dos riscos:* ou seja, identificar os eventos ou as situações que podem criar riscos; determinar a probabilidade de ocorrência e suas conseqüências; determinar a exposição ao risco; avaliar cada risco ou combinação de riscos e gerar alternativas para tratá-los, com base em uma ordem de prioridade.
- *Executar o tratamento dos riscos:* isto é, determinar se os riscos são aceitos pelas partes interessadas no projeto; e, em caso negativo, dar início às ações necessárias para reduzir os riscos a um nível aceitável.
- *Executar a monitoração dos riscos:* compreende revisar e atualizar o estado dos riscos e o contexto do gerenciamento de riscos; avaliar a eficácia do tratamento dos riscos; e procurar novos riscos.
- *Avaliar o processo de gerenciamento de riscos:* significa capturar informações sobre a qualidade do processo; identificar áreas para melhoria; e gerar lições aprendidas.

A seguir, as atividades acima descritas, que compõem o processo de gerenciamento de riscos, são detalhadas juntamente com as respectivas tarefas.

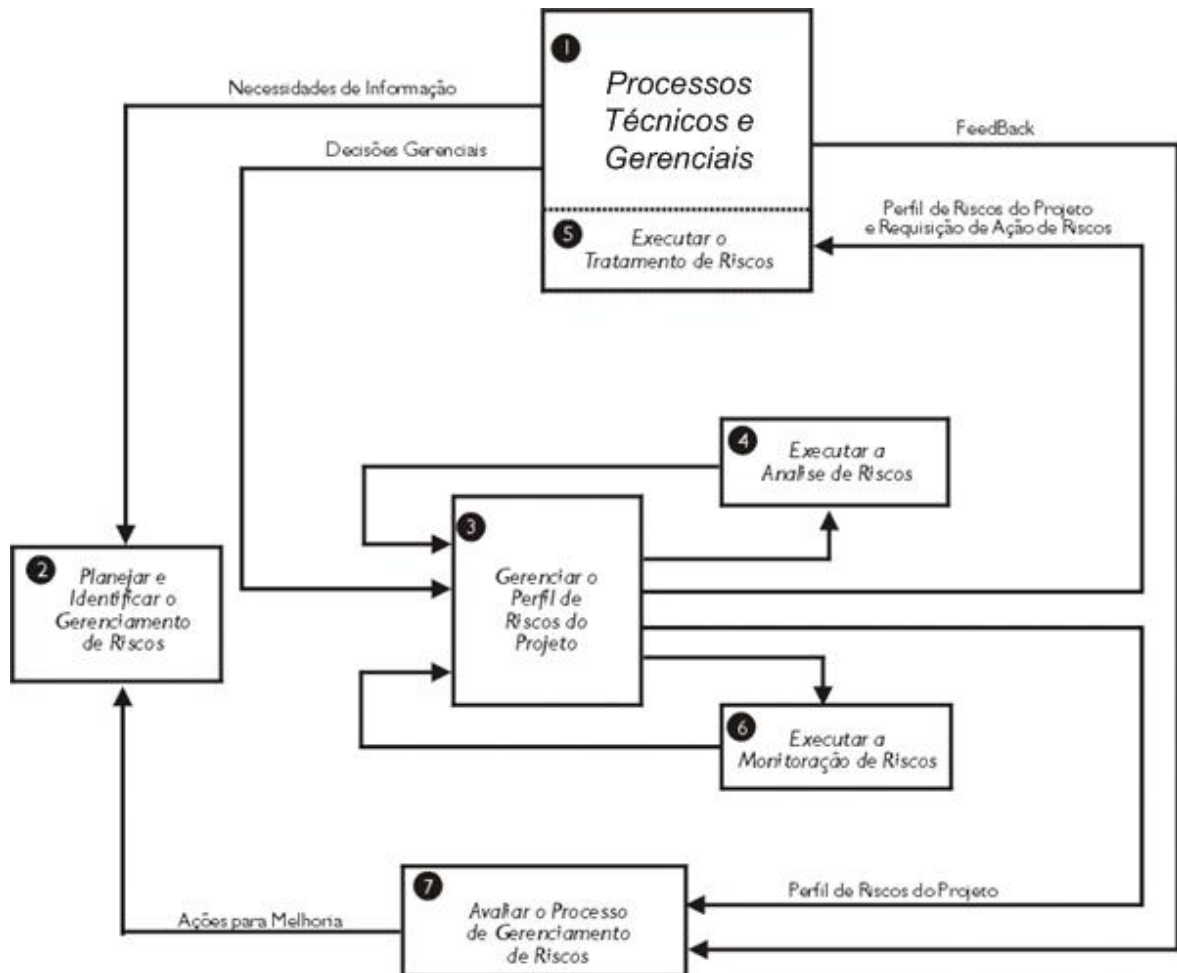


Figura 3.1 – Modelo do processo de gerenciamento de riscos do padrão IEEE (2001)

### 3.1.1 PLANEJAR E IMPLEMENTAR O GERENCIAMENTO DE RISCOS

Essa atividade tem por objetivo estabelecer o processo de gerenciamento de riscos de *software*, que deve estar alinhado com o processo de gerenciamento de riscos organizacional, caso este exista. A atividade estabelece quem deve executar o gerenciamento de riscos; definir o processo específico a ser utilizado; atribuir os recursos necessários para execução do processo; e definir como os riscos e seu tratamento serão comunicados entre as partes interessadas. Essa atividade deve ser executada no início do projeto, incluindo as seguintes tarefas: (i) *estabelecer políticas de gerenciamento de riscos*;

(ii) *estabelecer o processo de gerenciamento de riscos; (iii) estabelecer responsabilidades; (iv) designar recursos; e (v) estabelecer a avaliação do processo de gerenciamento de riscos.*

### **3.1.1.1 ESTABELEECER POLÍTICAS DE GERENCIAMENTO DE RISCOS**

As políticas de gerenciamento de riscos devem descrever orientações explícitas para execução do processo de gerenciamento de riscos do projeto que darão suporte à captura das informações referentes a riscos necessárias às partes interessadas, pondo-se em discussão questões como as seguintes:

- O gerenciamento de riscos deve ser implementado, administrado e suportado pela gerência e pela equipe.
- O compromisso das partes interessadas no projeto com o gerenciamento de riscos deve ser obtido e mantido.
- O processo de gerenciamento de riscos deve ser coordenado entre as partes interessadas no projeto.
- Devem ser providenciados treinamento e orientação da equipe no processo de gerenciamento de riscos.
- A informação sobre os riscos deve ser periodicamente comunicada e revisada pelas partes interessadas.
- Os recursos serão disponibilizados para o tratamento dos riscos.

### **3.1.1.2 ESTABELEECER O PROCESSO DE GERENCIAMENTO DE RISCOS**

Consiste na descrição do processo de gerenciamento de riscos a ser executado, com seus procedimentos e suas técnicas selecionadas de acordo com o projeto, incluindo:

- a frequência com que os riscos devem ser monitorados e analisados;
- o tipo de análise requerido, se a qualitativa e/ou a quantitativa;
- as escalas a serem utilizadas na estimativa da probabilidade e das conseqüências, com suas incertezas;
- os tipos de limite a ser estabelecidos;
- os tipos de medida a ser utilizados na monitoração do *status* dos riscos;
- como os riscos serão priorizados para tratamento;

- quais perspectivas das partes interessadas o processo poderá suportar;
- as categorias de riscos a serem consideradas.

Se houve uma definição desses itens no âmbito organizacional, basta registrar aquilo que diferir em relação ao projeto específico.

### **3.1.1.3 ESTABELEECER RESPONSABILIDADES**

Consiste na identificação explícita dos responsáveis pela execução do gerenciamento de riscos e de seus papéis e responsabilidades.

### **3.1.1.4 DESIGNAR RECURSOS**

Significa a disponibilização dos recursos adequados para os responsáveis, com vistas à execução do processo.

### **3.1.1.5 ESTABELEECER A AVALIAÇÃO DO PROCESSO DE GERENCIAMENTO DE RISCOS**

Corresponde à descrição da forma como o processo de gerenciamento de riscos será avaliado e melhorado e da maneira como as informações serão capturadas como lições aprendidas.

## **3.1.2 GERENCIAR O PERFIL DE RISCOS DO PROJETO**

O propósito dessa atividade é criar uma visão consistente, atual e histórica dos riscos e de seus tratamentos, de modo que os riscos possam ser comunicados de forma sucinta e completa às partes interessadas. Isso inclui o contexto do gerenciamento de riscos, o estado atual do risco e seu histórico. Essa atividade inclui as seguintes tarefas: *(i) definir o contexto do gerenciamento de riscos; (ii) estabelecer limites para os riscos; (iii) estabelecer e manter o perfil de risco do projeto; e (iv) comunicar o status dos riscos.*

### **3.1.2.1 DEFINIR O CONTEXTO DO GERENCIAMENTO DE RISCOS**

Consiste na definição e documentação do contexto do processo de gerenciamento de riscos, incluindo a descrição das perspectivas de uma ou mais partes interessadas que devem ser suportadas, e de uma ou mais categorias a serem gerenciadas.

As categorias de riscos de *software*, percebidas como de especial importância, devem ser tratadas separadamente. Devem também conter ou referenciar a descrição dos objetivos, premissas e restrições técnicas e gerenciais do projeto, e quaisquer outras informações relevantes.

### **3.1.2.2 ESTABELEECER LIMITES PARA OS RISCOS**

Consiste na determinação e documentação dos limites que definem os critérios de aceitabilidade de um risco. Os limites são os níveis máximos do risco aceitos pelas partes interessadas sem uma revisão explícita. Esses limites devem ser definidos para riscos individuais ou combinações de riscos e para todo o projeto. Os limites também podem ser definidos para os riscos, com conseqüências em custos, cronograma ou aspectos técnicos.

### **3.1.2.3 ESTABELEECER E MANTER O PERFIL DE RISCO DO PROJETO**

Consiste em estabelecer e manter um perfil de risco do projeto, incluindo uma visão geral das informações sobre os riscos do projeto, uma coleção dos perfis de cada risco, incluindo os estados atuais e históricos do risco, uma descrição detalhada de cada risco, suas causas, as escalas utilizadas, as medidas usadas para avaliar o *status*, planos de contingência e outras informações relacionadas ao risco. Um perfil do risco do projeto conterà, no mínimo:

- o contexto do gerenciamento de riscos;
- um registro cronológico do estado de cada risco, incluindo sua probabilidade, suas conseqüências e seus limites;
- uma ordem de prioridade de cada risco, baseada nos critérios fornecidos pelas partes interessadas;
- solicitação de ações para os riscos, juntamente com o seu *status*.

Esse perfil deverá ser atualizado sempre que houver mudança no *status* de um risco individual, no contexto do gerenciamento de riscos, ou quando for identificado um novo risco.

### **3.1.2.4 COMUNICAR O STATUS DOS RISCOS**

Consiste na periódica comunicação do *status* do risco do projeto às partes interessadas, com base em suas necessidades. As informações sobre o *status* dos riscos devem ser disponibilizadas a todos os interessados.

### **3.1.3 EXECUTAR A ANÁLISE DOS RISCOS**

O propósito dessa atividade é identificar os riscos; estimar sua probabilidade de ocorrência e suas conseqüências; e avaliar cada risco ou combinação de riscos, de acordo com seus limites. Além de gerar as alternativas para tratá-los, se esses limites forem alcançados, são feitas recomendações para o tratamento baseado em uma ordem de prioridade. Essa atividade inclui as seguintes tarefas: (i) *identificação dos riscos*; (ii) *estimativa dos riscos*; e (iii) *avaliação dos riscos*.

#### **3.1.3.1 IDENTIFICAÇÃO DOS RISCOS**

A identificação dos riscos é feita de acordo com as categorias incluídas no contexto do gerenciamento de riscos e na identificação de mudanças nesse contexto.

Podem ser utilizadas várias abordagens na identificação dos riscos, como questionários, taxonomias, *brainstorming*, análise de cenários, lições aprendidas, prototipação, etc. Os riscos não identificados são implicitamente aceitos.

As categorias de riscos devem ser usadas para uma eficaz comunicação com as partes interessadas. Os riscos relacionados podem ser combinados para facilitar a análise, a monitoração e o tratamento. Defeitos no *software*, relatórios de medidas e outros indicadores devem ser continuamente revistos como fontes de riscos.

#### **3.1.3.2 ESTIMATIVAS DOS RISCOS**

Consiste na estimativa da probabilidade de ocorrência e da conseqüência de cada risco identificado. A estimativa pode ser qualitativa ou quantitativa, de acordo com a definição das partes interessadas. As escalas devem ser utilizadas consistentemente, enquanto a incerteza inerente à escala deve ser descrita no *Plano de gerenciamento de*

*riscos*. O nível de confiabilidade da estimativa de um risco deve ser registrado no *status* do risco.

### **3.1.3.3 AVALIAÇÃO DOS RISCOS**

Os riscos são avaliados de acordo com seus limites. Os riscos devem ser avaliados isoladamente, em conjunto e de acordo com suas interações com os riscos do sistema e da empresa. Devem também ser avaliados em relação ao limite de riscos do projeto, para se assegurar de que um conjunto de riscos, mesmo posicionando-se abaixo de seus limites, se avaliados isoladamente, não se situem em um limite inaceitável, se considerados conjuntamente.

Na avaliação dos riscos, podem ser utilizadas diversas técnicas, tais como árvore de decisão, planejamento de cenários, teoria dos jogos, análise probabilística e programação linear. Os riscos devem ser priorizados de acordo com os critérios definidos pelas partes interessadas, podendo tomar por base os períodos das respectivas ocorrências, a exposição ao risco, as medidas relacionadas ao risco ou quaisquer outros critérios consistentes.

Para se reduzir ou eliminar riscos, podem ser utilizadas várias alternativas. Estratégias como eliminar o risco, reduzir sua probabilidade de ocorrência ou severidade, ou aceitar o risco, devem ser adotadas para os riscos que estão acima de seus limites. Essas estratégias são definidas e documentadas em uma requisição de ação para o risco. Deve ser desenvolvido um *Plano de contingências* para todos os riscos acima dos seus limites. Além disso, devem ser definidas métricas para se verificar a efetividade das opções de tratamento.

Os riscos, suas respectivas opções de tratamento e as medidas da sua efetividade devem ser comunicados às partes interessadas, para a competente aprovação.

### **3.1.4 EXECUTAR O TRATAMENTO DOS RISCOS**

O propósito dessa atividade é determinar se os riscos são aceitos pelas partes interessadas e, caso não sejam, iniciar ações para reduzir os riscos a um nível aceitável, compreendendo ações como selecionar o tratamento, planejar, monitorar e controlar as



ações, para diminuir a exposição ao risco. Essa atividade inclui as seguintes tarefas: (i) *selecionar tratamento dos riscos*; e (ii) *planejar e implementar o tratamento dos riscos*.

#### **3.1.4.1 SELECIONAR TRATAMENTO DOS RISCOS**

Consiste em fazer uma avaliação para se determinar se o risco se encontra em um nível aceitável e, caso necessário, executar uma ação para torná-lo aceitável, por meio da implementação de uma das alternativas apontadas no conjunto de ações para o risco. Caso as partes interessadas optem por uma alternativa de tratamento que não figure nesse conjunto, esta deverá retornar à atividade *análise*, para que as alternativas de tratamento sugeridas sejam novamente analisadas. A implementação da alternativa selecionada deverá ser suportada pelos recursos necessários, e monitorada e coordenada com as outras atividades do projeto.

Um risco pode ser aceito, mesmo que se encontre acima de seus limites aceitáveis. Por exemplo, se o custo do tratamento for demasiado elevado, ou se não houver tempo ou recursos para o tratamento. Nessa situação, o risco será considerado com elevada prioridade e continuamente monitorado, para se determinar se será necessária alguma ação de tratamento futura.

#### **3.1.4.2 PLANEJAR E IMPLEMENTAR O TRATAMENTO DOS RISCOS**

Essa tarefa tem duas alternativas, dependendo da aplicação desse padrão em conjunto com o padrão IEEE/EIA 12207.0-1996, ou independentemente dele, conforme explicitado a seguir.

##### **Tratamento dos riscos com IEEE/EIA 12207.0-1996**

Uma vez que um tratamento de risco seja selecionado, receberá as mesmas ações gerenciais que os problemas, de acordo com as atividades da execução e controle da IEEE/EIA 12207.0-1996.

##### **Tratamento dos riscos independentemente da IEEE/EIA 12207.0-1996**

Logo que a alternativa de tratamento seja aceita, deve ser elaborado um detalhado plano de tratamento, estabelecendo como o plano será executado e monitorado e definindo os recursos a serem alocados, inclusive o responsável pelo sucesso de cada ação de

tratamento. Esse plano deverá ser executado e integrado com os planos do projeto e com seus processos e atividades gerenciais. As partes interessadas devem definir ações de contingência, para o caso de falha no tratamento de um risco ou para os riscos considerados aceitáveis.

### **3.1.5 EXECUTAR A MONITORAÇÃO DOS RISCOS**

Constituem propósitos dessa atividade: revisar e atualizar os *status* dos riscos e o seu contexto; avaliar a efetividade do tratamento dos riscos; e procurar novos riscos. Essa atividade inclui as seguintes tarefas: (i) *monitorar riscos*; (ii) *monitorar o tratamento dos riscos*; e (iii) *procurar novos riscos*.

#### **3.1.5.1 MONITORAR RISCOS**

Consiste na contínua monitoração de todos os riscos, a fim de identificar mudanças em seu *status*, utilizando-se medidas que serão gravadas no perfil de riscos do projeto. Os riscos devem ser ordenados por prioridade para a monitoração, com base nos critérios estabelecidos pelas partes interessadas, recomendando-se que os riscos de elevada prioridade sejam freqüentemente monitorados.

Os riscos cujo *status* tenha sofrido alteração devem submeter-se a uma nova avaliação, logo após a descoberta da mudança. O contexto do gerenciamento de riscos também deverá ser monitorado para possíveis mudanças e documentado no perfil de riscos do projeto.

#### **3.1.5.2 MONITORAR O TRATAMENTO DOS RISCOS**

Compreende a implementação e a monitoração de métricas para avaliar a eficácia do tratamento, de modo que a causa de um tratamento ineficaz deve ser prontamente identificada e remediada. As partes interessadas definem os critérios que determinam quando a efetividade do tratamento de um risco não precisa mais ser monitorada.

### **3.1.5.3 PROCURAR NOVOS RISCOS**

Significa fazer a contínua monitoração do projeto, para a identificação de novos riscos durante todo o ciclo de vida do *software*. Os novos riscos serão comunicados às partes interessadas após serem analisados.

### **3.1.6 AVALIAR O PROCESSO DE GERENCIAMENTO DE RISCOS**

Essa atividade consiste em avaliar a qualidade do processo de gerenciamento de riscos, as áreas onde podem ser melhorados os procedimentos, os processos ou a política de gerenciamento de riscos organizacionais; e identificar oportunidades para modificá-los, a fim de se reduzir ou eliminar os riscos sistêmicos de forma mais efetiva, além de dar um retorno para as partes interessadas acerca da execução do processo.

A atividade compreende ainda a aquisição de informações a respeito do processo de gerenciamento de riscos e levantamento e implementação dos respectivos aprimoramentos (LEOPOLDINO, 2004). Essa atividade compõe-se, principalmente, das seguintes tarefas: (i) *capturar informações sobre o gerenciamento de riscos*; (ii) *avaliar e melhorar o processo de gerenciamento de riscos*; e (iii) *gerenciar lições aprendidas*.

#### **3.1.6.1 CAPTURAR INFORMAÇÕES SOBRE O GERENCIAMENTO DE RISCOS**

Significa a captura das informações sobre os riscos identificados, suas causas, seu tratamento e o sucesso dos tratamentos selecionados, que foram coletadas durante todo o ciclo de vida do projeto de *software*, com a finalidade de melhorar o processo de gerenciamento de riscos e gerar lições aprendidas.

As informações capturadas podem ser úteis para melhorar os procedimentos, os processos ou as políticas organizacionais de gerenciamento de riscos. Se isso for feito de forma eletrônica, tanto facilita a captura dessas informações, como sua comunicação e avaliação.

### **3.1.6.2 AVALIAR E MELHORAR O PROCESSO DE GERENCIAMENTO DE RISCOS**

Trata-se de promover a revisão periódica do processo de gerenciamento de riscos, para se avaliar sua eficácia e eficiência, identificando-se oportunidades para melhorá-lo no âmbito do projeto ou no contexto organizacional. Onde for aplicável, o processo deve ser melhorado, as políticas e os processos de gerenciamento de riscos organizacionais devem ser atualizados, e o Plano de gerenciamento de riscos do projeto deve ser atualizado, de acordo com a periodicidade determinada pelas partes interessadas.

### **3.1.6.3 GERAR LIÇÕES APRENDIDAS**

Corresponde à coleta das lições aprendidas do projeto, com o objetivo de ajudar na identificação de riscos sistêmicos e organizacionais. Essa coleta é feita com base na revisão periódica das informações sobre os riscos identificados, seu tratamento e o sucesso desse tratamento, realizada pelas partes interessadas, de acordo com a periodicidade determinada.

## **3.2 GERENCIAMENTO DE RISCOS NO CMMI**

O CMMI (*Capability Maturity Model Integration*) foi criado para integrar modelos do CMM, que atendem às atividades relacionadas ao desenvolvimento de *software*, incorporando melhorias, e ainda para compatibilizá-lo com a ISO/IEC 15504 (2003). Foi desenvolvido de maneira a possibilitar extensões, e atualmente abrange as disciplinas *engenharia de sistemas, engenharia de software, desenvolvimento integrado de produtos e processos e aquisição* (CHRISISS et al, 2004).

O CMMI (2002) contém duas representações: (i) por estágio e (ii) contínua. A representação por estágio trata do nível de maturidade da organização como um todo, compreendendo cinco níveis de maturidade: *inicial, gerenciado, definido, quantitativamente gerenciado e em otimização*.

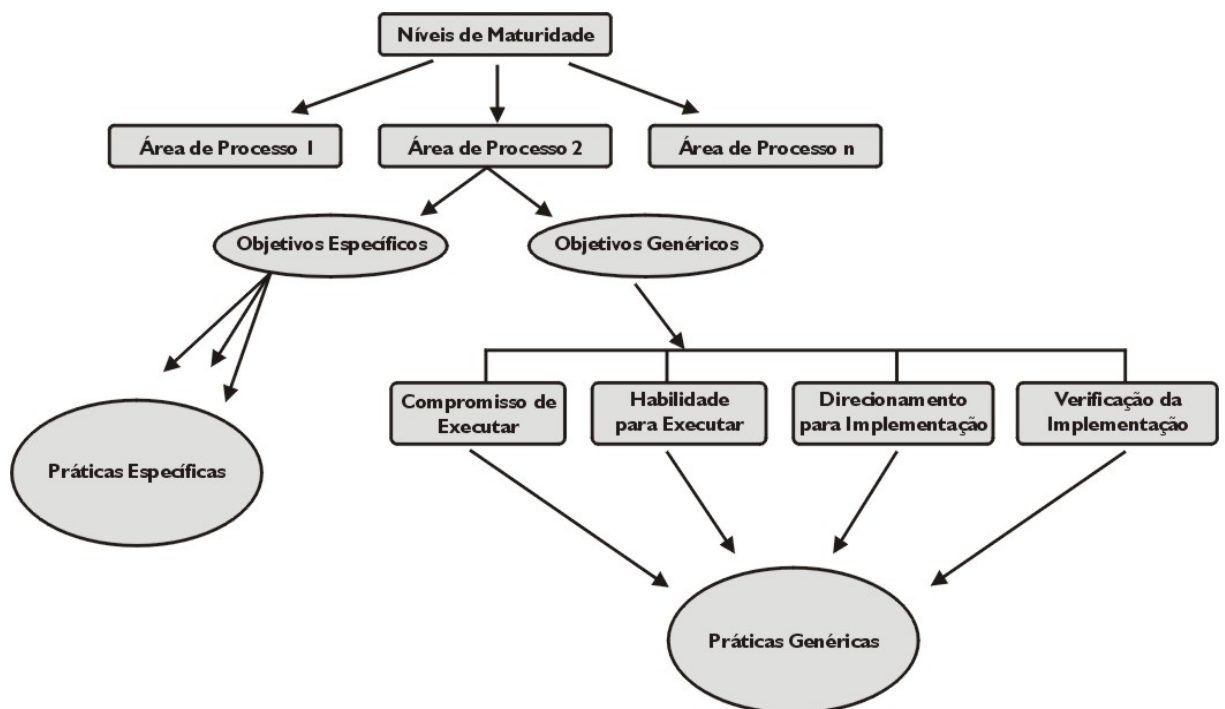
Cada nível é constituído por um conjunto de áreas de processo, compostas por *objetivos específicos* (SG) e *objetivos genéricos* (GG). Cada objetivo específico é

composto por um conjunto de *práticas específicas* (SP), enquanto os objetivos genéricos são compostos pelas *práticas genéricas*, conforme ilustrado na Figura 3.2.

Um objetivo específico descreve as características que devem estar presentes para satisfazer determinada área de processo. Uma prática específica é a descrição de uma atividade considerada importante para se alcançar o objetivo específico a ela associado.

Os objetivos genéricos são constituídos por características comuns relacionadas ao compromisso de executar, à habilidade para executar, ao direcionamento para implementação e à verificação da implementação do processo. As características comuns indicam se a implementação e a institucionalização da área de processo são eficazes, repetíveis e duradouras. Cada característica comum é composta por práticas genéricas.

A representação contínua utiliza níveis de capacidade para medir a melhoria do processo da organização. Essa representação apresenta seis níveis de capacidade: *incompleto, executado, gerenciado, definido, quantitativamente gerenciado e em otimização*.



**Figura 3.2 – Componentes do CMMI (2002)**

Este trabalho aborda a representação por estágio do CMMI, em que a problemática do risco é tratada em três áreas de processo, que compõem a categoria *Gerência de projeto*: (i) *Planejamento do projeto*; (ii) *Monitoração e controle do projeto*; e (iii) *Gerenciamento de riscos*. As duas primeiras pertencem ao nível 2 de maturidade, e a última pertence ao nível 3.

Na área de processo *Planejamento do projeto*, figura o objetivo específico *Desenvolvimento do plano do projeto*, que trata diretamente de riscos. Esse objetivo contém a prática específica *Identificar os riscos do projeto*, que identifica e analisa riscos, para determinar o impacto, a probabilidade e o período de ocorrência dos riscos, para que possam ser priorizados. Essa prática específica inclui as seguintes subpráticas:

- identificar riscos;
- documentar riscos;
- revisar os riscos, conforme apropriado; e
- obter a concordância dos *stakeholders* relevantes.

Na área de processo *Monitoração e controle do projeto*, inclui-se o objetivo específico *Monitorar o projeto de acordo com o plano*, em que está inserida a prática específica *Monitorar os riscos do projeto*. Essa prática específica inclui as seguintes subpráticas:

- revisar periodicamente a documentação dos riscos no contexto do *status* atual do projeto;
- revisar a documentação dos riscos à medida que novas informações se tornem disponíveis, a fim de incorporar mudanças;
- comunicar o *status* dos riscos às partes interessadas que sejam relevantes.

A cultura de riscos em organizações do nível 1 caracteriza-se pela negação. Em organizações do nível 2, o gerenciamento de riscos ocorre de maneira reativa, em que as organizações inicialmente focam na identificação dos riscos para a conscientização, e reagem à realização desses riscos à medida que eles ocorrem. Em organizações do nível 3, o gerenciamento de riscos é proativo; há total interesse em saber o que pode acontecer de errado e o que se pode fazer sobre isso (KULPA, 2003).

A área de processo *Gerenciamento de riscos* (RSKM) não existia no CMM, sendo inserida no CMMI, o que demonstra a constatação da importância do gerenciamento de riscos e a necessidade de formalização das suas práticas para projetos de *software*.

Além de estabelecer um gerenciamento de riscos mais proativo, os requisitos dessa área de processo possibilitam sua aplicação fora do contexto do projeto, utilizando seus conceitos para gerenciar riscos organizacionais (AHERN et al, 2003).

A área de processo *Gerenciamento de riscos* tem por finalidade identificar potenciais problemas antes que eles ocorram, de maneira que as atividades de administração desses riscos possam ser planejadas e realizadas ao longo do ciclo de vida do produto ou projeto, para mitigar eventuais impactos adversos ao alcance dos objetivos. A Tabela 3.1 apresenta o relacionamento dos objetivos específicos (SG) com suas respectivas práticas específicas (SP) para essa área de processo.

**Tabela 3.1 Gerenciamento de riscos do CMMI (2002)**

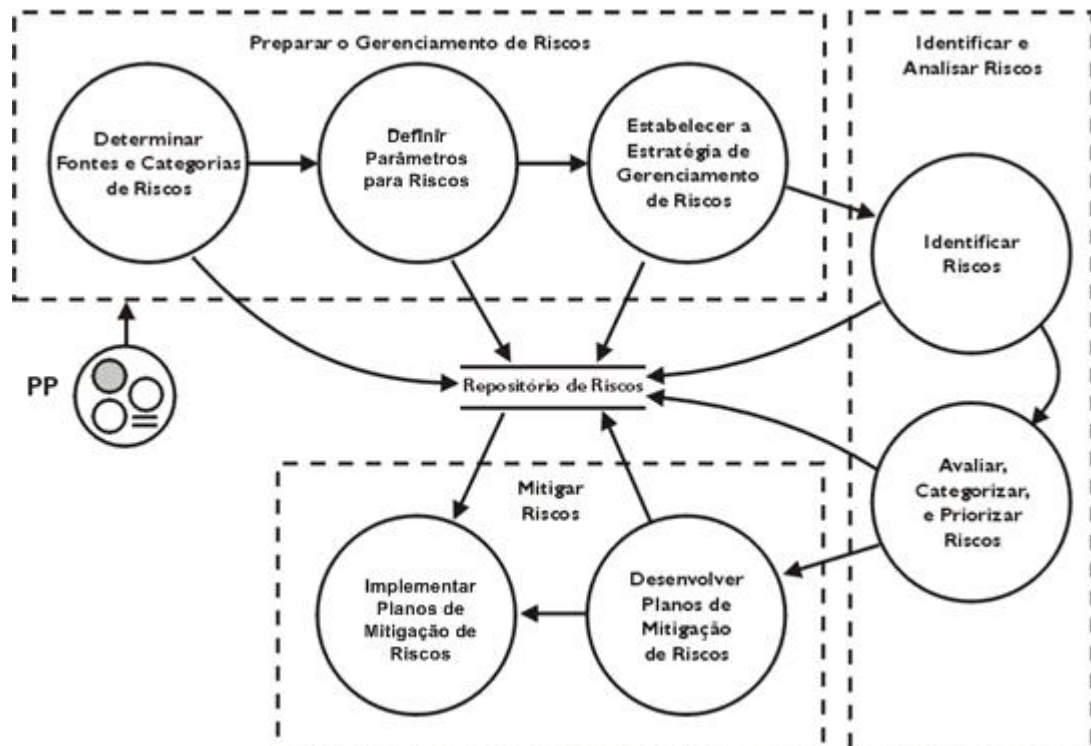
<b>SG 1</b>	<b>Preparar o gerenciamento de riscos</b>	
	<b>SP 1.1</b>	Determinar fontes e categorias de riscos
	<b>SP 1.2</b>	Definir parâmetros para os riscos
	<b>SP 1.3</b>	Estabelecer uma estratégia para o gerenciamento de riscos
<b>SG 2</b>	<b>Identificar e analisar riscos</b>	
	<b>SP 2.1</b>	Identificar riscos
	<b>SP 2.2</b>	Avaliar, categorizar, e priorizar riscos
<b>SG 3</b>	<b>Mitigar riscos</b>	
	<b>SP 3.1</b>	Desenvolver planos de mitigação de riscos
	<b>SP 3.2</b>	Implementar planos de mitigação de riscos

O gerenciamento de riscos refere-se a aspectos que podem pôr em risco a realização dos objetivos críticos do projeto. Uma abordagem de contínuo gerenciamento dos riscos deve ser aplicada, para efetivamente antecipar e mitigar esses riscos. Essa área de processo é uma parte importante dos processos de gerenciamento técnico e de negócios.

O efetivo gerenciamento dos riscos inclui a identificação antecipada e agressiva dos riscos por meio da colaboração e envolvimento dos *stakeholders* relevantes; a liderança mais forte entre esses *stakeholders* deve estabelecer um ambiente propício para a descoberta e a aberta discussão dos riscos.

Enquanto os aspectos técnicos constituem uma preocupação no início e durante todas as fases do projeto, o gerenciamento de riscos deve considerar fontes internas e externas para riscos de custo, cronograma e técnico. A detecção antecipada e agressiva do risco é fundamental, haja vista ser comprovadamente mais fácil e mais barato fazer mudanças e corrigir esforços no início, do que nas fases mais avançadas do projeto.

O gerenciamento de riscos pode ser dividido em três etapas: definição de uma estratégia para o gerenciamento de riscos; identificação e análise dos riscos; e acompanhamento dos riscos identificados, incluindo a implementação de planos de mitigação dos riscos, quando necessário. A definição da estratégia pode ser considerada uma tarefa em âmbito organizacional; a identificação, a análise e a mitigação dos riscos ocorrem no âmbito do projeto. O relacionamento entre essas etapas está esquematizado na Figura 3.3.



**Figura 3.3 – Diagrama do contexto do gerenciamento de riscos (CMMI, 2002)**

Como representado nas áreas de processo *Planejamento do projeto* e *Monitoração e controle do projeto*, as organizações podem, de início, focar tão-somente a identificação dos riscos para a conscientização. A reação a esses riscos ocorre à medida que eles se tornam realidade. A área de processo *Gerenciamento de riscos* descreve uma evolução



dessas práticas específicas para sistematicamente planejar, antecipar e mitigar riscos para minimizar proativamente seu impacto no projeto (MUTAFELIJA, 2003).

A área de processo *Gerenciamento de riscos* também está relacionada à área de processo *Análise de decisão e resolução*, na qual é descrito um processo formal de avaliação, que pode ser utilizado para avaliar alternativas para a seleção e a mitigação dos riscos identificados.

A seguir, são descritos os objetivos específicos da área de processo *Gerenciamento de riscos*, com suas respectivas práticas específicas e subpráticas. Essa área de processo compreende os seguintes objetivos específicos: (i) *preparar o gerenciamento de riscos*; (ii) *identificar e analisar riscos*; e (iii) *mitigar riscos*.

### **3.2.1 PREPARAR O GERENCIAMENTO DE RISCOS (SG1)**

A preparação do gerenciamento de riscos consiste no estabelecimento e na manutenção de uma estratégia para se identificar, analisar e mitigar riscos. Geralmente, isso é documentado em um *Plano de gerenciamento de riscos*. Essa estratégia refere-se às ações específicas e à abordagem gerencial utilizadas para aplicar e controlar o gerenciamento de riscos. Isso inclui a identificação das fontes de riscos, o esquema adotado para categorizar riscos, e os parâmetros empregados para avaliar, limitar e controlar riscos para uma manipulação eficaz.

Esse objetivo específico compõe-se das seguintes práticas específicas: (i) *determinar fontes e categorias de riscos*; (ii) *definir parâmetros para riscos*; e (iii) *estabelecer a estratégia de gerenciamento de riscos*.

#### **3.2.1.1 DETERMINAR FONTES E CATEGORIAS DE RISCOS (SP 1.1)**

A identificação de fontes de riscos fornece uma base para o exame sistemático das situações de mudanças, em tempo de descobrir as circunstâncias que impactam a habilidade do projeto de atingir seus objetivos. As fontes de riscos podem ser internas e externas ao projeto, e, enquanto o projeto progride, podem ser identificadas fontes adicionais de riscos.

Estabelecer categorias para riscos significa fornecer um mecanismo para coletar e organizar riscos, assegurando-se um exame detalhado e a atenção apropriada da gerência para aqueles riscos que podem ter conseqüências mais sérias para os objetivos do projeto.

Essa prática específica gera os seguintes produtos de trabalho:

- lista de fontes de riscos (externos e internos)
- lista de categorias de riscos

Essa prática específica inclui as seguintes subpráticas: (i) *determinar fontes de riscos*; e (ii) *determinar as categorias de riscos*.

As *fontes de riscos* são os elementos fundamentais que causam riscos dentro de um projeto ou de uma organização. Há muitas fontes de riscos, internas e externas a um projeto. As fontes de riscos identificam as áreas comuns onde os riscos podem originar-se.

Muitas dessas fontes de riscos são freqüentemente aceitas sem um planejamento adequado. A identificação antecipada de fontes internas e externas de riscos pode conduzir à identificação antecipada dos riscos, o que viabilizará a implementação de planos de mitigação de riscos no início do projeto, com o objetivo de evitar a ocorrência de riscos ou de reduzir suas conseqüências.

As *categorias de riscos* refletem as “caixas” para coleta e organização dos riscos. Uma razão para se identificar categorias de riscos é ajudar na consolidação futura das atividades nos planos de mitigação dos riscos.

Uma taxonomia do risco pode ser usada no sentido de fornecer uma estrutura para determinar fontes e categorias de riscos.

### **3.2.1.2 DEFINIR PARÂMETROS PARA RISCOS (SP 1.2)**

Consiste em definir os parâmetros empregados para analisar e categorizar riscos e os parâmetros utilizados para controlar o esforço do gerenciamento de riscos.

Parâmetros para avaliar, categorizar e priorizar os riscos envolvem:

- probabilidade de ocorrência dos riscos;
- conseqüência dos riscos (por exemplo, impacto e severidade da ocorrência dos riscos); e
- gatilhos para provocar atividades de gerência.

Os parâmetros de riscos são utilizados para fornecer critérios comuns e consistentes para comparar os vários riscos a serem gerenciados. Sem esses parâmetros, seria muito difícil calibrar

a severidade da mudança não desejada causada pelos riscos, e dar prioridade às ações necessárias requeridas pelo plano de mitigação dos riscos.

Essa prática específica gera os seguintes produtos de trabalho:

- critérios de avaliação, categorização e priorização dos riscos; e
- requisitos da gerência de riscos (níveis de controle e aprovação, intervalos de reavaliação, etc.).

Essa prática específica inclui as seguintes subpráticas: (i) *definir critérios*; (ii) *definir limites para cada categoria de riscos*; e (iii) *definir limites*.

### **Definir critérios**

Consiste na definição de critérios consistentes para avaliação e quantificação da probabilidade dos riscos e dos níveis de severidade. Esses critérios (por exemplo, os limites nos níveis de probabilidade e de severidade) possibilitam que os diferentes impactos de riscos sejam compreendidos, para receber o nível apropriado de detalhamento e para obter a atenção da gerência autorizada. Para controlar diferentes riscos, é fundamental assegurar a consistência no resultado final.

### **Definir limites para cada categoria de riscos**

Para cada categoria de riscos, podem ser estabelecidos limites com vistas a determinar a aceitabilidade dos riscos, auxiliar na priorização e indicar a necessidade de ação da gerência. A seguir, são citados exemplos de sinalizadores para esses limites:

- envolver a gerência sênior, quando os custos do produto excederem a 10% do custo-alvo ou quando os índices de desempenho do custo caírem abaixo de 0,95 , para custos;
- envolver a gerência sênior, quando os índices de desempenho do cronograma caírem abaixo de 0,95 , para cronograma;
- envolver a gerência sênior, quando itens-chave do projeto específico (por exemplo, utilização do processador) excederem a 125% do pretendido, para *performance*.

Esses itens podem ser refinados posteriormente, para cada risco identificado, a fim de se estabelecer os pontos em que a monitoração mais agressiva do risco deve ser empregada, ou para sinalizar a execução do plano de mitigação de riscos.

### **Definir limites**

A definição de limites (ou de condições de limite) pode ser empregada para ajudar a delimitar o escopo da extensão do esforço do gerenciamento de riscos e evitar despesas excessivas com recursos. Esses limites podem prever a exclusão de uma fonte específica de risco de uma categoria, como também excluir toda a condição que ocorrer abaixo de uma frequência específica.

#### **3.2.1.3 ESTABELEECER A ESTRATÉGIA DE GERENCIAMENTO DE RISCOS (SP 1.3)**

Significa estabelecer e manter uma estratégia a ser utilizada para o gerenciamento de riscos, contendo definições sobre itens como:

- o escopo do esforço do gerenciamento de riscos;
- métodos e ferramentas a serem utilizadas para: identificação do risco, análise do risco, mitigação do risco, monitoração do risco e comunicação;
- fontes de riscos específicas do projeto;
- como esses riscos deverão ser organizados, categorizados, comparados e consolidados;
- parâmetros, incluindo a probabilidade, a consequência, e os gatilhos que irão desencadear uma ação para riscos identificados;
- técnicas de mitigação a serem adotadas, como prototipação, simulação, projetos alternativos ou desenvolvimento evolucionário;
- definição das medidas para monitorar o *status* dos riscos; e
- intervalos de tempo para monitorar ou reavaliar riscos.

A estratégia do gerenciamento de riscos deve ser guiada de acordo com os resultados futuros almejados pelo projeto no tocante ao produto que será entregue, ao seu custo e às suas funcionalidades. A estratégia de gerenciamento de riscos deve ser documentada em um *Plano de*

*gerenciamento de riscos* organizacional ou do projeto. A estratégia de gerenciamento de riscos deve ser revista com os *stakeholders* relevantes, para promover o entendimento e o compromisso.

Essa prática específica gera como produto típico de trabalho a estratégia *Gerenciamento de riscos* do projeto, e não possui subpráticas associadas.

### **3.2.2 IDENTIFICAR E ANALISAR RISCOS (SG2)**

Os riscos são identificados e analisados para determinar sua importância relativa. O grau de importância de um risco gera impacto nos recursos atribuídos para administrá-lo e na determinação do momento em que é requerida a atenção apropriada da gerência.

