CHRISTIAN BECKER BUENO DE ABREU

MÉTODO PARA APLICAÇÃO DE MODELOS DE MELHORIA E AVALIAÇÃO DO PROCESSO DE DESENVOLVIMENTO DE *SOFTWARE* EM SISTEMAS CRÍTICOS DE SEGURANÇA

SÃO PAULO

2008

CHRISTIAN BECKER BUENO DE ABREU

MÉTODO PARA APLICAÇÃO DE MODELOS DE MELHORIA E AVALIAÇÃO DO PROCESSO DE DESENVOLVIMENTO DE *SOFTWARE* EM SISTEMAS CRÍTICOS DE SEGURANÇA

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para a obtenção do título de Mestre em Engenharia.

Área de Concentração: Sistemas Digitais

Orientador: Prof. Dr. Paulo Sérgio Cugnasca

SÃO PAULO

2008

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com anuência de seu orientador.

São Paulo, 15 de outubro de 2008

_____

Assinatura do Autor

_____

Assinatura do Orientador

FICHA CATALOGRÁFICA

Abreu, Christian Becker Bueno de

Método para aplicação de modelos de melhoria e avaliação do processo de desenvolvimento de software em sistemas críticos de segurança / C.B.B. de Abreu. -- ed. rev. -- São Paulo, 2008.

167 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Computação e Sistemas Digitais.

1. Melhoria de processo de software 2. Segurança de software 3. Qualidade de processo de software I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Computação e Sistemas Digitais II. t.

Às pessoas que confiam suas vidas e àquelas que dedicam suas vidas
ao *software* de complexos sistemas de segurança crítica.

"Que o Deus Eterno os abençoe e os guarde".
(Números 6.24)

DEDICATÓRIA

Ao mais querido amigo desta estrada, Leandro Gomes Calçada, com grande pesar, e em sua memória. Já não mais existem no mundo pessoas como nós. Encontre a paz em seu descanso.

À esposa, Camila Jaqueto Pinheiro de Abreu, por sua paciência, compreensão e, principalmente, por seu amor sincero e incondicional, esteja sempre feliz com Deus e ao meu lado, na realização dos seus sonhos e na construção de nossa família.

AGRADECIMENTOS

Na oportunidade da publicação da presente Dissertação de Mestrado, agradeço a todas as pessoas que contribuíram para a minha formação pessoal, acadêmica e profissional, indispensáveis para a realização deste trabalho.

Em primeiro lugar agradeço aos meus Pais, Adm. Heloisa Becker Bueno de Abreu e Prof. José Rubens Bueno de Abreu, pelo carinho, dedicação e incentivo à minha educação formal e formação de meu caráter, ao longo de todos os momentos de minha vida.

Meus sinceros agradecimentos a todos os Professores da Escola Politécnica da Universidade de São Paulo com quem tive o privilégio de conviver durante a realização do mestrado, em especial ao Prof. Dr. João Batista Camargo Júnior, pelo contagiante entusiasmo, e ao Prof. Dr. Jorge Rady de Almeida Júnior, pela confiança neste trabalho e seu valioso empenho e contribuição na Qualificação.

Ao orientador, Prof. Dr. Paulo Sérgio Cugnasca, pela dedicação, respeito e liberdade com que conduziu a realização deste trabalho.

Aos colegas e amigos do Grupo de Análise de Segurança da Escola Politécnica da Universidade de São Paulo, com quem tive o prazer do convívio acadêmico.

Aos colegas do Departamento de Projeto de Sistemas de Controle e Comunicação, Coordenação de Sinalização, da Companhia do Metropolitano de São Paulo, e em especial ao Eng. José Henrique Zaccardi Freitas pelo incentivo ao desenvolvimento de estudos na área de Qualidade de *Software* e sua visão sobre a importância em sistemas de Segurança Crítica.