A análise dos riscos depende da identificação de riscos oriundos das fontes internas e externas identificadas, que então são avaliados para se determinar suas probabilidades e conseqüências. A classificação dos riscos de acordo com as categorias e critérios estabelecidos pela estratégia *Gerenciamento de riscos* fornece a informação necessária para a manipulação dos riscos. Os riscos relacionados podem ser agrupados para a manipulação eficiente e o uso eficaz dos recursos do gerenciamento de riscos.

Esse objetivo específico contém as seguintes práticas específicas: (i) *identificar riscos*; e (ii) *avaliar, categorizar e priorizar riscos*.

#### **3.2.2.1 IDENTIFICAR RISCOS (SP 2.1)**

A identificação de potenciais problemas, perigos, ameaças e vulnerabilidades que podem afetar negativamente os esforços ou planos de trabalho constitui a base para o sólido e bem-sucedido gerenciamento de riscos. Os riscos devem ser identificados e descritos de uma maneira compreensível, para ser analisados e controlados corretamente. Os riscos devem ser documentados em uma linguagem concisa, que inclua o contexto, as condições e as conseqüências da sua ocorrência.

A identificação dos riscos deve ser feita de uma maneira organizada e completa, a fim de se identificar riscos prováveis ou realísticos, que irão afetar os objetivos do projeto. Para ser

eficaz, a identificação dos riscos não deve ser uma tentativa de referir-se a cada evento possível, sem levar em conta o quão improvável ele possa ser. O uso de categorias e parâmetros desenvolvidos na estratégia de gerenciamento de riscos, junto com as fontes identificadas dos riscos, pode fornecer a disciplina e a otimização apropriadas à identificação dos riscos. Os riscos identificados que podem compor uma lista de riscos formam uma *baseline* para iniciar as atividades de gerenciamento de riscos.

A lista dos riscos deve ser revista periodicamente, com vistas ao reexame de possíveis fontes de riscos e condições de mudança, para se descobrir fontes e riscos previamente negligenciados ou inexistentes, quando a estratégia do gerenciamento de riscos foi atualizada.

As atividades de identificação de riscos não têm por objetivo atribuir culpa às pessoas com relação aos riscos, e os resultados dessas atividades não devem ser utilizados pela gerência para avaliar o desempenho dos indivíduos.

Há vários métodos para identificar riscos, como, por exemplo:

- exame de cada elemento da estrutura analítica do projeto (wbs);
- condução de uma avaliação de riscos usando-se uma taxonomia de riscos;
- entrevista com peritos no assunto;
- revisão do esforço de gerenciamento de riscos de produtos similares;
- exame dos documentos ou bases de dados de lições aprendidas; e
- exame das especificações de projeto e requisitos acordados.

Essa prática específica gera como produto típico de trabalho a lista dos riscos identificados, incluindo o contexto, condições e conseqüências da sua ocorrência, sendo constituída das seguintes subpráticas: (i) *identificar riscos associados a custo, cronograma e performance*; (ii) *revisar elementos ambientais*; (iii) *revisar os elementos da estrutura analítica do projeto*; (iv) *revisar os elementos do plano do projeto*; (v) *documentar*; e (vi) *identificar os stakeholders relevantes*.

### **Identificar riscos associados a custo, cronograma e *performance***

Essa subprática corresponde à identificação dos riscos de custos, cronograma e *performance* em todas as fases apropriadas do ciclo de vida do produto, à medida que impactam

os objetivos do projeto. Pode haver riscos potenciais descobertos que estão fora do escopo dos objetivos do projeto, mas que são vitais para os interesses do cliente. Por exemplo, os riscos de custos de desenvolvimento, custos de aquisição do produto, custos de reposição (ou recolocação) de produtos e custos da distribuição do produto (ou a eliminação) têm implicações no projeto. O cliente pode não ter fornecido requisitos para o custo de suporte ao produto. O cliente deve ser informado de tais riscos, mas pode não haver necessidade de controlar ativamente esses riscos. Os mecanismos para se tomar tais decisões devem ser examinados no âmbito do projeto e da organização, e implementados, caso isso seja apropriado, especialmente no tocante aos riscos que impactam a habilidade de verificar e validar o produto.

Riscos relacionados ao cronograma devem incluir aqueles associados com atividades planejadas, eventos-chave e marcos.

Riscos relacionados à *performance* devem incluir aqueles associados com: requisitos, análise e projeto, aplicação de novas tecnologias, tamanho físico, formato, importância, fabricação e manufatura, *performance* funcional e operação, verificação, validação, atributos de manutenção da *performance* (características que possibilitam ao produto em uso prover a *performance* originalmente requerida).

Há outros riscos que não pertencem às categorias de custos, orçamento e *performance*.

### **Revisar elementos ambientais**

Significa revisar elementos ambientais que podem gerar impacto no projeto. Alguns riscos de projeto que freqüentemente são esquecidos incluem aqueles supostamente fora do escopo do projeto (por exemplo, o projeto não controla o momento da ocorrência, mas pode mitigar seu impacto), como condições climáticas, desastres naturais, mudanças políticas e falhas de telecomunicações.

### **Revisar os elementos da estrutura analítica do projeto**

A estrutura analítica do projeto deve ser revisada como parte da identificação de riscos, para ajudar a assegurar que foram considerados todos os aspectos do esforço de trabalho.

### **Revisar os elementos do plano do projeto**

A revisão dos elementos do plano do projeto deve fazer parte da identificação dos riscos, para ajudar a assegurar que foram considerados todos os aspectos do projeto.

## **Documentar**

Trata-se de documentar o contexto, as condições e as conseqüências potenciais dos riscos. A relação dos riscos geralmente é documentada em um formato-padrão, contendo o contexto dos riscos, condições e conseqüências da sua ocorrência.

O contexto dos riscos provê informações adicionais, para que a intenção dos riscos possa ser facilmente compreendida. Na documentação do contexto dos riscos, devem ser considerados o tempo relativo aos riscos e as circunstâncias ou condições que os cercam.

## **Identificar os *stakeholders* relevantes**

Significa identificar cada um dos *stakeholders* relevantes que estão direta ou indiretamente associados a cada risco levantado.

### **3.2.2.2 AVALIAR, CATEGORIZAR E PRIORIZAR RISCOS (SP 2.2)**

Trata-se de avaliar e categorizar cada risco identificado, utilizando-se as categorias e os parâmetros definidos, e determinar a sua prioridade relativa.

A avaliação dos riscos torna-se necessária para se determinar a importância relativa de cada risco identificado, sendo utilizada na determinação do momento em que é requerida a atenção apropriada da gerência. É sempre útil agregar riscos baseados nas suas inter-relações e desenvolver opções em um nível de agregação. Quando um risco agregado é formado pela chegada de riscos de mais baixo nível, deve-se tomar cuidado para assegurar que não foram ignorados importantes riscos de baixo nível.

Coletivamente, as atividades de avaliação, categorização e priorização dos riscos são, algumas vezes, chamadas de “análise de riscos”.

Essa prática específica gera como produtos de trabalho a lista dos riscos com as respectivas prioridades, e inclui as seguintes subpráticas: (i) *avaliar os riscos identificados*; (ii) *categorizar e agrupar os riscos*; e (iii) *priorizar riscos para mitigação*.



### **Avaliar os riscos identificados**

Cada risco identificado deve ser avaliado e receber a atribuição de valores de acordo com os parâmetros definidos, podendo-se incluir a probabilidade, a consequência (severidade ou impacto) e os limites. Os valores de parâmetros atribuídos aos riscos podem ser integrados para produzir medidas adicionais, como a exposição ao risco, que pode ser empregada para dar prioridade a riscos.

Freqüentemente, uma escala com três a cinco valores é utilizada para avaliar a probabilidade e a consequência. A probabilidade, por exemplo, pode ser categorizada como provável, altamente provável, remota, improvável ou quase certa. A consequência pode ser categorizada como baixa, média, insignificante, marginal, significativa, crítica ou catastrófica.

Valores prováveis são freqüentemente empregados para quantificar a probabilidade dos riscos. As consequências geralmente são relacionadas ao custo, ao cronograma, ao impacto ambiental ou a medidas como as horas de trabalho perdidas e a severidade do dano.

Essa avaliação é freqüentemente considerada uma tarefa complexa e que consome muito tempo. Uma avaliação especializada ou técnicas de grupo podem ser necessárias para avaliar os riscos e ganhar a confiança para a priorização. Além disso, as prioridades podem requerer reavaliações periódicas.

### **Categorizar e agrupar os riscos**

Significa categorizar e agrupar os riscos de acordo com as categorias definidas, provendo-se meios para a visualização dos riscos de acordo com suas fontes, taxonomia ou componente do projeto. Os riscos relacionados ou equivalentes podem ser agrupados, para uma eficiente manipulação. Os relacionamentos de causa e efeito entre os riscos devem ser documentados.

### **Priorizar riscos para mitigação**

Uma prioridade relativa é determinada para cada risco, baseada nos parâmetros atribuídos aos riscos. Critérios claros devem ser adotados para se determinar essa prioridade. A intenção da priorização consiste em determinar as áreas mais efetivas nas

quais os recursos para mitigação dos riscos podem ser aplicados com maior impacto positivo para o projeto.

### **3.2.3 MITIGAR RISCOS (SG 3)**

Os riscos são tratados e mitigados onde apropriado, para reduzir impactos adversos ao atendimento dos objetivos do projeto.

As etapas no tratamento de riscos incluem o desenvolvimento de opções de tratamento de riscos, a monitoração de riscos e a execução das atividades de tratamento, quando os limites definidos forem excedidos. Os planos de mitigação de riscos são desenvolvidos e executados para que o impacto potencial da ocorrência dos riscos selecionados seja proativamente reduzido. Isso pode também incluir planos de contingência, para tratar o impacto dos riscos selecionados e que venham a ocorrer, apesar das tentativas de mitigá-los. Os parâmetros utilizados para disparar as atividades de tratamento dos riscos são evidenciados na definição da estratégia de gerenciamento de riscos.

Esse objetivo específico compõe-se das seguintes práticas específicas: (i) *desenvolver planos de mitigação de riscos*; e (ii) *implementar planos de mitigação de riscos*.

#### **3.2.3.1 DESENVOLVER PLANOS DE MITIGAÇÃO DE RISCOS (SP 3.1)**

Tendo-se em mira os riscos mais importantes do projeto, deve-se desenvolver um plano de mitigação de riscos, conforme definido pela estratégia *Gerenciamento de riscos*.

Um componente crítico de um plano de mitigação de riscos consiste em desenvolver cursos de ação alternativos, formas de contornar o problema e posições de recuo, com um curso de ação recomendado para cada risco crítico. O plano de mitigação para um risco específico inclui técnicas e métodos empregados para evitar, reduzir e controlar a probabilidade de ocorrência do risco ou a extensão dos danos causados pelo risco (chamado às vezes “plano de contingência”), ou ambas as situações.

Os riscos são monitorados, e, quando excedem os limites estabelecidos, o plano de mitigação de riscos é implementado para fazê-los retornar a um nível aceitável. Se os riscos não puderem ser mitigados, um plano de contingência pode ser invocado. Os planos de mitigação e de contingências freqüentemente são gerados somente para os riscos selecionados, cujas conseqüências são classificadas como elevadas ou inaceitáveis; outros riscos podem ser aceitos e simplesmente monitorados.

No caso específico de riscos elevados, é aconselhável que seja gerada mais de uma abordagem para o seu tratamento.

Em muitos casos, os riscos são aceitos ou observados. A sua aceitação geralmente ocorre quando são julgados demasiado baixos para a mitigação formal, ou quando parece não haver forma viável de reduzi-los. Se um risco for aceito, a razão para essa decisão deve ser documentada. Os riscos são observados quando há limites objetivamente definidos e verificáveis para *performance*, tempo ou exposição ao risco (a combinação da probabilidade com a conseqüência) que disparem o plano de mitigação dos riscos ou o plano de contingências, quando necessário.

O quanto antes, deve ser dada a devida consideração às demonstrações de tecnologia, aos modelos, às simulações e aos protótipos, como partes do planejamento da mitigação dos riscos.

Essa prática específica gera os seguintes produtos de trabalho:

- opções documentadas de tratamento para cada risco identificado;
- plano de mitigação dos riscos;
- planos de contingência;
- lista das pessoas responsáveis pelo acompanhamento dos riscos.

Essa prática específica inclui as seguintes subpráticas: (i) *determinar os níveis e os limites*; (ii) *identificar responsável*; (iii) *determinar a relação custo/benefício*; (iv) *desenvolver um plano de mitigação de riscos*; e (v) *desenvolver planos de contingência*.

**Determinar os níveis e os limites**

Significa determinar os limites que definem o momento em que um risco torna-se inaceitável e provoca a execução de um plano de mitigação ou de um plano de contingências.

O nível de risco (derivado através da utilização de um modelo de risco) é uma medida que combina a incerteza de alcançar um objetivo com as conseqüências de não alcançá-lo.

Os níveis de risco e os limites para o desempenho aceitável ou planejado devem ser claramente compreendidos e definidos, de maneira a fornecer os meios para a compreensão dos riscos. A apropriada categorização do risco é essencial para assegurar a adequada prioridade, com base na severidade, e a resposta associada da gerência. Pode haver o emprego de múltiplos limites, para dar início a níveis variáveis de resposta da gerência. Geralmente, os limites para a execução de planos de mitigação dos riscos são empregados antes da execução dos planos de contingência.

**Identificar responsável**

Deverá ser identificada uma pessoa, ou um grupo, responsável pelo acompanhamento de cada risco levantado no projeto.

**Determinar a relação custo/benefício**

Deve-se determinar a relação custo/benefício da execução do plano de mitigação de cada risco. As atividades de mitigação dos riscos devem ser examinadas no tocante aos benefícios que oferecem, em comparação com os recursos que consomem. Como em qualquer outra atividade de projeto, devem ser desenvolvidos planos alternativos, avaliando-se os custos e benefícios de cada alternativa. Seleciona-se, então, para execução, o plano mais apropriado. Às vezes, o risco evidencia-se significativo, enquanto os benefícios revelam-se inexpressivos; mas os riscos devem ser mitigados, para reduzir a probabilidade de se incorrer em conseqüências inaceitáveis.

### **Desenvolver um plano de mitigação de riscos**

Trata-se de desenvolver um plano de mitigação de riscos para o projeto como um todo, envolvendo os planos individuais de mitigação e de contingência dos riscos.

O conjunto completo de planos de mitigação dos riscos pode não ser financeiramente viável. Deve ser feita uma análise, com vistas a se dar prioridade aos planos de mitigação de riscos a serem implementados.

### **Desenvolver planos de contingência**

Significa desenvolver *Planos de contingência* para os riscos críticos selecionados, tendo-se em mira a probabilidade de sua ocorrência e conseqüente concretização de seus impactos.

Quando necessário, os planos de mitigação dos riscos são desenvolvidos e executados para reduzir riscos proativamente, antes que venham a se transformar em problemas. Apesar dos melhores esforços, alguns riscos podem ser inevitáveis e transformar-se em problemas que produzirão impacto no projeto.

Os *Planos de contingência* podem ser desenvolvidos no sentido de descrever as ações que um projeto pode implementar na ocorrência dos riscos críticos, para lidar com seus impactos. A intenção é definir um plano proativo para acompanhar o risco, reduzi-lo (mitigação) ou neutralizá-lo (contingência), mas sem deixar de gerenciá-lo.

#### **3.2.3.2 IMPLEMENTAR PLANOS DE MITIGAÇÃO DE RISCOS (SP 3.2)**

Consiste em monitorar periodicamente o *status* de cada risco e, quando apropriado, executar o plano de mitigação de riscos. Para controlar e gerenciar eficazmente os riscos durante o esforço de trabalho, deve ser seguido um programa proativo para regular monitoração do *status* dos riscos e dos resultados das ações de tratamento dos riscos. A estratégia de gerenciamento de riscos define os intervalos em que deve ser revisado o *status* dos riscos. Essa atividade pode resultar na descoberta de novos riscos ou de novas opções de tratamento, os quais podem requerer o replanejamento e a reavaliação. Em

ambos os casos, os limites de aceitação associados ao risco devem ser comparados com o *status* respectivo, para se determinar a necessidade de execução do plano de mitigação de riscos.

Essa prática específica gera os seguintes produtos de trabalho:

- lista atualizada do *status* dos riscos;
- avaliações atualizadas da probabilidade, da consequência e dos limites dos riscos;
- listas atualizadas de opções de tratamento dos riscos;
- listas atualizadas de ações implementadas para tratar os riscos; e
- planos de mitigação dos riscos.

Essa prática específica inclui as seguintes subpráticas: (i) *monitorar o status dos riscos*; (ii) *prover um método para acompanhamento das respostas*; (iii) *invocar as opções de tratamento dos riscos*; (iv) *estabelecer um cronograma*; (v) *prover o contínuo comprometimento dos recursos*; e (vi) *coletar medidas*.

### **Monitorar o *status* dos riscos**

Depois que tem início a execução de um plano de mitigação dos riscos, estes ainda devem ser monitorados. Os limites são avaliados para se verificar a conveniência e oportunidade de execução do plano de contingências. Deve, então, ser empregado um mecanismo periódico para monitoração.

### **Prover um método para acompanhamento das respostas**

Consiste em prover um método para seguir os itens iniciais das ações em implementação no tratamento dos riscos, indo do início até o fechamento.

### **Invocar as opções de tratamento dos riscos**

Significa acionar a execução das opções de tratamento, quando os riscos monitorados excederem os limites definidos.

Freqüentemente, o tratamento dos riscos é executado somente para aqueles julgados “altos” ou “médios”. A estratégia de tratamento para um risco específico pode

incluir técnicas e métodos voltados para evitar, reduzir ou controlar a probabilidade de ocorrência do risco ou a extensão dos danos que ele poderá causar, ou ambas as situações. Nesse contexto, o tratamento do risco requer planos de mitigação e planos de contingência.

Técnicas de acompanhamento dos riscos são desenvolvidas para evitar, reduzir e controlar o impacto adverso nos objetivos do projeto, e para trazer resultados aceitáveis à luz dos prováveis impactos. As ações geradas para manipular um risco requerem a apropriada alocação de recursos e um cronograma, observando-se os planos e cronogramas da *baseline*. Esse esforço de replanejamento deve considerar os efeitos em iniciativas ou atividades adjacentes ou dependentes.

#### **Estabelecer um cronograma**

Trata-se de estabelecer um período de execução para cada atividade de acompanhamento do risco, incluindo-se a data de seu início e a de sua conclusão.

#### **Prover o contínuo comprometimento dos recursos**

Significa prover o contínuo comprometimento dos recursos para cada plano, de maneira a viabilizar a exitosa execução das atividades de tratamento dos riscos.

#### **Coletar medidas**

Faz-se necessário coletar medidas de desempenho das atividades de tratamento dos riscos identificados e categorizados do projeto.

### **3.3 GERENCIAMENTO DE RISCOS NO RUP**

O Processo Unificado (UP) ou Processo Unificado da Rational (RUP) é um processo de desenvolvimento de *software* baseado nas melhores práticas de desenvolvimento e em elementos essenciais (KRUCHTEN, 2003). Tais práticas significam abordagens comercialmente aprovadas para o desenvolvimento de *software*, utilizadas por empresas bem-sucedidas (MANZONI, 2001). Os elementos essenciais são as atividades e os artefatos mínimos exigidos em todos os projetos de desenvolvimento de *software*.

As melhores práticas para o desenvolvimento de *software* adotadas pelo RUP incluem: *Desenvolvimento iterativo*, *Gerenciamento de requisitos*, *Uso de arquitetura*





### Figura 3.4 – Arquitetura geral do RUP (RUP, 2003)

Um dos principais benefícios da abordagem iterativa é sua orientação para riscos (SANTANDER, 2000), sendo que, a cada iteração, riscos são identificados e avaliados, o que facilita o tempestivo tratamento dos principais riscos do projeto. Os riscos são mitigados mais cedo, porque os elementos são progressivamente integrados durante a execução do projeto. A abordagem em cascata tende a mascarar os riscos reais do projeto até que seja tarde demais para se tomar uma atitude sobre eles (KRUCHTEN, 2000).

Cada iteração do RUP incorpora um conjunto de atividades em modelagem de negócios, requisitos, análise e projeto, implementação, testes e implantação, em várias proporções, dependendo de onde a iteração esteja localizada no ciclo de desenvolvimento. Esse conjunto de atividades de engenharia de *software* apóia-se em três disciplinas: *Gerenciamento de projetos*, *Gerenciamento de configuração e mudanças* e *Ambiente*.

No RUP, o gerenciamento de riscos é tratado na disciplina *Gerenciamento de projetos* (Figura 3.5), que se propõe balancear objetivos concorrentes e gerenciar riscos e restrições, para que a entrega do produto satisfaça clientes e usuários e ocorra no prazo e com o custo previstos. Essa disciplina provê um *framework*, em que o projeto é criado e gerenciado, e guias para o planejamento, a execução e a monitoração de projetos.

O gerenciamento de riscos está integrado ao processo de desenvolvimento, cujas iterações são planejadas com base nos riscos de maior prioridade. Como cada iteração exercita muitos aspectos do projeto, torna-se mais fácil descobrir até que ponto os riscos percebidos estão-se materializando, como também descobrir novos riscos (KRUCHTEN, 2003).

O *Gerenciamento de riscos* no RUP cabe ao gerente do projeto, que executa as atividades *Desenvolver o plano de gerenciamento de riscos*, *Identificar e avaliar Riscos* e *Monitorar o status do projeto*.

A seguir apresenta-se o fluxo principal da disciplina *Gerenciamento de projetos*, assim como seus fluxos detalhados, compreendendo as seguintes atividades referentes ao gerenciamento de riscos: (i) *conceber novo projeto*; (ii) *avaliar escopo e risco do projeto*; (iii) *elaborar plano de desenvolvimento de software*; e (iv) *monitorar e controlar o projeto*.

Tabela 3.2. – Fases do RUP (2003)

Fase	Objetivos / Foco / Marco
<b>Iniciação</b>	<ul style="list-style-type: none"> <li>• Estabelecer uma boa compreensão do sistema a ser construído, por meio de requisitos de alto nível e do estabelecimento do escopo do projeto</li> <li>• Obter acordo com os <i>stakeholders</i>, para decisão acerca da continuidade do projeto</li> <li>• Preparar o ambiente para o projeto, estabelecendo o caso de desenvolvimento</li> <li>• Foco: o tratamento dos riscos relacionados aos casos de negócio, encorajando todos os <i>stakeholders</i> a tomar parte</li> <li>• Marco: objetivos do ciclo de vida</li> </ul>
<b>Elaboração</b>	<ul style="list-style-type: none"> <li>• Compreender como construir, analisando o domínio do problema</li> <li>• Estabelecer uma <i>baseline</i> da arquitetura.</li> <li>• Desenvolver o plano do projeto, eliminando seus riscos essenciais.</li> <li>• Foco: os riscos técnicos, assegurando a estabilidade da arquitetura de <i>software</i> e, se necessário, revisando o escopo do projeto, à medida que seus requisitos são mais bem compreendidos</li> <li>• Marco: arquitetura estabilizada</li> </ul>
<b>Construção</b>	<ul style="list-style-type: none"> <li>• Desenvolver e testar os componentes da solução, com base em critérios definidos</li> <li>• Integrar os componentes da solução em um só produto</li> <li>• Otimizar custos, cronograma e qualidade, por meio do gerenciamento dos recursos e do controle das operações</li> <li>• Avaliar <i>releases</i> do produto</li> <li>• Foco: os riscos de “logística” da construção do <i>software</i>, para agilizar a conclusão da maior parte do trabalho</li> <li>• Marco: capacidade operacional inicial</li> </ul>
<b>Transição</b>	<ul style="list-style-type: none"> <li>• Construir a versão final do produto, disponibilizando-a para os usuários finais.</li> <li>• Desenvolver artefatos de suporte à instalação e uso operação pelo usuário final.</li> <li>• Foco: os riscos associados com a logística de entrega do produto a seu usuário</li> <li>• Marco: entrega do produto</li> </ul>

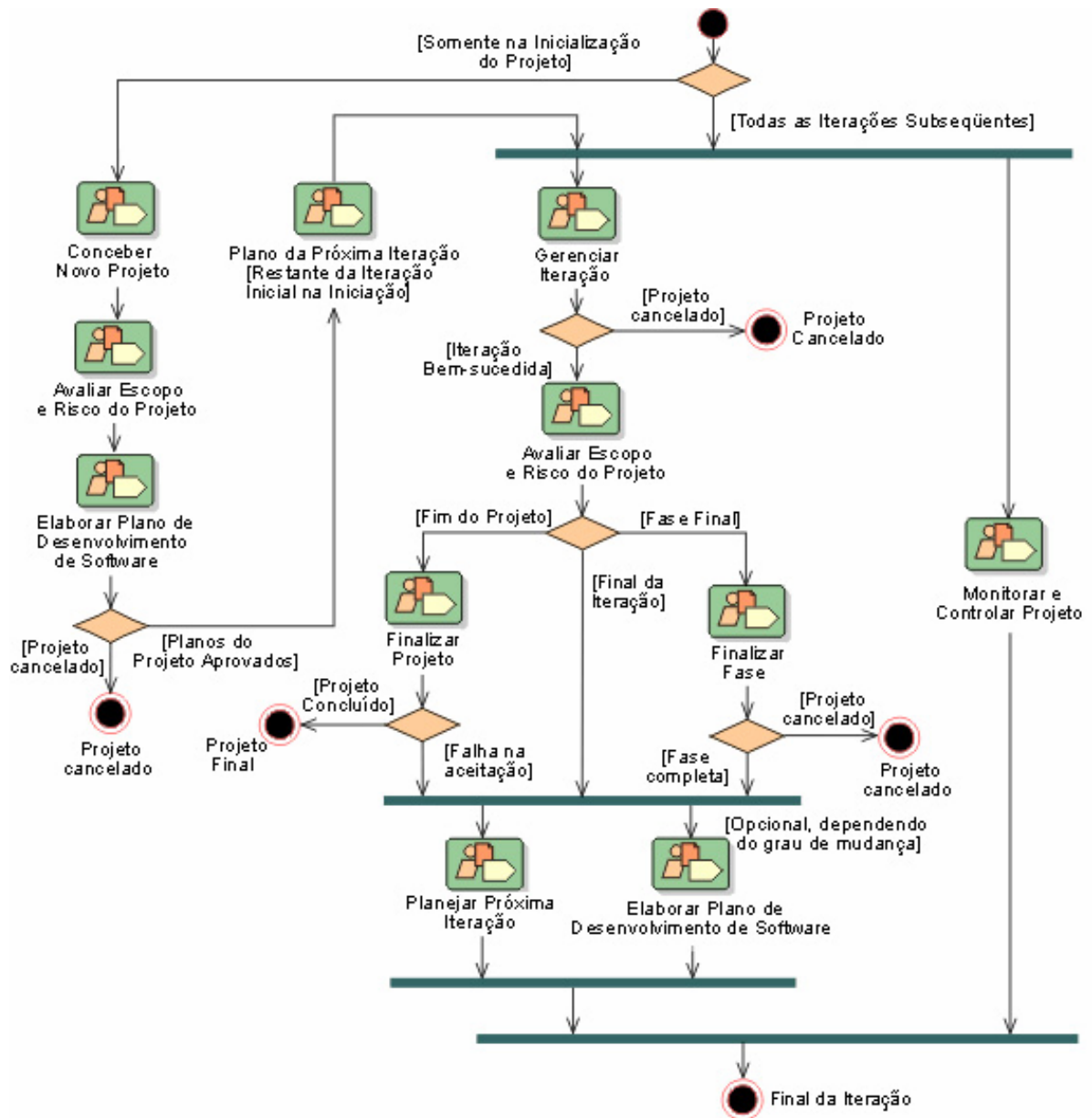
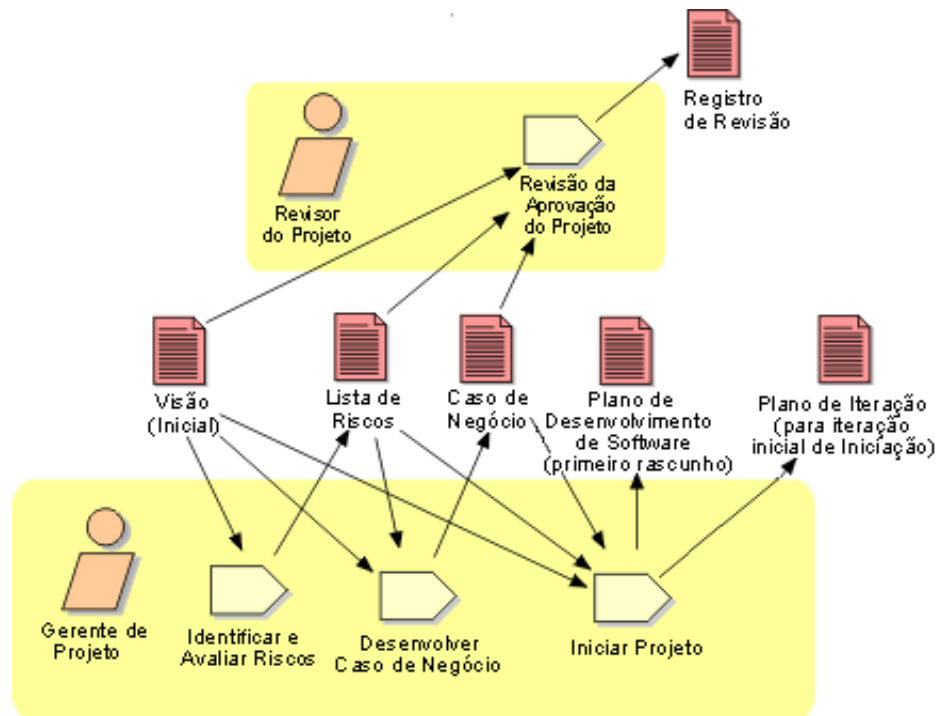


Figura 3.5 – Fluxo da disciplina *Gerenciamento de projetos* (RUP, 2003)

### 3.3.1 FLUXO CONCEBER NOVO PROJETO

No início de um novo projeto (fase *Iniciação*) é executado o fluxo detalhado *Conceber Novo Projeto* (Figura 3.6), composto pelas atividades (i) *identificar e avaliar riscos*; (ii) *desenvolver caso de negócio*; (iii) *iniciar o projeto* e (iv) *revisão da aprovação do projeto*. O propósito desse fluxo é trazer o projeto de uma idéia inicial para um ponto em que seja possível tomar decisões fundamentadas sobre sua continuação ou abandono.



**Figura 3.6 – Fluxo *Conceber novo projeto* (RUP, 2003)**

O gerente do projeto executa a atividade *Identificar e avaliar riscos*, objetivando identificar, analisar e priorizar riscos para o projeto, bem como determinar as estratégias apropriadas de gerenciamento de riscos. Essa identificação realiza-se com base no documento *Visão*, que contém as características mais importantes do produto a ser desenvolvido e uma descrição dos seus requisitos centrais. O produto dessa atividade é a *Lista de riscos* inicial do projeto, que servirá de base para a análise da sua viabilidade.

A partir da *Lista de riscos* inicial, o gerente executa a atividade *Desenvolver o caso de negócio*, cuja finalidade é desenvolver uma justificativa econômica do produto. Compreende a descrição do produto, a definição do contexto do negócio e dos objetivos do produto, a elaboração de uma previsão financeira e a descrição das restrições do projeto e das opções para o produto e para o projeto.

A pessoa que nesse momento desempenha o papel de gerente do projeto não necessariamente será a mesma que conduzirá o projeto depois de aprovado, pois nesse ponto a ênfase é maior na descoberta dos riscos e no estabelecimento do potencial retorno

do investimento. É fundamental alocar alguém que tenha a habilidade de destacar os riscos técnicos e de negócio e de gerenciar equipes ainda desfalcadas.

O *Revisor do projeto* realiza a atividade *Revisão da aprovação do projeto*, para determinar, do ponto de vista do negócio, se vale a pena investir nesse projeto, e gera o *Registro da revisão*.

Após a aprovação do projeto, o *caso de negócio* serve de base para a atividade *Iniciar o projeto*, sendo designados a equipe e o gerente do projeto, bem como aprovados os critérios para aceitação do projeto. Nessa atividade, são desenvolvidos o *Plano de desenvolvimento de software* (inicial) e o *Plano de iteração* para a primeira iteração.

A seguir, a atividade *Identificar e avaliar riscos*, que tem relação direta com o objetivo deste trabalho, é detalhada em finalidade, passos e artefatos de entrada e saída.

### **3.3.1.1 ATIVIDADE IDENTIFICAR E AVALIAR RISCOS**

Os propósitos dessa atividade são identificar, analisar e priorizar os riscos para o projeto, e determinar as estratégias apropriadas de gerenciamento de riscos, além de atualizar a *Lista de riscos*, para refletir o atual *status* do trabalho. Essa atividade é executada nos fluxos *Conceber novo projeto* e *Avaliar escopo e riscos do projeto*. Baseia-se nos artefatos *Visão* e *Plano de gerenciamento de riscos*, este último utilizado apenas durante o segundo fluxo, pois no primeiro ainda não tinha sido gerado. Os artefatos resultantes são a *Lista de riscos* e o *Plano de gerenciamento de riscos*. A seguir são descritos os passos dessa atividade: (i) *identificar eventuais riscos*; (ii) *analisar e priorizar riscos*; (iii) *identificar estratégias para evitar riscos*; (iv) *identificar estratégias para mitigar riscos*; (v) *identificar estratégias de contingência*; (vi) *reavaliar riscos durante a iteração*; e (vii) *reavaliar riscos no final da iteração*.

#### **Identificar eventuais riscos**

Esse passo consiste em relacionar tudo que pode dar errado com o projeto. Na fase *Iniciação*, deve-se reunir a equipe do projeto, para elaborar a *Lista de riscos*, que nesse ponto deve ser pequena, e para identificar e tentar eliminar eventuais barreiras que venham a dificultar o seu sucesso. Mais especificamente, procurar eventos capazes de diminuir a

probabilidade de o projeto ser concluído dentro do prazo e orçamento, e de entregar um produto com características corretas e o nível de qualidade exigido.

O RUP sugere a utilização de técnicas de *brainstorming* e listas de verificação genéricas de riscos, como as sugeridas em Jones (1994) e Carr (1993). Recomenda, ainda, que os participantes sejam esclarecidos de que “levantar um risco” não tem relação com “ser voluntário para tratá-lo”. Nas fases posteriores, os riscos são identificados a partir da *Lista de riscos* inicial. Isso geralmente acontece na avaliação da iteração.

### **Analisar e priorizar riscos**

Esse passo consiste em combinar riscos similares e classificá-los de acordo com os respectivos impactos para o projeto. Deve-se verificar se há grupamentos naturais (ocorrências do mesmo risco), e, sempre que possível, combinar os riscos, para se evitar duplicações. Algumas vezes os riscos identificados são sintomas de riscos mais básicos, devendo ser agrupados sob essa denominação.

Os riscos devem ser priorizados de acordo com a exposição geral que acarretam para o projeto. Para se determinar a exposição de cada risco, deve haver a estimativa das seguintes informações:

- *Impacto do risco*: desvios do planejamento referentes a cronograma, esforço ou custos.
- *Probabilidade de ocorrência*: probabilidade de que o risco efetivamente ocorra (geralmente expressa em porcentagem).
- *Exposição ao risco*: produto do impacto pela probabilidade de ocorrência (Impacto do risco  $\times$  Probabilidade de ocorrência).

A exposição de cada risco deve ser derivada de um consenso; diferenças de opinião significativas devem ser discutidas, para se avaliar de todos estão interpretando o risco da mesma maneira.

Os riscos devem ser classificados por ordem decrescente de exposição, para se criar a lista dos principais riscos. Convém ainda agrupar os riscos em categorias, com base nas

magnitudes dos respectivos impactos no projeto, com a seguinte gradação: alta, significativa, moderada, secundária e baixa.

Os riscos devem ser documentados, franqueando-se aos membros da equipe do projeto o acesso a essa documentação.

### **Identificar estratégias para evitar riscos**

O objetivo desse passo é reorganizar o projeto, para eliminar riscos. Algumas vezes, o risco pode ser completamente evitado. Por exemplo: riscos causados por um escopo pobre do sistema podem ser evitados pela redução desse escopo, eliminando-se requisitos não essenciais. O risco pode também ser transferido para outra organização.

### **Identificar estratégias para mitigar riscos**

Esse passo consiste em desenvolver planos de mitigação dos riscos, para reduzir seus impactos. Para riscos diretos, deve-se identificar as ações a serem implementadas para reduzir a probabilidade de sua ocorrência ou seu impacto no projeto. Como muitas vezes o risco origina-se da falta de informação, a estratégia de mitigação deve aprofundar o conhecimento sobre o tópico, a fim de reduzir a incerteza.

Há situações em que alguma ação pode ser implementada para fazer ocorrer o risco ou para eliminá-lo. Em um processo de desenvolvimento iterativo, essas ações devem acontecer nas iterações iniciais, para mitigar o risco o quanto antes. Por exemplo: se um risco está na forma “X pode não funcionar”, então “X” deve ser testado o mais cedo possível.

O resultado dessas ações deve ser a redução ou eliminação da probabilidade de ocorrência de certos riscos. Nos casos em que o risco seja confirmado, a resposta ao risco ocorre através de um *Plano de contingências*.

### **Identificar estratégias de contingência**

Esse passo consiste em desenvolver planos contendo ações alternativas. Para cada risco, deve ser elaborado um *Plano de contingências*, contendo as ações que devem ser implementadas se e quando o risco se materializar, independentemente de haver ou não um plano para mitigá-lo. Um *Plano de contingências* faz-se necessário quando falham as estratégias para evitar e transferir o risco, a tentativa de mitigação não obteve sucesso e é

necessário enfrentar o risco. Essa estratégia é sempre adotada no caso dos riscos indiretos, que são aqueles sobre os quais o projeto não tem controle, ou quando a implementação das estratégias de mitigação são muito dispendiosas. O *Plano de contingências* deve considerar:

- o risco identificado;
- o indicador, que irá sinalizar o momento em que o risco se concretizou; e
- a ação que deverá ser implementada para conter o prejuízo.

Segundo o RUP (2003), os indicadores podem ser as métricas do projeto, a observância de tendências e limites, os requisitos ou os resultados de testes ou eventos específicos. Sejam, por exemplo:

- gastos reais muito acima do planejado;
- tempo de resposta acima do exigido;
- componente de *software* não entregue no prazo por um terceiro.

O impacto dos planos de contingência costuma refletir-se nos custos e nos atrasos decorrentes da substituição da solução atual pela nova solução. A ocorrência do risco apresenta um lado positivo, ao forçar uma ação, podendo ainda indicar que houve falha nas estratégias implementadas para evitar ou mitigar os riscos, o que conduz à necessidade de reavaliação da *Lista de riscos*, para se determinar se a equipe do projeto apresenta algumas deficiências sistemáticas. A auto-avaliação é difícil, mas pode impedir outros problemas posteriores.

### **Reavaliar riscos durante a iteração**

O objetivo desse passo é garantir que a *Lista de riscos* seja continuamente atualizada no decorrer do projeto. A avaliação do risco é um processo contínuo, e não um processo que ocorre somente em intervalos específicos durante o projeto. As ações a seguir podem ser implementadas:

- reavaliar semanalmente a *Lista de riscos*, para verificar o que mudou;
- tornar visíveis para toda a equipe do projeto os dez principais riscos, e insistir que sejam tomadas providências específicas; e
- a *Lista de riscos* pode ser anexada aos relatórios de *Avaliação de status*.



### **Reavaliar riscos no final da iteração**

O objetivo desse passo é garantir que a *Lista de riscos* seja continuamente atualizada no decorrer do projeto. No final da iteração, devem-se focar novamente os objetivos da iteração com relação à *Lista de riscos*, especificamente para:

- eliminar riscos que tenham sido totalmente mitigados;
- introduzir riscos recém-descobertos; e
- reavaliar a magnitude e reordenar os riscos (analisar e priorizar os riscos).

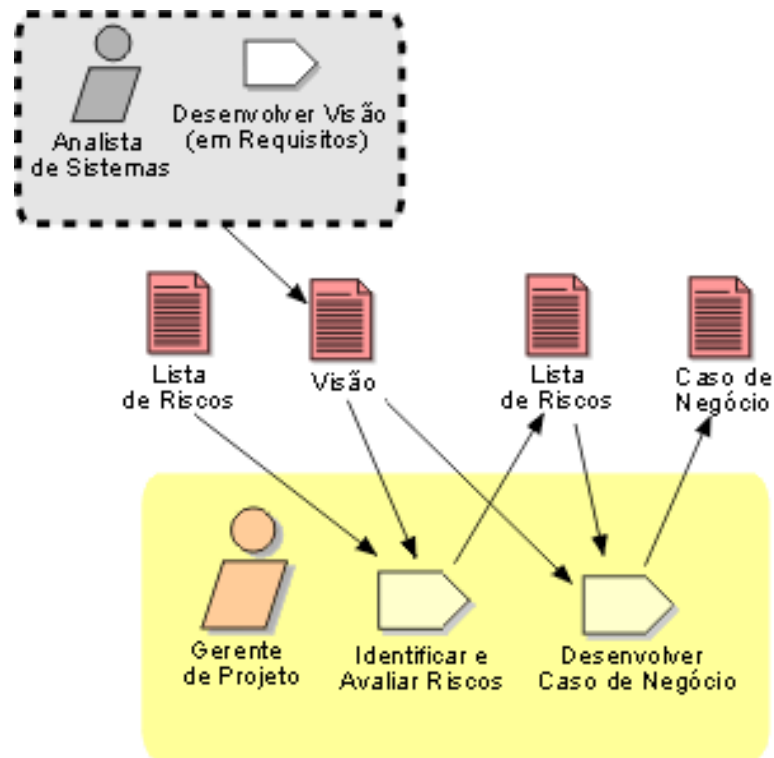
É natural que a *Lista de riscos* seja ampliada durante as fases *Iniciação* e *Elaboração*, pois, na medida em que fazem o trabalho, os membros da equipe verificam que algo que imaginaram ser trivial, na realidade contém riscos. Entretanto, os riscos devem diminuir à medida que o projeto alcança o fim da elaboração e durante a construção. Caso isso não ocorra, pode não estar havendo o controle apropriado dos riscos, ou o sistema pode ser muito complexo ou impossível de construir de uma forma sistemática e previsível.

### **3.3.2 FLUXO AVALIAR ESCOPO E RISCOS DO PROJETO**

Esse fluxo detalhado (Figura 3.7) é executado após a aprovação e o início do projeto, objetivando-se reavaliar as capacidades e características do projeto e os riscos associados, assim como fornecer uma base sólida para o planejamento detalhado. É também executado no final de cada iteração, quando há mais conteúdo sobre o projeto, e os riscos vão sendo eliminados.

O gerente do projeto executa a atividade Identificar e avaliar riscos (detalhada na seção 3.3.1.1) objetivando identificar, analisar e priorizar riscos para o projeto, bem como determinar as estratégias apropriadas de gerenciamento de riscos. Essa identificação efetiva-se com base no documento Visão, elaborado pelo analista de sistemas, e com base na Lista de riscos já elaborada.

Em seguida, o gerente do projeto executa a atividade *Desenvolver o caso de negócio*, pois, como as capacidades e os riscos agora são mais bem entendidos, o *caso de negócio* deve ser atualizado, com o objetivo de avaliar se o projeto continua merecedor do investimento na forma atual, ou se faz necessária uma mudança de direção.



**Figura 3.7 – Fluxo Avaliar escopo e riscos do projeto (RUP, 2003)**

### 3.3.3 FLUXO ELABORAR PLANO DE DESENVOLVIMENTO DE SOFTWARE

Após a reavaliação das capacidades e características do projeto, além dos riscos associados, deve-se partir para o planejamento, objeto desse fluxo, conforme ilustrado na Figura 3.8. Constituem propósitos desse fluxo desenvolver os componentes e delimitar o *Plano de desenvolvimento de software*, e, então, revisá-lo formalmente, para aceitação pelas partes interessadas e como base para refinar a granularidade do *Plano da iteração*.

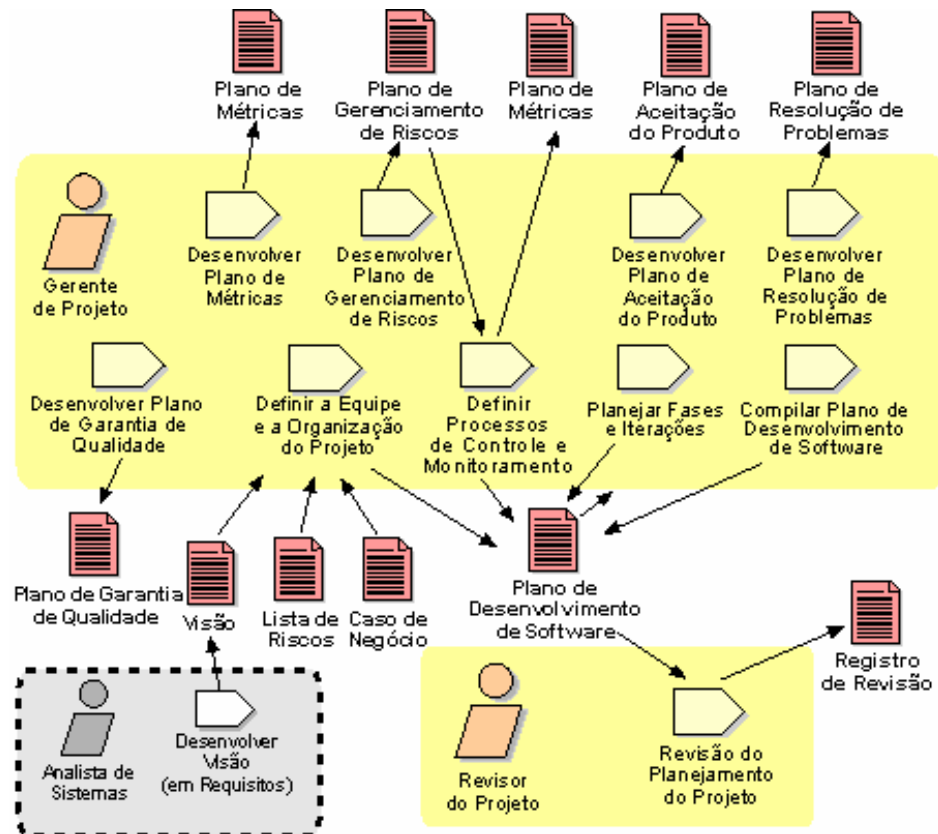
Esse fluxo reúne as seguintes atividades:

- *Desenvolver Plano de métricas*: definir metas de gerenciamento e determinar o que precisa ser periodicamente medido para suportar essas metas.
- *Desenvolver Plano de Gerenciamento de riscos*: detalhada na seção 3.3.3.1.

- *Desenvolver Plano de aceitação do produto*: criar um procedimento escrito, negociado com o cliente e com a equipe, para determinar a aceitabilidade dos produtos liberados.
- *Desenvolver Plano de resolução de problemas*: criar um procedimento documentado para gerenciar e resolver problemas ocorridos durante o projeto.
- *Desenvolver Plano de garantia de qualidade*: criar um plano documentado para as atividades de garantia da qualidade no projeto.
- *Definir a equipe e a organização do projeto*: definir a organização do projeto e os requisitos para os membros da equipe.
- *Definir processos de controle e monitoramento*: definir as informações e os processos a serem empregados para monitorar e controlar o andamento, a qualidade e os riscos do projeto.
- *Planejar fases e iterações*: fazer estimativas para o projeto; definir marcos das fases e suas metas; definir o número, o tamanho e os objetivos das iterações; definir os recursos para o projeto; e desenvolver o plano de finalização do projeto.
- *Compilar Plano de desenvolvimento de software*: coordenar o desenvolvimento de todos os planos associados, para publicação em um documento-mestre do *Plano de desenvolvimento de software*.
- *Revisão do planejamento do projeto*: aprovar o plano inicial ou revisar e aprovar mudanças efetuadas no *Plano de desenvolvimento de software*.

O maior esforço na criação dos artefatos ocorre logo na fase *Iniciação*; depois disso, quando esse fluxo é chamado no início de cada iteração, ocorre apenas uma revisão do *Plano de desenvolvimento de software*, com base na experiência da iteração anterior e no *Plano de iteração* para a próxima.

A seguir, a atividade *Desenvolver plano de gerenciamento de riscos*, que tem relação direta com o objetivo deste trabalho, é detalhada em finalidade, passos e artefatos e entrada e saída.



**Figura 3.8 – Fluxo *Elaborar plano de desenvolvimento de software* (RUP, 2003)**

### 3.3.3.1 ATIVIDADE *DESENVOLVER PLANO DE GERENCIAMENTO DE RISCOS*

São propósitos dessa atividade a criação de um plano documentado para identificação, análise e priorização dos riscos, como também a identificação das estratégias de gerenciamento de riscos para aqueles riscos mais significativos. É executada apenas no fluxo *Elaborar plano de desenvolvimento de software*, baseia-se no artefato *Lista de riscos*, e produz o artefato *Plano de gerenciamento de riscos*. A seguir são descritos os passos dessa atividade.

#### **Definir procedimentos e ferramentas para o gerenciamento de riscos**

O objetivo é definir os procedimentos a serem seguidos para se identificar, analisar e priorizar riscos. Além disso, deverão ser identificadas as ferramentas e técnicas a serem utilizadas na captura e armazenagem das informações sobre os riscos.

**Criar lista de riscos inicial**

Significa criar uma lista inicial de riscos, a ser utilizada como guia na seleção das estratégias da gerência de riscos, para que se tenha uma idéia dos tipos de risco a serem tratados.

**Designar a equipe de gerenciamento de riscos**

Consiste em decidir quais membros da equipe do projeto serão responsáveis pelo gerenciamento de riscos. Uma boa combinação seria a alocação do gerente do projeto, de representante do cliente ou o gerente de produto, o arquiteto de *software* e representantes das equipes de teste, desenvolvimento, documentação e distribuição. Uma boa prática é indicar um membro dessa equipe para ser o responsável oficial pelos riscos no projeto, competindo-lhe reunir e classificar os riscos à medida que forem identificados, relatar o *status* e programar reuniões de revisão dos riscos.

**Definir estratégias para gerenciar os dez maiores riscos**

Trata-se de decidir a abordagem a ser utilizada para manter os riscos sob controle e como remediar a situação caso os riscos venham a ocorrer. As abordagens de gerenciamento de riscos incluem prevenção, transferência, aceitação e mitigação.

**Definir indicadores para os dez maiores riscos**

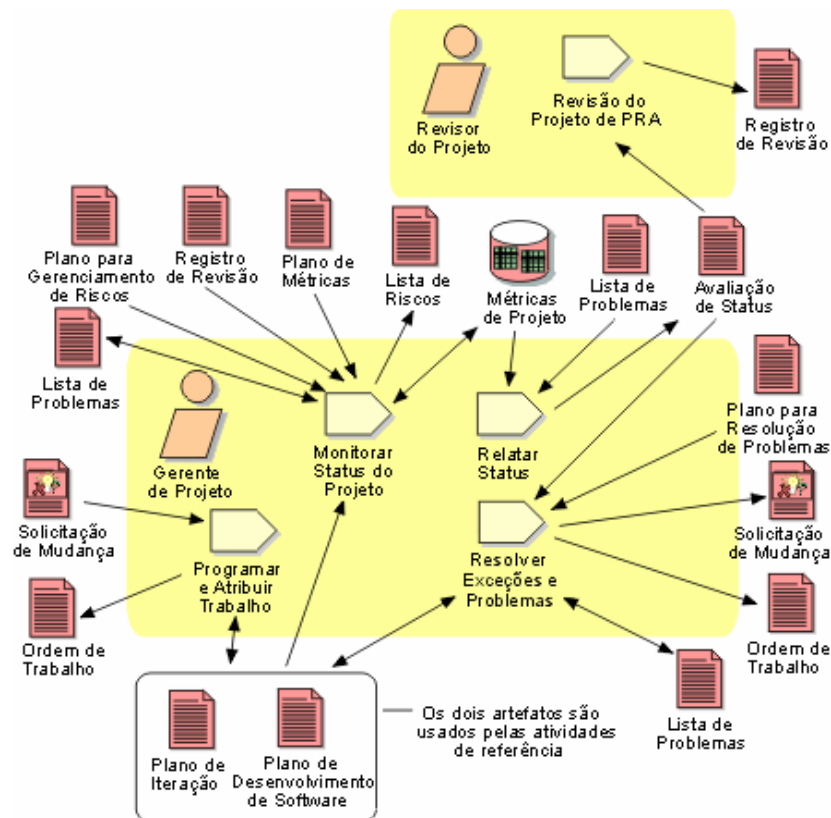
O objetivo desse passo é identificar uma condição mensurável que, se ocorrer, indique que o risco está prestes a se transformar em realidade. Essas condições são os indicadores do risco, devendo ser monitoradas pelo gerente ao longo do projeto, a fim de se detectar a necessidade de implementação do *Plano de contingências*.

**Definir cronograma para revisar e reportar riscos**

O objetivo é estabelecer um cronograma para a realização de reuniões de revisão dos riscos e emissão de relatórios regulares de *status* dos riscos. Também dever-se-á identificar as circunstâncias que determinam a necessidade de reuniões não programadas para a revisão dos riscos.

### 3.3.4 FLUXO MONITORAR E CONTROLAR O PROJETO

Esse fluxo (Figura 3.9) captura o trabalho cotidiano do gerente do projeto, incluindo a monitoração contínua do *status* do projeto no tocante a riscos ativos, medições objetivas do andamento e da qualidade, o tratamento das solicitações de mudanças aprovadas e dos problemas descobertos e o relato do *status* à *Autoridade de revisão de projeto* (PRA – *Project Review Authority*).



**Figura 3.9 – Fluxo Monitorar e controlar o projeto (RUP, 2003)**

A *Autoridade de revisão de projeto* é a entidade organizacional responsável por assegurar que um projeto de *software* esteja de acordo com políticas, práticas e padrões.

O gerente do projeto executa a atividade *Monitorar o status do projeto* e a atividade *Relatar status*, detalhadas adiante (seções 3.3.4.1 e 3.3.4.2), por envolverem a monitoração e o relato do *status* dos riscos.

O gerente do projeto executa ainda as atividades *Programar e atribuir trabalho* e *Resolver exceções e problemas*. A primeira consiste na acomodação das mudanças aprovadas, decorrentes de defeitos e de aprimoramentos, para produto e processo, surgidos

durante uma iteração. A segunda diz respeito à avaliação de exceções e problemas detectados, à determinação de ações corretivas e à emissão de solicitações de mudanças. O *Revisor do projeto* realiza a revisão do andamento do projeto com a PRA. A seguir são detalhadas as atividades *Monitorar o status do projeto* e *Relatar status*.

#### **3.3.4.1 ATIVIDADE MONITORAR O STATUS DO PROJETO**

O propósito dessa atividade é capturar o *status* atual do projeto e avaliá-lo a partir dos planos. Baseia-se em um conjunto de artefatos, entre os quais o *Plano de gerenciamento de riscos* e a *Lista de riscos*, atualizando a *Lista de riscos*, as *Métricas do projeto* e a *Lista de problemas*. A seguir são descritos os passos dessa atividade.

##### **Capturar o *status* do trabalho**

Significa coletar as informações de qualidade e de andamento do projeto, para avaliar seu *status* atual. O gerente de projeto captura as métricas primitivas sobre o andamento do projeto e a qualidade do produto, de acordo com os métodos descritos no *Plano de métricas* do projeto.

##### **Derivar indicadores de andamento**

O objetivo é derivar indicadores por meio das métricas primitivas reportadas pela equipe de projeto, a fim de se obter um panorama geral do andamento do projeto com relação aos planos. O *Plano de métricas* do projeto descreve como são calculados as métricas derivadas e os indicadores.

##### **Derivar indicadores de qualidade**

Trata-se de derivar indicadores para monitorar a qualidade dos artefatos do projeto de acordo com as métricas de qualidade definidas no *Plano de métricas* do projeto, que são consolidadas para fornecer um panorama geral do *status* do projeto, com base nos objetivos de qualidade especificados.

##### **Avaliar indicadores x planos**

Consiste em comparar os indicadores de andamento e de qualidade derivados, com o estado esperado do projeto, conforme definido no *Plano de desenvolvimento de software* e nos *Planos de iteração*.

O gerente do projeto revisa os indicadores dos riscos identificados para cada item da *Lista de riscos*, a fim de decidir se quaisquer estratégias de mitigação de riscos devem ser ativadas nesse momento. Avalia se todas as atividades planejadas foram concluídas, se os artefatos foram publicados conforme planejado, se o esforço estimado para concluir as tarefas em andamento está de acordo com o plano e se as métricas de qualidade observam as tolerâncias planejadas.

#### **3.3.4.2 ATIVIDADE REPORTAR STATUS**

Essa atividade propõe-se fornecer atualizações regulares no *status* do projeto para revisão pela *Autoridade de revisão de projeto*, e repassar para a PRA os problemas que se encontram além da autoridade do gerente do projeto, para que sejam solucionados. Baseia-se nos artefatos *Lista de riscos*, *Métricas do projeto*, *Lista de problemas* e *Avaliação de status*, e tem como saída a *Avaliação de status*. Descreve-se, a seguir, o passo que compõe essa atividade.

##### **Preparar avaliação de status**

Significa documentar o *status* atual do projeto para revisão pela PRA. A *Avaliação de status* deve abordar o progresso técnico, o progresso no orçamento, o progresso com base nos marcos do cronograma, o escopo total do projeto e do produto, o *status* da equipe, o *status* dos riscos, o surgimento de problemas e itens de ação.

### **3.4 MAPEAMENTO DO GERENCIAMENTO DE RISCOS**

Esta seção apresenta o mapeamento entre as abordagens de gerenciamento de riscos, nas quais se baseia este trabalho, e as seis macroatividades propostas para o *Processo de gerenciamento de riscos*, apresentadas detalhadamente no Capítulo 4. A tabela 3.3 contém um resumo desse mapeamento.

#### **3.4.1 PLANEJAR O GERENCIAMENTO DE RISCOS**

O *Planejamento do gerenciamento de riscos* no padrão AS/NZS 4360:2004 consiste em estabelecer o contexto e definir os critérios para o gerenciamento de riscos, enfatizando a importância da comunicação clara e tempestiva para o sucesso desse processo.



No PMBOK, o *Planejamento do gerenciamento de riscos* é o processo que consiste em decidir como abordar e conduzir as atividades da gerência de riscos para um projeto. Ressalta-se sua importância para assegurar que o nível, o tipo e a visibilidade da gerência de riscos sejam proporcionais ao risco e à importância do projeto para a organização. Isso garantirá também recursos e prazos suficientes para as atividades da gerência de risco, estabelecendo-se uma base consensual para a avaliação dos riscos. O resultado desse processo é o *Plano de gerenciamento de riscos*, que descreve como o gerenciamento deve ser estruturado e executado no projeto.

No CMMI-SW, a preparação para a *Gerência de riscos* é conduzida por meio do estabelecimento e da manutenção de uma estratégia para identificar, analisar e mitigar riscos. Geralmente, isso é documentado em um *Plano de gerenciamento de riscos*. A estratégia da gerência de risco refere-se às ações específicas e à abordagem gerencial implementadas para aplicar e controlar o processo.

No padrão IEEE Std 1540-2001, o planejamento consiste em estabelecer quem deve executar o gerenciamento de riscos; definir o processo específico a ser utilizado; atribuir os recursos necessários para a execução do processo; e definir como os riscos e seu tratamento serão comunicados entre as partes interessadas.

No RUP, o *Plano de gerenciamento de riscos* é um artefato de saída da atividade *Desenvolver o plano de gerenciamento de riscos*, que pertence à macroatividade *Planejamento do projeto*. Essa atividade tem como propósitos criar um plano documentado para identificação, análise e priorização dos riscos e identificar as estratégias de gerenciamento para os riscos mais relevantes do projeto.

As cinco abordagens apontam para a necessidade de se planejar o gerenciamento dos riscos de modo semelhante. Este trabalho procurou reunir os elementos essenciais de cada uma delas, com o objetivo de conduzir a um planejamento do gerenciamento de riscos que contemple todos os aspectos importantes. O CMMI exerceu forte influência sobre essa macroatividade.

Tabela 3.3 – Mapeamento do gerenciamento de riscos (PMBOK, CMMI, RUP, IEEE Std 1540, AS/NZS 4360)

Proposta de processo de gerenciamento de riscos para projetos de <i>software</i> (Macroatividade)	PMBOK	Norma AS/NZS 4360	Padrão IEEE STD 1540-2001	CMMI	RUP
	Área de conhecimento: Gerenciamento de riscos	Padrão específico para o gerenciamento de riscos	Padrão específico para o gerenciamento de riscos	Área de processo: Gerenciamento de riscos	Disciplina: Gerenciamento de projetos
<b>Planejar o gerenciamento de riscos</b>	Planejamento do gerenciamento de riscos	Comunicar e consultar  Estabelecer o contexto	Planejar e implementar o gerenciamento de riscos  Gerenciar o perfil de riscos do projeto	Preparar o gerenciamento dos riscos (SG 1): <ul style="list-style-type: none"> <li>Determinar fontes e categorias de riscos (SP 1.1)</li> <li>Definir parâmetros de riscos (SP 1.2)</li> <li>Estabelecer uma estratégia para o gerenciamento de riscos (SP 1.3)</li> </ul>	Planejamento do projeto <ul style="list-style-type: none"> <li>Desenvolver o plano de gerenciamento de riscos</li> </ul>
<b>Identificar riscos</b>	Identificação dos riscos	Identificar riscos	Executar a análise dos riscos <ul style="list-style-type: none"> <li>Identificação dos riscos</li> </ul>	Identificar e analisar riscos (SG 2) <ul style="list-style-type: none"> <li>Identificar riscos (SP 2.1)</li> </ul>	Avaliar o escopo do projeto e os riscos <ul style="list-style-type: none"> <li>Identificar e avaliar os riscos</li> </ul>
<b>Analisar riscos</b>	Análise qualitativa dos riscos	Analisar riscos <ul style="list-style-type: none"> <li>Análise qualitativa</li> <li>Análise semi-quantitativa</li> <li>Análise quantitativa</li> </ul>	Executar a análise dos riscos <ul style="list-style-type: none"> <li>Estimativas dos riscos</li> <li>Avaliação dos riscos</li> </ul>	Identificar e analisar riscos (SG 2) <ul style="list-style-type: none"> <li>Avaliar, categorizar e priorizar riscos (SP 2.2)</li> </ul>	Avaliar o escopo do projeto e os riscos <ul style="list-style-type: none"> <li>Identificar e avaliar os riscos</li> </ul>
	Análise quantitativa dos riscos	Avaliar riscos			
<b>Tratar riscos</b>	Planejamento das respostas aos riscos	Tratar riscos	Executar o tratamento dos riscos	Mitigar riscos (SG 3) <ul style="list-style-type: none"> <li>Desenvolver planos de mitigação de riscos (SP 3.1)</li> </ul>	Avaliar o escopo do projeto e os riscos <ul style="list-style-type: none"> <li>Identificar e avaliar os riscos</li> </ul>
<b>Monitorar e controlar riscos</b>	Monitoração e controle dos riscos	Monitorar e revisar	Executar a monitoração dos riscos	Mitigar riscos (SG 3) <ul style="list-style-type: none"> <li>Implementar os planos de mitigação de riscos (SP 3.2)</li> </ul>	Monitorar e controlar o projeto <ul style="list-style-type: none"> <li>Monitorar o <i>status</i> do projeto</li> </ul>
<b>Avaliar o processo de gerenciamento de riscos</b>			Avaliar o processo de gerenciamento de riscos	Práticas genéricas (GP) <ul style="list-style-type: none"> <li>Monitorar e controlar o processo (GP 2.8)</li> <li>Verificar implementação (GP 2.9)</li> </ul>	

### 3.4.2 IDENTIFICAR RISCOS

O padrão AS/NZS 4360:2004 considera fundamental um processo de identificação de riscos bem estruturado, pois os riscos não identificados nesse ponto serão excluídos de análises posteriores.

A *Identificação de riscos* no PMBOK envolve a determinação dos eventuais riscos em um projeto específico, assinalando-se quais deles podem afetar esse projeto e documentando-se suas características. Trata-se de um processo iterativo, porque novos riscos podem surgir durante o ciclo de vida do projeto. A frequência das iterações e a definição de quem deve participar de cada ciclo varia caso a caso. A equipe do projeto deve estar envolvida de maneira a desenvolver um senso de responsabilidade pelos riscos e implementar as ações necessárias.

No padrão IEEE Std 1540-2001, a identificação dos riscos está incluída no processo de análise dos riscos, composto também da avaliação dos riscos. Consiste em identificar os riscos de acordo com as categorias incluídas no contexto do gerenciamento de riscos e na identificação de mudanças nesse contexto.

Segundo o CMMI-SW, a identificação de potenciais situações, perigos, ameaças e vulnerabilidades, que poderiam afetar negativamente os esforços ou planos de trabalho, constitui a base para a bem-sucedida gerência de riscos. Os riscos devem ser identificados e documentados em uma linguagem concisa, que inclua o contexto, as condições e as conseqüências de sua ocorrência, para que possam ser corretamente analisados e controlados. O uso de categorias e parâmetros desenvolvidos na estratégia de gerenciamento dos riscos, juntamente com as fontes identificadas de riscos, pode fornecer disciplina e otimização apropriadas à identificação dos riscos.

A atividade *Identificar e avaliar riscos* do RUP tem como propósitos identificar, analisar e priorizar os riscos para o projeto e determinar as estratégias apropriadas de gerenciamento de riscos. Produto dessa atividade, a *Lista de riscos* é um artefato fundamental para o RUP, ao atuar como ponto focal para as atividades do projeto, representando a base em torno da qual são organizadas as iterações.

Verifica-se que as cinco abordagens mantêm forte sintonia no tocante ao processo de identificação dos riscos. Todas enfatizam que a identificação dos riscos deve ocorrer de forma iterativa durante o ciclo de vida do projeto, com o envolvimento da equipe do projeto, constituindo um processo fundamental para o gerenciamento do projeto como um todo. O processo proposto baseou-se nos pontos mais relevantes de cada uma delas.

### 3.4.3 ANALISAR RISCOS

No padrão AS/NZS 4360:2004, a análise de riscos é subdividida em análise e avaliação dos riscos. A análise consiste no processo sistemático de entender a natureza dos riscos, estabelecer o nível desses riscos e considerar as possíveis conseqüências. A avaliação compara o nível estimado de cada risco com os critérios pré-estabelecidos, a fim de embasar as decisões que serão tomadas, bem como a extensão e a natureza do tratamento requerido.

O PMBOK subdivide a análise dos riscos em análise qualitativa e análise quantitativa. A análise qualitativa geralmente constitui um meio rápido de estabelecer prioridades para o planejamento da resposta aos riscos, avalia a prioridade dos riscos identificados, usando sua probabilidade de ocorrência e o impacto correspondente nos objetivos do projeto, se os riscos ocorrerem. O resultado dessa análise fornece a base para a análise quantitativa dos riscos, caso esta seja requerida. A análise quantitativa caracteriza-se pela medição e pela análise numérica, que vai além das escalas utilizadas na análise qualitativa. É opcional, devendo ser utilizada apenas para os riscos mais críticos.

No padrão IEEE Std 1540-2001, a análise dos riscos envolve a identificação e avaliação dos riscos. A avaliação dos riscos envolve também a análise quantitativa. O que no processo proposto é denominado *análise dos riscos*, nesse padrão, uma parcela está contida na identificação de riscos, incluindo-se a outra parcela na avaliação de riscos.

No CMMI-SW, a análise qualitativa dos riscos está especificada na prática específica *Avaliar, categorizar e priorizar riscos*, que pertence ao objetivo específico *Identificar e analisar riscos*. A avaliação e a categorização de cada risco identificado utiliza as categorias e os

parâmetros de riscos, sendo, em seguida, determinada a sua prioridade. Os parâmetros de riscos definidos podem incluir a probabilidade, a consequência (severidade ou impacto) e os limites.

A atividade *Identificar e avaliar riscos* do RUP tem como propósitos identificar, analisar e priorizar os riscos para o projeto e determinar as estratégias apropriadas de gerenciamento de riscos. Os passos *Analisar e priorizar riscos*, *Reavaliar riscos durante a iteração* e *Reavaliar riscos no final de uma iteração* estão diretamente ligados à análise dos riscos.

Todas as abordagens pesquisadas tratam da análise dos riscos, ressaltando-se a importância de se determinar a probabilidade e o impacto da ocorrência dos riscos, a categorização desses riscos e a contínua atualização da *Lista de riscos*. O processo proposto baseou-se nos pontos mais relevantes de cada uma delas, recebendo forte influência do PMBOK, no tocante à análise quantitativa dos riscos.

#### **3.4.4 TRATAR RISCOS**

De acordo com o padrão AS/NZS 4360:2004, tratar riscos consiste em identificar as opções de tratamento, avaliar essas opções e preparar e executar planos de tratamento. Ressalta-se o fato de não ser viável, em termos de custos, a implementação de todas as opções de tratamento, devendo ser selecionada a combinação ideal de opções ou a opção mais apropriada.

O *Planejamento das respostas aos riscos* compreende o desenvolvimento de opções e a definição de ações para ampliar oportunidades e reduzir ameaças aos objetivos do projeto. Inclui a identificação e a atribuição dos indivíduos ou grupos que irão responsabilizar-se por cada resposta planejada aos riscos, e insere recursos e tarefas no orçamento, no cronograma e no plano de gerenciamento do projeto, se necessário. Esse processo deve ser realístico dentro do contexto do projeto, levando-se em conta os custos envolvidos. Ressalta-se também que às vezes torna-se necessário selecionar a melhor resposta aos riscos dentre diversas opções disponíveis.

No padrão IEEE Std 1540-2001, o tratamento dos riscos consiste em determinar se os riscos são aceitos pelas partes interessadas, e, em caso negativo, dar-se início a ações para reduzir

os riscos a um nível aceitável. Significa selecionar o tratamento, planejar, monitorar e controlar as ações para diminuir a exposição aos riscos.

Segundo o CMMI-SW, as etapas do tratamento de riscos incluem o desenvolvimento de opções de tratamento de riscos, a monitoração de riscos e a execução das atividades de tratamento, quando forem excedidos os limites definidos. Os planos de mitigação de riscos são desenvolvidos e executados, para que o eventual impacto da ocorrência dos riscos selecionados seja proativamente reduzido. Isso deve também incluir planos de contingência, para tratar do impacto dos riscos selecionados, que, apesar das tentativas de mitigá-los, podem vir a ocorrer.

No RUP, alguns passos especificados na atividade *Identificar e avaliar riscos* correspondem ao tratamentos dos riscos: *Identificar estratégias para evitar riscos*, *Identificar estratégias para mitigar riscos* e *Identificar estratégias de contingência*.

Todas as abordagens referem-se ao tratamento dos riscos considerando as estratégias para lidar com os riscos por meio de sua eliminação, aceitação ou transferência, da elaboração do plano de mitigação e do plano de contingências. O processo proposto recebeu contribuição de todas elas, em especial do padrão AS/NZS 4360:2004 e do PMBOK.

### **3.4.5 MONITORAR E CONTROLAR RISCOS**

No padrão AS/NZS 4360:2004, a monitoração e controle dos riscos encontra-se no processo *Monitorar e revisar*, que se fundamenta no acompanhamento dos riscos, identificando-se mudanças que possam afetar sua probabilidade e consequência, comparando-se periodicamente o progresso atual com as ações previstas para tratamento dos riscos. Constitui um dos aspectos mais importantes do gerenciamento de riscos, pois é o que vai garantir a efetividade do processo.

Segundo o padrão IEEE Std 1540-2001, a monitoração dos riscos consiste em revisar e atualizar o *status* dos riscos e o seu contexto, avaliando-se a efetividade do tratamento dos riscos e identificando-se novos riscos.

No PMBOK, processo *Monitoração e controle dos riscos* consiste em identificar, analisar e planejar os novos riscos, mediante acompanhamento dos riscos identificados e daqueles incluídos na lista de observação, monitorando-se as “condições de disparo” dos planos de contingência, assim como riscos residuais, e revendo-se a execução das respostas aos riscos. A execução desse processo pode conduzir à implementação do plano de contingências, ou mesmo ao replanejamento do projeto. Prevê, também, a inclusão de lições aprendidas nas bases de dados do projeto e modelos da gerência de riscos, para beneficiar futuros projetos.

O CMMI-SW determina que para se controlar e gerenciar eficazmente os riscos durante o esforço de trabalho, deve-se seguir um programa proativo para monitorar regularmente os riscos e seu *status*, além dos resultados das ações de acompanhamento dos riscos, o que pode resultar na descoberta de novos riscos ou de novas opções de tratamento, que podem requerer o replanejamento e a reavaliação. A prática específica de que trata essa monitoração denomina-se *Implementar planos de mitigação de riscos*.

No RUP, a monitoração dos riscos está referenciada na atividade *Monitorar o status do projeto*, por meio da captura do *status* do trabalho, da derivação dos indicadores de progresso e de qualidade e da comparação dos indicadores com os planos.

Todas as abordagens indicam a necessidade de se monitorar e controlar os riscos durante todo o ciclo de vida do projeto, por meio da reavaliação dos riscos e do acompanhamento dos indicadores. O processo proposto recebeu contribuição de todas elas, procurando-se dar destaque à importância da comunicação do *status* dos riscos, bastante enfatizado na AS/NZS 4360:2004.

### **3.4.6 AVALIAR O PROCESSO DE GERENCIAMENTO DE RISCO**

O padrão IEEE Std 1540-2001 inclui a atividade *Avaliar o processo de gerenciamento de riscos*, que objetiva avaliar a qualidade do processo e identificar as áreas em que os procedimentos, os processos e a política de gerenciamento de riscos podem ser melhorados.

O CMMI-SW contém em sua essência a melhoria contínua dos processos. Esse aspecto pontua as práticas genéricas de todas as áreas de processo.

A avaliação do processo objetivando a melhoria contínua é tratada explicitamente apenas nas duas citadas abordagens. Optou-se por incluí-la neste trabalho para destacar a sua importância, seguindo-se a estrutura do padrão IEEE Std 1540-2001. Entretanto, caso a organização possua um processo específico para o gerenciamento e melhoria de todos os processos, essa atividade poderá compor esse processo, como foi o caso da empresa de *software* em que foi aplicado o estudo de caso deste trabalho.

### **3.5 CONCLUSÃO**

Este capítulo apresentou processos para gerenciamento de riscos de *software* desenvolvidos pelo IEEE Std 1540-2001, pelo CMMI e pelo RUP. O capítulo seguinte aborda o *Processo de gerenciamento de riscos de software* proposto neste trabalho.



## Capítulo 4

# PROCESSO DE GERENCIAMENTO DE RISCOS DE SOFTWARE

---

*Este capítulo apresenta o Processo de gerenciamento de riscos proposto para projetos de software.*

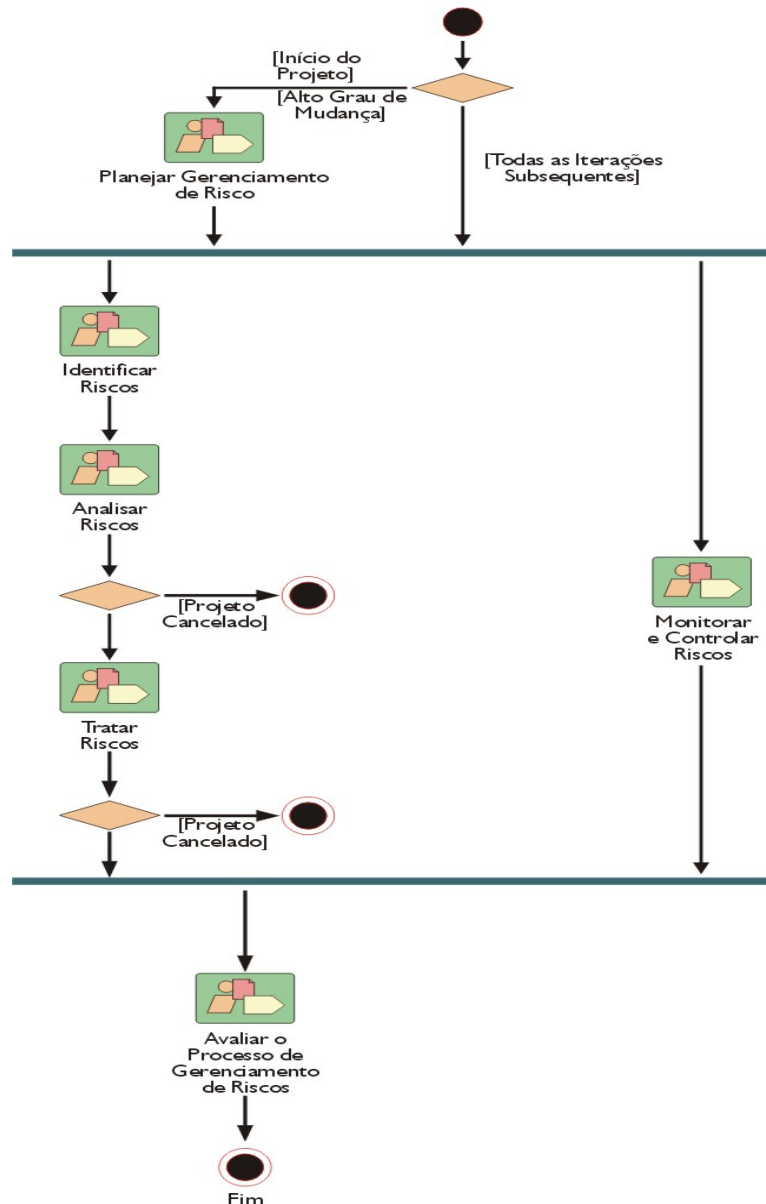
O *Processo de gerenciamento de riscos para projetos de software* ora proposto baseia-se no padrão AS/NZS 4360 (2004), na área de conhecimento *Gerenciamento de riscos* do PMBOK (2004), no padrão IEEE Std 1540 (2001), na área de processo *Gerenciamento de riscos* do CMMI (2002) e na *Abordagem de riscos* do RUP (2003).

Esse processo visa auxiliar o planejamento, a identificação, a análise, o tratamento e a sistemática monitoração dos riscos em projetos de *software*, contribuindo para o processo decisório durante o ciclo de vida do projeto. Esse processo poderá ser utilizado diretamente em organizações de *software*, ou especializado para essas organizações, e, posteriormente, instanciado para projetos de *software* independentemente dos respectivos portes. Para projetos de pequeno porte, por exemplo, pode ser executado apenas um subconjunto das atividades desse processo, o que deve ser previamente definido no planejamento do gerenciamento de riscos do referido projeto.

A partir da experiência de implantação do processo ora proposto em uma organização de *software* (Capítulo 5), foram elaboradas *guidelines* para a especialização desse processo (seção 4.7). Além disso, a partir dos resultados da especialização empreendida, foram feitos ajustes, para seu refinamento.

O formato de apresentação do processo segue a estrutura do RUP (2003), por ser amigável e ter sido utilizado em várias organizações. Além disso, o processo proposto de gerenciamento de riscos para projetos de *software* também é aderente ao ciclo de vida iterativo incremental.

O principal fluxo do processo proposto (Figura 4.1) possui as seguintes macroatividades: (i) *Planejar o gerenciamento de riscos*; (ii) *Identificar riscos*; (iii) *Analisar riscos*; (iv) *Tratar riscos*; (v) *Monitorar e controlar riscos*; e (vi) *Avaliar o processo de gerenciamento de riscos*.



**Figura 4.1 – Fluxo do Processo de gerenciamento de riscos de software**

A macroatividade *Planejar o gerenciamento de riscos* deve ser executada no início do projeto, e ser repetida, se houver um grau de mudança significativo, que justifique a necessidade de um novo planejamento. As atividades dos itens *ii* a *v* devem ocorrer a cada iteração, quando for utilizado o ciclo de vida iterativo incremental. A macroatividade *Avaliar o processo de gerenciamento de riscos* deve ser executada ao final do projeto, para averiguar a efetividade do processo e capturar lições aprendidas. A

Tabela 4.1 apresenta um resumo das macroatividades, com respectivas atividades e passos correspondentes.

**Tabela 4.1 – Detalhamento do fluxo do *Processo de gerenciamento de riscos***

Macroatividade	Atividades	Passos
Planejar o gerenciamento de riscos	Determinar fontes e categorias de riscos	Determinar as fontes de riscos
		Determinar as categorias de riscos
	Definir parâmetros para os riscos	Definir critérios para a análise dos riscos
		Definir critérios para o tratamento dos riscos
		Definir métricas
		Definir limites para cada categoria de riscos
		Definir indicadores para a avaliação do processo
	Estabelecer estratégia	Adaptar o processo ao projeto
		Definir metodologia
		Atribuir papéis e responsabilidades
		Definir periodicidade
		Planejar comunicação
		Definir a avaliação do processo
Identificar riscos	Identificar riscos potenciais	Identificar os riscos associados às fontes e categorias
		Revisar a documentação do projeto
		Revisar as informações históricas
	Estabelecer o contexto dos riscos	Detectar as circunstâncias ou condições dos riscos
Analisar riscos	Categorizar os riscos	Agrupar os riscos de acordo com as categorias
	Avaliar impacto e probabilidade	Avaliar o impacto dos riscos
		Avaliar a probabilidade de ocorrência dos riscos
		Determinar a exposição aos riscos
	Priorizar riscos	Determinar a prioridade relativa dos riscos
Analisar riscos quantitativamente	Analisar os riscos quantitativamente	
Tratar riscos	Selecionar estratégias	Definir limites
		Selecionar estratégias para ameaças
		Selecionar estratégias para oportunidades
		Selecionar riscos que serão aceitos
	Definir e selecionar respostas aos riscos	Definir ações de respostas aos riscos
		Avaliar e selecionar as ações
		Definir plano de contingências
		Associar gatilhos aos riscos
Monitorar e controlar riscos	Monitorar e controlar riscos	Designar proprietário e envolvidos
		Acompanhar o estado atual dos riscos
		Executar plano de tratamento dos riscos
	Reportar estados dos riscos	Acompanhar o plano de tratamento dos riscos
		Revisar a documentação dos riscos
		Comunicar estados dos riscos
Avaliar o processo de gerenciamento de riscos	Avaliar o processo	Capturar informações sobre o processo
		Avaliar e melhorar o processo
		Gerar lições aprendidas

Para o *Processo de gerenciamento de riscos* proposto, foram identificados como importantes para a realização de suas atividades os seguintes papéis: o *Gerente do projeto*, o *Especialista em riscos* e o *Envolvido no projeto (stakeholder)*.

O *Gerente do projeto* é o responsável pelo gerenciamento do projeto como um todo, e participa ou é responsável por grande parte das atividades de gerenciamento de riscos. É fundamental que o gerente incentive a equipe do projeto a considerar os riscos efetivamente.

O papel do *Especialista em riscos* deve ser desempenhado por um profissional com embasamento em riscos e experiência consolidada em projetos de desenvolvimento de *software*. Esse especialista participa de algumas atividades do processo, ora como ator principal, ora apoiando o *Gerente do projeto*.