RESUMO

O avanço recente da tecnologia na área de sistemas digitais representa uma grande oportunidade para realizar um importante progresso em diversos aspectos dos sistemas de controle e proteção tradicionais. No entanto, os requisitos provenientes do uso intensivo de software em sistemas críticos de segurança, aumenta a demanda por uma abordagem adequada que possa ser baseada na experiência nesta área. Apesar de vários modelos de capacidade de maturidade estarem em constante desenvolvimento, ainda é um desafio estabelecer uma forma coerente para a melhoria e avaliação do processo de desenvolvimento de software. O objetivo desta pesquisa é propor um método para obtenção de perfis de capacidade baseados na aplicação do modelo de referência brasileiro para melhoria do processo de software MR-MPS, em conjunto com a extensão de segurança do modelo de capacidade e maturidade CMMI-DEV +SAFE, embasado pela percepção de especialistas em segurança por meio da aplicação de um modelo de decisão por múltiplos critérios.

Palavras-chave: sistemas de segurança, melhoria de processo de software, qualidade de software

ABSTRACT

The recent technology advance in the digital systems area represents a great opportunity to make important progress in many aspects of traditional control and protection systems. However, requirements derived from the intensive use of software in safety critical systems raises the demand for a suitable approach that can be based on the expertise in this area. Although a number of capability maturity models have been in constant development, it is still challenging to establish a coherent path for software process improvement and evaluation. The goal of this research work is to propose a method for building capability profiles based on the application of the Brazilian Reference Model for Software Process Improvement MR-MPS, along with the Capability Maturity Model for Development safety extension CMMI-DEV +SAFE, supported by safety engineers' insight through the application of a multi criteria decision model.

Keywords: system safety, software process improvement, software quality.

SUMÁRIO

1 Introdução 17
1.1 Objetivo 17
1.2 Justificativa 18
1.3 Motivação 19
1.4 Estrutura do Trabalho 19
2 Conceitos e Definições 22
2.1 Conceituação de Sistemas Críticos de Segurança 22
2.1.1 Definição de Segurança 22
2.1.2 Exemplo da Segurança em Sistemas Críticos 24
2.1.3 O Emprego de *Software* em Aplicações de Segurança Crítica 26
2.2 Definições Relacionadas com o Software 27
2.3 Elementos da Qualidade de Software 29
2.4 A Qualidade no Processo de Desenvolvimento de Software 30
2.4.1 Norma ISO 9000-3 30
2.4.2 Modelo CMU/SEI CMMI-DEV 34
2.5 Segurança como um Atributo da Qualidade de Produto 42
2.5.1 Norma ISO/IEC 9126-1 43
2.5.2 Outras Abordagens para Qualidade de Produto 46
2.5.3 Uma Abordagem para Qualidade de Produto com Enfoque na Segurança 47
2.6 Confiabilidade de Software 49
2.7 Emprego de Técnicas e Modelos de Engenharia de Software no Desenvolvimento de Sistemas Críticos 50
2.8 Considerações Finais do Capítulo 51
3 Modelo de Referência MPS.BR 52
3.1 A Representação em Estágios do MR-MPS 54
3.1.1 Níveis de Maturidade do MR-MPS 56
3.2 A Representação Contínua no MR-MPS 57
3.3 Níveis de Capacidade e Atributos de Processos no MR-MPS 59
3.4 Áreas de Processos Definidas no MR-MPS 62
3.5 Considerações Finais do Capítulo 63
4 Extensões de Segurança para o CMMI 64
4.1 Extensão do Modelo CMMI para RAMS 64