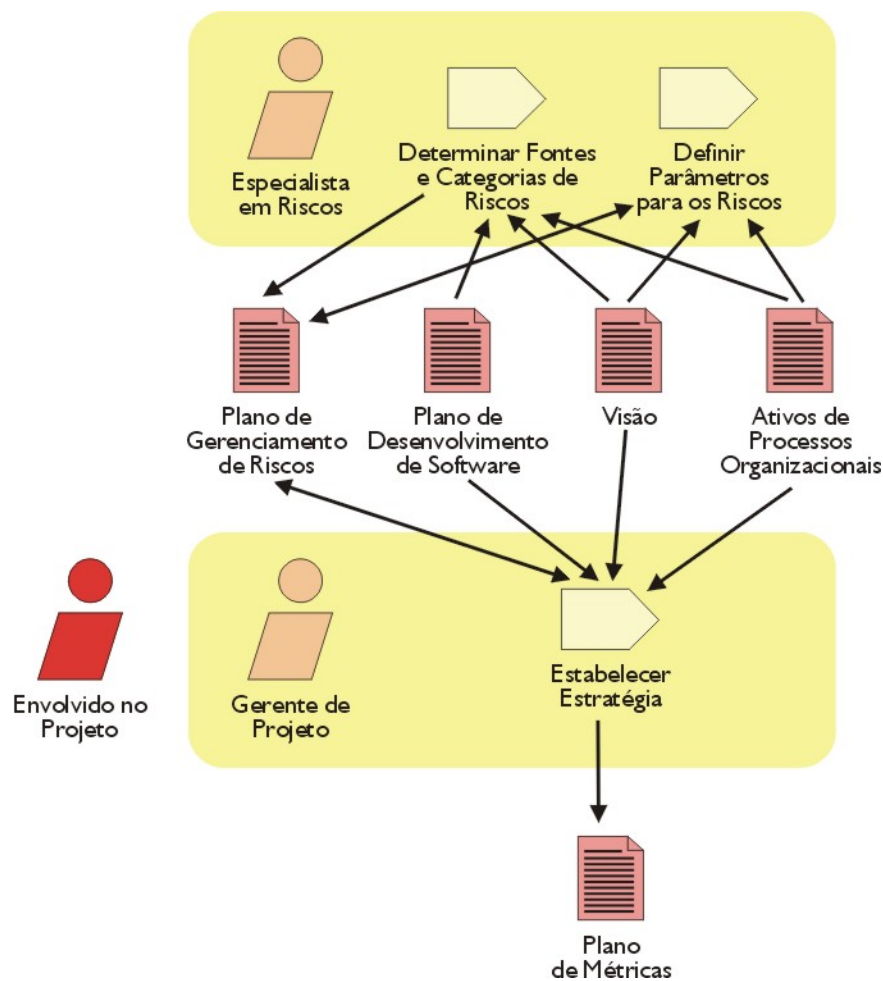
O papel do *Envolvido no projeto* deve ser desempenhado por qualquer indivíduo que possa ser afetado pelo resultado do projeto (*stakeholder*). O envolvido pode ser externo ou interno; o primeiro é parte interessada no projeto, e o segundo integra a equipe do projeto. Este último poderá ser designado proprietário de determinado risco, ou seja, responsável por cada resposta planejada ao risco (PMBOK, 2004). Este trabalho apresenta também os *templates* dos artefatos específicos para o *Processo de gerenciamento de riscos*: o *Plano de gerenciamento de riscos* (Apêndice A) e o *Registro de riscos* (Apêndice B). Os *templates* dos demais artefatos de entrada e saída, cuja utilização é sugerida neste trabalho, podem ser obtidos no RUP (2003).

O artefato *Ativos de processos organizacionais* consiste dos ativos relacionados aos processos da organização, que podem incluir políticas, planos, procedimentos, diretrizes, processos definidos, métricas e bases de conhecimento, como lições aprendidas e informações históricas. Os ativos do processo de riscos podem integrar também esse artefato, contendo abordagens predefinidas em relação ao gerenciamento de riscos, como fontes e categorias de riscos, parâmetros, definição comum de conceitos e termos e funções e responsabilidades.

A seguir são apresentadas as macroatividades do processo proposto: (i) *Planejar o gerenciamento de riscos*; (ii) *Identificar riscos*; (iii) *Analisar riscos*; (iv) *Tratar riscos*; (v) *Monitorar e controlar riscos*; e (vi) *Avaliar o processo de gerenciamento de riscos*.

#### 4.1 MACROATIVIDADE *PLANEJAR O GERENCIAMENTO DE RISCOS*

A macroatividade *Planejar o gerenciamento de riscos* contém as atividades detalhadas na Figura 4.2, que devem ser executadas no início do planejamento do projeto. Quando ocorrer mudanças significativas, que exijam um novo planejamento do gerenciamento de riscos no projeto, essa macroatividade deve ser novamente executada. O objetivo desse planejamento é descrever como os elementos e recursos do processo de gerenciamento de riscos serão tratados no projeto.



**Figura 4.2 – Macroatividade *Planejar o gerenciamento de riscos***

Caso a organização já utilize em algum grau as práticas de gerenciamento de riscos, e esteja utilizando o processo proposto para a definição de seu processo de gerenciamento de riscos, torna-se oportuna uma análise de projetos anteriores, a fim de se definir previamente os ativos do processo de riscos, para posterior utilização nos projetos. Essa

definição tem o objetivo de preparar a organização para um gerenciamento de riscos mais proativo, e que venha a atender ao processo *Gerenciamento de riscos* do CMMI nível 3.

Em Pinho (2005) é apresentada uma metodologia para análise do tratamento de riscos, proposta para uma dada organização, mas que pode ser aplicada a outras organizações que já adotem o gerenciamento de riscos.

Entretanto, numa organização que não utilize práticas de gerenciamento de riscos e que esteja utilizando o processo proposto para iniciar a implantação das atividades relacionadas a riscos, as informações sobre fontes, categorias, parâmetros e estratégias a serem utilizadas no projeto podem ser definidas com base na literatura. Nesse caso, por meio do exercício do processo nos projetos serão gerados os ativos do processo de riscos adequados à organização.

Nessa macroatividade, o *Especialista em riscos* determina as fontes e as categorias de riscos com base nos *Ativos de processos organizacionais* e nas características do projeto a ser desenvolvido. Define também os parâmetros a serem utilizados para analisar, tratar e controlar o esforço do gerenciamento de riscos. As fontes, as categorias e os parâmetros previamente definidos pela organização figuram nos *Ativos de processos organizacionais*, devendo ser revisados para utilização no projeto.

O *Gerente do projeto* estabelece a estratégia a ser adotada para a condução das atividades de gerenciamento de riscos no projeto, por meio da seleção das estratégias recomendadas pela organização constantes nos *Ativos de processos organizacionais*. Essa estratégia envolve a adaptação do processo ao projeto, as abordagens, técnicas e ferramentas a serem utilizadas, a atribuição dos papéis e responsabilidades, a definição da periodicidade da monitoração e controle dos riscos, o planejamento da comunicação interna e externa ao projeto e a avaliação do processo de gerenciamento de riscos.

Essas informações devem ser registradas no *Plano de gerenciamento de riscos*, que descreve como o gerenciamento de riscos deverá ser estruturado e executado no projeto. O Apêndice B contém um *template* para o artefato *Plano de gerenciamento de riscos*.

A macroatividade *Planejar o gerenciamento de riscos* é composta por três atividades: (i) *Determinar as fontes e categorias de riscos*; (ii) *Definir parâmetros para os riscos*; e (iii) *Estabelecer estratégia*. Cada atividade é detalhada em: propósito, artefatos de

entrada, artefatos resultantes e papel responsável. Os artefatos estão definidos no glossário e constituem exemplos de artefatos do projeto que podem ser utilizados.

#### 4.1.1 ATIVIDADE *DETERMINAR FONTES E CATEGORIAS DE RISCOS*

De acordo com o CMMI-SW (2002), a determinação de fontes de riscos e a decisão sobre a categorização de riscos a ser utilizada são fundamentais para a identificação dos riscos e para a sua organização, para efeito de avaliação. O quadro 4.1 apresenta essa atividade.

**Quadro 4.1 – Atividade *Determinar fontes e categorias de riscos***

<b>Propósito:</b> Fornecer a base para identificação e organização dos riscos no projeto	
<b>Passos:</b> <ul style="list-style-type: none"> <li>• Determinar as fontes de riscos</li> <li>• Determinar as categorias de riscos</li> </ul>	
<b>Artefatos de entrada:</b> <ul style="list-style-type: none"> <li>• Ativos de processos organizacionais</li> <li>• Visão</li> <li>• Plano de desenvolvimento de <i>software</i></li> </ul>	<b>Artefatos resultantes:</b> <ul style="list-style-type: none"> <li>• Plano de gerenciamento de riscos</li> </ul>
<b>Papel:</b> Especialista em riscos	

A seguir são apresentados os dois passos dessa atividade.

##### 4.1.1.1 DETERMINAR AS FONTES DE RISCOS

O propósito desse passo é identificar as fontes internas e externas de riscos, para a identificação antecipada dos riscos. Uma lista de fontes de riscos prováveis para a organização deve figurar nos *Ativos de processos organizacionais*.

As fontes de riscos são elementos essenciais, que podem causar danos em um projeto ou em uma organização, e mostram as áreas comuns em que os riscos podem originar-se. A identificação dessas fontes fornece uma base para a observação sistemática, possibilitando a descoberta das circunstâncias que podem impactar a capacidade do projeto de atingir seus objetivos.

De acordo com PFLEEGER et al (2001), as decisões de projeto devem ser analisadas, pois representam potenciais fontes de riscos. Essas fontes podem ser internas ou externas ao projeto. Enquanto o projeto progride, podem ser identificadas fontes adicionais de riscos. Segundo o CMMI (2002), as fontes típicas de riscos internas e externas incluem:

- requisitos instáveis;
- esforços sem precedentes – estimativas não disponíveis;
- projeto inviável;
- tecnologia não disponível;
- estimativas de cronograma ou alocação de recursos não realísticas;
- equipe e habilidades inadequadas;
- fluxo de custos ou financiamentos;
- capacidade incerta ou inadequada do subcontratante;
- capacidade incerta ou inadequada do fornecedor.

De acordo com Chrissis (2004), as mudanças são as maiores fontes para a introdução de novos riscos em um sistema ou processo, sejam mudanças nos requisitos do cliente, mudanças organizacionais ou nos recursos.

Muitas dessas fontes de riscos são freqüentemente aceitas sem um planejamento adequado. A identificação das fontes internas e externas de riscos no início do projeto pode conduzir à identificação antecipada dos riscos. Planos de mitigação dos riscos podem, então, ser implementados no início do projeto, para evitar a ocorrência dos riscos ou para reduzir suas conseqüências.

#### **4.1.1.2 DETERMINAR AS CATEGORIAS DE RISCOS**

São propósitos desse passo fornecer um mecanismo para coletar e organizar riscos, além de assegurar um exame detalhado e a atenção apropriada da gerência para os grupos de riscos que podem ter conseqüências mais sérias para os objetivos do projeto.

As categorias de riscos são grupamentos organizados de riscos que têm forte correlação, provendo uma estrutura que possibilite a sua identificação sistemática com qualidade e efetividade. Uma razão para identificar categorias de riscos consiste em ajudar na futura consolidação das atividades nos planos de tratamento dos riscos. A habilidade



para segmentar as categorias de riscos possibilita o direcionamento dos recursos para aquelas áreas de maior interesse ou dificuldade (JIANG, 1999).

Os riscos do projeto podem ser categorizados por área afetada, por fase do ciclo de vida ou outro critério que seja útil para determinar as áreas do projeto mais expostas aos efeitos da incerteza (PMBOK, 2004).

Segundo o CMMI (2002), ao se determinar as categorias de riscos, podem ser considerados os seguintes fatores:

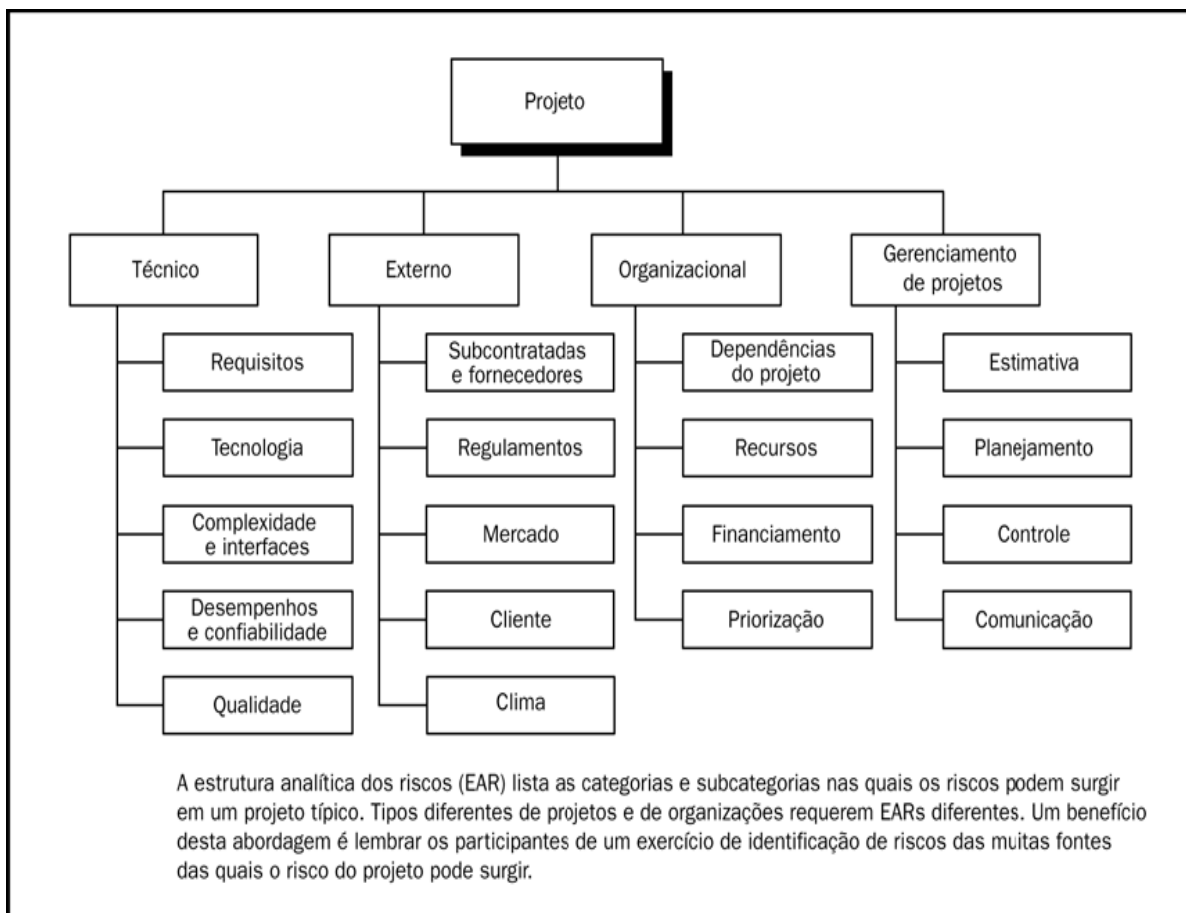
- tipos de processos utilizados;
- tipos de produtos utilizados;
- riscos de gerência (por exemplo: riscos de contrato, riscos de orçamento / custos, riscos relacionados aos recursos, riscos de desempenho);
- fases do modelo de ciclo de vida do projeto.

Ropponen (2000) sugere a seguinte categorização para riscos de desenvolvimento de *software*:

- riscos de cronograma e prazo;
- riscos de funcionalidade do sistema;
- riscos de subcontratação;
- riscos de gerenciamento de requisitos;
- riscos de uso de recursos e desempenho;
- riscos de gerenciamento de recursos humanos.

A identificação dessas categorias assegurará a atenção apropriada da gerência aos grupos de riscos que poderão gerar conseqüências mais sérias para os objetivos do projeto e facilitar a elaboração de respostas adequadas.

De acordo com o PMBOK (2004), uma organização pode usar uma categorização previamente definida de riscos típicos, como a *Estrutura analítica dos riscos* (EAR). Essa abordagem provê uma representação hierarquicamente organizada dos riscos dispostos por categoria e subcategoria, representando as diversas áreas de riscos potenciais, que serão utilizadas no processo de identificação dos riscos. A EAR geralmente é adaptada para tipos específicos de projetos. A Figura 4.3 apresenta um exemplo de EAR.



**Figura 4.3 – Estrutura Analítica de Riscos (PMBOK, 2004)**

Uma taxonomia de riscos, como a proposta pelo SEI (*Software Engineering Institute*) em *Taxonomy-Based Risk Identification* (CARR, 1993), pode ser utilizada no sentido de fornecer uma estrutura adequada para determinar fontes e categorias de riscos (CMMI, 2002).

#### **4.1.2 ATIVIDADE *DEFINIR PARÂMETROS PARA OS RISCOS***

Essa atividade tem como principais objetivos a definição de parâmetros para a análise, a categorização, o tratamento e o controle do esforço do gerenciamento de riscos no projeto, conforme Quadro 4.2.

Uma revisão dos parâmetros predefinidos para a organização deve ser conduzida, no sentido de avaliar a sua adequação para a utilização no projeto, de acordo com suas características.

### Quadro 4.2 – Atividade *Definir parâmetros para os riscos*

<b>Propósito:</b> Definir critérios para comparar os vários riscos a serem gerenciados	
<b>Passos:</b> <ul style="list-style-type: none"> <li>• Definir critérios para a análise dos riscos</li> <li>• Definir critérios para o tratamento dos riscos</li> <li>• Definir métricas</li> <li>• Definir limites para cada categoria de riscos</li> <li>• Definir indicadores para a avaliação do processo</li> </ul>	
<b>Artefatos de entrada:</b> <ul style="list-style-type: none"> <li>• Ativos de processos organizacionais</li> <li>• Visão</li> <li>• Plano de gerenciamento de riscos</li> </ul>	<b>Artefatos resultantes:</b> <ul style="list-style-type: none"> <li>• Plano de gerenciamento de riscos</li> </ul>
<b>Papel:</b> Especialista em riscos	

A seguir são apresentados os cinco passos dessa atividade.

#### 4.1.2.1 DEFINIR CRITÉRIOS PARA A ANÁLISE DOS RISCOS

O propósito desse passo é definir critérios comuns e consistentes para a avaliação, a definição dos níveis de probabilidade e do impacto dos riscos a serem gerenciados, e para a priorização e o tratamento dos riscos. Além disso, identifica as categorias de riscos mais importantes para o projeto, de acordo com as suas características e seus objetivos, e levando em conta a tolerância a riscos dos envolvidos no projeto.

Essas regras de classificação de riscos podem ser definidas pela organização e figurar nos *Ativos de processos organizacionais*. Nesse caso, deve-se fazer uma adequação dessas regras para o projeto em foco (PMBOK, 2004).

Os critérios consistentemente utilizados (por exemplo, probabilidade de ocorrência e impacto) possibilitam a compreensão da severidade de diferentes riscos, ensejando que sejam tratados em um nível apropriado de detalhamento, de modo a se obter a atenção da gerência.

Para controlar diferentes tipos de risco, é essencial assegurar a consistência no resultado final. Sem critérios bem definidos seria muito difícil calibrar a severidade de uma mudança não desejada, causada por um risco, e priorizar as ações necessárias requeridas por

seu plano de respostas. Os critérios estabelecidos poderão também potencializar os ganhos obtidos por meio do aproveitamento de oportunidades.

Os parâmetros para avaliação, categorização e priorização dos riscos incluem: (i) *Probabilidade de ocorrência do risco*; (ii) *Impacto do risco*; e (iii) *Exposição ao risco*.

### **Probabilidade de ocorrência do risco**

Consiste em definir a escala a ser utilizada e os parâmetros para classificar a probabilidade dos riscos de acordo com essas escalas. Por exemplo:

- Quase certa → com histórico de ocorrências anteriores e fortes indícios de que o evento voltará a ocorrer;
- Provável → sem histórico de ocorrências anteriores e com fortes indícios de que o evento ocorrerá;
- Moderada → com ou sem histórico de ocorrências anteriores e indícios de que o evento ocorrerá;
- Eventual → com ou sem histórico de ocorrências anteriores e indícios de que o evento só ocorrerá em circunstâncias excepcionais;
- Improvável → sem histórico de ocorrências anteriores e sem indícios de que o evento ocorrerá.

### **Impacto do risco**

Significa definir a escala a ser utilizada, os fatores a serem considerados e os parâmetros para classificar o impacto dos riscos de acordo com essas escalas. Os parâmetros devem ser definidos de acordo com as conseqüências dos riscos para os objetivos do projeto, conforme mostra a definição de impacto apresentada na Figura 4.4.

Esses parâmetros devem ser estabelecidos com base em dados históricos que possibilitem a utilização de um adequado critério de mensuração.

<b>Condições definidas para escalas de impacto de um risco em objetivos importantes do projeto</b> (os exemplos são mostrados somente para impactos negativos)					
<b>Objetivo do projeto</b>	São mostradas escalas relativas ou numéricas				
	Muito baixo / 0,05	Baixo / 0,10	Moderado / 0,20	Alto / 0,40	Muito alto / 0,80
<b>Custo</b>	Aumento de custo não significativo	Aumento de custo < 10%	Aumento de custo de 10% a 20%	Aumento de custo de 20% a 40%	Aumento de custo > 40%
<b>Tempo</b>	Aumento de tempo não significativo	Aumento de tempo < 5%	Aumento de tempo de 5% a 10%	Aumento de tempo de 10% a 20%	Aumento de tempo > 20%
<b>Escopo</b>	Diminuição do escopo quase imperceptível	Áreas menos importantes do escopo afetadas	Áreas importantes do escopo afetadas	Redução do escopo inaceitável para o patrocinador	Item final do projeto sem nenhuma utilidade
<b>Qualidade</b>	Degradação da qualidade quase imperceptível	Somente as aplicações mais críticas são afetadas	Redução da qualidade exige a aprovação do patrocinador	Redução da qualidade inaceitável para o patrocinador	Item final do projeto sem nenhuma utilidade

Esta tabela apresenta exemplos de definições de impactos de riscos para quatro objetivos diferentes do projeto. Elas devem ser adequadas no processo Planejamento do gerenciamento de riscos ao projeto individual e aos limites de risco da organização. As definições de impactos podem ser desenvolvidas de forma semelhante para as oportunidades.

**Figura 4.4 – Definição de escalas de impacto para quatro objetivos do projeto (PMBOK, 2004)**

### Exposição ao risco

A exposição ao risco consiste nas combinações de probabilidade e impacto que resultam em uma classificação de risco como alto, moderado ou baixo.

Geralmente, a exposição é calculada para cada risco por meio da multiplicação do impacto pela probabilidade de ocorrência (Impacto do risco X Probabilidade de ocorrência). O relacionamento entre esses dois elementos dependerá de muitos fatores que refletem a verdadeira natureza do risco e a maneira como ele é percebido. Uma técnica bastante difundida para o cálculo da exposição é a *Matriz de probabilidade e impacto* (PMBOK, 2004). A Figura 4.5 contém um exemplo dessa matriz.

A descrição da incerteza inerente à medida da escala utilizada para mensurar os riscos também deve ser descrita no *Plano de gerenciamento de riscos*. É essencial especificar também como será realizada a priorização dos riscos no projeto em questão, definindo-se os fatores a serem considerados, além da exposição calculada.

Matriz de probabilidade e impacto										
Probabilidade	Ameaças					Oportunidades				
<b>0,90</b>	0,05	0,09	0,18	0,36	0,72	0,72	0,36	0,18	0,09	0,05
<b>0,70</b>	0,04	0,07	0,14	0,28	0,56	0,56	0,28	0,14	0,07	0,04
<b>0,50</b>	0,03	0,05	0,10	0,20	0,40	0,40	0,20	0,10	0,05	0,03
<b>0,30</b>	0,02	0,03	0,06	0,12	0,24	0,24	0,12	0,06	0,03	0,02
<b>0,10</b>	0,01	0,01	0,02	0,04	0,08	0,08	0,04	0,02	0,01	0,01
	0,05	0,10	0,20	0,40	0,80	0,80	0,40	0,20	0,10	0,05

Impacto (razão) em um objetivo (por exemplo, custo, tempo, escopo ou qualidade)

Cada risco é classificado de acordo com sua probabilidade de ocorrência e com seu impacto em um objetivo, caso realmente ocorra. Os limites da organização para riscos baixos, moderados ou altos são mostrados na matriz e determinam a classificação do risco como baixo, moderado ou alto em relação a esse objetivo.

**Figura 4.5 – Matriz de probabilidade e impacto (PMBOK, 2004)**

#### 4.1.2.2 DEFINIR CRITÉRIOS PARA O TRATAMENTO DOS RISCOS

O propósito é definir critérios comuns e consistentes para o tratamento dos riscos, por meio da definição dos parâmetros a serem utilizados como indicativos para a seleção da estratégia a ser adotada.

Boehm (1991) recomenda monitorar os “dez maiores riscos”; porém, esse número é um tanto arbitrário. O número de riscos a ser monitorado deve depender do projeto. Contudo, a quantidade deve ser gerenciável, pois um grande volume de riscos pode exigir a coleta de muitas informações (SOMMERVILLE, 2003).

O CMMI (2002) sugere que o tratamento dos riscos seja executado somente para riscos considerados de exposição Alta ou Média.

Exemplos de critérios a serem utilizados para a seleção dos riscos a serem tratados:

- selecionar todos os riscos com severidade (exposição) Alta;
- selecionar riscos com severidade Média, mas que sejam relevantes em função das características do projeto;

- não selecionar riscos com severidade Baixa, a menos que haja um motivo justificável para isso. Entretanto, esses riscos devem ser acompanhados, uma vez que sua severidade pode aumentar ou diminuir no decorrer do projeto.

Deve também ser estabelecida uma orientação a ser utilizada na seleção das estratégias, como a exemplificada na Tabela 4.2.

**Tabela 4.2 – Critério para seleção de estratégias**

		Exposição		
		Baixa	Média	Alta
Estratégia	Aceitar	X	X	
	Mitigar		X	X
	Transferir	X		
	Evitar		X	X

#### 4.1.2.3 DEFINIR MÉTRICAS

A idéia é estabelecer as métricas a serem coletadas e utilizadas como limites para determinar o grau de aceitabilidade dos riscos, com vistas ao estabelecimento de prioridades, para atuar como sinalizadores de ação da gerência e para a monitoração e controle dos riscos e do nível de sucesso da estratégia de resposta aos riscos.

As métricas podem cobrir alterações na probabilidade, no impacto e na temporalidade da ocorrência dos riscos. De acordo com o RUP (2003), muitos riscos podem ser monitorados utilizando-se métricas de projetos, observando-se tendências e limites, assim como medidas objetivas de progresso e qualidade, como:

- retrabalho restante;
- ruptura excessiva;
- gastos reais muito acima do planejado.

Em pontos de controle predeterminados, devem ser aplicadas as medições definidas para avaliar o progresso esperado e o nível de sucesso da estratégia da gerência de riscos, conforme explicitado a seguir:

- aferir a mudança na situação e o progresso das atividades de redução dos riscos;

- verificar o desempenho (métricas a ser coletadas nas atividades de tratamento de riscos); e
- executar a atividade de monitoração e controle do processo, a fim de se verificar a efetividade do gerenciamento de riscos no projeto.

#### **4.1.2.4 DEFINIR LIMITES PARA CADA CATEGORIA DE RISCOS**

Significa selecionar as métricas a serem utilizadas como fronteiras para cada categoria de riscos.

Esses limites servirão como marcos para a definição de ações ou para a implementação de ações, devendo ser refinados posteriormente, para cada risco identificado, com vistas a se estabelecer os pontos em que a monitoração mais agressiva do risco deve ser empregada, ou para sinalizar a execução do *Plano de tratamento dos riscos*.

É fundamental para o gerenciamento de riscos a definição de uma condição mensurável que, em caso de se concretizar, sinalize que o risco ocorreu ou que está a ponto de se transformar em realidade. Esses sinais de alerta da ocorrência dos riscos são utilizados como gatilhos para a execução de ações de respostas aos riscos.

Por exemplo, podem ser estabelecidos limites para envolver a gerência sênior, quando os custos do produto excederem um percentual do custo total do projeto, ou quando o índice de desempenho do cronograma cair abaixo de determinado valor (CMMI, 2002).

A definição dessas condições de limite pode ser utilizada para ajudar a delimitar o escopo da extensão do esforço da gerência de riscos, evitando-se despesas excessivas com recursos. Esses limites podem considerar a exclusão de uma fonte do risco de uma categoria, como podem também excluir toda a condição que ocorra abaixo de uma frequência estipulada (CMMI, 2002).

#### **4.1.2.5 DEFINIR INDICADORES PARA AVALIAÇÃO DO PROCESSO**

Consiste em definir os indicadores a serem coletados com o objetivo de se avaliar o processo de gerenciamento de riscos.



Segundo Leopoldino (2004), a mera aplicação de técnicas de gestão de riscos pode não ser o mais adequado. Osmundson et al (2002) alertam para a necessidade de métricas de avaliação da qualidade da condução de projetos de *software*, incluindo o gerenciamento de riscos.

Indicadores são dados ou representações numéricas de características de produtos e processos utilizados para acompanhar e melhorar os resultados ao longo do tempo. Esses indicadores são expressos em uma unidade de medida, estabelecendo-se as metas a serem alcançadas, o que periodicamente é levado ao conhecimento dos gestores dos processos, com a finalidade de apoiá-los na avaliação do desempenho (HAZAN, 2003).

De acordo com o CMMI (2002), diversas métricas podem ser utilizadas como indicadores para monitorar e controlar o processo de gerenciamento de riscos, destacando-se:

- número de riscos identificados, gerenciados e controlados;
- exposição ao risco e mudanças nessa exposição para cada risco avaliado;
- mudanças nas atividades do *Plano de mitigação do riscos* (por exemplo: processos, cronograma, orçamento).
- ocorrência de riscos não previstos;
- volatilidade da categorização dos riscos;
- comparação do esforço de mitigação de riscos estimado com o esforço real;
- comparação entre o impacto dos riscos estimado e o real.

Outras métricas, segundo KULPA (2003):

- o esforço e o tempo gastos nas atividades de gerenciamento de riscos comparados com os números de riscos atuais;
- o custo do gerenciamento de riscos comparado com o custo dos riscos atuais;
- para cada risco identificado, a comparação do impacto realizado com o impacto estimado.

Algumas atividades de gerenciamento de riscos podem ser difíceis de medir, o que, todavia, não as torna menos importantes. Para medi-las, podem ser utilizados indicadores

derivados. Por exemplo, os recursos alocados ao gerenciamento de riscos podem servir como indicativos do compromisso com esse gerenciamento (AS/NZS 4360, 2004).

#### 4.1.3 ATIVIDADE *ESTABELECEER ESTRATÉGIA*

A atividade consiste em estabelecer e manter a estratégia a ser utilizada para o gerenciamento de riscos no projeto, conforme especificado no Quadro 4.3.

**Quadro 4.3 – Atividade *Estabelecer estratégia***

<b>Propósito:</b> Estabelecer as estratégias de gerenciamento de riscos a serem usadas no projeto	
<b>Passos</b>	
<ul style="list-style-type: none"> <li>• Adaptar o processo ao projeto</li> <li>• Definir metodologia</li> <li>• Atribuir papéis e responsabilidades</li> <li>• Definir periodicidade</li> <li>• Planejar comunicação</li> <li>• Definir a avaliação do processo</li> </ul>	
<b>Artefatos de entrada</b>	<b>Artefatos resultantes</b>
<ul style="list-style-type: none"> <li>• Ativos de processos organizacionais</li> <li>• Visão</li> <li>• Plano de desenvolvimento de <i>software</i></li> <li>• Plano de gerenciamento de riscos</li> </ul>	<ul style="list-style-type: none"> <li>• Plano de gerenciamento de riscos</li> <li>• Plano de métricas</li> </ul>
<b>Papel:</b> Gerente do projeto	

A seguir são apresentados os seis passos dessa atividade.

##### 4.1.3.1 ADAPTAR O PROCESSO AO PROJETO

A idéia é possibilitar a adaptação do processo de gerenciamento de riscos, na forma proposta neste trabalho, segundo as características e o contexto de cada projeto, e de acordo com os critérios de seleção dos elementos do processo definidos nos *Ativos de processos organizacionais*. Um ponto essencial é que sejam definidos os itens obrigatórios do processo.

Assim, para projetos de pequeno porte, pode ser executado apenas um subconjunto das atividades do processo proposto. A Tabela 4.3 contém um exemplo de classificação de projetos de acordo com os respectivos portes.

**Tabela 4.3 – Classificação de projetos de acordo com os respectivos portes**

<b>Esforço estimado (em número de homens/hora)</b>	Igual ou superior a 3 mil e inferior a 7 mil	Igual ou superior a 7 mil e inferior a 15 mil	Igual ou superior a 15 mil e inferior a 25 mil	Igual ou superior a 25 mil
<b>Porte do projeto</b>	Pequeno	Médio	Grande	Programa (definido no glossário)

Os itens a serem adaptados devem ser descritos como atividades ou passos que não serão executados, sendo documentados os motivos correspondentes. Exemplos de itens de adaptação:

- o *Plano de gerenciamento de riscos* poderá integrar o *Plano de desenvolvimento de software* para projetos de pequeno porte;
- o *Plano de tratamento dos riscos* poderá integrar o *Registro de riscos*;
- projetos de pequeno porte podem não utilizar a ferramenta definida pela organização para registrar os riscos, fazendo-o por meio de planilha.

#### **4.1.3.2 DEFINIR METODOLOGIA**

Consiste em definir abordagens, técnicas, procedimentos e ferramentas a serem utilizadas no gerenciamento dos riscos no projeto, dentre as opções contidas nos *Ativos de processos organizacionais*. É essencial para o processo de gerenciamento de riscos a definição de procedimentos a serem seguidos para a identificação, a análise, o tratamento, a monitoração, o controle e a comunicação dos riscos.

Seguem exemplos de técnicas usualmente utilizadas na identificação de riscos (CMMI, 2002; PMBOK, 2003; IEEE Std 1540-2001, 2001), detalhadas no Anexo A:

- *Checklist*
- *Brainstorming*

- Técnica Delphi
- Entrevistas com peritos no assunto
- Análise SWOT
- Taxonomia de riscos (CARR et al, 1993)

Essa definição deve especificar as técnicas a serem utilizadas para analisar e priorizar os riscos, assim como as estratégias para lidar com ameaças e oportunidades, as quais servirão de base para a definição de ações de tratamento. As estratégias indicadas para o planejamento das respostas aos riscos podem ser:

- *Riscos negativos ou ameaças*: evitar, transferir, mitigar.
- *Riscos positivos ou oportunidades*: explorar, compartilhar, melhorar.

Os riscos para os quais não for selecionada nenhuma das citadas estratégias poderão ser aceitos ativa ou passivamente. Essas estratégias estão definidas mais detalhadamente no item 4.4.1 Atividade *Selecionar estratégias*.

Também devem ser identificadas todas as ferramentas ou técnicas especializadas a serem utilizadas para capturar e armazenar as informações sobre riscos e formas de acompanhamento, o que pode ser feito por meio de gráficos ou da análise de um resultado específico contra os gatilhos.

#### **4.1.3.3 ATRIBUIR PAPÉIS E RESPONSABILIDADES**

A intenção é especificar papéis e responsabilidades a serem adotados no gerenciamento de riscos no projeto; designar pessoas que exercerão funções no processo de gerenciamento de riscos; e estabelecer suas responsabilidades. Nesse ponto, deve ser verificado se há necessidade de treinamento para as pessoas designadas para desempenhar essas funções.

Os *Ativos de processos organizacionais* deverão conter os papéis, as responsabilidades e a autoridade para a execução do processo, o desenvolvimento dos produtos de trabalho e o fornecimento dos serviços de gerenciamento de riscos na organização.

É fundamental que a equipe designada seja representativa de funções técnicas e gerenciais. De acordo com o RUP (2003), uma boa combinação inclui o gerente de projeto, o representante do cliente (ou o gerente de produto), o arquiteto de *software* e representantes das equipes de teste, desenvolvimento, documentação e distribuição. Uma boa prática é apontar um membro dessa equipe como responsável oficial pelos riscos no projeto, cabendo-lhe, dentre outras atividades, reunir e classificar os riscos, à medida que forem identificados, e relatar o *status* dos riscos nas reuniões de revisão. Geralmente, esse papel é desempenhado pelo *Gerente do projeto*.

#### **4.1.3.4 DEFINIR PERIODICIDADE**

Trata-se de definir a periodicidade para o acompanhamento dos riscos. Consiste em definir quando e com que frequência o processo de gerenciamento de riscos será executado durante todo o ciclo de vida do projeto, e estabelecer as atividades de gerenciamento de riscos a serem incluídas no cronograma. A periodicidade mínima recomendada deve integrar os *Ativos de processos organizacionais*.

De acordo com o RUP (2003), o gerenciamento de riscos tem maior eficácia se tratado como um processo contínuo. O *Plano de gerenciamento de riscos* deve estabelecer um cronograma para a realização de reuniões de revisão dos riscos e emissão de relatórios regulares de *status*. Deve também identificar as circunstâncias em que poderão ocorrer reuniões de revisão não programadas.

#### **4.1.3.5 PLANEJAR COMUNICAÇÃO**

A idéia consiste em desenvolver um plano de comunicação para os riscos no projeto de acordo com as diretrizes estabelecidas pela organização, e levando-se em conta as características do projeto.

O plano de comunicação deve abranger a comunicação interna e externa ao projeto, devendo abordar questões relacionadas aos próprios riscos e também ao processo de gerenciamento (AS/NZS 4360, 2004).

Uma efetiva comunicação interna e externa é essencial para garantir que os responsáveis pela implementação do gerenciamento dos riscos e os envolvidos no projeto

entendam as razões de cada decisão, assim como o porquê da necessidade de ações específicas. Como a visão dos participantes do projeto pode gerar significativo impacto no processo decisório, é fundamental que tenham uma adequada percepção dos riscos envolvidos no projeto.

O planejamento da comunicação, que compõe o *Plano de gerenciamento de riscos*, deverá conter os seguintes elementos:

- os participantes necessários;
- as perspectivas dos participantes a ser consideradas;
- os métodos de comunicação a ser utilizados (esses métodos podem ser modificados no decorrer do ciclo de gerenciamento de riscos); e
- o formato dos relatórios de *status* dos riscos.

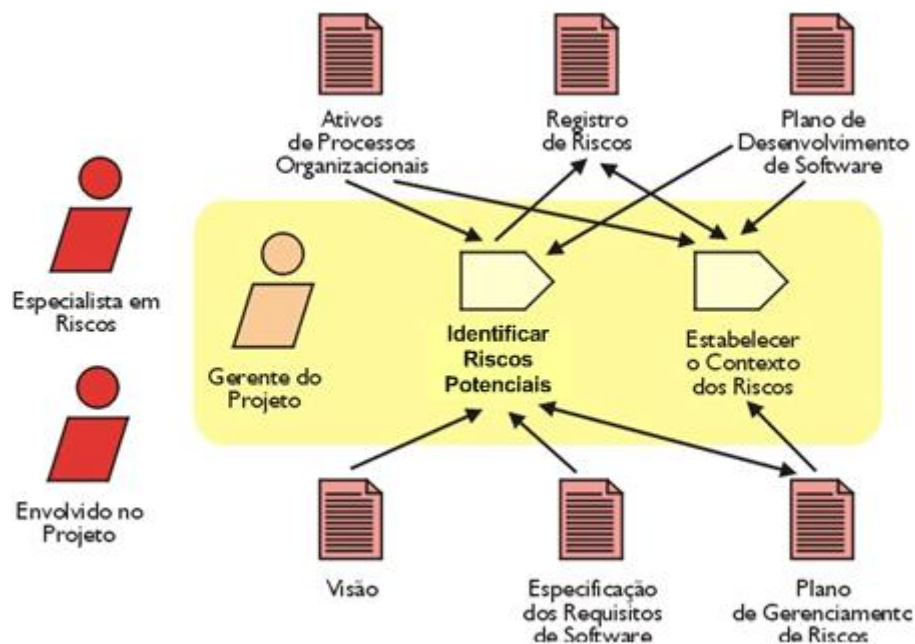
#### **4.1.3.6 DEFINIR A AVALIAÇÃO DO PROCESSO**

Significa definir como será realizada a avaliação do processo de gerenciamento de riscos. Consiste em descrever como esse processo será avaliado, a fim de se identificar a necessidade de melhoria, definindo-se a forma de captura das informações, como, por exemplo, lições aprendidas. Essa descrição define quais artefatos, atividades ou passos serão avaliados, a fim de se avaliar a sua aderência ao processo (IEEE Std 1540-2001, 2001).

#### **4.2 MACROATIVIDADE IDENTIFICAR RISCOS**

A Figura 4.6 detalha as atividades da macroatividade *Identificar riscos*, a qual consiste em descobrir os riscos que podem ocorrer em um projeto específico, e estabelecer seu contexto.

A disponibilidade de informações de boa qualidade é fundamental para a identificação de riscos, assim como de dados históricos sobre projetos similares e a subsequente discussão com os participantes do projeto. A participação de envolvidos internos e externos ajuda no compromisso com o processo de gerenciamento de riscos, garantindo que os riscos tenham o mesmo significado para os diferentes envolvidos (AS/NZS 4360, 2004).



**Figura 4.6 – Macroatividade *Identificar riscos***

As características dos riscos devem ser documentadas em uma linguagem concisa, incluindo o contexto, as condições e as conseqüências de sua ocorrência. Essas atividades geram o artefato *Registro de riscos*, cuja preparação começa com a identificação dos riscos, e tem continuidade com a sua análise, tratamento, monitoração e controle. O Apêndice C contém um *template* para o artefato *Registro de riscos*.

A macroatividade *Identificar riscos* compõe-se das seguintes atividades: (i) *Identificar riscos potenciais*; e (ii) *Estabelecer o contexto dos riscos*.

#### **4.2.1 ATIVIDADE *IDENTIFICAR RISCOS POTENCIAIS***

A identificação de riscos especifica os eventos incertos que podem afetar o projeto, dando início à elaboração do *Registro de riscos*. A identificação de possíveis barreiras, perigos, ameaças e vulnerabilidades que poderiam afetar negativamente os esforços ou planos de trabalho representa a base para uma adequada e bem-sucedida gerência de risco. Os riscos devem ser identificados e descritos de maneira compreensível, para serem corretamente analisados e controlados. O Quadro 4.4 apresenta a atividade *Identificar riscos potenciais*.

**Quadro 4.4 – Atividade *Identificar riscos potenciais***

<b>Propósito:</b> Identificar os riscos que podem afetar o projeto	
<b>Passos</b>	
<ul style="list-style-type: none"> <li>• Identificar os riscos associados às fontes e categorias</li> <li>• Revisar a documentação do projeto</li> <li>• Revisar informações históricas</li> </ul>	
<b>Artefatos de entrada</b>	<b>Artefatos resultantes</b>
<ul style="list-style-type: none"> <li>• Ativos de processos organizacionais</li> <li>• Especificação dos requisitos de <i>software</i></li> <li>• Visão</li> <li>• Plano de desenvolvimento de <i>software</i></li> <li>• Plano de gerenciamento de riscos</li> </ul>	<ul style="list-style-type: none"> <li>• Registro de riscos</li> </ul>
<b>Papel:</b> Gerente do projeto	

A seguir são apresentados os três passos dessa atividade.

#### 4.2.1.1 IDENTIFICAR OS RISCOS ASSOCIADOS ÀS FONTES E CATEGORIAS

O que se propõe é identificar os riscos que podem afetar o projeto de acordo com as fontes e categorias selecionadas para o projeto, utilizando-se as ferramentas e técnicas especificadas no *Plano de gerenciamento de riscos*.

A identificação dos riscos deve ocorrer de forma organizada e completa, a fim de se detectar prováveis riscos cuja ocorrência possa afetar os objetivos do projeto. Para que se obtenha a desejada eficácia, a identificação do risco não deve ser uma tentativa de referir-se a cada evento possível, sem levar em conta o quão improvável ele seja (CMMI, 2002).

O uso de fontes, categorias e parâmetros identificados no planejamento do gerenciamento de riscos pode ensinar a disciplina e a otimização apropriadas à identificação dos riscos. Os riscos identificados formam uma *baseline* para as atividades de gerenciamento de riscos.

O *Registro de riscos* deve ser revisto periodicamente, para que se possa adequadamente reexaminar possíveis fontes de riscos e detectar eventuais condições de



mudança, com o intuito de se descobrir as fontes e os riscos previamente negligenciados ou inexistentes, quando a estratégia de gerenciamento de riscos tiver sido anteriormente definida para o projeto (CMMI, 2002).

#### **4.2.1.2 REVISAR A DOCUMENTAÇÃO DO PROJETO**

Cuida-se de revisar documentos importantes do projeto, como parte da identificação de riscos. Consiste na realização de uma revisão estruturada da documentação do projeto, incluindo planos, premissas, arquivos de projetos anteriores e outras informações. A qualidade e a consistência dos planos e também as premissas e requisitos do projeto podem ser indicadores de riscos.

As premissas do projeto pertencentes ao documento *Visão* devem ser analisadas, explorando-se sua validade e sua aplicabilidade no referido projeto, a fim de se identificar eventuais riscos causados pelas condições de inexatidão, inconsistência ou incompletude dessas premissas.

Os elementos do *Plano de desenvolvimento de software*, inclusive a *Estrutura analítica do projeto* (EAP), ou WBS, também devem ser revisados como parte da identificação dos riscos, para assegurar que todos os aspectos do projeto foram considerados.

#### **4.2.1.3 REVISAR INFORMAÇÕES HISTÓRICAS**

Revisar informações históricas significa examinar documentos ou bases de dados de lições aprendidas e do esforço de gerenciamento de riscos em projetos que produziram produtos similares.

O ponto de partida para a identificação dos riscos podem ser as informações históricas, que devem ser discutidas com os envolvidos no projeto. Isso poderá ajudar a construir um compromisso com o processo e a garantir que diferentes envolvidos sejam adequadamente abordados ou considerados, quando isso se fizer necessário ou se julgar apropriado.

Entretanto, é fundamental verificar se as informações disponíveis na base histórica têm boa qualidade, para se evitar a indução de distorções no gerenciamento de riscos do projeto.

#### 4.2.2 ATIVIDADE *ESTABELECER O CONTEXTO DOS RISCOS*

Consiste em se estabelecer e documentar as características e o contexto de cada risco identificado, provendo-se informações adicionais que facilitem sua compreensão (CMMI, 2002).

O documento deve ser revisado com os participantes do projeto, a fim de se obter a concordância de que ele está completo e correto. Isso é essencial para garantir que o contexto do projeto e a extensão de seus riscos foram corretamente avaliados.

O Quadro 4.5 apresenta a atividade *Estabelecer o contexto dos riscos*.

**Quadro 4.5 – Atividade Estabelecer o contexto dos riscos**

<b>Propósito:</b> Estabelecer o contexto de cada risco identificado	
<b>Passos</b>	
<ul style="list-style-type: none"> <li>• Detectar as circunstâncias ou condições do risco</li> <li>• Identificar possíveis conseqüências dos riscos</li> </ul>	
<b>Artefatos de entrada</b>	<b>Artefatos resultantes</b>
<ul style="list-style-type: none"> <li>• Ativos de processos organizacionais</li> <li>• Registro de riscos</li> <li>• Plano de gerenciamento de riscos</li> <li>• Plano de desenvolvimento de <i>software</i></li> </ul>	<ul style="list-style-type: none"> <li>• Registro de riscos</li> </ul>
<b>Papel:</b> Gerente do projeto	

A seguir são apresentados os dois passos dessa atividade.

##### 4.2.2.1 DETECTAR AS CIRCUNSTÂNCIAS OU CONDIÇÕES DOS RISCOS

Significa identificar as condições ou eventos que podem produzir o risco identificado, as circunstâncias em que o risco foi identificado e quando poderá ocorrer.

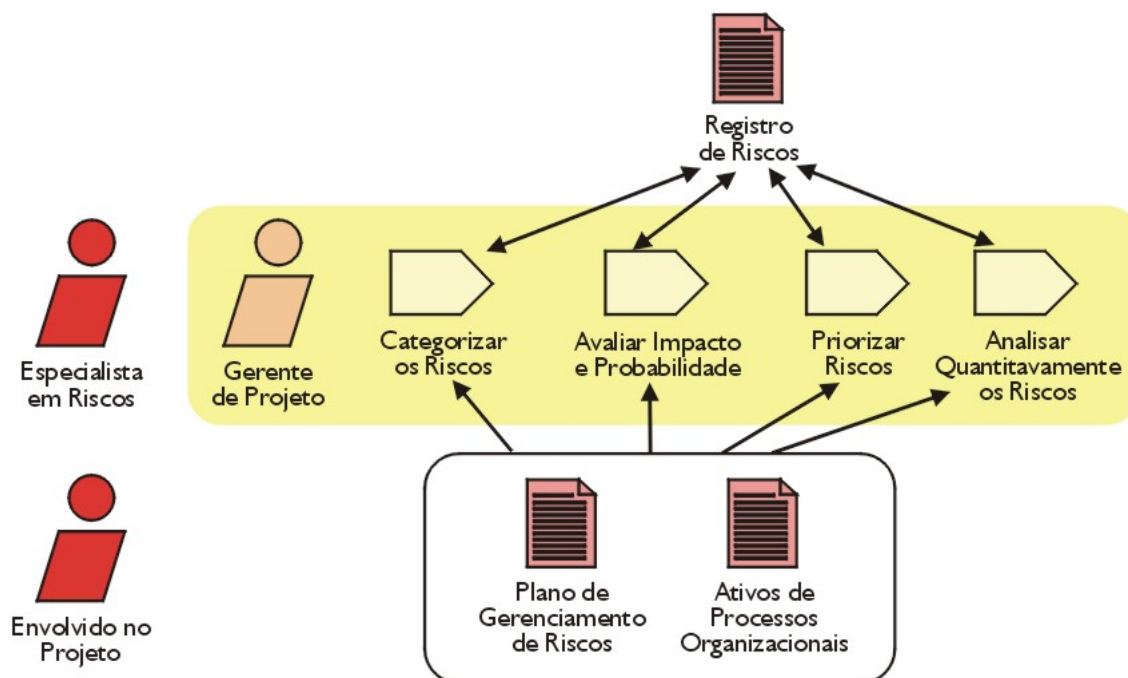
Isso envolve a identificação das eventuais causas, a abordagem ou técnica utilizada na identificação, o escopo coberto e os participantes envolvidos. Deve também ser considerada a estrutura de tempo relativa ao risco; ou seja, deve-se documentar a data e em que fase do projeto o risco foi identificado e em que fase sua ocorrência é mais provável. Outros pontos a serem considerados são a origem do risco, se interna ou externa, e o nível de decisão sobre o risco.

### 4.2.2.2 IDENTIFICAR POSSÍVEIS CONSEQUÊNCIAS DOS RISCOS

Trata-se de identificar possíveis conseqüências de cada risco identificado para os objetivos do projeto e documentar suas características. Importantes objetivos do projeto relacionam-se a custo, cronograma, prazo e qualidade. Significa estabelecer os desvios do planejamento referentes a cronograma, esforço, custos ou qualidade (tais como as horas de trabalho perdidas e a severidade do dano), em caso de ocorrência do risco.

### 4.3 MACROATIVIDADE ANALISAR RISCOS

A Figura 4.7 detalha as atividades da macroatividade *Analisar riscos*, compreendendo basicamente a categorização, a avaliação e a priorização dos riscos. A análise quantitativa deverá ser executada apenas para os riscos de maior prioridade, nos casos em que o nível de risco do projeto justifique o investimento.



**Figura 4.7 – Macroatividade *Analisar riscos***

A análise dos riscos tem por objetivo estabelecer uma compreensão dos riscos do projeto e de sua natureza. Os riscos similares devem ser classificados de acordo com as categorias selecionadas para o projeto; a categorização dos riscos pode conduzir ao desenvolvimento de respostas mais eficazes.

A avaliação do impacto e da probabilidade de ocorrência dos riscos faz-se necessária para determinar a importância relativa de cada risco identificado, para efeito de priorização, sendo usada também para chamar a atenção da gerência. Os riscos devem ser priorizados de acordo com a exposição geral que eles acarretam ao projeto e com os critérios estabelecidos no planejamento. A necessidade de priorização dos riscos decorre do fato de os projetos trabalharem com recursos escassos, não havendo recursos disponíveis para tratar todos os riscos identificados. O objetivo da priorização é justamente determinar as áreas onde os recursos devem ser aplicados com maior impacto positivo para o projeto.

A forma de expressar o impacto, a probabilidade e a combinação de ambos, para fornecer a severidade do risco, poderá variar de acordo com a categoria do risco e o objetivo da avaliação. A incerteza e a variação no cálculo do impacto e da probabilidade devem ser consideradas na análise, como também eficazmente comunicadas.

#### 4.3.1 ATIVIDADE *CATEGORIZAR OS RISCOS*

Esta atividade tem por objetivo agrupar e classificar os riscos de acordo com as categorias especificadas, provendo meios para a sua análise, conforme ilustrado no Quadro 4.6.

**Quadro 4.6 – Atividade Categorizar os riscos**

<b>Propósito:</b> Agrupar os riscos para facilitar a priorização e a identificação das possíveis respostas	
<b>Passos</b>	
<ul style="list-style-type: none"> <li>• Agrupar os riscos de acordo com as categorias</li> </ul>	
<b>Artefatos de entrada</b>	<b>Artefatos resultantes</b>
<ul style="list-style-type: none"> <li>• Ativos de processos organizacionais</li> <li>• Plano de gerenciamento de riscos</li> <li>• Registro de riscos</li> </ul>	<ul style="list-style-type: none"> <li>• Registro de riscos</li> </ul>
<b>Papel:</b> Gerente do projeto	

Segue-se o detalhamento do passo que integra essa atividade.

#### 4.3.1.1 AGRUPAR OS RISCOS DE ACORDO COM AS CATEGORIAS

Significa revisar a categorização dos riscos já classificados durante a identificação e verificar as similaridades entre os demais riscos identificados, a fim de categorizá-los.

Os riscos relacionados devem ser agrupados para viabilizar uma manipulação eficiente e o uso eficaz dos recursos da gerência de riscos. Os riscos são agrupados de acordo com as categorias, provendo-se meios para análise de acordo com sua fonte, taxonomia ou componente do projeto. Os relacionamentos de causa e efeito entre riscos relacionados devem ser documentados (CMMI, 2002).

A categorização pode revelar causas comuns dos riscos ou áreas do projeto que requerem atenção especial. A descoberta de áreas de concentração de riscos pode aumentar a eficácia das respostas aos riscos.

#### 4.3.2 ATIVIDADE AVALIAR IMPACTO E PROBABILIDADE

Objetiva analisar a probabilidade e a magnitude da consequência da ocorrência de um risco, além de determinar sua severidade, conforme esquematizado no Quadro 4.7. Um risco pode ter múltiplas consequências e afetar diferentes objetivos do projeto.

**Quadro 4.7 – Atividade Avaliar impacto e probabilidade**

<b>Propósito:</b> Determinar a exposição que cada risco acarreta para o projeto	
<b>Passos</b>	
<ul style="list-style-type: none"> <li>• Avaliar o impacto dos riscos</li> <li>• Avaliar a probabilidade de ocorrência dos riscos</li> <li>• Determinar a exposição aos riscos</li> </ul>	
<b>Artefatos de entrada</b>	<b>Artefatos resultantes</b>
<ul style="list-style-type: none"> <li>• Ativos de processos organizacionais</li> <li>• Plano de gerenciamento de riscos</li> <li>• Registro de riscos</li> </ul>	<ul style="list-style-type: none"> <li>• Registro de riscos</li> </ul>
<b>Papel:</b> Gerente do projeto	

A seguir são apresentados os três passos dessa atividade.

#### **4.3.2.1 AVALIAR O IMPACTO DOS RISCOS**

Trata-se de investigar as conseqüências negativas das ameaças e os efeitos positivos das oportunidades de cada risco identificado para os objetivos do projeto, como tempo, custo, escopo e qualidade.

Para se avaliar o impacto da ocorrência do risco, podem ser utilizados os critérios estabelecidos no passo *Definir critérios para a análise dos riscos* (subseção 4.1.2.1). Esses critérios podem facilitar uma compreensão mais adequada dos impactos de diferentes riscos.

#### **4.3.2.2 AVALIAR A PROBABILIDADE DE OCORRÊNCIA DOS RISCOS**

Consiste em identificar a probabilidade de ocorrência dos riscos identificados. A probabilidade de ocorrência significa a possibilidade de efetiva ocorrência do risco (geralmente expressa em porcentagem). A probabilidade pode ser avaliada de acordo com os critérios estabelecidos no passo *Definir critérios para a análise dos riscos* (subseção 4.1.2.1).

#### **4.3.2.3 DETERMINAR A EXPOSIÇÃO AOS RISCOS**

Trata-se de avaliar a repercussão de cada risco identificado para os objetivos do projeto.

É da natureza humana preocupar-se com os riscos de mais alto impacto; mas, se a sua ocorrência é mais improvável, eles podem ser, na realidade, menos importantes do que riscos mais moderados de ocorrência iminente. Ao considerar a magnitude do impacto do risco e sua probabilidade de ocorrência, o gerente do projeto tende a focar o esforço de gerenciamento de riscos em áreas que terão um efeito mais relevante na entrega do projeto (RUP, 2003).

Técnicas de gerenciamento de riscos recomendam que os riscos sejam priorizados de acordo com a exposição geral que acarretam ao projeto. A exposição de cada risco pode ser calculada de acordo com os parâmetros estabelecidos na subseção 4.1.2.1. A exposição de cada risco deve ser obtida por meio consenso entre os envolvidos relevantes no projeto. Diferenças de opinião significativas devem ser discutidas e bem tratadas, para se garantir a todos os envolvidos igual interpretação do risco.

### 4.3.3 ATIVIDADE *PRIORIZAR RISCOS*

Objetiva a priorização dos riscos com base na análise das demais atividades da macroatividade *Analisar riscos*, com vistas a fornecer subsídios para as decisões no âmbito do projeto, conforme apresentado no Quadro 4.8.

**Quadro 4.8 – Atividade Priorizar riscos**

<b>Propósito:</b> Classificar os riscos no projeto por ordem de prioridade	
<b>Passos</b>	
<ul style="list-style-type: none"> <li>• Determinar a prioridade relativa dos riscos</li> </ul>	
<b>Artefatos de entrada</b>	<b>Artefatos resultantes</b>
<ul style="list-style-type: none"> <li>• Ativos de processos organizacionais</li> <li>• Plano de gerenciamento de riscos</li> <li>• Registro de riscos</li> </ul>	<ul style="list-style-type: none"> <li>• Registro de riscos</li> </ul>
<b>Papel:</b> Gerente do projeto	

Segue-se o detalhamento do passo que integra essa atividade.

#### 4.3.3.1 DETERMINAR A PRIORIDADE RELATIVA DOS RISCOS

Cria-se a lista de prioridades dos riscos de acordo com os critérios especificados na subseção 4.1.2.1. Uma vez determinada a exposição de cada risco e organizada a lista de riscos por categoria, podem-se dispor os riscos em ordem decrescente de exposição, para se elaborar a relação dos riscos mais importantes. Deve-se também levar em conta outros critérios especificados para a priorização, como, por exemplo, considerar prioritários os riscos de categorias específicas.

A finalidade da priorização é determinar as áreas nas quais os recursos para tratamento dos riscos sejam aplicados com maior impacto positivo para o projeto (CMMI, 2002). O gerente do projeto utiliza a relação priorizada dos riscos para concentrar-se nos itens cujas respostas podem levar a melhores resultados para o projeto.

Os riscos podem ser listados por prioridade, separadamente, de acordo com suas conseqüências para custo, prazo, escopo e qualidade, pois as organizações podem valorizar alguns objetivos mais do que outros (PMBOK, 2004).

#### 4.3.4 ATIVIDADE ANALISAR QUANTITATIVAMENTE OS RISCOS

Propõe-se a realização de uma análise numérica, que vai além das escalas utilizadas na análise qualitativa dos riscos. Essa análise é opcional, devendo ser utilizada apenas nos riscos de maior prioridade identificados na subseção 4.3.3.1, de acordo com a disponibilidade de tempo e orçamento. A análise quantitativa nem sempre é viável ou prática, requerendo a disponibilidade de dados numéricos confiáveis. O Quadro 4.9 apresenta essa atividade.

**Quadro 4.9 – Atividade Analisar quantitativamente os riscos**

<b>Propósito:</b> Analisar quantitativamente os riscos de maior impacto para os objetivos do projeto	
<b>Passos</b>	
<ul style="list-style-type: none"> <li>• Analisar riscos quantitativamente</li> </ul>	
<b>Artefatos de entrada</b>	<b>Artefatos resultantes</b>
<ul style="list-style-type: none"> <li>• Ativos de processos organizacionais</li> <li>• Plano de gerenciamento de riscos</li> <li>• Registro de riscos</li> </ul>	<ul style="list-style-type: none"> <li>• Registro de riscos</li> </ul>
<b>Papel:</b> Gerente do projeto	

Segue-se o detalhamento do passo que integra essa atividade.

##### 4.3.4.1 ANALISAR QUANTITATIVAMENTE OS RISCOS

A análise quantitativa caracteriza-se por medição, análise numérica das dimensões de probabilidade e impacto dos riscos, em caráter individual, e projeções numéricas para o projeto como um todo (DINSMORE, 2003). Apresenta uma abordagem quantitativa para subsidiar decisões na presença da incerteza, com os seguintes principais objetivos (PMBOK, 2004):

- quantificar as conseqüências possíveis para o projeto e sua probabilidade;



- avaliar a probabilidade de atingir objetivos específicos do projeto;
- identificar riscos que requeiram maior atenção por meio da quantificação de sua contribuição relativa no risco total do projeto;
- identificar custos, cronogramas e objetivos de escopo realísticos e factíveis; e.
- determinar a melhor decisão da gerência do projeto, quando algumas circunstâncias ou conseqüências são incertas.

Duas categorias de técnicas são comumente utilizadas na análise quantitativa de riscos, sugeridas pelo PMBOK (2004): técnicas de representação e coleta de dados e técnicas de modelagem. As técnicas de representação e coleta de dados criam as bases para estimativas mais precisas e confiáveis, destacando-se três tipos:

- entrevista;
- distribuição de probabilidades;
- opinião especializada.

São exemplos de técnica de modelagem:

- análise de sensibilidade;
- análise do valor monetário esperado;
- análise da árvore de decisão;
- modelagem e simulação.

A análise quantitativa dos riscos envolve uma análise probabilística do projeto, na qual são feitas estimativas sobre as possíveis datas de conclusão e custos do projeto e os níveis de confiança associados. À medida que esse passo é repetido, evidencia-se uma tendência que poderá influenciar as respostas aos riscos no projeto.

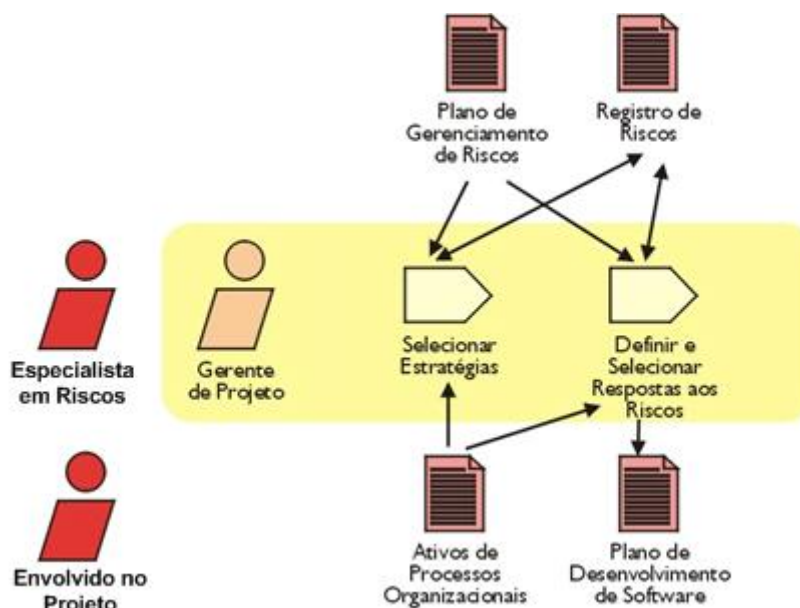
Essa análise requer métricas de projetos disponíveis. Deve ser possível determinar, por exemplo, a probabilidade de o projeto atingir seus objetivos de custo e tempo, de acordo com o plano atual.

A determinação do impacto da ocorrência do risco no custo do projeto e da exposição a esse custo é bastante útil na seleção das estratégias para tratamento do risco. Calcula-se a exposição ao custo multiplicando-se o custo do risco por sua probabilidade de ocorrência.

#### 4.4 MACROATIVIDADE *TRATAR RISCOS*

A Figura 4.8 detalha as atividades da macroatividade *Tratar riscos*, a qual consiste na avaliação e seleção das estratégias a serem adotadas para lidar com as ameaças e as oportunidades e na definição de ações para implementá-las.

A estratégia ou combinação de estratégias mais apropriada para tratar os riscos deve ser selecionada levando-se em conta alguns fatores, entre eles a relação custo/benefício. Não faz sentido, por exemplo, o custo de uma resposta ao risco ser maior que o do próprio risco.



**Figura 4.8 – Macroatividade *Tratar riscos***

O gerenciamento de riscos é considerado *cost-effective* somente se o custo do gerenciamento de riscos for consideravelmente menor que o custo decorrente da materialização do risco (HALL, 1998). De acordo com a norma AS/NZS 4360 (2004), o gerenciamento de riscos pode ser utilizado para identificar e priorizar os riscos positivos ou oportunidades, caso em que muda apenas o foco na ação de capturar e explorar a oportunidade.

As estratégias para responder às ameaças incluem evitar, transferir, aceitar ou mitigar o risco. A mitigação consiste em implementar uma ação imediata e proativa para reduzir a probabilidade e/ou o impacto do risco. As estratégias para potencializar as oportunidades consistem em explorar, compartilhar, ampliar ou aceitar o risco.

As estratégias de contingência referem-se ao desenvolvimento de planos alternativos, a serem postos em prática no caso de o risco tornar-se realidade, e à criação de reservas a serem incluídas no *Plano de desenvolvimento de software*, objetivando-se minimizar riscos relacionados a custo e prazo.

Além disto, com base nos parâmetros definidos, devem-se determinar os limites para os riscos e os possíveis sinais de advertência da sua ocorrência. Esses limites devem ser estabelecidos para cada risco identificado, assim como devidamente documentados no *Registro dos riscos*. O proprietário de cada risco e os executores das ações de tratamento também devem ser definidos, assim como as responsabilidades de cada um.

A macroatividade *Tratar riscos* compõe-se das seguintes atividades: (i) *Selecionar estratégias*; e (ii) *Definir e selecionar respostas aos riscos*.

#### 4.4.1 ATIVIDADE SELECIONAR ESTRATÉGIAS

Consiste na definição dos limites dentro dos quais cada risco é considerado aceitável, e na seleção da estratégia, ou conjunto de estratégias, a ser utilizado no tratamento de cada um dos riscos identificados e selecionado. Essa seleção deverá ser feita em conformidade com os parâmetros definidos no *Plano de gerenciamento de riscos*. A atividade é apresentada no Quadro 4.10.

**Quadro 4.10 - Atividade Selecionar estratégias**

<b>Propósito:</b> Definir e selecionar estratégias para lidar com os riscos negativos	
<b>Passos</b>	
<ul style="list-style-type: none"> <li>• Definir limites</li> <li>• Selecionar estratégias para ameaças</li> <li>• Selecionar estratégias para oportunidades</li> <li>• Selecionar riscos que serão aceitos</li> </ul>	
<b>Artefatos de entrada</b>	<b>Artefatos resultantes</b>
<ul style="list-style-type: none"> <li>• Ativos de processos organizacionais</li> <li>• Registro de riscos</li> <li>• Plano de gerenciamento de riscos</li> </ul>	<ul style="list-style-type: none"> <li>• Registro de riscos</li> </ul>
<b>Papel:</b> Gerente do projeto	

A seguir são apresentados os quatro passos dessa atividade.

#### **4.4.1.1 DEFINIR LIMITES**

Significa definir as fronteiras do risco, para melhor compreensão dos níveis de risco aceitáveis pelas partes envolvidas, de acordo com o que foi definido na subseção 4.1.2.4. Esses níveis irão influenciar a seleção da estratégia ou a combinação de estratégias a ser adotada para tratar o risco.

Os limites podem ser definidos para indicar a necessidade de mudança de estratégia, para a implementação de ações, ou ainda como um indicativo da necessidade de um acompanhamento mais efetivo do risco. Pode haver múltiplos limites empregados para os vários níveis de resposta.

#### **4.4.1.2 SELECIONAR ESTRATÉGIAS PARA AMEAÇAS**

Trata-se de selecionar a estratégia ou associação de estratégias com maior probabilidade de ser eficaz como resposta, para cada um dos riscos negativos selecionados. De acordo com o PMBOK (2004), constituem estratégias recomendadas para abordar os riscos negativos: evitar, transferir e mitigar.

##### **Evitar**

Consiste em mudar o *Plano de desenvolvimento de software* de modo a eliminar a condição que dá origem a sua possível ocorrência, com vistas a isolar os objetivos do projeto do impacto do risco, ou flexibilizar o objetivo sob ameaça. Neste último caso, vale citar como exemplo a extensão do cronograma ou a redução do escopo.

Algumas vezes, o risco pode ser completamente evitado. Frequentemente, a origem do risco nada mais é do que uma definição pobre do escopo do sistema. Caso seja possível reduzir esse escopo (pela eliminação de requisitos não essenciais), as seções do *Registro de riscos* também poderão ser excluídas juntamente com os requisitos eliminados. O esclarecimento dos requisitos, a obtenção de informações, a melhoria da comunicação e a aquisição de especialistas podem prevenir alguns riscos que sempre surgem no início do

projeto. Em outros casos, pode ser adquirida tecnologia para reduzir o risco de desenvolver uma funcionalidade em particular (RUP, 2003).

### **Transferir**

A transferência de riscos requer a passagem do impacto negativo de uma ameaça para terceiros, juntamente com a responsabilidade pela resposta ao risco. Essa transferência de riscos simplesmente confere a uma outra parte a responsabilidade por seu gerenciamento; ou seja, ela não elimina riscos. A transferência da responsabilidade pelo risco é mais eficaz quando relacionada à exposição a riscos financeiros. A transferência de riscos quase sempre envolve o pagamento de um prêmio de risco à parte que assume o risco. Os contratos podem ser utilizados para transferir responsabilidades por riscos especificados para a outra parte.

A organização que transfere o risco adquire outro risco: o de que a organização para a qual foi transferido o risco não consiga gerenciá-lo efetivamente.

### **Mitigar**

A mitigação de riscos leva à redução da probabilidade e/ou do impacto de um evento de risco adverso até um limite aceitável. Isso consiste em identificar as ações que devem ser implementadas antecipadamente, para reduzir a probabilidade de ocorrência do risco ou seu impacto no projeto. A implementação de ações com essa finalidade no início do projeto é sempre mais eficaz do que a tentativa de reparar os danos após a ocorrência do risco.

Prototipação, simulação, projetos alternativos e desenvolvimento evolucionário são técnicas de mitigação sugeridas no CMMI (2002). Quando não for possível reduzir a probabilidade, uma resposta de mitigação poderá diminuir o impacto do risco, concentrando-se em aspectos que determinam sua gravidade. Por exemplo, ao se projetar a redundância em um subsistema pode-se reduzir o impacto de uma falha no componente original.

Geralmente há alguma ação que pode ser implementada para fazer o risco acontecer ou para eliminá-lo. Em um processo de desenvolvimento iterativo, essas ações devem acontecer nas iterações iniciais, para mitigar o risco tão cedo quanto possível. Se um risco está na forma “X pode não funcionar”, então deve haver um planejamento para testar “X” logo que possível (RUP, 2003).

O resultado dessas ações deve reduzir a probabilidade de ocorrência de certos riscos, tendendo para valores próximos de zero. Nos casos em que o risco seja confirmado, a resposta ao risco deve ocorrer por meio de um *Plano de contingências*.

#### **4.4.1.3 SELECIONAR ESTRATÉGIAS PARA OPORTUNIDADES**

Significa selecionar, para cada um dos riscos positivos, a estratégia ou associação de estratégias com maior probabilidade de ser eficaz como resposta. De acordo com o PMBOK (2004), constituem estratégias recomendadas para abordar os riscos positivos: explorar, compartilhar e ampliar.

##### **Explorar**

Essa estratégia pode ser selecionada para riscos com impactos positivos, em que a organização pretenda garantir a concretização da oportunidade. Essa estratégia procura eliminar a incerteza associada a um dado risco positivo, fazendo com que a oportunidade efetivamente venha a acontecer. Por exemplo, alocar recursos mais capacitados para o projeto, a fim de antecipar sua conclusão ou para garantir-lhe mais qualidade (PMBOK, 2004).

##### **Compartilhar**

O compartilhamento de um risco positivo envolve a atribuição da propriedade do risco a terceiros que possam capturar melhor as oportunidades em benefício do projeto. Isso pode acontecer mediante fornecimento de recursos que venham a aumentar a probabilidade de se concretizar a oportunidade e a extensão dos seus ganhos. Os exemplos de ações compartilhadas incluem a formação de parcerias, equipes ou empresas estabelecidas com o objetivo expresso de gerenciar oportunidades para o compartilhamento do risco.

##### **Ampliar**

Essa estratégia tem como objetivo reduzir a incerteza, fazendo a oportunidade acontecer. Isso ocorre através de ações para modificar o “tamanho” de uma oportunidade por meio do aumento da probabilidade e/ou dos impactos positivos e pela identificação e maximização dos principais acionadores desses riscos de impacto positivo. Para aumentar a probabilidade, pode-se facilitar ou fortalecer a sua causa e direcionar e reforçar de forma proativa suas condições de

acionamento. Os acionadores de impacto também podem ser direcionados, tentando-se aumentar a suscetibilidade do projeto à oportunidade.

#### **4.4.1.4 SELECIONAR OS RISCOS QUE SERÃO ACEITOS**

Propõe-se avaliar qual estratégia de aceitação será adotada para quais riscos positivos ou negativos.

Os projetos utilizam recursos limitados, e isso restringe os montantes a serem aplicados no tratamento dos riscos. Sendo assim, torna-se necessário selecionar os riscos que serão tratados, por ser admissível tolerar alguns riscos, de acordo com as circunstâncias, e dependendo dos benefícios esperados. A estratégia de aceitação do risco pode ser adotada pela decisão da equipe do projeto em não alterar o planejamento do projeto em decorrência do risco ou pela dificuldade de encontrar uma resposta adequada. A equipe pode aceitar o risco mesmo que este exceda os limites estabelecidos, se o custo do tratamento for muito elevado ou não houver tempo suficiente para realizá-lo. Assim, por exemplo, se o custo do tratamento for superior à exposição ao custo calculada, a estratégia selecionada poderá ser de aceitação. Essa estratégia pode ser adotada tanto para ameaças como para oportunidades.

De acordo com o PMBOK (2004), a estratégia adotada pode ser passiva ou ativa. A aceitação passiva não requer qualquer ação, deixando a equipe do projeto tratar os riscos à medida que ocorram; deve-se, porém, documentar o motivo dessa aceitação. Quando a aceitação é ativa, torna-se necessário planejar ações de contingência, além de estabelecer uma reserva de tempo e custo para contingências. A decisão de não tratar os riscos deve ser adotada de acordo com os critérios estabelecidos, e após a concordância dos participantes do projeto. Os riscos aceitos devem ser inseridos em uma lista de observação.

#### **4.4.2 ATIVIDADE *DEFINIR E SELECIONAR RESPOSTAS AOS RISCOS***

Consiste na definição, avaliação e seleção das ações de resposta a serem executadas para o tratamento dos riscos, incluindo a elaboração do *Plano de contingências*. Devem ser designados o proprietário de cada risco e os demais envolvidos no acompanhamento e na execução das respostas, conforme Quadro 4.11.

**Quadro 4.11 – Atividade *Definir e selecionar respostas aos riscos***

<b>Propósito:</b> Avaliar e selecionar opções para tratar os riscos do projeto	
<b>Passos</b>	
<ul style="list-style-type: none"> <li>• Definir ações de resposta aos riscos</li> <li>• Avaliar e selecionar as ações</li> <li>• Definir plano de contingências</li> <li>• Associar gatilhos aos riscos</li> <li>• Designar proprietário e envolvidos</li> </ul>	
<b>Artefatos de entrada</b>	<b>Artefatos resultantes</b>
<ul style="list-style-type: none"> <li>• Ativos de processos organizacionais</li> <li>• Registro de riscos</li> <li>• Plano de gerenciamento de riscos</li> </ul>	<ul style="list-style-type: none"> <li>• Registro de riscos</li> <li>• Plano de desenvolvimento de <i>software</i></li> </ul>
<b>Papel:</b> Gerente do projeto	

A seguir são apresentados os cinco passos dessa atividade.

#### 4.4.2.1 DEFINIR AÇÕES DE RESPOSTA AOS RISCOS

Consiste em definir as ações de resposta para cada risco crítico, de acordo com a estratégia ou conjunto de estratégias selecionadas.

A organização pode criar uma lista contendo as técnicas mais efetivas como ações de resposta aos principais riscos, como aquela sugerida por Boehm (1989) e atualizada em Boehm (2001). Essa lista estará disponível nos *Ativos de processos organizacionais*, devendo ser revista periodicamente, com base nos dados obtidos de novos projetos. Essas ações deverão ser avaliadas, para se verificar a viabilidade de sua implementação.

#### 4.4.2.2 AVALIAR E SELECIONAR AS AÇÕES

Significa avaliar as ações desenvolvidas em resposta aos riscos, para se selecionar adequadamente a opção ou conjunto de opções, mediante reorganização do projeto, e inseri-las em um cronograma. Para tanto, deve-se assegurar que o risco foi compreendido, e verificar se as opções de tratamento satisfazem os objetivos do tratamento, ou seja, se:



- são realísticas;
- podem ser monitoradas e controladas;
- não introduzem riscos secundários (novos riscos decorrentes da ação de resposta) ou, em caso positivo, se o risco é menor que o anterior.

A norma AS/NZS 4360 (2004) sugere que se levem em conta, antes de se tomar qualquer decisão sobre a opção de tratamento mais indicada, os seguintes aspectos:

- aceitabilidade;
- eficiência;
- compatibilidade;
- continuidade dos efeitos;
- custos;
- tempo;
- criação de novos riscos; e
- objetivos.

O CMMI (2002) recomenda que as ações de resposta aos riscos sejam examinadas no tocante aos benefícios oferecidos em relação aos recursos consumidos. Então, as ações mais apropriadas devem ser selecionadas para implantação.

Com base na avaliação realizada, selecionam-se as ações a serem implementadas. As ações selecionadas devem ser documentadas no *Plano de tratamento dos riscos*, além de serem inseridas no cronograma do projeto. O conteúdo do *Plano de tratamento dos riscos* poderá figurar no artefato *Registro de riscos*, se a organização assim o desejar.

#### **4.4.2.3 DEFINIR PLANO DE CONTINGÊNCIAS**

Consiste em definir as ações a serem implementadas no caso de ocorrência do risco. Essas ações comporão o *Plano de contingências*, devendo ser identificadas independentemente da estratégia selecionada. Apenas com relação aos riscos cuja estratégia selecionada tenha sido a aceitação passiva, não serão definidas ações de contingência. O contexto e os limites dos riscos também devem ser considerados para a definição dessas ações.

Apesar dos esforços despendidos, alguns riscos são inevitáveis, podendo transformar-se em problemas com conseqüências para o projeto. A estratégia de contingência atua para modificar as conseqüências decorrentes da ocorrência do risco. Se o risco não puder ser tratado ou se falhar a estratégia de tratamento, o *Plano de contingências* pode ser acionado. O *Plano de contingências* descreve as ações que um projeto deve adotar ao verificar a ocorrência de riscos, de modo a lidar com seus impactos. Esse plano contém as respostas que somente serão executadas se vierem a ocorrer determinados eventos. O *Plano de contingências* deverá integrar o *Plano de tratamento dos riscos*, que, por sua vez, pode estar contido no *Registro de riscos*.

#### **4.4.2.4 ASSOCIAR GATILHOS AOS RISCOS**

Consiste em associar gatilhos aos riscos identificados e selecionados para tratamento. Esses gatilhos deverão ser selecionados entre as métricas definidas como limites para a categoria do risco, conforme subseção 4.1.2.4, e funcionarão como sinalizadores para o acompanhamento dos riscos. Um gatilho deve corresponder a uma condição mensurável e passível de acompanhamento.

Podem ser estabelecidos gatilhos para indicar a necessidade de um acompanhamento mais intenso ou para provocar a definição ou o acionamento de ações de resposta aos riscos.

Deve ser definido pelo menos um gatilho indicando a ocorrência do risco ou a sua iminência. Esse gatilho será utilizado para sinalizar a necessidade de execução do *Plano de contingências*. Sempre que possível, deve ser feita uma associação do gatilho com as tarefas do cronograma do projeto a serem monitoradas. São exemplos de gatilho:

- marcos intermediários não cumpridos;
- a volatilidade dos requisitos ultrapassar determinado percentual;
- ao se promover um teste de protótipo ou um teste simulado, se o tempo de resposta for maior do que determinado percentual;
- o impacto no caminho crítico maior do que determinado período; e
- projeção do custo maior que determinado percentual da reserva de gerenciamento.

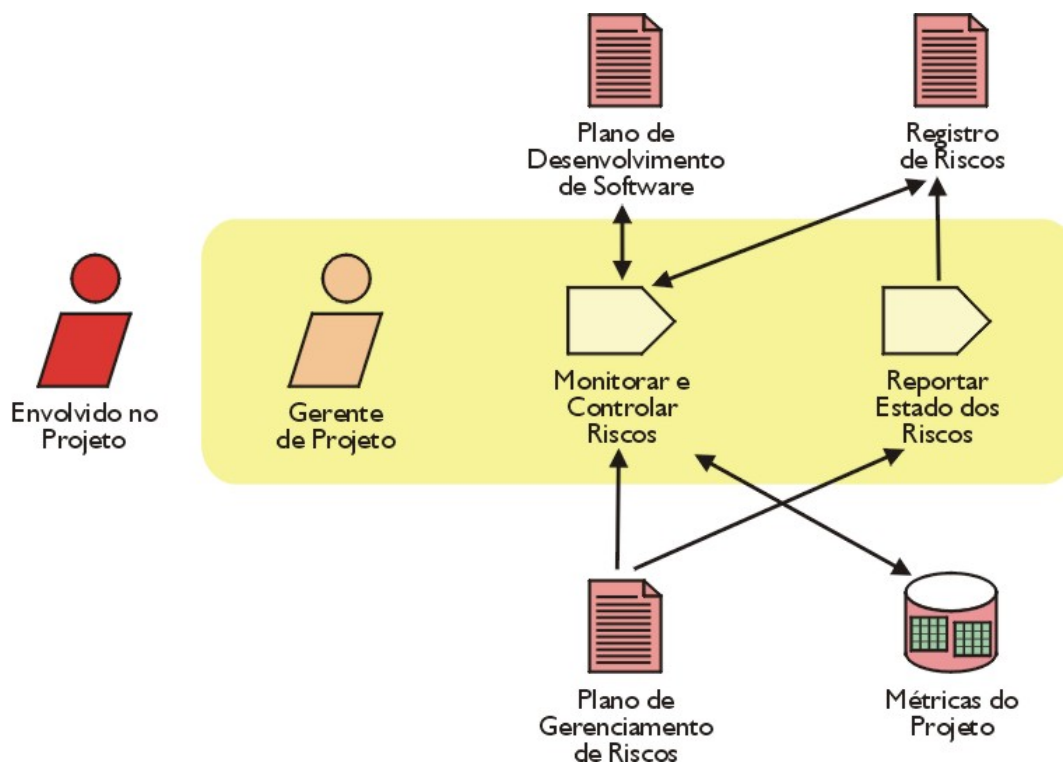
#### 4.4.2.5 DESIGNAR PROPRIETÁRIO E ENVOLVIDOS

Designar o proprietário de cada risco identificado, que será a pessoa responsável pelo acompanhamento do risco e das tarefas correspondentes previstas no *Plano de tratamento dos riscos*.