4.1.1 Gestão de RAMS - RM 66
4.1.2 Garantia de RAMS - RA 67
4.1.3 Engenharia de RAMS - RE 67
4.1.4 Infra-Estrutura Organizacional de RAMS - ROI 69
4.2 Extensão de Segurança FAA para iCMM 69
4.2.1 Área de Aplicação: Segurança (*Safety and Security*) 70
4.2.2 Área de Processo: Ambiente de Trabalho 72
4.3 Extensão do Modelo ADD/DMO CMMI-DEV +SAFE 72
4.4 Áreas de Processos Definidas no CMMI-DEV +SAFE 73
4.4.1 Gerenciamento de Segurança – GSEG 74
4.4.2 Engenharia de Segurança – ESEG 74
4.5 Relacionamento entre as Áreas de Processos 75
4.6 Descrição de Níveis do CMMI-DEV +SAFE 76
4.6.1 Gerenciamento de Segurança – GSEG 77
4.6.2 Engenharia de Segurança – ESEG 78
4.6.3 Engenharia de Segurança – ESEG (evolução) 78
4.6.4 Engenharia de Segurança – ESEG (evolução) 79
4.7 Considerações Finais do Capítulo 79
5 Método de Decisão por Múltiplos Critérios 80
5.1 Definições Relacionadas aos MDMC 80
5.2 Justificativa do Analytic Hierarchy Process (AHP) 81
5.3 Aplicações do AHP 82
5.4 Decomposição de um Problema Usando o AHP 83
5.5 Métricas e Escalas no AHP 85
5.6 A Medida de Todas as Coisas – o julgamento humano (SAATY, 1990) 86
5.7 Atribuição de Valores: Julgamentos 88
5.8 Análise por Várias Pessoas 88
5.9 Descrição Matemática do AHP 89
5.9.1 Cálculo das Prioridades em uma Matriz (SAATY, 1991) 90
5.9.2 Inconsistência de Julgamento 93
5.9.3 Cálculo da Razão de Consistência 97
5.9.4 Correção de Valores 98
5.9.5 Cálculo das Prioridades da Hierarquia 98
5.10 Considerações Finais do Capítulo 100
6 Método Proposto 101

6.1 Premissas para a Aplicação do Método 101
6.1.1 Visibilidade do Processo de Desenvolvimento de *Software* 102
6.1.2 Validação do Processo de Desenvolvimento de *Software* 103
6.1.3 Defeitos Inseridos no Desenvolvimento de *Software* 103
6.1.4 Representação da Segurança em Níveis 104
6.2 Descrição do Método Proposto 105
6.2.1 Definição das Áreas de Processo (PAs) 109
6.2.2 Preparação para o AHP 109
6.2.3 Realização de Julgamentos 112
6.2.4 Análise de Sensibilidade 116
6.2.5 Aplicação do Método AHP 117
6.2.6 Obtenção do Perfil de Capacidade 118
6.3 Considerações Finais do Capítulo 118
7 Estudo de Caso 120
7.1 Emprego do Método Proposto 120
7.1.1 Escolha das Áreas de Processo 120
7.1.2 Preparação para o AHP 121
7.1.3 Realização do Julgamento 123
7.1.4 Aplicação do Método AHP 125
7.1.5 *Obtenção de Diferentes Perfis de Capacidade* 129
7.2 Considerações Finais do Capítulo 137
8 Conclusão e Considerações Finais 139
8.1 Conclusões 139
8.2 Propostas de Trabalhos Futuro 141
8.3 Considerações Finais 142
REFERÊNCIAS BIBLIOGRÁFICAS 143
ANEXO A 148
A.1 Gerência de Projetos – GPR 149
A.2 Gerência de Requisitos – GRE 150
A.3 Aquisição – AQU 151
A.4 Gerência de Configuração – GCO 152
A.5 Garantia da Qualidade – GQA 152
A.6 Medição – MED 153
A.7 Melhoria do Processo Organizacional – AMP 154
A.8 Definição do Processo Organizacional – DFP 155

A.9 Gerência de Recursos Humanos – GRH 156
A.10 Gerência de Reutilização – GRU 157
A.11 Gerência de Projetos – GPR (evolução) 157
A.12 Desenvolvimento de Requisitos – DRE 158
A.13 Integração do Produto – ITP 159
A.14 Projeto e Construção do Produto – PCP 160
A.15 Validação – VAL 161
A.16 Verificação – VER 162
A.17 Gerência de Reutilização – GRU (evolução) 162
A.18 Análise de Decisão e Resolução – ADR 163
A.19 Desenvolvimento para Reutilização – DRU 164
A.20 Gerência de Riscos – GRI 165
A.21 Gerência de Projetos – GPR (evolução) 166
A.22 Análise de Causas de Problemas e Resolução – ACP 167