O executor da ação de resposta ao risco também deve ser especificado, assim como os demais direta ou indiretamente envolvidos no gerenciamento do risco, com a especificação de suas respectivas responsabilidades.

#### 4.5 MACROATIVIDADE *MONITORAR E CONTROLAR RISCOS*

A Figura 4.9 detalha as atividades da macroatividade *Monitorar e controlar riscos*, que se relaciona com as demais macroatividades do *Processo de gerenciamento de riscos* e seus artefatos, os quais devem ser revisados no decorrer do projeto.



**Figura 4.9 – Macroatividade *Monitorar e controlar riscos***

A execução dessa macroatividade pode conduzir à identificação de novos riscos e à necessidade de uma nova análise ou de um planejamento de respostas adicional, adotando-

se os procedimentos especificados no *Processo de gerenciamento de riscos*. Envolve também a execução do *Plano de tratamento dos riscos*, quando necessário, assim como a monitoração das ações correspondentes.

Além disso, a depender do grau de mudanças requerido, pode ser necessário acionar a macroatividade *Planejar o gerenciamento de riscos*, caso torne-se necessário elaborar um novo planejamento do projeto.

A macroatividade *Monitorar e controlar riscos* compõe-se das seguintes atividades: (i) *Monitorar e controlar riscos*; e (ii) *Reportar os estados dos riscos*.

#### 4.5.1 ATIVIDADE MONITORAR E CONTROLAR RISCOS

A atividade *Monitorar e controlar riscos* consiste em revisar o estágio de cada risco, avaliar se os limites definidos para cada risco atingem pontos críticos que indiquem a necessidade de uma nova análise ou mesmo a execução do *Plano de tratamento dos riscos* e o conseqüente acompanhamento das ações correspondentes, como também de identificação de novos riscos, conforme Quadro 4.12. Essa atividade é implementada ao longo do processo de gerenciamento de riscos.

**Quadro 4.12 – Atividade *Monitorar e controlar riscos***

<b>Propósito:</b> Detectar mudanças nos estados dos riscos e o surgimento de novos riscos	
<b>Passos</b>	
<ul style="list-style-type: none"> <li>• Acompanhar os estados atuais dos riscos</li> <li>• Executar o plano de tratamento dos riscos</li> <li>• Acompanhar o plano de tratamento dos riscos</li> </ul>	
<b>Artefatos de entrada</b>	<b>Artefatos resultantes</b>
<ul style="list-style-type: none"> <li>• Plano de desenvolvimento de <i>software</i></li> <li>• Registro de riscos</li> <li>• Plano de gerenciamento de riscos</li> <li>• Métricas do projeto</li> </ul>	<ul style="list-style-type: none"> <li>• Registro de riscos</li> <li>• Plano de desenvolvimento de <i>software</i></li> <li>• Métricas do projeto</li> </ul>
<b>Papel:</b> Gerente do projeto	

#### 4.5.1.1 ACOMPANHAR OS ESTADOS ATUAIS DOS RISCOS

Trata-se de monitorar os riscos de acordo com os gatilhos associados a cada um deles, para se identificar a necessidade de execução do *Plano de contingências* ou de implementação de novas ações.

Os riscos identificados durante o processo de gerenciamento de riscos devem ser periodicamente revisados, observando-se a frequência especificada no *Plano de gerenciamento de riscos*, no contexto de seu estado atual e das circunstâncias do projeto. Para a monitoração dos riscos, deve ser considerada sua prioridade. Entretanto, mesmo os riscos de baixa severidade devem ser monitorados, uma vez que sua severidade pode elevar-se no decorrer do projeto. Seguem-se alguns exemplos de situação em que os riscos devem ser revisados (CMMI, 2002):

- quando novos riscos são identificados;
- quando o risco torna-se um problema;
- quando o risco é eliminado; e
- quando as circunstâncias do projeto mudam significativamente.

O gerente do projeto revisa os limites associados a cada risco consignado no *Registro de riscos*, para compará-los com o estado atual do risco, no âmbito do projeto. Essa revisão conduz à identificação da necessidade de acionar a execução das ações previstas no *Plano de tratamento dos riscos*, ou, ainda, à definição de novas ações.

Essa avaliação pode propiciar a descoberta de novos riscos ou de novas opções de resposta, capazes de levar a uma nova análise ou a um novo planejamento do tratamento dos riscos. Um ponto essencial a ser observado é a possibilidade de ocorrência de riscos secundários.

Para os casos em que for adotado o ciclo de vida iterativo incremental, ao final da iteração devem-se focar novamente os objetivos da iteração em relação ao *Registro de riscos*, especificamente para (RUP, 2003):

- eliminar riscos totalmente mitigados;
- introduzir riscos recém-descobertos; e
- reavaliar a magnitude dos riscos e reordená-los (analisar e priorizar os riscos).

As seguintes questões devem ser consideradas para essa avaliação:

- O evento ainda é possível?
- A probabilidade ainda é a mesma?
- O impacto ainda é o mesmo?
- A tolerância ao risco dos envolvidos ainda é a mesma?

#### **4.5.1.2 EXECUTAR O PLANO DE TRATAMENTO DOS RISCOS**

O propósito é disparar a execução das ações previstas no *Plano de tratamento dos riscos*, quando essa necessidade for identificada por ocasião do acompanhamento dos estados atuais dos riscos (passo 4.5.1.1).

#### **4.5.1.3 ACOMPANHAR O PLANO DE TRATAMENTO DOS RISCOS**

Trata-se de acompanhar a execução das atividades de tratamento dos riscos previstas no cronograma do projeto, e avaliar sua efetividade.

Esse acompanhamento envolve também os riscos residuais, ou seja, aqueles que permanecem ativos apesar das ações de tratamento implementadas em resposta a eles, incluindo-se também os riscos aceitos (DINSMORE et al, 2003).

Se as respostas aos riscos não produzirem o resultado esperado, deve ser identificado o motivo respectivo, implementando-se novas ações no sentido de solucionar o problema.

A eficiência do tratamento de um risco pode ser avaliada por meio de métricas que devem ser implementadas e monitoradas. As causas de um tratamento ineficiente devem ser prontamente identificadas e solucionadas (IEEE Std 1540-2001, 2001).

O proprietário do risco é o responsável primário pelo acompanhamento das ações de resposta, competindo-lhe verificar se as ações estão sendo implementadas pelo executor.

#### **4.5.2 REPORTAR OS ESTADOS DOS RISCOS**

Significa atualizar a documentação de riscos do projeto e comunicar os estados dos riscos aos envolvidos no projeto, conforme explicitado no Quadro 4.13.

**Quadro 4.13 – Atividade Reportar os estados dos riscos**

<b>Propósito:</b> Registrar e comunicar mudanças nos estados dos riscos	
<b>Passos</b>	
<ul style="list-style-type: none"> <li>• Revisar a documentação dos riscos</li> <li>• Comunicar os estados dos riscos</li> </ul>	
<b>Artefatos de entrada</b>	<b>Artefatos resultantes</b>
<ul style="list-style-type: none"> <li>• Registro de riscos</li> <li>• Plano de gerenciamento de riscos</li> </ul>	<ul style="list-style-type: none"> <li>• Registro de riscos</li> </ul>
<b>Papel:</b> Gerente do projeto	

#### 4.5.2.1 REVISAR A DOCUMENTAÇÃO DOS RISCOS

Deve-se garantir que as informações sobre os riscos sejam atualizadas no decorrer do projeto. Consiste na revisão da documentação dos riscos à medida que novas informações sejam disponibilizadas, de modo a incorporar as mudanças identificadas e garantir que o *Registro de riscos* mantenha-se atualizado no decorrer do projeto.

O *Registro de riscos* deve ser atualizado mediante incorporação das alterações identificadas para cada risco. Por exemplo, sempre que houver alteração no impacto, na probabilidade de ocorrência, no estado, ou em qualquer outro atributo do risco, o *Registro de riscos* deve ser atualizado.

É fundamental responder as questões a seguir:

- O estado está atualizado?
- Os riscos recém-identificados foram incluídos?
- As mudanças de probabilidade e impacto foram registradas?
- Os riscos estão ordenados corretamente pela prioridade (em função de uma nova análise e priorização)?
- O *Plano de tratamento dos riscos* foi atualizado?

#### **4.5.2.2 COMUNICAR OS ESTADOS DOS RISCOS**

A idéia é comunicar aos envolvidos os atuais estados dos riscos do projeto, de modo a garantir a visibilidade dos riscos e do andamento dos esforços de tratamento.

Consiste na comunicação e no relato do *estado* do gerenciamento dos riscos, para assegurar a visibilidade do potencial de exposição do projeto ao risco e do estado dos esforços de tratamento dos riscos. Os principais riscos devem ser visíveis para todos os envolvidos no projeto, assim como as ações que estão sendo implementadas sobre eles.

A comunicação entre a equipe e os demais envolvidos no projeto constitui um dos fatores mais importantes para um bem-sucedido gerenciamento de riscos (HUMPHREY, 1990). É fundamental uma boa comunicação durante todo o processo, para garantir que os responsáveis pela implementação do gerenciamento de riscos, assim como os envolvidos no projeto, entendam as bases nas quais as decisões serão adotadas, e os motivos da implementação de determinadas ações. Quando a estrutura de comunicação de uma organização está debilitada, podem surgir riscos, problemas e crises.

#### **4.6 MACROATIVIDADE AVALIAR O PROCESSO DE GERENCIAMENTO DE RISCOS**

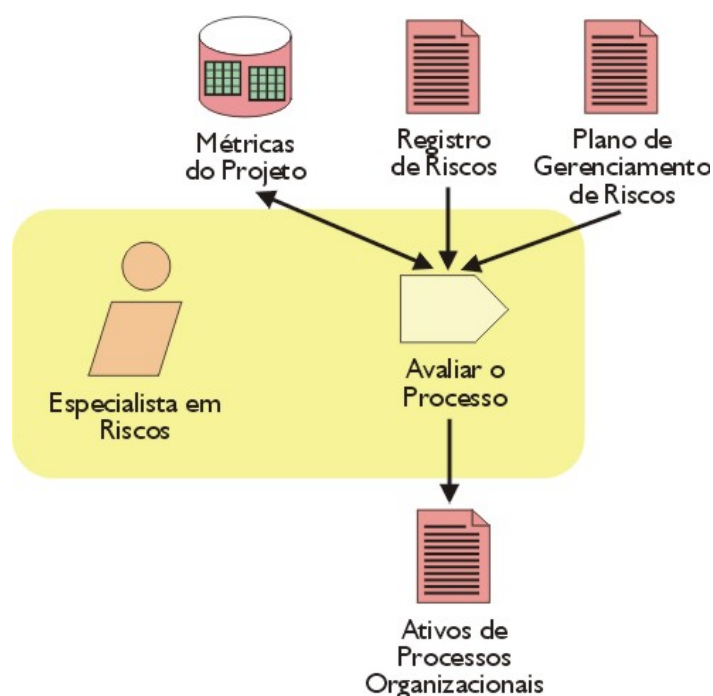
A Figura 4.10 mostra a macroatividade *Avaliar o processo de gerenciamento de riscos*, o qual consiste em verificar a sua eficácia por meio dos artefatos produzidos, indicadores e resultados sobre a melhoria derivada do planejamento e execução desse processo. Essas informações irão suportar o uso e a melhoria do processo de *software* da organização e dos recursos do processo.

Essa macroatividade tem como propósitos capturar e organizar as informações sobre a qualidade do processo de gerenciamento de riscos, assim como identificar as necessidades e oportunidades de melhoria no processo, procedimentos ou ferramentas, com vistas a aumentar a capacidade de reduzir ou eliminar riscos sistêmicos.



De acordo com Costa et al (2005), os riscos sistêmicos são aqueles que afetam todos os projetos de *software* de uma determinada categoria (sistemas de informação, sistemas militares, sistemas comerciais, etc.).

As informações sobre o processo devem ser capturadas, para melhorar o processo e a habilidade da organização para gerenciar riscos. A macroatividade *Avaliar o processo de gerenciamento de riscos* compõe-se da atividade *Avaliar o processo de gerenciamento de riscos*.



**Figura 4.10 – Macroatividade *Avaliar o processo de gerenciamento de riscos***

#### **4.6.1 ATIVIDADE AVALIAR O PROCESSO DE GERENCIAMENTO DE RISCOS**

Essa atividade consiste na monitoração e revisão do processo de gerenciamento de riscos, para avaliação de sua efetividade. Propõe-se, também, avaliar se a abordagem utilizada está consistente com os objetivos da organização. O Quadro 4.14 apresenta essa atividade.

**Quadro 4.14 – Atividade *Monitorar e controlar o processo***

<b>Propósito:</b> Avaliar e melhorar o processo de gerenciamento de riscos	
<b>Passos</b>	
<ul style="list-style-type: none"> <li>• Capturar informações sobre o processo</li> <li>• Avaliar e melhorar o processo</li> <li>• Gerar lições aprendidas</li> </ul>	
<b>Artefatos de entrada</b>	<b>Artefatos resultantes</b>
<ul style="list-style-type: none"> <li>• Ativos de processos organizacionais</li> <li>• Registro de riscos</li> <li>• Plano de gerenciamento de riscos</li> <li>• Métricas do projeto</li> </ul>	<ul style="list-style-type: none"> <li>• Ativos de processos organizacionais</li> <li>• Métricas do projeto</li> </ul>
<b>Papel:</b> Especialista em Riscos	

#### 4.6.1.1 CAPTURAR INFORMAÇÕES SOBRE O PROCESSO

O propósito é capturar informações sobre o processo de gerenciamento de riscos, os riscos identificados, suas causas, seu tratamento e o sucesso das opções de tratamento selecionadas no decorrer do ciclo de vida do projeto, a fim de melhorar o processo e gerar lições aprendidas (IEEE Std 1540-2001, 2001).

Essas informações devem ser coletadas durante todo o projeto, por meio de produtos de trabalho, dos indicadores definidos na subseção 4.1.2.5 e de dados sobre a melhoria derivada do planejamento e da execução do processo de gerenciamento de riscos. As informações coletadas subsidiarão o uso futuro e a melhoria dos processos da organização e dos recursos do processo.

Um repositório de riscos pode ser construído no âmbito organizacional, contendo os riscos mais frequentes nos projetos, e suas soluções. Esse repositório pode ajudar os gerentes de projetos a evitar os riscos já conhecidos em seus projetos (KULPA, 2003).

#### 4.6.1.2 AVALIAR E MELHORAR O PROCESSO

Significa verificar a efetividade e a eficiência do processo de gerenciamento de riscos. Avalia-se se os artefatos estão sendo produzidos adequadamente e se são

considerados na devida importância nas decisões relacionadas ao projeto. Além disso, verifica-se a conformidade do processo com o plano, para se implementar ações corretivas apropriadas, se e quando necessário.

Consiste ainda na avaliação objetiva da aderência do processo de gerenciamento de riscos, em relação a sua descrição, padrões, procedimentos e endereçamento das não-conformidades.

São exemplos de atividades a serem revisadas:

- fontes e categorias de riscos utilizadas no projeto;
- parâmetros utilizados para o gerenciamento de riscos;
- estabelecimento e manutenção de estratégias de gerenciamento de riscos;
- identificação e análise de riscos; e
- tratamento de riscos.

São exemplos de produtos de trabalho revisados:

- estratégia de gerenciamento dos riscos; e
- planos de tratamento dos riscos.

#### **4.6.1.3 GERAR LIÇÕES APRENDIDAS**

Cuida-se aqui em gerar as lições aprendidas do projeto, com o objetivo de ajudar na identificação de riscos sistêmicos e organizacionais, que podem ser organizados de acordo com as características do projeto. Essa coleta é feita com base na revisão periódica das informações sobre os riscos identificados, a ser realizada pelas partes interessadas, de acordo com a periodicidade determinada. O tratamento dos riscos e o sucesso desse tratamento serão revistos, assim como as causas dos riscos concretizados. As lições aprendidas de cada projeto devem ser coletadas e registradas para posterior utilização. Devem também ser revisados as fontes, as categorias e os parâmetros utilizados no gerenciamento de riscos do projeto. As lições aprendidas devem ser documentadas de maneira a integrar os *Ativos de processos organizacionais*, de modo a serem úteis para outros projetos da organização.

Ao se analisar sucessos e fracassos, deve-se atentar para as seguintes questões (AS/NZS 4360, 2004):

- Os riscos envolvidos foram previamente identificados e analisados?
- As causas reais dos riscos foram identificadas?
- O processo de monitoração e controle foi efetivo?
- Os planos de tratamento foram efetivos? Se não, quais melhorias poderiam ser realizadas?
- Como o processo de gerenciamento de riscos poderia ser melhorado?
- Quem precisa conhecer essas lições aprendidas, e como estas podem ser disseminadas para garantir maior eficácia ao aprendizado?
- Como poder-se-ia assegurar que os eventos de fracasso não sejam repetidos, mas que os de sucesso o sejam?

Uma das principais causas da ineficiente utilização ou da não-utilização do gerenciamento de riscos nas organizações que desenvolvem *software* é a falta de documentação de experiências de sucesso ou fracasso (PRIKLADNICKI, 2005). A seguir são apresentadas algumas orientações (*guidelines*) para a utilização do processo proposto em organizações de *software*.

#### **4.7 GUIDELINES PARA A IMPLANTAÇÃO DO PROCESSO PROPOSTO**

A partir da experiência de implantação do processo proposto em uma organização de *software* (Capítulo 5), sugere-se o seguinte conjunto de passos para a especialização e instanciação desse processo em uma organização de *software*:

- **Especialização do processo**
  - ✓ obter inicialmente o comprometimento da superior- administração;
  - ✓ promover reuniões com gerentes de projeto, para exposição do processo a ser implantado;
  - ✓ analisar os processos já definidos na organização, se houver;
  - ✓ realizar um mapeamento entre papéis e artefatos propostos, com aqueles existentes na organização;
  - ✓ verificar a existência de bases organizacionais históricas de projetos anteriores, para colher informações sobre seus riscos;

- ✓ promover entrevistas com gerentes e equipe dos projetos sobre sua experiência em projetos anteriores, no tocante aos riscos;
  - ✓ identificar as fontes de riscos mais comuns nos projetos da organização;
  - ✓ elaborar uma categorização de riscos de acordo com as características da organização;
  - ✓ definir parâmetros para o gerenciamento dos riscos nos projetos da organização (por exemplo, critérios a serem utilizados na análise dos riscos);
  - ✓ definir, sempre que possível, uma ferramenta para gerenciar os riscos de projetos; e
  - ✓ treinar os membros das equipes dos projetos .
- **Instanciação do processo**
    - ✓ Aplicar o *processo especializado* em projetos-piloto;
    - ✓ realizar um acompanhamento supervisionado nesses projetos;
    - ✓ fazer os ajustes necessários no processo especializado, de acordo com as lições aprendidas nos projetos-piloto; e
    - ✓ aplicar o *processo especializado* nos demais projetos da organização.

A cada projeto concluído, deve-se tentar capturar as possíveis lições aprendidas, que possam ser replicadas para outros projetos e utilizadas para a melhoria contínua do *Processo de gerenciamento de riscos de software*.

## 4.8 CONCLUSÃO

Este capítulo propôs o *Processo de gerenciamento de riscos para projetos de software*, baseado em normas e padrões largamente reconhecidos, que abordam o gerenciamento de riscos. O capítulo seguinte trata da aplicação prática do processo proposto em uma organização de *software*.

## Capítulo 5

# APLICAÇÃO DO PROCESSO DE GERENCIAMENTO DE RISCOS

---

*Este capítulo apresenta um estudo de caso realizado em uma empresa de software, com o objetivo de validar o processo proposto.*

O presente capítulo apresenta os resultados obtidos com a aplicação do *Processo de gerenciamento de riscos*, proposto no capítulo anterior, em uma organização de *software*, denominada Instituto Atlântico, situada em Fortaleza. Foi procedida a especialização do processo proposto para essa organização, seguida de sua aplicação em três projetos-piloto.

Esse processo de gerenciamento de riscos também se encontra em implementação em uma segunda organização, que será denominada Organização X. Trata-se de uma empresa de grande porte, mas ainda não há dados conclusivos sobre o processo aplicado.

Nas seções seguintes, são apresentados os perfis das organizações onde foram realizados os experimentos, assim como os resultados obtidos da especialização desse processo no Instituto Atlântico. Em seguida, descrevem-se os perfis dos projetos em que foi aplicado o processo especializado, como também os seus resultados.

### 5.1 PERFIL DO INSTITUTO ATLÂNTICO

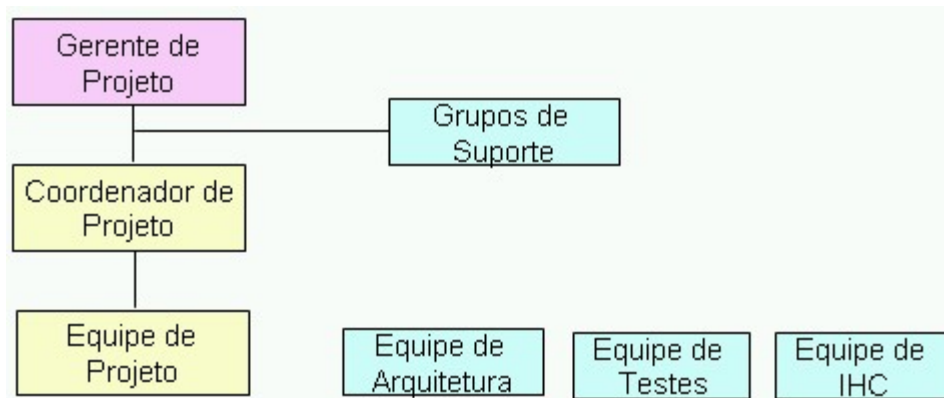
Trata-se de uma instituição de pesquisa e desenvolvimento (P&D), fundada em novembro de 2001 por iniciativa do Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD). A organização foi certificada como SW-CMM, nível 2, em outubro de 2003, e tem como meta organizacional a certificação CMMI, nível 3, no primeiro trimestre de 2006. Nesse nível, a área de processo *Gerência de riscos* (RSKM) constitui um dos processos de gerência de projetos a ser definido e institucionalizado.

O escopo de atuação do Instituto abrange pesquisa e desenvolvimento de soluções de *software* (Web e Automação de processos), *hardware* e serviços de consultoria na área

de Tecnologia da Informação e telecomunicações. Essas soluções são desenvolvidas mediante projetos próprios ou específicos para clientes, podendo ter como objetivo uma nova tecnologia, um novo produto ou a atualização de algum produto já existente. Os projetos desenvolvidos pertencem a diversas áreas, possuem tamanhos variados e são desenvolvidos em diferentes plataformas (J2EE, J2ME, .NET, C, C++, etc.).

Essa diversidade de projetos, muitas vezes envolvendo novas tecnologias, e desenvolvidos em diferentes plataformas, para atender a clientes com perfis os mais diversos, caracterizam um ambiente bastante favorável ao surgimento e concretização de riscos. Sendo assim, com o aumento da complexidade dos projetos desenvolvidos, o gerenciamento de riscos passou a ter grande relevância para o Instituto Atlântico, sendo essencial a definição de um processo organizacional de gerenciamento de riscos.

Os processos organizacionais são desenvolvidos com base no *Processo unificado* (RUP, 2003), sendo definidos pelos próprios funcionários, e adaptados à realidade da organização. A dinâmica de trabalho do Instituto Atlântico na condução de projetos é, em geral, operacionalizada como se segue: cada projeto tem um *gerente de projeto*, um *coordenador de projeto*, *analistas de sistemas* e *programadores*, conforme ilustrado na Figura 5.1.



**Figura 5.1 – Estrutura de trabalho do Instituto Atlântico**

O *gerente de projeto* tem como responsabilidades fazer o acompanhamento gerencial técnico, financeiro e dos recursos humanos para o projeto, negociar alterações de compromissos com o cliente, quando isso envolver mudanças contratuais, além de designar o coordenador de projeto.

O *coordenador de projeto* é responsável por coordenar tecnicamente a equipe de projeto, planejar e acompanhar o projeto, conduzir reuniões de acompanhamento técnico, adotar as medidas pertinentes para corrigir eventuais desvios e acompanhar a execução das correções até a sua solução efetiva, alocar pessoal para os papéis de líder de requisitos e líder de configuração, entre outros, negociar compromissos com os *Grupos de suporte: Equipe de arquitetura, Equipe de testes e Equipe de IHC*, além de negociar com o gerente de projeto a alocação de recursos humanos e financeiros. O coordenador foi escolhido como o responsável pelo gerenciamento de riscos nos projetos da organização.

A *equipe de projeto* compõe-se de *analistas de sistemas e programadores*, destacando-se dois papéis fundamentais no processo dessa organização: o *líder de requisitos* e o *líder de configuração*.

Apesar de a equipe possuir competências para desenvolver as atividades necessárias no projeto, conta ainda com o apoio do *Grupo de suporte* institucional, compreendendo a *Equipe de arquitetura*, a *Equipe de testes* e a *Equipe de IHC*. A *Equipe de arquitetura* tem a responsabilidade de participar direta ou indiretamente (consultoria) da elaboração e da revisão da arquitetura dos projetos e apoiar o líder de requisitos na especificação dos requisitos do projeto, quando necessário. A *Equipe de testes* é responsável pela execução dos testes sistêmicos do projeto e pela geração de relatórios com resultados desses testes, além apoiar grupos internos do projeto em testes (unitários e integração, por exemplo).

Além dos citados papéis, que atuam diretamente no projeto, há outros papéis da organização utilizados nas macroatividades do *Processo de gestão de riscos*. São eles: *Stakeholders*, Gerente Técnico e Superintendente. Nesse contexto, os *Stakeholders* são os envolvidos no projeto que não fazem parte da equipe do projeto. O Gerente Técnico e o Superintendente são papéis que atuam acima do nível do projeto, no âmbito administrativo, mas que têm influência nos projetos, quando necessário.

Apesar da segmentação de papéis na organização, um membro da equipe do projeto, sempre que isso se justificar, poderá vir a desempenhar papéis próprios do *Grupo de suporte*.

Na seção seguinte, apresenta-se a especialização do *Processo de gerenciamento de riscos* para o Instituto Atlântico.



## 5.2 ESPECIALIZAÇÃO DO PROCESSO PARA O INSTITUTO ATLÂNTICO

O *Processo de gerenciamento de riscos para projetos de software* foi especializado no Instituto Atlântico, para institucionalizar a área de processo *Gerenciamento de riscos* do CMMI, nível 3, uma vez que essa organização encontra-se em vias de obter a certificação CMMI, nível 3.

Inicialmente, foi realizada uma apresentação do processo proposto para um grupo de gerentes de projetos e coordenadores experientes, todos com certificação PMP (*Project Management Professional*), que é a certificação em gerenciamento de projetos do PMI (*Project Management Institute*). O objetivo dessa apresentação foi avaliar a aplicabilidade do processo à realidade da organização. Chegou-se à conclusão de que o processo era perfeitamente aplicável na organização. Entretanto, deveria ser feita uma especialização desse processo de acordo com os padrões da organização, utilizando-se seu *framework* de processos.

Os papéis considerados essenciais para o gerenciamento de riscos no processo proposto foram mapeados nos papéis já definidos no *framework* de processos da organização. Havia o papel de *Gerente de projeto*, com a mesma denominação, sendo-lhe atribuídas as responsabilidades previstas para esse papel referentes ao gerenciamento de riscos, sem alterações. As responsabilidades previstas para o *Envolvido no projeto* foram atribuídas aos papéis *Equipe do projeto* e *Stakeholders*. Não havia o papel de *Especialista em riscos*, decidindo-se a organização pela não-criação desse papel, apesar do reconhecimento de sua importância para as atividades de gerenciamento de riscos. As responsabilidades desse papel foram incorporadas às atividades dos coordenadores externos.

Os artefatos do processo proposto também deveriam ser mapeados nos artefatos correspondentes no repositório de processos da organização. Apenas seriam criados os artefatos específicos de gerenciamento de riscos. Os dois artefatos específicos do processo foram então criados com base nos *templates* apresentados no Apêndice B, para o *Plano de gestão de riscos*, e no Apêndice C, para a *Lista de riscos*. O vocábulo “gerenciamento” do nome do primeiro artefato foi substituído por “gestão”, por ser este o termo utilizado em outros *templates*, como o *Plano de gestão da qualidade*, por

exemplo. A denominação *Registro de riscos* foi substituída por *Lista de riscos*, adotada no RUP (que era utilizado na organização).

Em seguida, foram realizadas entrevistas com gerentes de projetos e coordenadores, para obtenção de informações sobre as práticas de gerenciamento de riscos utilizadas no dia-a-dia dos projetos e sobre as dificuldades enfrentadas. Apesar de não haver um processo definido, a organização já utilizava as práticas de identificação, atribuição de valores à probabilidade e ao impacto dos riscos identificados, planejamento das respostas e acompanhamento dos riscos. Entretanto, a exposição ao risco não era utilizada para a priorização dos riscos, e não havia critérios definidos para a seleção dos riscos a serem tratados. Na maioria dos projetos, não havia a definição de gatilhos para os riscos identificados.

O coordenador do projeto tentava acompanhar todos os riscos, ou mesmo apenas os identificava no início do projeto e depois reagia quando constatava que um risco havia ocorrido, por meio da execução do *Plano de contingências*. O acompanhamento pouco efetivo dos riscos e das ações definidas para seu tratamento foi uma das principais falhas apontadas pelos coordenadores em seus projetos. A seguir, citam-se algumas dificuldades apontadas pelos coordenadores no gerenciamento de riscos:

- acompanhamento dos riscos;
- acompanhamento das ações no cronograma;
- definição de quando a ação deveria ocorrer;
- como verificar se a estratégia de mitigação estaria sendo efetiva;
- ausência de uma base histórica dos riscos mais comuns; e
- ferramenta utilizada não facilitava o acompanhamento dos riscos.

As práticas de gerenciamento de riscos faziam parte do processo de *Gestão de projetos*. As práticas *identificar, analisar, priorizar, associar ações de mitigação e contingência* e *acompanhar os riscos* eram mencionadas nos procedimentos institucionais para o planejamento de projetos e para o acompanhamento de projetos. Essa forma de implementação atendia às exigências do nível 2 do CMM.

O passo seguinte foi a elaboração dos fluxos do *Processo de gerenciamento de riscos* especializado, utilizando-se o modelo de definição de processos e os papéis

existentes para os processos da organização. A organização optou por fluxos mais simplificados e um maior detalhamento nos procedimentos descritos para cada atividade. O fluxo principal adaptado e os fluxos das macroatividades foram submetidos a aprovação, dando-se em seguida o aval para a continuidade do trabalho. Depois disso, foram elaborados os procedimentos, que constituem o instrumento utilizado pela organização para a institucionalização do processo.

O processo especializado e os procedimentos foram apresentados à equipe do EPG (*Engineering Process Group*) e à consultoria externa, contratada para a validação dos processos que estão sendo definidos para a certificação CMMI, nível 3. Foram feitas algumas observações e sugestões; entretanto, não foram encontradas não-conformidades com a área de processo *Gerenciamento de riscos* do CMMI, que vinha sendo institucionalizada a partir do processo especializado de gerenciamento de riscos.

Os ajustes recomendados foram referentes a um maior detalhamento das ferramentas e técnicas e dos parâmetros a serem utilizados para o gerenciamento de riscos na organização. Assim, foi criado o documento *Orientação para identificação de riscos*, contendo as técnicas a serem adotadas para a identificação dos riscos. Foram levantadas as escalas possíveis para os valores de probabilidade e impacto, reunidas em uma matriz de impacto e probabilidade.

O passo seguinte foi a definição das categorias de riscos a serem utilizadas pelos projetos; um levantamento das fontes de riscos mais comuns aos projetos da organização; e a elaboração de um documento de orientação para o levantamento dos riscos baseados nas fontes e categorias de riscos identificadas.

Foram também elaborados modelos para os documentos *Plano de gestão de riscos* e *Lista de riscos*<sup>1</sup>, este último implementado em uma ferramenta de gestão de

---

<sup>1</sup> A organização optou pela substituição da denominação *Registro de riscos*, por se tratar de termo adotado anteriormente e com o qual as equipes dos projetos já estavam familiarizadas.

riscos. O processo e seus artefatos foram revisados pelo EPG, para em seguida serem publicados no repositório de processos.

Após a publicação do processo especializado e início de sua utilização em três projetos-piloto, o processo foi submetido à avaliação classe C do método de avaliação SCAMPI<sup>2</sup> (*Standard CMMI Assessment Method for Process Improvement*). Essa avaliação utiliza métodos de avaliação para identificar oportunidades de melhoria e adotar ações coerentes com a realidade e os objetivos da organização. Identificam-se lacunas nos processos atuais, quando comparados às práticas do nível do CMMI desejado pela organização avaliada. O resultado compreende um relatório conclusivo sobre as lacunas e um plano de ação.

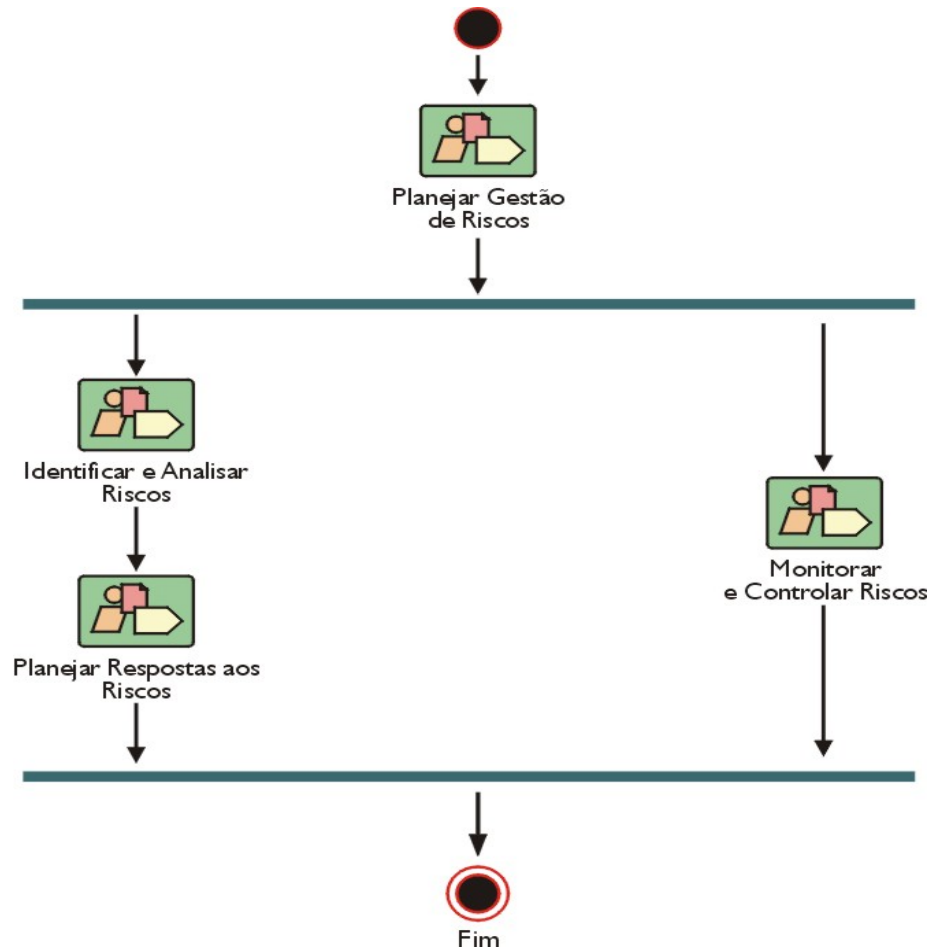
O plano de ação resultante dessa avaliação considerou totalmente definido o processo especializado de gerenciamento de riscos, registrando-se apenas uma lacuna, referente ao acompanhamento dos riscos de baixa severidade. O texto do procedimento foi melhorado, eliminando-se, assim, a lacuna identificada.

Foram também registradas algumas recomendações referentes a uma melhor definição das fronteiras (limites) dos riscos e da utilização dos gatilhos para o acompanhamento, além de um acompanhamento mais efetivo dos riscos e de suas ações. A implantação dessas recomendações viabilizou-se mediante substituição da ferramenta utilizada, relatada com mais detalhes na seção 5.3.

A Figura 5.2 ilustra o fluxo principal do processo especializado. Cada uma das macroatividades que compõem o processo vem detalhada a seguir.

---

<sup>2</sup> O SCAMPI é o método de avaliação desenvolvido pelo *Software Engineering Institute* (SEI). A SCAMPI classe A é a avaliação oficial para a obtenção do nível de maturidade ou capacidade.



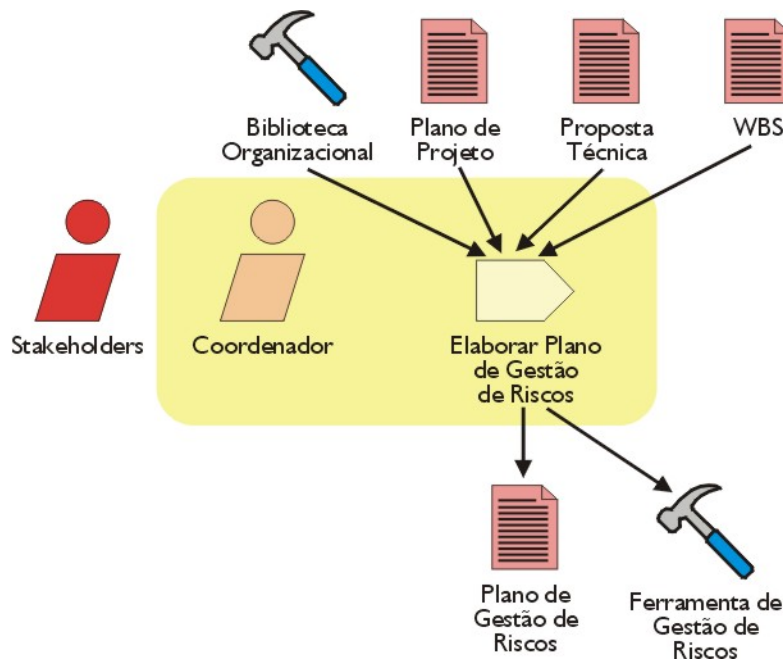
**Figura 5.2 – Fluxo principal do *Processo especializado de gestão de riscos***

### 5.2.1 PLANEJAR A GESTÃO DE RISCOS

Como a organização já utilizava as práticas de gerenciamento de riscos e tinha como propósito a especialização do processo proposto de acordo com suas necessidades, as atividades previstas nessa macroatividade foram realizadas em âmbito organizacional, devendo ser revistas para aplicação nos projetos.

Fontes, categorias e parâmetros utilizados no processo foram previamente definidos para utilização por todos os projetos da organização. Caso fosse identificada alguma fonte adicional de risco ou ainda riscos que não pudessem ser classificados em nenhuma das categorias predefinidas, as novas fontes ou categorias deveriam ser incluídas no *Plano de gestão de riscos* do projeto e na ferramenta *Gestão de riscos*.

Essa macroatividade contém a atividade *Elaborar o plano de gestão de riscos*, conforme ilustrado na Figura 5.3.



**Figura 5.3 – Planejar a gestão de riscos**

A Tabela 5.1 apresenta o mapeamento da macroatividade *Planejar gerenciamento de riscos* do processo proposto, com os artefatos gerados e os processos utilizados pela macroatividade *Planejar gestão de riscos* do processo especializado.

As atividades *Determinar fontes e categorias de riscos*, *Definir parâmetros para os riscos* e *Estabelecer estratégia* foram parcialmente implementadas por meio da macroatividade *Planejar gestão de riscos* (Figura 5.3) na atividade *Elaborar plano de gestão de riscos*, detalhada no procedimento especificado no item 2.1 do Apêndice A.

Apenas o passo *Definir limites para cada categoria de riscos* da atividade *Definir parâmetros para os riscos* não foi considerado viável nesse primeiro momento da especialização do processo. Para viabilizar essa definição, seria necessária uma base histórica de métricas referentes a riscos nos projetos da organização, o que não havia no momento da implantação do processo proposto. Esses limites seriam definidos a partir dos dados a serem obtidos por meio do exercício do processo de gerência de riscos.