ÍNDICE DE FIGURAS

Figura 1 – Efeito de Falhas em um Sistema (CENELEC, 1999) 26
Figura 2 – Representação em Estágios do CMMI-DEV (CHRISSIS; KONRAD; SHRUM, 2007) 41
Figura 3 – Representação Contínua do CMMI-DEV (CHRISSIS; KONRAD; SHRUM, 2007) 42
Figura 4 – Segurança como um atributo da qualidade (FIRESMITH, 2005) 46
Figura 5 – Atributos da qualidade relativos à segurança (FIRESMITH, 2003) 47
Figura 6 – Níveis de Maturidade do MR-MPS 55
Figura 7 – Níveis de Capacidade do MR-MPS 58
Figura 8 – Níveis de Capacidade por Áreas de Processo (PAs) 59
Figura 9 – Análise Hierárquica (BHUSHAN, 2004) 84
Figura 10 – Passos do Método Proposto Usando o AHP 107
Figura 11 – Melhoria do Processo de Software 108
Figura 12 – Representação da Hierarquia 112
Figura 13 – Julgamentos Modo Questionário 114
Figura 14 – Julgamentos Modo Matricial 115
Figura 15 – Estudo de caso - Hierarquia 123
Figura 16 – Questionário Piloto 124
Figura 17 – Representação na Forma Matricial 125
Figura 18 – Software Super Decisions – Hierarquia 126
Figura 19 – Software Super Decisions - Julgamentos 127
Figura 20 – Software Super Decisions – Índice de Consistência 128
Figura 21 – Software Super Decisions - Resultados 129
Figura 22 – Planilha para Obtenção do Perfil de Capacidade – Caso 1 130
Figura 23 – Perfil de Capacidade 1 132
Figura 24 – Planilha para Obtenção do Perfil de Capacidade – Caso 2 134
Figura 25 – Perfil de Capacidade 2 134
Figura 26 – Planilha para Obtenção do Perfil de Capacidade – Caso 3 136
Figura 27 – Perfil de Capacidade 3 136

ÍNDICE DE TABELAS

Tabela 1 – Ciclo de Vida (ISO/IEC, 2004b) 33
Tabela 2 – Atividades de suporte (ISO/IEC, 2004b) 34
Tabela 3 – Áreas de Processo do CMMI-DEV 37
Tabela 4 – Níveis de Capacidade do CMMI-DEV 38
Tabela 5 – Metas e Práticas Genéricas CMMI-DEV 39
Tabela 6 – Níveis de Maturidade CMMI-DEV 40
Tabela 7 – Qualidade Interna e Externa (ISO/IEC, 1991) 44
Tabela 8 – Qualidade em uso (ISO/IEC, 1991) 45
Tabela 9 – Áreas de Processos e Atributos de Processos do MR-MPS 57
Tabela 10 – Atributos de Processo (AP) para cada Nível de Capacidade 60
Tabela 11 – Resultados Esperados dos Atributos do Processo (RAPs) (MPS-BR, 2007a) 60
Tabela 12 – Práticas Específicas RM 66
Tabela 13 – Práticas Específicas RA 67
Tabela 14 – Práticas Específicas RE 68
Tabela 15 – Práticas Específicas ROI 69
Tabela 16 – Práticas da Área de Aplicação “Segurança” 71
Tabela 17 – Práticas Específicas - Ambiente de Trabalho 72
Tabela 18 – Práticas Específicas GSEG 74
Tabela 19 – Práticas Específicas ESEG 75
Tabela 20 – Práticas Específicas GSEG (nível S1) 77
Tabela 21 – Práticas Específicas ESEG (nível S1) 78
Tabela 22 – Práticas Específicas ESEG (nível S2) 78
Tabela 23 – Práticas Específicas ESEG (nível S3) 79
Tabela 24 – Escala Fundamental de Números Absolutos (SAATY, 2006) 86
Tabela 25 – Índice Randômico (SAATY, 1990) 97
Tabela 26 – Práticas Específicas GPR 149
Tabela 27 – Práticas Específicas GRE 150
Tabela 28 – Práticas Específicas AQU 151
Tabela 29 – Práticas Específicas GCO 152
Tabela 30 – Práticas Específicas GQA 152
Tabela 31 – Práticas Específicas MED 153
Tabela 32 – Práticas Específicas AMP 154
Tabela 33 – Práticas Específicas DFP 155

Tabela 34 – Práticas Específicas GRH 156
Tabela 35 – Práticas Específicas GRU 157
Tabela 36 – Práticas Específicas GRU (nível E) 157
Tabela 37 – Práticas Específicas DRE 158
Tabela 38 – Práticas Específicas ITP 159
Tabela 39 – Práticas Específicas PCP 160
Tabela 40 – Práticas Específicas VAL 161
Tabela 41 – Práticas Específicas VER 162
Tabela 42 – Práticas Específicas GRU (nível C) 162
Tabela 43 – Práticas Específicas ADR 163
Tabela 44 – Práticas Específicas DRU 164
Tabela 45 – Práticas Específicas GRI 165
Tabela 46 – Práticas Específicas GPR (nível B) 166
Tabela 47 – Práticas Específicas ACP 167

SIGLAS

ACP	Análise de causas e resolução de problemas
ADD/DMO	Departamento de defesa da Australia *(Australian Department of Defence / Defence Materiel Organisation)*
ADR	Análise de decisão e resolução
AHP	Método de análise hierárquica (*analytic hierarchy process*)
AMP	Avaliação e melhoria do processo organizacional
ANSI	*American National Standards Institute*
AP	Atributo de processo
AQU	Aquisição
BID	Banco Interamericano de Desenvolvimento
CENELEC	*Comité Européen de Normalisation Électrotechnique*
CMMI	*Capability Maturity Model Integration*
CMMI-DEV	*CMMI for development*
CMMI-SE/SW	*CMMI for systems engineering and software engineering*
CMU/SEI	*Carnegie Mellon University / Software Engineering Institute*
COTS	Comercial de prateleira (*commercial off the shelf*)
DoD	Departamento de defesa dos Estados Unidos da América *(The United States of America Department of Defense)*
DFP	Definição do processo organizacional
DRE	Desenvolvimento de requisitos
DRU	Desenvolvimento para reutilização
FAA	*The United States Federal Aviation Administration*
FAA-iCMM	*FAA-Integrated Capability Maturity Model*
FINEP	Financiadora de estudos e projetos
GCO	Gerência de configuração
GG	Meta genérica (*generic goal*)
GP	Prática genérica (*generic practice*)
GPR	Gerência de projetos
GQA	Garantia da qualidade
GRE	Gerência de requisitos
GRH	Gerência de recursos humanos
GRI	Gerência de riscos
GRU	Gerência de reutilização
IEC	*International Electrotechnical Commission*

IPPD	Desenvolvimento integrado de produto e processo (*Integrated Product and Process Development*)
ISO	*International Organization for Standards*
ITP	Integração do produto
MA-MPS	Método da avaliação - melhoria de processo de *software*
MED	Medição
MCT	Ministério da ciência e tecnologia
MDMC	Modelo de decisão por múltiplos critérios
MPS.BR	Melhoria de processo do s*oftware* Brasileiro
MR-MPS	Modelo de referência - melhoria de processo de *software*
MTTUF	Tempo médio até falha insegura *(mean time to unsafe failure)*
PA	Área de processo (*process area*)
PCP	Projeto e construção do produto
RAM	Confiabilidade, disponibilidade e manutenibilidade (*Reliability, availability and maintainability*)
RAMS	Confiabilidade, disponibilidade, manutenibilidade e segurança (*Reliability, availability, maintainability and safety*)
SCAMPI	*Método de Avaliação Padrão CMMI para a Melhoria de Processos* (*Standard CMMI Appraisal Method for Process Improvement*)
SG	Meta específica (*specific goal*)
SIL	Nível de integridade de segurança (*Safety integrity level*)
SOFTEX	Associação para promoção da excelência do *software* brasileiro
SP	Prática específica (*specific practice*)
SW-SIL	Nível de integridade de segurança de *software* (*software* SIL)
VAL	Validação
VER	Verificação

1 Introdução

A utilização correta da tecnologia representa uma oportunidade de se melhorar a qualidade de vida das pessoas no mundo moderno. Da mesma forma, a mudança de paradigmas que garantem a segurança em sistemas complexos deve ser continuamente rediscutida, à medida que novos desafios surgem decorrentes do avanço tecnológico.

A adequação dos modelos de melhoria de processos de desenvolvimento *software* às aplicações de segurança crítica vem sendo estudada na última década, e já foram propostas e publicadas diversas extensões aos modelos com este propósito, como em (ADD/DMO, 2007), (IBRAHIM et al., 2004), (FONSECA, 2005).