Tabela 5.1 – Macroatividade *Planejar o gerenciamento de riscos*

Processo Proposto		Processo Especializado
Atividade	Passo	
Determinar fontes e categorias de riscos	Determinar as fontes de riscos	<ul style="list-style-type: none"> <li>• Documento de orientação detalhando as fontes e categorias de riscos</li> </ul>
	Determinar as categorias de riscos	<ul style="list-style-type: none"> <li>• Ferramenta de gestão de riscos</li> </ul>
Definir parâmetros para os riscos	Definir critérios para a análise dos riscos	<ul style="list-style-type: none"> <li>• Procedimento analisar riscos</li> </ul>
	Definir critérios para o tratamento dos riscos	<ul style="list-style-type: none"> <li>• Procedimento planejar respostas aos riscos</li> </ul>
	Definir métricas	<ul style="list-style-type: none"> <li>• Processo de Medição e Análise</li> </ul>
	Definir Limites para cada Categoria de Riscos	<ul style="list-style-type: none"> <li>• A serem definidos posteriormente como resultado do exercício do processo</li> </ul>
	Definir indicadores para a avaliação do processo	<ul style="list-style-type: none"> <li>• Processo de medição e análise</li> <li>• Ferramenta de gestão de riscos</li> </ul>
Estabelecer estratégia	Adaptar o processo ao projeto	<ul style="list-style-type: none"> <li>• Processo de gestão de projetos</li> </ul>
	Definir metodologia	<ul style="list-style-type: none"> <li>• Elaborar plano de gestão de riscos</li> </ul>
	Atribuir papéis e responsabilidades	<ul style="list-style-type: none"> <li>• Processo gestão de projetos</li> </ul>
	Definir periodicidade	<ul style="list-style-type: none"> <li>• Elaborar plano de gestão de riscos</li> </ul>
	Planejar comunicação	<ul style="list-style-type: none"> <li>• Processo gestão de projetos</li> </ul>
	Definir a avaliação do processo	<ul style="list-style-type: none"> <li>• Processo de garantia da qualidade</li> </ul>

### 5.2.2 IDENTIFICAR E ANALISAR RISCOS

A macroatividade *Identificar e analisar riscos* (Figura 5.4) do processo especializado corresponde a duas atividades: *Identificar riscos* e *Analisar riscos*.

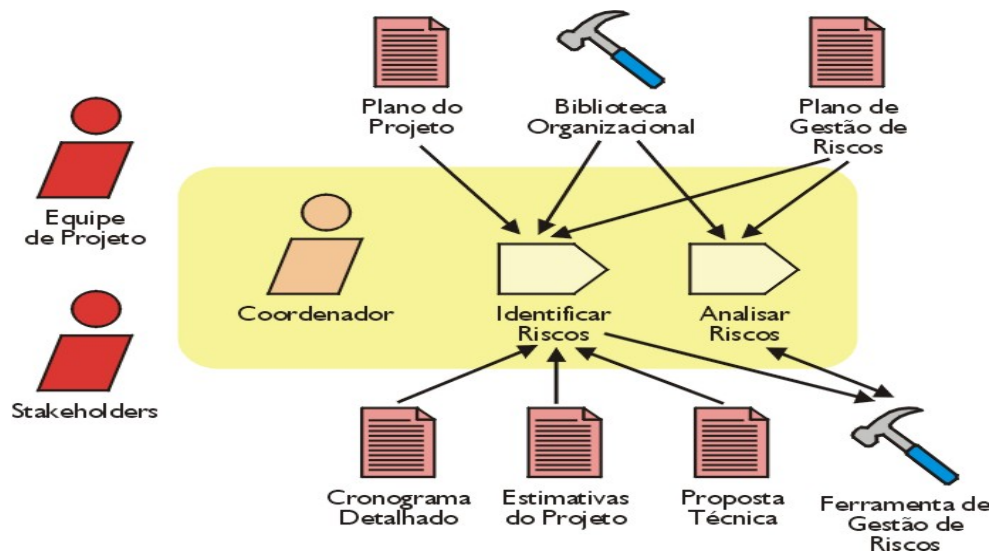


Figura 5.4 – Identificar e analisar riscos

A Tabela 5.2 apresenta o mapeamento da macroatividade *Identificar riscos* do processo proposto, com os artefatos que implementam na organização a atividade *Identificar riscos* do processo especializado.

**Tabela 5.2 – Macroatividade *Identificar riscos***

Processo Proposto		Processo Especializado
Atividade	Passo	
Identificar riscos potenciais	Identificar os riscos associados às fontes e categorias	<ul style="list-style-type: none"> <li>• Procedimento <i>Identificar riscos</i></li> </ul>
	Revisar a documentação do projeto	<ul style="list-style-type: none"> <li>• Procedimento <i>Elaborar plano de gestão de riscos</i></li> <li>• Documento de orientação – Técnicas de identificação dos riscos</li> </ul>
	Revisar as informações históricas	<ul style="list-style-type: none"> <li>• Elaborar plano de gestão de riscos</li> <li>• Documento de orientação – Técnicas de identificação dos riscos</li> </ul>
Estabelecer o contexto dos riscos	Detectar as circunstâncias ou condições do risco	<ul style="list-style-type: none"> <li>• Procedimento <i>Identificar riscos</i></li> </ul>
	Identificar possíveis conseqüências do risco	<ul style="list-style-type: none"> <li>• Procedimento <i>Identificar riscos</i></li> </ul>

A Tabela 5.3 apresenta o mapeamento da macroatividade *Analisar riscos* do processo proposto, com os artefatos que implementam na organização a atividade *Analisar riscos* do processo especializado.

**Tabela 5.3 – Macroatividade *Analisar riscos***

Processo Proposto		Processo Especializado
Atividade	Passo	
Categorizar os riscos	Agrupar os riscos de acordo com as categorias	<ul style="list-style-type: none"> <li>• Procedimento <i>Identificar riscos</i></li> </ul>
Avaliar impacto e probabilidade	Avaliar o impacto dos riscos	<ul style="list-style-type: none"> <li>• Procedimento <i>analisar riscos</i></li> </ul>
	Avaliar a probabilidade de ocorrência dos riscos	<ul style="list-style-type: none"> <li>• Procedimento <i>analisar riscos</i></li> </ul>
	Determinar a exposição ao risco	<ul style="list-style-type: none"> <li>• Procedimento <i>analisar riscos</i></li> </ul>
Priorizar riscos	Determinar a prioridade relativa dos riscos	<ul style="list-style-type: none"> <li>• Procedimento <i>analisar riscos</i></li> </ul>
Analisar riscos quantitativamente	Analisar os riscos quantitativamente	<ul style="list-style-type: none"> <li>• Atividade não realizada inicialmente</li> </ul>



A lista de riscos do projeto começa a ser elaborada na atividade *Identificar riscos*. Essa lista de riscos é implementada por meio de uma ferramenta de gestão de riscos utilizada na organização. Todas as informações referentes aos riscos do projeto geradas por meio da execução de referida atividade e das próximas estão registradas nessa ferramenta.

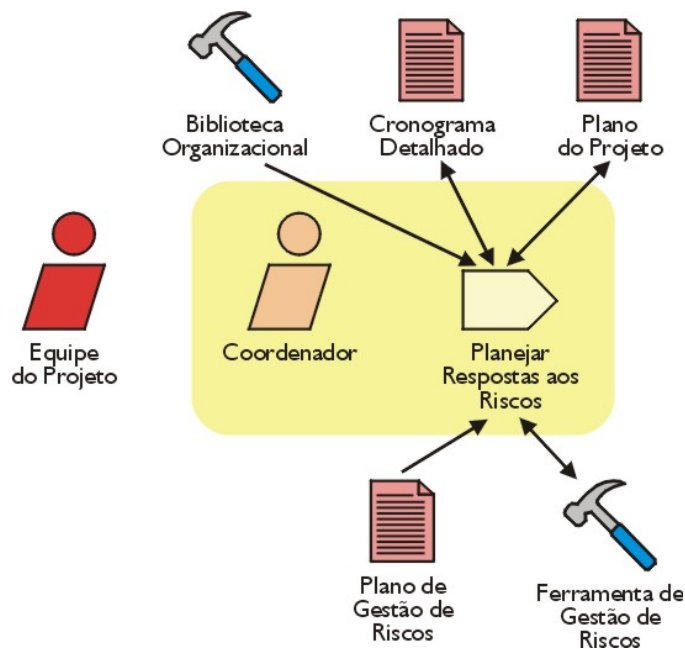
A atividade *Analisar riscos quantitativamente* não foi utilizada inicialmente na especialização do processo. Essa análise requer um grau de quantificação muito elevado, envolvendo análises estatísticas e simulações. Em alguns casos, não é possível ou é pouco prático, além de requerer mais tempo e recursos do que a análise qualitativa. A organização investirá nesse tipo de análise quando estiver preparando-se para o nível 4 (Gerenciado Quantitativamente) do CMMI, cujo processo deverá ser submetido a um controle quantitativo.

### **5.2.3 PLANEJAR RESPOSTAS AOS RISCOS**

A macroatividade *Planejar respostas aos riscos* do processo especializado (Figura 5.5) corresponde à macroatividade *Tratar riscos* do processo proposto.

A Tabela 5.4 contém o mapeamento da macroatividade *Tratar riscos* do processo proposto, com os artefatos que implementam na organização a macroatividade *Planejar respostas aos riscos*.

Deixou de ser utilizado apenas o passo *Selecionar estratégias para oportunidades*, da atividade *Selecionar estratégias* do processo proposto. A organização preferiu inicialmente não incluir esse passo, que envolve o conceito de risco positivo, uma vez que o CMMI (2002), foco principal da organização, não aborda essa questão.



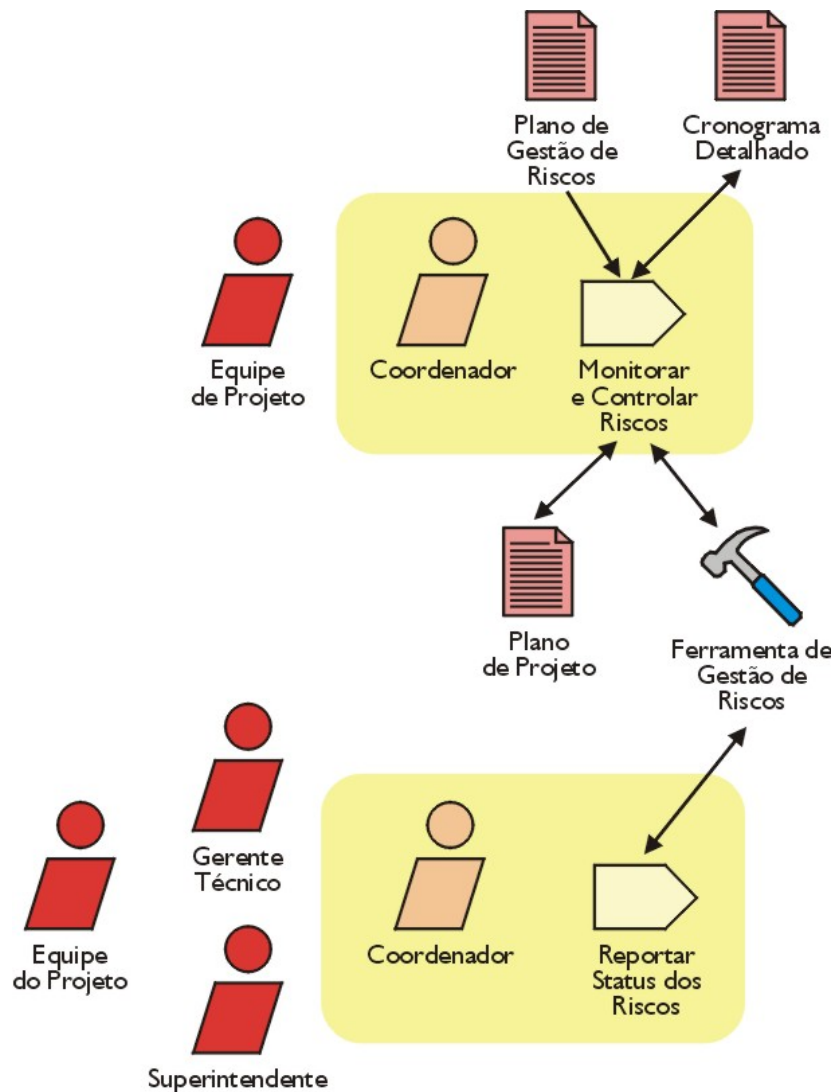
**Figura 5.5 – Planejar respostas aos riscos**

**Tabela 5.4 – Macroatividade *Tratar riscos***

Processo Proposto		Processo Especializado
Atividade	Passo	
Selecionar estratégias	Definir limites	• Procedimento <i>Planejar respostas aos riscos</i>
	Selecionar estratégias para ameaças	• Procedimento <i>Planejar respostas aos riscos</i>
	Selecionar estratégias para oportunidades	• Os riscos positivos não serão tratados inicialmente
	Selecionar riscos que serão aceitos	• Procedimento <i>Planejar respostas aos riscos</i>
Definir e selecionar respostas aos riscos	Definir ações de resposta aos riscos	• Procedimento <i>Planejar respostas aos riscos</i>
	Avaliar e selecionar as ações	• Procedimento <i>Planejar respostas aos riscos</i>
	Definir plano de contingências	• Procedimento <i>Planejar respostas aos riscos</i>
	Associar gatilhos aos riscos	• Procedimento <i>Planejar respostas aos riscos</i>
	Designar proprietários e envolvidos	• Procedimento <i>Planejar respostas aos riscos</i>

## 5.2.4 MONITORAR E CONTROLAR RISCOS

A macroatividade *Monitorar e controlar riscos* do processo especializado (Figura 5.6) corresponde à macroatividade de mesma denominação do processo proposto. Essa macroatividade é composta das atividades *Monitorar e controlar riscos* e *Reportar status dos riscos*.



**Figura 5.6 – Monitorar e controlar riscos**

A Tabela 5.5 contém o mapeamento da macroatividade *Monitorar e controlar riscos* do processo proposto com os artefatos que implementam na organização a macroatividade de mesma denominação.

**Tabela 5.5 – Macroatividade *Monitorar e controlar riscos***

Processo Proposto		Processo Especializado
Atividade	Passo	
Monitorar e controlar riscos	Acompanhar os estados atuais dos riscos	• Procedimento <i>Monitorar e controlar riscos</i>
	Executar plano de tratamento dos riscos	• Procedimento <i>Monitorar e controlar riscos</i>
	Acompanhar plano de tratamento dos riscos	• Procedimento <i>Monitorar e controlar riscos</i>
Reportar estados dos riscos	Revisar a documentação dos riscos	• Procedimento <i>Reportar estados dos riscos</i>
	Comunicar estados dos riscos	• Procedimento <i>Reportar estados dos riscos</i>

### 5.2.5 AVALIAR O PROCESSO DE GERENCIAMENTO DE RISCOS

A macroatividade *Avaliar o processo de gerenciamento de riscos* está integralmente implementada nos processos *Gestão de processos* e *Gestão de projetos* da organização, conforme demonstra a Tabela 5.6.

**Tabela 5.6 – Macroatividade *Avaliar o processo de gerenciamento de riscos***

Processo Proposto		Processo Especializado
Atividade	Passo	
Avaliar o processo	Capturar informações sobre o processo	Processo de gestão de processos
	Avaliar e melhorar o processo	Processo de gestão de processos
	Gerar lições aprendidas	Processo de gestão de projetos

### 5.3 IMPLANTAÇÃO DO PROCESSO DE GERENCIAMENTO DE RISCOS

A ferramenta de gestão de riscos utilizada na organização foi configurada de acordo com o processo de gerenciamento de riscos especializado. A *Lista de riscos* foi implementada nessa ferramenta, com inserção de informações explicativas referentes a cada um dos campos a serem preenchidos na execução das atividades de gerenciamento de riscos.

Em seguida, foi realizado um treinamento com gerentes de projetos e coordenadores, ocasião em que foi apresentado o processo e foram dadas as orientações necessárias à sua utilização.

Foram selecionados três projetos-piloto, nos quais foi realizado um acompanhamento supervisionado da utilização do processo. Nesses projetos, a equipe do EPG está monitorando diariamente a utilização do processo e fornecendo orientações para solução das não-conformidades identificadas.

Através do acompanhamento supervisionado foram identificadas as seguintes principais não-conformidades:

- a) fontes de riscos não identificadas;
- b) riscos não analisados;
- c) falta de indicação das estratégias apropriadas para responder aos riscos identificados;
- d) falta de identificação das ações de resposta aos riscos;
- e) falta de identificação dos gatilhos para os riscos; e
- f) falta de acompanhamento dos riscos.

A não-conformidade do item “a” foi sanada por meio da divulgação do documento contendo as fontes de riscos mais comuns da organização e da inserção dessas fontes na ferramenta. Inicialmente, essas fontes não haviam sido inseridas, ficando cada projeto livre para identificar suas próprias fontes de riscos. Atualmente, apenas novas fontes identificadas devem ser informadas no *Plano de gestão de riscos* e inseridas na ferramenta para utilização pelo projeto.

A não-conformidade do item “b” foi solucionada mediante revisão dos parâmetros utilizados para a análise dos riscos. Passou a ser adotada uma escala qualitativa, sendo elaborada a matriz de impacto e probabilidade. A solução para a não-conformidade do item “c” consistiu de uma explicação mais detalhada de cada uma das estratégias no procedimento.

Com relação às não-conformidades expressas nos itens “d”, “e” e “f”, foi dada uma maior ênfase à definição de ações para responder aos riscos e de gatilhos para viabilizar o acompanhamento dos riscos, assim como para sinalizar a necessidade de execução dessas

ações. Entretanto, essas dificuldades ainda persistiram nesses projetos-piloto e em outros projetos que iniciaram a utilização do processo. Foi então realizada uma reunião com gerentes de projeto e coordenadores, para discutir essas e outras questões.

Nessa reunião, chegou-se ao consenso de que a ferramenta para gestão de riscos utilizada não atendia às necessidades da organização no tocante ao acompanhamento dos riscos dos projetos e à coleta dos indicadores.

A ferramenta foi, então, substituída por outra que possibilitou a solução das dificuldades apresentadas nos itens “d”, “e” e “f” e a implementação das recomendações oriundas da avaliação classe C do método de avaliação SCAMPI, possibilitando a inclusão das seguintes facilidades:

- segregação das atividades de gestão de riscos<sup>3</sup>;
- possibilitar a inclusão de fontes e categorias para utilização no projeto específico;
- maior destaque às ações e seu acompanhamento;
- possibilitar o cadastro de vários gatilhos; e
- maior facilidade na coleta de indicadores.

A possibilidade de cadastrar vários gatilhos propicia uma melhor definição dos limites dos riscos e a utilização dos gatilhos para acompanhamento e definição de ações, e não apenas para a implementação de ações.

Como vantagens da adoção da nova ferramenta, pudemos observar, além da definição de ações, gatilhos e um acompanhamento mais efetivo dos riscos, uma maior motivação das equipes dos projetos para a realização das atividades de gerenciamento de riscos e a diminuição de retrabalho. Essa motivação deveu-se à facilidade de utilização e de sua interface mais amigável, assim como da conseqüente diminuição de retrabalho, decorrente da maior portabilidade dos dados.

---

<sup>3</sup> Na ferramenta anteriormente adotada, as informações resultantes da execução das atividades foram registradas sequencialmente em uma única visão, o que não impedia o necessário destaque à distinção existente entre elas.

Após a realização dos ajustes relativos às não-conformidades identificadas, outros oito projetos iniciaram a utilização do processo de gerência de riscos. Até o momento da elaboração deste trabalho, onze projetos já utilizavam o processo de gerenciamento de riscos especializado.

### **5.3.1 APLICAÇÃO DO PROCESSO EM PROJETOS**

Nas seções seguintes, apresenta-se a utilização do processo de gerenciamento de riscos em três projetos-piloto da organização, que, para se assegurar o necessário sigilo de suas informações, passam a denominar-se Projeto A, Projeto B e Projeto C.

Há também limitações com relação à divulgação das informações dos projetos. Assim sendo, parte das informações desses projetos foi descaracterizada para publicação neste trabalho, por respeito ao caráter de confidencialidade da organização. Atualmente, o processo vem sendo aplicado em onze projetos nessa organização, incluídos os três projetos-piloto.

#### **5.3.1.1 PROJETO A**

O Projeto A tem como objetivo o desenvolvimento de um sistema corporativo para a área financeira, utilizando a plataforma J2EE (*Java 2 Platform, Enterprise Edition*) e o ambiente de desenvolvimento Eclipse. O ciclo de vida utilizado nesse projeto é o iterativo-incremental, sendo o sistema modelado em UML (*Unified Modeling Language*).

Esse projeto é considerado de grande porte, devido ao esforço estimado de aproximadamente 50 mil homens/hora. A equipe alocada reúne cerca de trinta pessoas. O sistema tem como um dos principais requisitos a integração com sistemas legados.

Para esse projeto estão sendo apresentados o *Plano de gerenciamento de riscos* (Apêndice D) e o *Registro de riscos* (Apêndice E), em uma versão parcial. O *Registro de riscos*, na prática, está implementado em uma ferramenta de gestão de riscos da organização. Esse projeto foi selecionado para exemplificar a utilização dos *templates* propostos neste trabalho.

Os principais riscos do Projeto A estão relacionados a seguir. Desses riscos, os dois primeiros foram selecionados para serem detalhados (Apêndice E), sendo que um deles já foi eliminado, enquanto o outro permanece ativo.

- atraso na entrega da proposta e do contrato;
- problemas na integração;
- atraso na validação do documento de escopo;
- redesenho de processos;
- descontrole de componentes por projetos paralelos;
- retrabalho;
- atraso na indefinição do modelo único (efetivado);
- baixo reuso devido à falta de padrão nos casos de uso;
- solução para tratamento das regras de negócios não ser factível;
- mudanças nos requisitos;
- problemas com a utilização de diferentes ferramentas de análise e projeto; e
- problemas com a geração de relatórios.

### 5.3.1.2 PROJETO B

O Projeto B tem como objetivo o desenvolvimento de um sistema corporativo de controle de processos, em uma interface Web na plataforma J2EE (*Java 2 Platform, Enterprise Edition*), utilizando as tecnologias HTML, *Javascript*, *Struts Tiles*, *Servlets / JSP*, XML, JBoss, MSSQL e EJB (*Enterprise Java Beans*). O ciclo de vida utilizado nesse projeto é o iterativo-incremental, sendo o sistema modelado em UML.

Trata-se de projeto de grande porte, sendo o esforço estimado de aproximadamente 40 mil homens/hora. A equipe atualmente alocada reúne 24 pessoas.

O sistema possui como principais requisitos *possuir uma alta escalabilidade e a integração com vários outros sistemas*. Segue-se relação de alguns dos principais riscos identificados nesse projeto:

- dificuldade na definição de escopo;
- iniciar análise e *design*, sem se ter casos de uso aprovados;
- dificuldades na análise de impacto de mudanças;
- a aplicação não suportar a carga necessária para atender a todas as suas filiais;
- mudança de arquitetura não atende às necessidades do cliente; e
- adoção de novas tecnologias (*hibernate*, *spring*, novo *Process Flow*).



### 5.3.1.3 PROJETO C

O Projeto C tem como objetivo o desenvolvimento de um sistema corporativo para a indústria de telecomunicações, no ambiente Web, utilizando a plataforma J2SE (*Java 2 Platform, Standard Edition*) e as tecnologias HTML, *Javascript*, *Struts Tiles*, *Servlets / JSP*, XML, UML, *Hibernate*, *Spring*, SQL, *Tomcat*, MySQL, *Acege*. O projeto utiliza também o ciclo de vida iterativo-incremental, sendo o sistema modelado em UML.

Trata-se de projeto de grande porte, com um esforço estimado de aproximadamente 20 mil homens/hora. A equipe alocada reúne um total de 21 pessoas.

O sistema apresenta como principais requisitos a utilização de uma arquitetura facilmente adaptável, e que possa evoluir para uma solução completa, tolerância a falhas, e um ambiente escalável de alta disponibilidade.

Segue uma relação de alguns dos principais riscos identificados nesse projeto:

- falta de comunicação entre os membros da equipe;
- dificuldades no acompanhamento do projeto;
- escopo do projeto difícil de definir e priorizar;
- perda de patrocínio do projeto;
- perda de membros da equipe;
- equipe do projeto poder ser alocada fisicamente em laboratórios diferentes;
- utilização de novas tecnologias;
- falta de profissionais qualificados para completar a equipe;
- equipe desmotivada; e
- elevado número de clientes envolvidos.

### 5.4 IMPLANTAÇÃO DO PROCESSO NA ORGANIZAÇÃO X

O processo de gerenciamento de riscos proposto encontra-se na fase inicial de implantação, na unidade de desenvolvimento de *software* de uma segunda organização de grande porte, com sede em Fortaleza.

#### 5.4.1 CARACTERIZAÇÃO DA ORGANIZAÇÃO X

A organização possui cerca de duzentos profissionais que atuam na área de Tecnologia da Informação (TI), em projetos que atendem às necessidades das áreas de negócios da própria empresa, caracterizando-se a tecnologia como uma atividade-meio.

A organização possui mais de duzentos sistemas em produção. Atualmente, encontra-se em desenvolvimento mais de trinta novos sistemas, embora sua atividade principal seja a manutenção dos sistemas existentes. As principais plataformas utilizadas nessa organização são:

- IBM Mainframe: Cobol, VSAM, DB2, OS390.
- Intel: MS-Windows, Visual Basic, Powerbuilder, ASP, ASP.Net, C#, Delphi.
- plataforma J2EE (*Java 2 Platform, Enterprise Edition*).

Para a grande maioria dos sistemas em produção (legado), não há documentação adequada e organizada.

Recentemente a organização implantou um processo de *software* baseado no *framework* do RUP (*Rational Unified Process*). Esse processo é iterativo-incremental e utiliza as quatro fases do RUP, juntamente com suas nove disciplinas, modelando-se o sistema em UML.

A implantação desse processo objetivou minimizar problemas de não-atendimento ou mudanças de requisitos, assim como mapear adequadamente as necessidades de seus clientes (unidades de negócios) em casos de uso de sistema. Outro problema enfrentado pela organização reside na dificuldade da sua área de TI em conseguir entregar os produtos a seus clientes no prazo estabelecido.

Recentemente, a organização realizou uma auditoria de qualidade em dois projetos-piloto, desenvolvidos no processo de desenvolvimento recém-implantado, com o objetivo de identificar gargalos nesse processo. Essa auditoria identificou os seguintes problemas relacionados ao gerenciamento de riscos:

- A distribuição inicial das atividades no cronograma do projeto foi realizada sem se utilizar de maneira adequada a estratégia de divisão por fase, dificultando-se, assim, as ações do projeto de tratamento dos riscos.
- Houve dúvidas quanto à seqüência de passos a serem realizados para gestão do projeto, seguindo-se o processo implantado. As principais dúvidas estiveram relacionadas à distribuição das atividades do projeto ao longo das fases, à identificação dos riscos e ao planejamento das iterações e fases, seguindo-se o processo iterativo.
- A análise e tratamento de riscos foi um dos aspectos de maior dificuldade. A equipe do projeto consegue identificar alguns riscos, mas não consegue priorizá-los, nem definir uma adequada estratégia de tratamento, nem muito menos acompanhar esses riscos.

#### **5.4.2 ESTRATÉGIA DE IMPLANTAÇÃO DO PROCESSO NA ORGANIZAÇÃO X**

A organização não utiliza práticas de gerenciamento de riscos, como também não possui documentação confiável dos sistemas legados. Ela vai basear-se no processo de gerenciamento de riscos proposto para a implantação de suas atividades relacionadas a riscos. A implantação desse processo objetiva minimizar as dificuldades encontradas pelos projetos para gerenciar riscos e que geram impacto em todo o processo de desenvolvimento de *software*.

As informações sobre fontes, categorias, parâmetros e estratégias a serem utilizados nos projetos serão definidas com base na literatura e por meio de entrevistas com gerentes de projetos. A especialização do processo de gerenciamento de riscos encontra-se em sua fase inicial, de modo que ainda não há resultados conclusivos.

#### **5.5 CONCLUSÃO**

Este capítulo apresentou um estudo de caso com a aplicação do processo de gerenciamento de riscos proposto em duas organizações de *software*. O próximo capítulo apresenta a conclusão deste trabalho, suas contribuições e as perspectivas futuras.

## Capítulo 6

# CONCLUSÃO

---

*Neste capítulo são apresentadas as principais conclusões e as perspectivas que se descortinam como resultante e continuidade das pesquisas e análises reunidas neste trabalho.*

Um processo de gerenciamento de riscos formal é fundamental para um bem-sucedido gerenciamento de projetos de *software*, devido à complexidade desse tipo de projeto. Apesar dessa constatação, bastante reforçada na literatura, o gerenciamento de riscos ainda é pouco executado na prática, o que torna necessária a realização de novas pesquisas na área (RAZ et al, 2002).

Este trabalho analisou apuradamente alguns modelos, padrões e processos que tratam do gerenciamento de riscos – uns desenvolvidos para a indústria em geral e outros com foco em projetos de *software*. Essa análise teve como objetivo selecionar as melhores práticas de gerenciamento de riscos para serem aplicadas em projetos de *software*.

A partir dessa análise, foi proposto um processo de gerenciamento de riscos para projetos de software, compreendendo um fluxo principal com macroatividades, atividades e passos. Esse nível de detalhamento do processo trouxe facilidade para sua aplicação. Isso foi comprovado por meio da implantação desse processo em uma organização de *software* certificada CMM, nível 2 (Instituto Atlântico), com vistas a se institucionalizar sua área de processo de *Gerenciamento de riscos* (essa organização encontra-se em vias de ser certificada CMMI, nível 3).

A implantação do processo de gerenciamento de riscos no Instituto Atlântico trouxe como principal benefício o fato de as equipes dos projetos passarem a identificar riscos mais realistas, de modo a poder selecionar aqueles de maior impacto para o projeto. A partir daí, ficou mais fácil focar esses riscos e selecionar respostas apropriadas,

implementadas de acordo com a necessidade evidenciada por um acompanhamento efetivo. Essas ações conseguiram reduzir ou até eliminar a probabilidade de ocorrência ou impacto de alguns riscos.

À medida que se foram evidenciando os benefícios do gerenciamento dos riscos, essa atividade passou a ser exercida com mais entusiasmo, e não apenas como uma obrigação determinada pela necessidade de institucionalizar o processo para certificação CMMI, nível 3. Isso leva a inferir que o amadurecimento das equipes na utilização desse processo de gerenciamento de riscos, bem como a criação de uma base histórica de riscos, conduzirão à melhoria do próprio processo.

Como principais lições aprendidas na implantação do processo de gerenciamento de riscos proposto, destaca-se que:

- o processo de gerenciamento de riscos deve ser suportado por uma ferramenta de fácil manuseio, sob pena de criar resistência em seus usuários (gerentes e equipe dos projetos);
- a ferramenta de gerenciamento de riscos utilizada deverá também facilitar o acompanhamento dos riscos dos projetos;
- a criação dos ativos do processo de riscos revela-se altamente significativa para auxiliar na identificação, na análise, no tratamento e no acompanhamento dos riscos nos novos projetos; e
- o apoio da alta administração da organização é condição indispensável para a bem-sucedida implantação de um processo.

A aplicação do processo proposto por meio de um estudo de caso no Instituto Atlântico, em três projetos-piloto (até esta data onze projetos já o utilizam) demonstrou que o processo pode ser facilmente especializado, para utilização em outras organizações desenvolvedoras de *software*, especialmente naquelas cujo processo de desenvolvimento baseia-se no *Processo unificado* (RUP, 2003). Ficou patente também que o processo proposto atende às exigências da área de processo *Gerenciamento de riscos* do CMMI (2002).

Uma segunda aplicação teve início em uma organização com um processo de desenvolvimento de *software* imaturo, e que desenvolve *software* internamente, para

utilização em suas áreas de negócios. Isso tem o objetivo de comprovar que o processo proposto é aplicável também nesse tipo de organização. Nesse caso, ainda não há registro de resultados conclusivos.

## 6.1 CONTRIBUIÇÕES DESTE TRABALHO

O processo de gerenciamento de riscos para projetos de *software*, proposto neste trabalho, traz as seguintes principais contribuições:

- destacar a importância do gerenciamento de riscos para projetos de *software*, agregando-se em um só processo os fundamentos de modelos de riscos reconhecidos pela comunidade científica, e que são amplamente utilizados;
- formalizar um processo de gerenciamento de riscos para projetos de *software* em geral, sendo especialmente aderente ao ciclo de vida iterativo incremental, no qual se enquadra o *Processo unificado*;
- destacar a importância das categorias para a adequada priorização dos riscos;
- ensinar maior efetividade ao gerenciamento de riscos em projetos de *software*, resultando em um desenvolvimento de software com mais qualidade;
- fornecer um guia para a implantação da área de processo *Gerência de riscos* do CMMI, nível 3.
- enfatizar a importância dos *Ativos do processo organizacional* no gerenciamento de riscos para projetos específicos; e
- incorporar o conceito de riscos positivos ou oportunidades, assim como as estratégias para potencializar seus efeitos no projeto.

Como contribuições secundárias deste trabalho, destacam-se:

- mapeamento entre as atividades de gerenciamento de riscos do PMBOK (2004), CMMI (2002), RUP (2003), padrão IEEE STD 1540 (2001), e da AS/NZS 4360 (2004) (vide Capítulo 3);
- levantamento de avançadas técnicas recomendadas para o gerenciamento de riscos, cobrindo a identificação, a análise, a priorização, o planejamento de respostas e a monitoração e o controle (Anexo A); e

- criação de modelos de documentos de *Plano de gerenciamento de riscos* (Apêndice A) e *Registro de riscos* (Apêndice B).

## 6.2 PERSPECTIVAS FUTURAS

Este trabalho foi aplicado em uma organização, e apenas iniciado em outra, com características bastante distintas. Entretanto, ambas utilizam processos de desenvolvimento baseados no *Processo unificado*. É essencial a validação desse processo em outros contextos, como, por exemplo, em organizações que adotem outros processos de desenvolvimento. Outra aplicação interessante seria a especialização desse processo para pequenas e médias empresas.

Vislumbra-se o desenvolvimento de uma ferramenta para dar suporte ao processo de gerenciamento de riscos para projetos de *software* proposto. Uma característica desejável dessa ferramenta seria a facilidade de integração com outras ferramentas de apoio ao desenvolvimento, como, por exemplo, a ferramenta de gerenciamento de requisitos.

Defende-se, finalmente, a elaboração de uma base histórica que dê suporte às atividades de gerenciamento de riscos do Instituto Atlântico. Essa base histórica poderá facilitar a definição de parâmetros mais acurados para o gerenciamento de riscos e, de acordo com as categorias de riscos adotadas pela organização, a seleção de respostas aos riscos mais eficazes, assim como favorecer a própria melhoria desse processo.

## GLOSSÁRIO

Termo	Descrição/Objetivo
Ativos do processo organizacional (artefato)	Ativos relacionados aos processos da organização, compreendendo políticas, planos, procedimentos, diretrizes, processos definidos, métricas e bases de conhecimento como lições aprendidas e informações históricas
Categorias de riscos	Grupamentos organizados de riscos com forte correlação entre si e fraca correlação com riscos de outras categorias (KÄNSÄLÄ, 1997)
Especificação de requisitos de <i>software</i> (artefato)	Documento destinado a capturar e organizar todos os requisitos funcionais e não-funcionais que envolvem o projeto. Geralmente, os requisitos funcionais formam o detalhamento das características ( <i>features</i> ) do projeto (Documento de visão)
EAR	Estrutura analítica dos riscos / <i>Risk Breakdown Structure</i> (RBS)
EAP	Estrutura analítica do projeto / <i>Work Breakdown Structure</i> (WBS)
Fonte de riscos	Elemento que tem potencial intrínseco para gerar um problema para o projeto (HB 4360, 2004)
Métricas do projeto (repositório)	Local onde é armazenado um conjunto de métricas que devem contribuir para a avaliação da qualidade do projeto, informando seu andamento em um formato consistente ao longo de seu ciclo de vida
Plano de desenvolvimento de <i>software</i> (artefato)	Documento que reúne as informações necessárias ao gerenciamento do projeto. Descreve a abordagem dada ao desenvolvimento do <i>software</i> , sendo o plano de mais alto nível gerado e usado pelos gerentes para direcionar o esforço de desenvolvimento. Deve receber manutenção ao longo do projeto. Em algumas abordagens é denominado <i>Plano do projeto</i>
Plano de gerenciamento de riscos (artefato)	Documento que descreve como gerenciar os riscos associados ao projeto, detalhando as fontes e categorias de riscos, as estratégias de gerenciamento de riscos a serem utilizadas e a periodicidade de acompanhamento dos riscos. Esse plano pode ser incorporado ao <i>Plano de desenvolvimento de software</i>



Plano de Métricas	Caracteriza os vários tipos de métrica utilizados no projeto, compreendendo tipo, tamanho, complexidade e formalidade. As métricas devem ser adequadamente registradas, certificando-se de que haja detalhes suficientes para caracterizar o projeto com precisão
Programa	Um grupo de projetos relacionados, gerenciados de modo coordenado, para a obtenção de benefícios e controle que não estariam disponíveis se eles fossem gerenciados individualmente (PMBOK, 2004)
Registro de riscos (artefato)	Documento que descreve cada um dos riscos identificados, registrando seu impacto e probabilidade de ocorrência, indicadores e as ações a serem realizadas para tratar o risco, além de estabelecer o que deve ser feito no caso de sua ocorrência. Esses riscos devem ser dispostos em ordem decrescente de prioridade. Recomenda-se que esse artefato seja implementado em uma ferramenta
SWOT	Pontos fortes e fracos, oportunidades e ameaças / <i>Strengths, Weaknesses, Opportunities, and Threats</i> (PMBOK, 2004)
Visão (artefato)	Documento com a finalidade de coletar, analisar e definir necessidades e características de alto nível dos envolvidos e usuários-alvo do projeto

## REFERÊNCIAS BIBLIOGRÁFICAS

- AHERN, D. M. et al. CMMI distilled: a practical introduction to integrated process improvement. 2. ed. Set, 2003.
- AS/NZS 4360. “Australian/New Zealand Standard for Risk Management”, 2004.
- BARTIÉ, Alexandre. Garantia da qualidade de software. Rio de Janeiro: Ed. Campus, 2002.
- BRANCO, J. E. C.; BELCHIOR, A. D. Um modelo para avaliação da qualidade da gerência de projetos de software. Dissertação (Mestrado em Informática) – Universidade de Fortaleza, Fortaleza, 2001.
- Boehm, B. W. A spiral model of software development and enhancement. IEEE Software, v. 8, n. 1, p. 32-41, Jan, 1991.
- BOEHM B. W. IEEE tutorial on software risk management. New York: IEEE Computer Society Press, 1989.
- BOEHM, B. W. Software risk management: principles and practices. IEEE Software, v. 8, n. 1, p. 32-41, Jan, 1991.
- BOEHM, B. W.; PORT, D. Educating software engineering students to manage risk. In: INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING, IEEE, 2001.
- BROWN, N. Industrial-strength management strategie. IEEE, Jul, 1996.
- CHARETTE, R. N. Software engineering risk analysis and management. McGraw Hill, 1989.
- CHARETTE, R. N. Large-scale project management is risk management. IEEE Software, p. 110-117, Jul, 1996.
- MARVIN, J. Carr et al. Taxonomy-based risk identification. Technical Report, CMU/SEI-93-TR-6. Pittsburgh: Jun, 1993, 24p.
- CHRISSIS, Mary B.; KONRAD, Mike; SHRUM, Sandy. CMMI: guidelines for process integration and product improvement. SEI Series in Software Engineering, 2004.
- CMMI Product Team. “CMMI for Systems Engineering/Software Engineering”, Version 1.1 Staged Representation (CMU/SEI-2002-TR-029, ESC-TR-2002-029). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2002.

COSTA, H. R.; BARROS, M. O.; TRAVASSOS, G. H. Uma abordagem econômica baseada em riscos para avaliação de uma carteira de projetos de software. In: SIMPÓSIO BRASILEIRO DE ENGENHARIA DE SOFTWARE, Uberlândia. Out, 2005.

DINSMORE, P. et al. Como se tornar um profissional em gerenciamento de projetos. Rio de Janeiro: Qualitymark, 2003.

FARIAS, L. L. Planejamento de riscos em ambientes de desenvolvimento de software orientados à organização. 2002. Dissertação (Mestrado em Informática) – COPPE/UFRJ, Rio de Janeiro, Ago. 2002.

FUGGETTA, A. Software process: a roadmap. ACM 2000 1-58113-253-0/00/6.

FULLER, A.; CROLL, P.; Garcia, O. Why software engineering is riskier than ever. In: ASIA-PACIFIC CONFERENCE ON QUALITY SOFTWARE, 2001.

GUSMÃO, C. M. G.; MOURA, H. P. ISO, CMMI-SW and PMBOK risk management: a comparative analysis. The International Journal of Applied Management and Technology, v. 1, n. 1, 2003.

GUSMÃO, C. M. G.; MOURA, H. P. Gerência de riscos em processos de qualidade de software: uma análise comparativa. In: SIMPÓSIO BRASILEIRO DE QUALIDADE DE SOFTWARE, 2004.

HALL E. M. Managing risk: methods for software systems development. Addison-Wesley, 1998.

HAZAN, C.; LEITE, J. C. S. P. Indicadores para a gerência de requisito. In: WORKSHOP EM ENGENHARIA DE REQUISITOS, Piracicaba, 2003, p 285-301.

Risk Management Guidelines, Companion to AS/NZS 4360:2004, Standards Australia/Standards New Zealand, 2004.

HERBSLEB, James et al. Benefits of CMM-based software process improvement initial results. CMM/SEI-94-TR-13, Ago, 1994.

HUMPHREY, W. S. Managing the software process. Addison-Wesley, p. 9-17, 1990.

IEEE Std 1540. “Standard for Software Life Cycle Processes-Risk Management”. 2001

ISO/IEC 15504. “Software Process Assessment”, 2003.

JALOTE, P.; CMM in practice: processes for executing software projects at Infosys. Addison-Wesley, June, 2003.

JIANG, J. J.; KLEIN, G. Risks to different aspects of system success. *Information & Management*, n. 36, 1999, p. 263-272.

JONES, C. *Assessment and control of software risks*. Yourdon Press, 1994.

KÄNSÄLÄ, Kari. Integrating risk assessment with cost estimation. *IEEE Software*, v. 14, n. 3, p. 61-67, Mai/Jun, 1997.

KERZNER, K. *Gestão de projetos: as melhores práticas*. Bookman, 2002.

KROLL, Per; KRUCHTEN, Philippe. *The rational unified process made easy: a practitioner's guide to the RUP*. Pearson Education, 2003.

KRUCHTEN, P. From waterfall to iterative lifecycle: a tough transition for project managers. *Rational Software White Paper*, 2000.

KRUCHTEN, P. Agility with the RUP. *Cutter IT Journal*, v. 14, n. 12, Dez, 2001, p. 27-33.

KRUCHTEN, P. *The rational unified process: un introduction*. Addison-Wesley, 2003.

KULPA, Margaret K.; JOHNSON, Kent A. *Interpreting the CMMI: a process improvement approach*. CRC Press LLC, 2003.

KWAC, Y. H.; STODDARD, J. *Project risk management: lessons learned from software development*. Tecnovation, In Press, Corrected, 2003.

LEOPOLDINO, C. B. *Avaliação de riscos em desenvolvimento de software*. 2004. Dissertação (Mestrado em Informática) – Universidade Federal do Rio Grande do Sul, 2004.

LIMA, K. V. C. *Definição e construção de ambientes de desenvolvimento de software orientados a organização*. 2004. Tese (Doutorado em Informática) – COPPE/UFRJ, 2004.

MACHADO, C. A. F. *A-risk: Um método para identificar e quantificar risco de prazo de projetos de desenvolvimento de software*. Dissertação (Mestrado em Informática) – PUC, Curitiba, 2002.

MANZONI, L. V. *Uso de sistema de gerência de workflow para apoiar o desenvolvimento de software baseado no processo unificado racional estendido para alcançar níveis 2 e 3 do modelo de maturidade*. Porto Alegre: UFRGS, 2001.

MANZONI, L. V.; PRICE, R. T. Identifying extensions required by RUP (rational unified process) to comply with CMM (capability maturity model) levels 2 and 3. *IEEE Transactions on Software Engineering*, v. 29, n. 2, Fev. 2003.

MACHADO, C. A. F.; ROCHA, A. R. C. MPS.BR: melhoria de processo do software brasileiro. Guia Geral Versão 1.1. Softttx, Mai, 2006.

MUTAFELIJA, B. STROMBERG, H. W. S. Systematic process improvement using ISO 9001:2000 and CMMI. Artech House computing library, 2003.

OSMUNDSON, J. S. et al. Quality management metrics for software development. Information & Management, v. 40, n. 8, p. 799-812, 2003.

PFLEEGER, S. L.; HATIB, L. H. Risk management, project success, and technological uncertainty. R & D Management. Oxford, v. 32, n. 2, p. 101-109, 2002.

PINHO, V. D. M.; NETO, M. G. M. Análise do tratamento de riscos em projetos de desenvolvimento de software de uma organização. In: SIMPÓSIO BRASILEIRO DE ENGENHARIA DE SOFTWARE, Uberlândia, 2005.

PMBOK. A guide to the project management body of knowledge. 3. ed.. Philadelphia: PMI Publishing Division, 2004.

PMBOK. A guide to the project management body of knowledge. Pennsylvania: PMI Project Management Institute, 2000.

PMBOK A guide to the project management body of knowledge. North Carolina: PMI Standard Committee, PMI Publishing Division, 1996.

PRIKLADNICKI, R. et al. Um caso prático de implantação da gerência de risco em ambientes de desenvolvimento distribuído de software, baseado no modelo CMMI. In: SIMPÓSIO BRASILEIRO DE QUALIDADE DE SOFTWARE, 2005.

PROBASCO, L. The ten essentials of rup the essence of an effective development process. Rational Software Corporation, 2000.

RAZ, T.; SHENHAR, A. J.; DVIR, D. Risk management, project success, and technological uncertainty. R & D Management. v. 32, n. 2, p. 101-109, Oxford, 2002.

REINEHR, S. S. et al. Implementing ISO/IEC 12207 standard using rational unified process. Software Engineering Research and Practice, 2003.

ROCHA, A. R. C. et al. Qualidade de software. São Paulo: Prentice Hall, 2001.

ROCHA, P. C. Mapeamento do gerenciamento de riscos no PMBOK, CMMI-SW e RUP. In: SIMPÓSIO INTERNACIONAL DE MELHORIA DE PROCESSO DE SOFTWARE, 2004.

ROPPONEN, J.; LYYTINEN, K. Components of software development risk: how to address them? a project management survey. IEEE Transactions on Software Engineering, Fev. 2000, v. 26, n. 2, p. 98-112.

RUP. “Rational Unified Process®”, Version 2003.06.00.65, CD-ROM. Rational Software Corporation, Cupertino, Califórnia, 2003.

SANTANDER, V.; VASCONCELOS, A. M. L. Mapeando o processo unificado em relação ao CMM, nível 2. In: Conferência Internacional de Tecnologia de Software: Qualidade de Software, Curitiba, 2000.

SECRETARIA DE PLANEJAMENTO EM INFORMÁTICA, MINISTÉRIO DA CIÊNCIA E TECNOLOGIA. Relatório preliminar da qualidade e produtividade de software. Brasília. Disponível em: <<http://www.mct.gov.br>>. Acesso em: 21/05/2005.

SOMMERVILLE, Ian. Engenharia de software. 7. ed. São Paulo: Addison Wesley, 2003.

VALERIANO, D. Moderno gerenciamento de projetos. São Paulo: Prentice Hall, 2005.

WEBSTER, K. P. B.; OLIVEIRA, K. M.; ANQUETIL, N. Taxonomia de riscos para manutenção de software. In: SIMPÓSIO BRASILEIRO DE QUALIDADE DE SOFTWARE, 2005.

**ANEXO  
E  
APÊNDICES**

## ANEXO A

# TÉCNICAS DE IDENTIFICAÇÃO DE RISCOS

## 1 INTRODUÇÃO

Este documento apresenta algumas técnicas utilizadas na identificação de riscos em projetos de desenvolvimento de *software*, baseados no CMMI (2002), no PMBOK (2003) e no IEEE Std 1540-2001 (2001).

## 2 IDENTIFICAÇÃO DE RISCOS

### 2.1 *Brainstorming*

A meta do *brainstorming* é obter uma lista abrangente de riscos do projeto. A equipe do projeto pode utilizar essa técnica com um grupo contendo especialistas, que não fazem parte da equipe do projeto. Idéias sobre riscos do projeto são geradas sob a liderança de um facilitador. As categorias de riscos podem ser utilizadas como referência. Em seguida, é feito um agrupamento dos riscos semelhantes e um refinamento nas suas definições.

### 2.2 Entrevistas

As entrevistas com participantes experientes do projeto, *stakeholders* e especialistas no assunto podem ser úteis na identificação dos riscos, e constituem uma importante fonte de coleta de informações sobre identificação de riscos.

A entrevista tem como primeiro passo a identificação dos entrevistados e a preparação da agenda e das perguntas a serem feitas. Após esses preparativos, as entrevistas são conduzidas a partir das perguntas preparadas pelo entrevistador.

Uma das vantagens dessa técnica é a obtenção de diversas visões dos riscos, pois os entrevistados podem possuir perfis diferentes, contribuindo assim para a identificação de diversos aspectos relacionados aos riscos. É de fácil aplicação. Dentre as desvantagens, destaca-se a necessidade de o entrevistador definir as perguntas de modo a não limitar a entrevista. Essa técnica é fortemente dependente do entrevistado e do entrevistador.



### 2.3 Lista de verificação (*Checklist*)

Nessa técnica, os *stakeholders* utilizam listas prontas na identificação dos riscos. O *checklist* pode ser desenvolvido com base nas informações históricas acumuladas de projetos anteriores, devendo adequar-se à realidade da organização.

Uma das vantagens de se usar um *checklist* é que a identificação dos riscos pode tornar-se rápida e simples. Dentre as desvantagens dessa técnica, destaca-se a impossibilidade de montagem de um *checklist* completo de todos os riscos e de a equipe envolvida na identificação limitar-se à identificação nas categorias e nas fontes de riscos listados. Uma alternativa a isso é combinar a utilização dessa com outras técnicas de identificação, explorando-se, assim, os riscos que não aparecem no *checklist*-padrão.

### 2.4 Técnica Delphi

A técnica Delphi tem como objetivo obter um consenso de especialistas em relação a determinado assunto, como, por exemplo, riscos. Especialistas em riscos devem fazer parte da equipe, mas com participação anônima. Um facilitador utiliza um questionário para solicitar idéias sobre riscos importantes. As respostas são apresentadas, e circulam para inserção de comentários adicionais. Quando se utiliza essa técnica, o consenso quanto aos principais riscos pode ser atingido em poucas rodadas.

Dentre as vantagens, ressalta-se que essa técnica pode ajudar a reduzir desvios nos dados, e mantém o equilíbrio de influência dos participantes, pois estes não são identificados. Como desvantagem, figura a dependência em relação ao questionário elaborado pelo facilitador, e que pode limitar o intercâmbio de idéias.

Uma consolidação das opiniões deverá ser formalizada. Assim sendo, o planejamento do projeto poderá ter início. O objetivo final é uma consolidação do julgamento intuitivo do grupo de especialistas.

### 2.5 Análise SWOT

O termo SWOT vem do inglês, e é formado pelas iniciais das palavras *Strength* (força), *Weakness* (fraqueza), *Opportunities* (oportunidades) e *Threats* (ameaças). A idéia central dessa técnica é justamente avaliar os pontos fortes, os pontos fracos, as oportunidades e as ameaças da organização ou do projeto. No gerenciamento de riscos, isso pode ser utilizado para aumentar a amplitude dos riscos considerados.

## **2.6 Diagramas de causa e efeito**

Esses diagramas são também conhecidos como Diagrama de Ishikawa ou Espinha de Peixe. Podem ser utilizados no gerenciamento de riscos, para identificar as causas dos riscos, com vistas a eliminá-las, evitando-se, assim, o surgimento de novos riscos.

## **APÊNDICE A**

### **PROCEDIMENTO PARA A GESTÃO DE RISCOS**

**REVISÃO HISTÓRICA**

<b>Data</b>	<b>Versão</b>	<b>Descrição</b>	<b>Autor</b>
02/11/2005	V 1.0	Elaboração deste procedimento	Pascale Correia

## ÍNDICE

1	INTRODUÇÃO .....	197
1.1	Finalidade.....	197
2	PROCESSO DE GESTÃO DE RISCOS.....	197
2.1	Planejar Gestão de Riscos .....	197
2.1.1	Determinar as fontes de riscos.....	197
2.1.2	Determinar as categorias de riscos.....	198
2.1.3	Definir estratégias de gestão de riscos.....	198
2.2	Identificar e Analisar Riscos.....	199
2.2.1	Identificar riscos .....	199
2.2.2	Analisar riscos .....	200
2.3	Planejar Respostas aos Riscos.....	201
2.3.1	Selecionar estratégias .....	201
2.3.2	Planejar respostas aos riscos.....	202
2.4	Monitorar e Controlar Riscos.....	203
2.4.1	Monitorar riscos.....	204
2.4.2	Executar planos de respostas aos riscos.....	204
2.4.3	Acompanhar as respostas aos riscos.....	204
2.4.4	Reportar <i>status</i> dos riscos .....	205

## 1 INTRODUÇÃO

### 1.1 Finalidade

O propósito deste procedimento é fornecer diretrizes para a execução das atividades de gerenciamento de riscos. Apresenta o processo de gestão de riscos, envolvendo as etapas de planejamento do gerenciamento de riscos, identificação, análise, tratamento e acompanhamento dos riscos do projeto.

## 2 PROCESSO DE GESTÃO DE RISCOS

O objetivo deste processo é viabilizar a identificação de riscos antes de sua concretização, para que as atividades relacionadas aos riscos possam ser planejadas e executadas quando necessário, durante o ciclo de vida do projeto, para eliminar ou minimizar a probabilidade de sua ocorrência e os impactos adversos ao alcance dos objetivos.

O processo de gestão de riscos compõe-se das seguintes macroatividades: (i) Planejar Gestão de Riscos; (ii) Identificar e Analisar Riscos; (iii) Planejar Respostas aos Riscos; e (iv) Monitorar e Controlar Riscos.

### 2.1 Planejar Gestão de Riscos

Essa macroatividade compõe-se da atividade Elaborar o Plano de Gestão de Riscos, que reúne as informações necessárias para a gestão de riscos no projeto. Esse plano deve ser criado no início do projeto, e atualizado a cada iteração, ou sempre que necessário.

O Plano de Gestão de Riscos deve contemplar as seguintes ações: (i) Determinar as fontes de riscos; (ii) Determinar as categorias de riscos; e (iii) Definir estratégias de gestão de riscos.

#### 2.1.1 Determinar as fontes de riscos

Significa identificar as fontes internas e externas de riscos, objetivando a identificação antecipada dos riscos. As fontes de riscos podem causar riscos em um projeto ou em uma organização, e mostram as áreas comuns onde os riscos podem originar-se. Dentre os tipos de fontes típicas de riscos, destacam-se:

- alta rotatividade de pessoal;
- equipe com habilidades inadequadas;
- estimativas de cronograma ou alocação de recursos não realistas;
- requisitos instáveis;

- restrições e premissas; e
- tecnologia não disponível.

### 2.1.2 Determinar as categorias de riscos

As categorias de riscos são grupamentos organizados de riscos que apresentam forte correlação, provendo uma estrutura que possibilita a identificação sistemática dos riscos com qualidade e efetividade. A categorização pode revelar fontes comuns de riscos ou áreas do projeto que requerem atenção especial. A descoberta de áreas de concentração de riscos pode aumentar a eficácia das respostas aos riscos.

Deve-se procurar descobrir quais categorias de riscos são mais importantes para o projeto, de acordo com seus objetivos, e levando-se em conta a tolerância do cliente ao risco. Cita-se aqui, como exemplo, a categorização proposta pelo SEI (CARR et al, 1993):

- **Engenharia do Produto**
  - Requisitos;
  - Projeto;
  - Codificação e Teste Unitário;
  - Teste e Integração;
  - Especialidades de Engenharia.
- **Ambiente de Desenvolvimento**
  - Processo de Desenvolvimento;
  - Sistema de Desenvolvimento;
  - Processo de Gerenciamento;
  - Métodos Gerenciais;
  - Ambiente de Trabalho.
- **Restrições de Programa**
  - Recursos;
  - Contrato;
  - Interfaces do Projeto.

### 2.1.3 Definir estratégias de gestão de riscos

Os riscos do projeto deverão ser acompanhados, no mínimo, nas reuniões técnicas, gerenciais e estratégicas, de acordo com suas características, ou em outras, definidas pelo coordenador do projeto.

As técnicas recomendadas para identificação de riscos são descritas no documento *Técnicas de identificação de riscos* (Anexo A).

As estratégias indicadas para o planejamento das respostas aos riscos devem ser detalhadas, como, por exemplo: *Que reuniões específicas podem ocorrer? Quais os envolvidos com o risco e sua atuação? Como um resultado poderá ser acompanhado a partir de um gatilho? Como uma ação deve ser avaliada para se verificar se ela atingiu seu objetivo?*

As estratégias indicadas para o planejamento das respostas aos riscos são:

- *Aceitar*: aceitar a probabilidade, o impacto e as conseqüências de um risco;
- *Mitigar*: reduzir a probabilidade e/ou o impacto de um risco;
- *Transferir*: transferir o risco para terceiros;
- *Evitar*: eliminar totalmente a probabilidade de ocorrência do risco.

## 2.2 Identificar e Analisar Riscos

Essa macroatividade compõe-se de duas atividades: (i) Identificar riscos; e (ii) Analisar riscos.

### 2.2.1 Identificar riscos

Significa identificar os riscos que possam afetar o projeto, de acordo com as fontes e categorias definidas, utilizando-se as Técnicas de identificação de riscos (Apêndice A). Documentos como *Estimativas de Projeto*, *Cronograma Detalhado*, e *Proposta Técnica*, além da base histórica de riscos, são fontes essenciais para a identificação dos riscos.

Para se estabelecer o contexto de cada risco, torna-se necessário registrar as seguintes informações:

- *Identificador*: código identificador do risco.
- *Descrição*: descrição do risco.
- *Data*: data de identificação do risco.
- *Responsável*: designação do responsável para acompanhar o risco identificado.
- *Técnica*: técnica utilizada para a identificação do risco.
- *Fonte*: identificação da fonte do risco.
- *Categoria*: identificação da categoria do risco.



- *Tipo*: indicar se o risco tem origem interna ou externa.
- *Causas*: verificação das possíveis causas dos riscos.
- *Conseqüências*: identificação das possíveis conseqüências do risco para os objetivos do projeto.

### 2.2.2 Analisar riscos

Significa analisar os riscos identificados, segundo os seguintes itens:

- *Impacto*: avalia o impacto do risco para os objetivos do projeto, tais como tempo, custo, escopo e qualidade. Pode ser usada a seguinte classificação:
  - Muito alto
  - Alto
  - Médio
  - Baixo
  - Muito baixo
- *Probabilidade*: calcula a probabilidade de ocorrência do risco identificado. Pode ser usada a seguinte classificação:
  - Muito alta
  - Alta
  - Média
  - Baixa
  - Muito baixa
- *Exposição*: obtida através da multiplicação do impacto pela probabilidade de ocorrência. A exposição ao risco pode ser classificada como baixa, média ou alta, de acordo com a matriz de probabilidade e impacto apresentada no quadro abaixo. As zonas sombreadas apresentam a seguinte classificação: cinza escuro – alto risco; cinza médio – baixo risco; e cinza claro – risco médio.

Os riscos devem ser priorizados através da sua ordenação de acordo com os resultados obtidos no cálculo da exposição ao risco e de sua classificação, para em seguida definir-se a estratégia de tratamento para cada risco. O objetivo da priorização é determinar as áreas nas quais os recursos para tratamento dos riscos podem ser aplicados com maior impacto positivo para o projeto.

## Quadro – Matriz de Probabilidade e Impacto

PROBABILIDADE		IMPACTO				
		Muito Baixo	Baixo	Médio	Alto	Muito Alto
		0,05	0,10	0,20	0,40	0,80
Muito Alta	0,90	0,05	0,09	0,18	0,36	0,72
Alta	0,70	0,04	0,07	0,14	0,28	0,56
Média	0,50	0,03	0,05	0,10	0,20	0,40
Baixa	0,30	0,02	0,03	0,06	0,12	0,24
Muito Baixa	0,10	0,01	0,01	0,02	0,04	0,08

## Legenda:

■ Alta    ■ Média    ■ Baixa

## 2.3 Planejar Respostas aos Riscos

Significa selecionar a estratégia ou combinação de estratégias mais apropriada para responder aos riscos e definir as ações a serem implementadas no projeto.

## 2.3.1 Selecionar estratégias

Para cada risco, selecionar a estratégia ou associação de estratégias com maior probabilidade de eficácia, considerando-se a sua prioridade. As estratégias devem ser definidas com base na tabela e indicações apresentadas abaixo:

Estratégia	Exposição		
	Baixa	Média	Alta
Aceitar	X	X	
Mitigar		X	X
Transferir	X		
Evitar		X	X

Adicionalmente, devem ser observados os seguintes critérios com vistas à seleção dos riscos para tratamento:

- selecionar todos os riscos com severidade (exposição) *alta*;
- selecionar riscos com severidade *média*, que sejam relevantes em função das características do projeto;

- não selecionar riscos com severidade *baixa*, a menos que haja um motivo explícito para isso. Entretanto, esses riscos devem ser acompanhados, porque sua severidade pode tornar-se maior ao longo do projeto.

É necessário planejar ações para lidar com as ameaças, ou riscos não aceitos (se ocorrerem, poderão causar grandes impactos negativos para o projeto). Para esses riscos, são selecionadas as seguintes estratégias:

- **Aceitar:** a aceitação de um risco pode ser ativa ou passiva. No caso da aceitação Ativa, faz-se necessário planejar ações (contingência). Para a aceitação Passiva, torna-se necessário documentar essa aceitação sem o planejamento de ações.
- **Evitar:** modifica-se com o Plano do Projeto, para eliminar a ameaça apresentada por um risco, no sentido de isolar os objetivos do projeto do impacto do risco, ou para flexibilizar o objetivo ameaçado. As ações selecionadas devem ser refletidas no cronograma do projeto. São exemplos de estratégias para evitar riscos:
  - reduzir o escopo;
  - alterar requisitos, ou torná-los mais claros;
  - evitar abordagens ou situações desconhecidas;
  - especializar-se; e
  - melhorar a comunicação.
- **Transferir:** passar para terceiros o impacto negativo de uma ameaça, juntamente com a responsabilidade pela resposta ao risco, embora sem eliminá-lo. A partir dessa estratégia, pode-se alterar o cronograma do projeto.
- **Mitigar:** identificar as ações a ser previamente implementadas, para reduzir a probabilidade de ocorrência do risco, ou seu impacto no projeto, até um limite aceitável. São exemplos de estratégias de mitigação de riscos:
  - conduzir testes ou estudos de viabilidade;
  - estender o cronograma;
  - projetar redundância no sistema; e
  - adicionar recursos.

### 2.3.2 Planejar respostas aos riscos

Planejar e selecionar as ações de resposta aos riscos identificados, de acordo com a estratégia selecionada e com base no contexto e nas fronteiras do risco no projeto. Para cada risco, definem-se os seguintes itens:

- **Gatilhos para o risco:** definir gatilhos para implementação de ações para os riscos de exposição *alta* e, opcionalmente, para riscos de exposição *média*. Para os riscos de exposição *baixa* não há necessidade de identificar limites. Os gatilhos indicam que o risco ocorreu ou é iminente, e serão utilizados para provocar o acionamento ou a definição de ações. O gatilho deve corresponder a uma condição mensurável e passível de acompanhamento. A identificação de gatilhos para os riscos nem sempre é possível, devendo, nessa hipótese, deixar registro. São exemplos de gatilhos de riscos:
  - *Estabilidade de Requisitos:* se a volatilidade dos requisitos ultrapassar os 30%.
  - *Requisito não Funcional de Desempenho:* em um teste de protótipo ou simulado, se o tempo de resposta for superior a 90% do previsto.
  - *Prazo:* quando o impacto no caminho crítico for superior a uma semana.
  - *Custo:* se a projeção do custo for superior a 50% da reserva de gerenciamento.
- **Envolvidos:** descrever outros direta ou indiretamente envolvidos no gerenciamento do risco.
- **Estado do Risco:** estado atual do risco.
- **Ação:** planejar ações de acordo com a estratégia selecionada para tratamento dos riscos, baseado no contexto e nos limites do risco no projeto, por meio de um *Plano de contingências*, não considerando aqueles de estratégia de aceitação passiva. As ações devem ser registradas indicando as seguintes informações:
  - *Tipo da Ação:* se é uma ação de mitigação, contingência, transferência ou eliminação.
  - *Gatilho:* apresentar o gatilho que dispara essa ação.
  - *Responsável:* designar o responsável pela execução das ações correspondentes às respostas selecionadas.
  - *Data de Início:* exibir a data em que a ação foi iniciada.
  - *Prazo:* mostrar a data de conclusão da ação.
  - *Estado da Ação:* indicar se a ação foi iniciada, concluída ou cancelada.

## 2.4 Monitorar e Controlar Riscos

Significa acompanhar os riscos durante o projeto, executar ações de resposta aos riscos segundo suas necessidades e acompanhá-las na periodicidade definida no *Plano de gestão de riscos*, ou sempre que for necessário. Essa macroatividade compreende: monitorar riscos,

executar planos de respostas aos riscos, acompanhar as respostas aos riscos e reportar *status* dos riscos.

#### 2.4.1 Monitorar riscos

Os riscos identificados durante o processo de gestão de riscos devem ser periodicamente revisados, como especificado no *Plano de gestão de riscos*, no contexto do estado atual e das circunstâncias do projeto. Para a monitoração dos riscos, deve ser considerada sua prioridade. Entretanto, mesmo os riscos de *baixa* severidade devem ser monitorados, uma vez que esse nível pode elevar-se ao longo do projeto.

Situações nas quais os riscos devem ser revisados:

- quando são identificados novos riscos;
- quando o risco torna-se um problema;
- quando o risco deixa de existir;
- quando as circunstâncias do projeto mudam de forma significativa.

Os gatilhos dos riscos devem ser acompanhados, para identificar a necessidade de execução das respostas aos riscos, incluindo o plano de contingências, ou a implementação de novas ações. Os registros das alterações identificadas para cada risco devem ser permanentemente atualizados.

#### 2.4.2 Executar planos de respostas aos riscos

Consiste em providenciar a execução das ações previstas para a implementação da estratégia de resposta aos riscos selecionada. Quando o gatilho para o risco for disparado, deve-se executar o plano de contingências; e quando o gatilho para a ação for disparado, cabe executar a ação correspondente.

#### 2.4.3 Acompanhar as respostas aos riscos

Significa acompanhar a execução das ações de resposta aos riscos, avaliando-se sua efetividade. Se as respostas aos riscos executadas não produzirem o resultado esperado, o motivo deve ser identificado, e novas ações devem ser adotadas no sentido de solucionar o problema.

O principal responsável pelo acompanhamento das ações de resposta é o responsável pelo risco. Ele deve verificar se as ações estão sendo implementadas pelo responsável pela ação. Deve, ainda, reportar a situação ao coordenador do projeto sempre que ocorrer algum problema na execução da ação ou em sua efetividade.

#### 2.4.4 Reportar *status* dos riscos

Compreende atualizar e comunicar o *status* dos riscos aos envolvidos do projeto, e envolve documentar o *status* dos riscos e comunicar o *status* dos riscos.

Cabe, portanto, documentar o estado atual dos riscos do projeto, através da revisão da documentação dos riscos, logo que novas informações tornarem-se disponíveis, para incorporar mudanças e garantir que os riscos sejam devidamente registrados e atualizados. Deve-se observar se:

- o *status* do risco está atualizado;
- foram incluídos novos riscos identificados;
- foram registradas mudanças de probabilidade e impacto;
- riscos estão devidamente ordenados pela prioridade;
- planos de respostas foram corretamente atualizados.

Comunicar os estados dos riscos, com o objetivo de fornecer a visibilidade dos riscos do projeto e do estado dos esforços de mitigação. Os principais riscos devem ser visíveis a todos os participantes do projeto, bem como as ações implementadas sobre eles.

A comunicação é fundamental durante todo o processo, para garantir que as pessoas responsáveis por implementar a gestão de riscos, e também as interessadas no projeto, entendam as bases nas quais as decisões estão sendo tomadas, e o porquê da execução de determinadas ações.

## APÊNDICE B

### PLANO DE GERENCIAMENTO DE RISCOS

<*Nome do Projeto*>

Versão <*x.y*>

**REVISÃO HISTÓRICA**

<b>Data</b>	<b>Versão</b>	<b>Descrição</b>	<b>Autor</b>
<dd/mm/aaaa>	<x.y>	<descrição>	<nome>



## CONTEÚDO

<b>1. Introdução</b>	<b>209</b>
1.1 Finalidade	209
1.2 Escopo	209
1.3 Definições, Acrônimos e Abreviações	209
1.4 Referências	209
<b>2. Fontes e Categorias de Riscos</b>	<b>209</b>
2.1 Fontes de Riscos	209
2.2 Categorias de Riscos	209
<b>3. Parâmetros para o Gerenciamento de Riscos</b>	<b>209</b>
3.1 Critérios para a Análise dos Riscos	209
3.2 Critérios para o Tratamento dos Riscos	209
3.3 Métricas	209
3.4 Limites para cada Categoria de Riscos	209
3.5 Indicadores para Avaliação do Processo	209
<b>4. Estratégias para o Gerenciamento de Riscos</b>	<b>209</b>
4.1 Processo Adaptado	209
4.2 Metodologia	210
4.3 Papéis e Responsabilidades	210
4.4 Periodicidade	210
4.5 Plano de Comunicação	210
4.6 Avaliação do Processo	210

## **Plano de Gerenciamento de Riscos**

### **1. Introdução**

#### **1.1 Finalidade**

*[Especifique a finalidade deste documento.]*

#### **1.2 Escopo**

*[Descreva brevemente o escopo deste documento.]*

#### **1.3 Definições, Acrônimos e Abreviações**

*[Apresente as definições dos termos, acrônimos e abreviações que são necessárias para a correta interpretação deste documento.]*

#### **1.4 Referências**

*[Referencie os documentos citados neste documento.]*

### **2. Fontes e Categorias de Riscos**

#### **2.1 Fontes de Riscos**

*[Descreva as fontes de riscos identificadas.]*

#### **2.2 Categorias de Riscos**

*[Descreva a categorização de riscos que será adotada no projeto.]*

### **3. Parâmetros para o Gerenciamento de Riscos**

#### **3.1 Critérios para a Análise dos Riscos**

*[Defina os critérios para avaliação, para definição dos níveis de probabilidade e impacto dos riscos, para o cálculo da exposição e para priorização dos riscos.]*

#### **3.2 Critérios para o Tratamento dos Riscos**

*[Estabeleça os critérios para o tratamento dos riscos, através de parâmetros a serem utilizados como indicativos para a seleção da estratégia a ser adotada.]*

#### **3.3 Métricas**

*[Defina as métricas que serão coletadas para utilização no processo de gerenciamento de riscos.]*

#### **3.4 Limites para cada Categoria de Riscos**

*[Selecione as métricas que poderão ser utilizadas como fronteiras para cada categoria de risco.]*

#### **3.5 Indicadores para Avaliação do Processo**

*[Estabeleça os indicadores a serem coletados para a avaliação do processo de gerenciamento de riscos.]*

### **4. Estratégias para o Gerenciamento de Riscos**

#### **4.1 Processo Adaptado**

*[Faça a adaptação do processo de acordo com as características e o contexto do projeto.]*

**4.2 Metodologia**

*[Defina abordagens, técnicas e ferramentas que serão utilizadas para o gerenciamento de riscos no projeto, contemplando, por exemplo:*

- *a técnica a ser utilizada para identificar riscos;*
- *as estratégias de tratamento de riscos que serão utilizadas;*
- *como serão monitorados o status de cada risco relevante e suas atividades de tratamento.]*

**4.3 Papéis e Responsabilidades**

*[Elabore uma lista de grupos e pessoas que estarão diretamente envolvidos nas atividades de gerenciamento de riscos do projeto e uma descrição das tarefas e responsabilidades de cada um.]*

**4.4 Periodicidade**

*[Determine a periodicidade para o acompanhamento dos riscos.]*

**4.5 Plano de Comunicação**

*[Desenvolva um plano de comunicação para os riscos do projeto, de acordo com as diretrizes estabelecidas pela organização, e levando em conta as características do projeto.]*

**4.6 Avaliação do Processo**

*[Estabeleça como será realizada a avaliação do processo de gerenciamento de riscos.]*

## APÊNDICE C

### REGISTRO DE RISCOS

<*Nome do Projeto*>

Versão <*x.y*>

## REVISÃO HISTÓRICA

Data	Versão	Descrição	Autor
<dd/mm/aaaa>	<x.y>	<detalhes>	<nome>

## CONTEÚDO

<b>1. Introdução</b>	<b>214</b>
1.1 Finalidade	214
1.2 Escopo	214
1.3 Definições, Acrônimos e Abreviações	214
1.4 Referências	214
<b>2. Riscos</b>	<b>214</b>
2.1 Identificação	214
2.1.1 Identificador e Descrição do Risco	214
2.1.2 Fonte	214
2.1.3 Contexto do Risco	214
2.2 Análise	214
2.2.1 Categoria	214
2.2.2 Probabilidade	214
2.2.3 Impactos	214
2.2.4 Exposição ao Risco	215
2.2.5 Priorização	215
2.2.6 Análise Quantitativa	215
2.3 Plano de Tratamento dos Riscos	215
2.3.1 Limites do Risco	215
2.3.2 Estratégias	215
2.3.3 Ações	215
2.3.3.1 Ações de Tratamento	215
2.3.3.2 Plano de Contingências	215
2.3.4 Gatilhos	215
2.3.5 Proprietário e Envolvidos	215
2.4 Monitoração e Controle	215
2.4.1 Estado Atual do Risco	215
2.4.2 Acompanhamento das Ações	215

<b>Registro de Riscos</b> <Nome do Projeto>	<b>Página:</b> 214
	<b>Data:</b> 11/10/2006 11:36 AM

# Registro de Riscos

## 1. Introdução

### 1.1 Finalidade

*[Especifique a finalidade deste documento.]*

### 1.2 Escopo

*[Descreva brevemente o escopo deste documento.]*

### 1.3 Definições, Acrônimos e Abreviações

*[Apresente as definições dos termos, acrônimos e abreviações que são necessárias para a correta interpretação deste documento. Caso não existam, incluir a frase “Não se aplica”.]*

### 1.4 Referências

*[Referencie os documentos citados neste documento.]*

## 2. Riscos

### 2.1 Identificação

*[Registre os riscos identificados e documente suas características, considerando para cada risco os itens abaixo.]*

#### 2.1.1 Identificador e Descrição do Risco

*[Crie um identificador e descreva brevemente o risco.]*

#### 2.1.2 Fonte

*[Liste os elementos que poderão originar o risco.]*

#### 2.1.3 Contexto do Risco

*[Documente as características e o contexto do risco. Nesta seção, descreva, por exemplo, o seguinte:*

- *Data: data em que o risco foi identificado;*
- *Técnica: técnica utilizada para a caracterização do risco;*
- *Causa: identificação de eventos que poderão causar o risco, e se este é externo ou interno;*
- *Conseqüências: levantar as possíveis conseqüências do risco para os objetivos do projeto;*
- *Nível: nível de decisão sobre o risco.]*

### 2.2 Análise

*[Registre a avaliação, categorização e priorização dos riscos, considerando para cada risco os itens abaixo.]*

#### 2.2.1 Categoria

*[Agrupar o risco de acordo com as categorias definidas.]*

#### 2.2.2 Probabilidade

*[Estime a probabilidade de ocorrência do risco.]*

#### 2.2.3 Impactos

*[Estime o impacto do risco nos objetivos do projeto.]*

<b>Registro de Riscos</b> <Nome do Projeto>	<b>Página:</b> 215
	<b>Data:</b> 11/10/2006 11:36 AM

#### 2.2.4 Exposição ao Risco

*[Calcule a severidade do risco, com base na probabilidade de ocorrência e no impacto.]*

#### 2.2.5 Priorização

*[Ordene os riscos de acordo com a exposição e os parâmetros definidos.]*

#### 2.2.6 Análise Quantitativa

*[Realize a análise quantitativa do risco, caso seja necessário.]*

### 2.3 Plano de Tratamento dos Riscos

*[Registre as estratégias de tratamento dos riscos, considerando, para cada risco, os itens abaixo.]*

#### 2.3.1 Limites do Risco

*[Descreva as fronteiras do risco, para melhor compreensão dos níveis de risco aceitos pelas partes envolvidas.]*

#### 2.3.2 Estratégias

*[Selecione a estratégia ou associação de estratégias que será adotada para tratar o risco:*

- *Estratégias para riscos negativos ou ameaças: evitar, transferir, mitigar.*
- *Estratégias para riscos positivos ou oportunidades: explorar, compartilhar, melhorar.*
- *Estratégia para ambos: aceitação (incluir o risco em uma Lista de Observação.)*

#### 2.3.3 Ações

##### 2.3.3.1 Ações de Tratamento

*[Liste as ações de resposta ao risco que foram definidas e selecionadas para o tratamento do risco, antes da sua ocorrência.]*

##### 2.3.3.2 Plano de Contingências

*[Descreva as ações que deverão ser executadas, se o risco efetivamente materializar-se.]*

#### 2.3.4 Gatilhos

*[Associe gatilhos aos riscos selecionados para tratamento. Esses gatilhos serão utilizados no acompanhamento dos riscos.]*

#### 2.3.5 Proprietário e Envolvidos

*[Designa o proprietário, o executor da ação de tratamento e os envolvidos no gerenciamento do risco.]*

### 2.4 Monitoração e Controle

*[Documente o acompanhamento do risco e de suas ações correspondentes, considerando, para cada risco, os itens abaixo.]*

#### 2.4.1 Estado Atual do Risco

*[Documente o estado atual do risco e a data em que foi revisado.]*

#### 2.4.2 Acompanhamento das Ações

*[Registre o acompanhamento da execução das atividades de tratamento dos riscos, que constam do cronograma do projeto, e a avaliação da sua efetividade.]*



## **APÊNDICE D**

### **PLANO DE GERENCIAMENTO DE RISCOS**

**Projeto A**

**Versão 1.0**

## REVISÃO HISTÓRICA

<b>Data</b>	<b>Versão</b>	<b>Descrição</b>	<b>Autor</b>
03/11/2005	1.0	Criação do plano	Pascale

## CONTEÚDO

<b>1. Introdução</b>	<b>219</b>
1.1 Finalidade	219
1.2 Escopo	219
1.3 Definições, Acrônimos e Abreviações	219
1.4 Referências	219
<b>2. Fontes e Categorias de Riscos</b>	<b>219</b>
2.1 Fontes de Riscos	219
2.2 Categorias de Riscos	219
<b>3. Parâmetros para o Gerenciamento de Riscos</b>	<b>219</b>
3.1 Critérios para a Análise dos Riscos	219
3.2 Critérios para o Tratamento dos Riscos	219
3.3 Métricas	219
3.4 Limites para cada Categoria de Riscos	219
3.5 Indicadores para Avaliação do Processo	219
<b>4. Estratégias para o Gerenciamento de Riscos</b>	<b>219</b>
4.1 Processo Adaptado	219
4.2 Metodologia	220
4.3 Papéis e Responsabilidades	220
4.4 Periodicidade	220
4.5 Plano de Comunicação	220
4.6 Avaliação do Processo	220

<b>Plano de Gerenciamento de Riscos</b> <b>Projeto A</b>	<b>Página:</b> 219
	<b>Data:</b> 11/7/2006 4:10 PM

## Plano de Gerenciamento de Riscos

### 1. Introdução

#### 1.1 Finalidade

O *Plano de gerenciamento de riscos* descreve como gerenciar os riscos associados ao projeto. Ele detalha as fontes e categorias de riscos, as estratégias de gestão de riscos a serem utilizadas e a periodicidade de acompanhamento dos riscos. Esse plano pode ser incorporado ao *Plano do projeto*.

#### 1.2 Escopo

Este documento tem por objetivo garantir que os riscos do Projeto A sejam corretamente identificados, analisados, documentados, tratados, monitorados e controlados.

#### 1.3 Definições, Acrônimos e Abreviações

Não se aplica.

#### 1.4 Referências

- [1] Orientação – Levantamento de Riscos
- [2] Procedimento – Analisar Riscos
- [3] Procedimento – Planejar Respostas aos Riscos
- [4] Processo de Medição e Análise
- [5] Processo de Gestão de Projetos
- [6] Processo de Gestão de Processos
- [7] Ferramenta de Gestão de Riscos

### 2. Fontes e Categorias de Riscos

#### 2.1 Fontes de Riscos

O Projeto A utiliza as fontes de riscos predefinidas para a organização, descritas no documento *Orientação – Levantamento de Riscos* [1].

#### 2.2 Categorias de Riscos

O Projeto A utiliza as categorias de riscos predefinidas para a organização, descritas no documento *Orientação – Levantamento de Riscos* [1].

### 3. Parâmetros para o Gerenciamento de Riscos

#### 3.1 Critérios para a Análise dos Riscos

Definidos no *Procedimento – Analisar Riscos* [2].

#### 3.2 Critérios para o Tratamento dos Riscos

Definidos no *Procedimento – Planejar Respostas aos Riscos* [3].

#### 3.3 Métricas

Definidas no *Processo de Medição e Análise* [4].

#### 3.4 Limites para cada Categoria de Riscos

Não se aplica.

#### 3.5 Indicadores para Avaliação do Processo

Definidas no *Processo de Medição e Análise* [4] e coletados através da *Ferramenta de Gestão de Riscos* [7].

### 4. Estratégias para o Gerenciamento de Riscos

#### 4.1 Processo Adaptado

Adaptação realizada no *Processo de Gestão de Projetos* [5].

#### **4.2 Metodologia**

As técnicas utilizadas para a identificação de riscos no projeto são as seguintes: *brainstorming*, revisão da documentação e base histórica.

Para cada risco, serão definidos, no mínimo, os limites de aceitação e o gatilho, para indicar que o mesmo ocorreu. Esses gatilhos serão utilizados na monitoração do risco e para a tomada de ação.

As estratégias de tratamento estão definidas no *Procedimento – Planejar Respostas aos Riscos* [3].

#### **4.3 Papéis e Responsabilidades**

Definidos no *Processo de Gestão de Projetos* [5].

#### **4.4 Periodicidade**

Os riscos do projeto serão acompanhados nas reuniões de assessoramento técnico. Caso a estratégia de resposta ao risco precise do aval do gerente do projeto ou de gerência de instância superior, o risco será abordado nas reuniões de assessoramento gerencial ou estratégico, conforme o caso.

#### **4.5 Plano de Comunicação**

Definido no *Processo de Gestão de Projetos* [5].

#### **4.6 Avaliação do Processo**

Definida no *Processo de Gestão de Processos* [6].