A quantidade de alternativas para a adoção desses modelos exige grandes esforços para a total compreensão do volume de informações presentes nesses modelos e para a tomada de decisões. Tudo isso com o objetivo de empregar a melhor e mais adequada tecnologia para a obtenção de processos adequados à obtenção de *software* em sistemas críticos de segurança.

Considerando a utilização de critérios e julgamentos qualitativos e subjetivos como prática comum, quando não a única alternativa disponível, para a definição destes processos, torna-se muito atrativa a utilização de ferramentas de auxílio à síntese de informações e a tomada de decisões coerentes dentro desse cenário.

1.1 Objetivo

O objetivo deste trabalho de investigação científica é propor um método para aplicação de um modelo de melhoria e avaliação do processo de desenvolvimento de *software* com extensão em aspectos de segurança, para aplicação em sistemas críticos, utilizando como

critério de priorização das atividades prescritas nesse modelo a experiência de especialistas desta área.

1.2 Justificativa

A área de qualidade do processo de desenvolvimento de *software* tem evoluído muito nos últimos anos (CHRISSIS; KONRAD; SHRUM, 2007). Essa evolução representa uma oportunidade de avanço tecnológico no desenvolvimento de novos sistemas e, em particular, nos sistemas críticos, permitindo um melhor aproveitamento de recursos (financeiros, materiais, etc.), sem o comprometimento das suas características de segurança.

Os atributos típicos das arquiteturas dos sistemas computacionais mais avançados relacionados, por exemplo, ao seu comportamento diante de situações imprevisíveis provocadas por falhas de *hardware* ou pela complexidade do ambiente, impõem uma grande responsabilidade no *software* pela segurança desses sistemas críticos. Por exemplo, quando algum componente de *hardware* apresenta um comportamento anômalo, que possa levar o sistema a uma situação insegura, espera-se muitas vezes que o *software* possa detectar e mitigar esse problema.

Em aplicações críticas de segurança, nas quais o avanço tecnológico amplia continuamente o escopo do emprego de dispositivos programáveis, como os microprocessadores, e por conseqüência aumentam a dependência do *software* para a realização de funções de segurança, as atividades de especificação e avaliação do processo de desenvolvimento de *software* devem ser cuidadosamente realizadas.

1.3 Motivação

A principal motivação para este trabalho é a necessidade de se encontrar pontos de convergência entre a produção acadêmico-científica, no seu estado atual da arte, e os desafios práticos encontrados nos projetos de sistemas críticos de segurança, considerando o emprego intensivo de *software* para a realização de funções de segurança (*safety*).

A experiência e o interesse do autor, especialmente nas etapas de projeto de sistemas de sinalização e controle metro-ferroviários microprocessados, em particular aqueles baseados em tecnologias recentes, indica que o uso intensivo de *software* deva receber uma especial atenção devido à sua grande implicação na segurança desses sistemas.

A importância deste trabalho de pesquisa, para os sistemas metro-ferroviários, justifica-se pela crescente necessidade do emprego de novas tecnologias que permitam um incremento na velocidade comercial e redução do intervalo entre trens (*headway*), considerando inclusive sistemas totalmente automáticos, sem a atuação na condução das composições (*driverless*), ou até mesmo sem a presença de operadores (*manless*), para viabilizar o projeto e implantação de sistemas de transporte de massa de alta capacidade, em grandes centros urbanos, sem comprometer a segurança (*safety*) em sua operação.

1.4 Estrutura do Trabalho

Esta dissertação encontra-se dividida em capítulos, como segue:

O Capítulo 1 compreende a introdução, os objetivos do trabalho, a motivação e a justificativa para a sua realização, bem como a estruturação deste trabalho de pesquisa.

No Capítulo 2 são apresentadas as definições de segurança e a conceituação de sistemas críticos no contexto deste trabalho. É apresentada, ainda, uma abordagem da segurança

(*safety*), buscando situar o *software* em um sistema crítico e sua relação com a segurança. Ainda neste capítulo, são apresentadas duas perspectivas distintas da qualidade de *software*: a qualidade do processo de desenvolvimento de *software* e a qualidade do produto de *software*.

No Capítulo 3 é apresentado o modelo de melhoria de processo do *software* brasileiro (MPS.BR), construído a partir do modelo CMU/SEI CMMI-DEV "Modelo de Capacidade e Maturidade para Desenvolvimento" (*Software Engineering Institute / Carnegie Mellon University Capability Maturity Model for Development*) e a partir das normas ISO/IEC 12207 Tecnologia da Informação - Processos do Ciclo de Vida de *Software* (*Information Technology - Software Life Cycle Processes*) (ISO/IEC, 1995) e ISO/IEC 15504 Tecnologia da Informação - Validação de Processo (*Information Technology - Process Assessment*) (ISO/IEC, 2004a).

O Capítulo 4 apresenta as extensões de segurança ao CMMI propostas por (FONSECA, 2005) em sua tese de doutorado "Uma Extensão de RAMS para o Modelo CMMI baseada nas Normas Ferroviárias CENELEC" e pela FAA (*Federal Aviation Administration*) norte americana, com o " FAA *Safety and Security Extensions for Integrated Capability Maturity Models*" (IBRAHIM et al., 2004). Ainda, este capítulo apresenta uma breve discussão sobre a possibilidade da extensão do modelo MPS-BR com base no ADD/DMO CMMI +SAFE (*Australian Department of Defence / Defence Materiel Organisation +SAFE, A Safety Extension to* CMMI-DEV).

No Capítulo 5 é detalhado um modelo de decisão por múltiplos critérios (MDMC), o Método de Análise Hierárquica (*Analytic Hierarchy Process* - AHP), processo escolhido para o auxílio à decisão proposto neste trabalho para facilitar a definição de níveis de capacidade em uma representação contínua CMMI.

O Capítulo 6 representa a principal contribuição desta dissertação, com o modelo proposto para a determinação do conjunto de processos de obtenção de *software* mais

favorável à segurança de um determinado sistema crítico em análise, pressupondo uma série de julgamentos qualitativos e subjetivos em relação à importância ou relevância de áreas de processo comparadas entre si, e obedecendo a uma estrutura hierárquica proposta.

A seguir, no Capítulo 7, são apresentados estudos de caso para o modelo proposto, com base em pesquisa realizada por meio de questionários direcionados a especialistas em sistemas de segurança de aplicação crítica. Os resultados obtidos são apresentados e discutidos para validar a potencialidade deste modelo.

No Capítulo 8 são apresentadas as considerações finais deste trabalho, ressaltando as principais contribuições desta pesquisa de mestrado, e as decorrentes possibilidades para o desenvolvimento de trabalhos futuros.

2 Conceitos e Definições

Para o desenvolvimento desta dissertação é necessária a definição do conceito de segurança e termos relacionados, que serão utilizados no contexto apresentado, bem como a conceituação de sistemas críticos. Em seguida, neste capítulo, o *software* é inserido no contexto dos sistemas críticos de segurança e são apresentados elementos da qualidade de processo e produto de *software*.

2.1 Conceituação de Sistemas Críticos de Segurança

Para este trabalho de pesquisa, a segurança é considerada um atributo dentro de um contexto de sistemas eletrônicos programáveis que utilizam microprocessadores, microcontroladores ou outros componentes programáveis, sendo então abordada especificamente a influência do processo de desenvolvimento de *software* para tais sistemas.

2.1.1 Definição de Segurança

A definição de segurança "*safety*" de acordo com o guia "*Functional safety and IEC 61508: A basic guide*" (IEC, 2002) é a ausência de risco inaceitável de dano físico ou à saúde de pessoas, direta ou indiretamente, como de dano ao patrimônio ou ao meio ambiente.

A segurança operacional "*functional safety*", tratada pela norma "*Functional safety of electrical/electronic/programmable electronic safety related systems*" (IEC, 1998), e objeto deste trabalho, pode ser definida como a parcela da segurança que depende do funcionamento correto de um sistema ou equipamento elétrico/eletrônico/programável em resposta às suas entradas. Outras formas de se obter a segurança, como o emprego de barreiras físicas ou uso

de materiais adequados, como absorvedores de impacto ou reforços estruturais, por exemplo, não estão sendo consideradas.

No contexto deste trabalho, o termo "sistema" pode significar um sistema de controle ou proteção completo, um subsistema, um equipamento, ou mesmo parte deste. É possível afirmar que nenhum sistema pode ser absolutamente seguro; portanto, o objetivo ao se projetar um sistema é fazê-lo de forma a atender ao nível de segurança apropriado para o seu propósito (CENELEC, 1999).

A determinação de um nível de segurança apropriado pode envolver opiniões e julgamentos pessoais, o que é afetado ainda pelo fato da segurança estar ligada a fatores emocionais. Frente a situações de perigo, as percepções a respeito da segurança obtidas das pessoas muitas vezes são distintas, quando não ilógicas. Um exemplo freqüentemente observado é que muitas pessoas têm medo de voar, apesar do fato de que estatisticamente estão mais seguras viajando de avião do que dirigindo seus carros até o aeroporto (STOREY, 1996).

Pode-se definir a segurança de um sistema como a probabilidade desse sistema efetuar suas operações de forma correta, ou descontinuar seu funcionamento de forma a não comprometer a operação de outros sistemas ou comprometer a segurança (JOHNSON, 1989).

É importante notar que outro conceito, o da segurança da informação ou "*security*", deve ter um tratamento à parte nos sistemas críticos. Os aspectos da segurança da informação considerados centrais são confidencialidade, integridade e disponibilidade, mas também existem outros tais como autenticação, não repúdio, legalidade, privacidade e auditoria (ALBUQUERQUE, 2002). Existem sistemas críticos em que estes fatores podem afetar a segurança, como por exemplo os sistemas dependentes de comunicação de dados por meio da livre propagação; no entanto, estes atributos não fazer parte do escopo deste trabalho de pesquisa.

2.1.2 Exemplo da Segurança em Sistemas Críticos

A norma "Aplicações Ferroviárias – A Especificação e Demonstração de Confiabilidade, Disponibilidade, Manutenibilidade e Segurança" (*Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety* - RAMS) (CENELEC, 1999) apresenta às autoridades e indústria ferroviárias uma abordagem consistente para o gerenciamento da confiabilidade, disponibilidade, manutenibilidade e segurança, denotados pelo acrônimo RAMS, com base em processos para a especificação e demonstração desses requisitos.

A abordagem no nível de sistema definida por essa norma, promove a avaliação das interações entre os elementos RAMS (confiabilidade, disponibilidade, manutenibilidade e segurança) de aplicações ferroviárias complexas, ao longo de todas as fases do ciclo de vida do sistema.

O conceito de segurança apresentado considera:

a) Todas possíveis ameaças ("*hazards*") ao sistema, sob todas as condições de operação, manutenção e do ambiente;

b) As características de cada ameaça em termos de gravidade das conseqüências;

c) Falhas relacionadas à segurança, entendidas como:

- Todos os modos de falha que podem levar a uma ameaça (modos de falha relacionados à segurança). Este é um subconjunto de todos os modos de falha considerados para a confiabilidade;
- A probabilidade da ocorrência de cada modo de falha do sistema, relacionado à segurança;
- Seqüência e/ou coincidência de eventos, falhas, estados operacionais, condições ambientais, etc., na aplicação, que podem resultar em um acidente; (por exemplo, uma ameaça resultando em um acidente);

- A probabilidade da ocorrência de cada um dos eventos, falhas, estados operacionais, condições ambientais, etc., na aplicação.

d) Manutenibilidade dos componentes do sistema relacionados à segurança, entendida como:

- A facilidade de efetuar manutenção em partes do sistema ou componentes que estão associados a uma ameaça ou a um modo de falha relacionado à segurança;
- A probabilidade da ocorrência de erros durante ações de manutenção nestas partes relacionadas à segurança do sistema;
- Tempo para restauração do sistema a um estado seguro.

e) Operação do sistema e manutenção de partes relacionadas à segurança do sistema em termos de:

- Influência de fatores humanos na manutenção efetiva de todas as partes relacionadas à segurança do sistema e a operação segura do sistema;
- Ferramentas, instalações e procedimentos para manutenção efetiva das partes relacionadas à segurança do sistema e à operação segura;
- Controles e medidas efetivas para lidar com uma ameaça e reduzir suas conseqüências.

A figura 1 ilustra possíveis efeitos de ameaças ou perturbações à confiabilidade e segurança de um Sistema Ferroviário, em decorrência de estados ou modos de falha relacionados ou não à segurança.

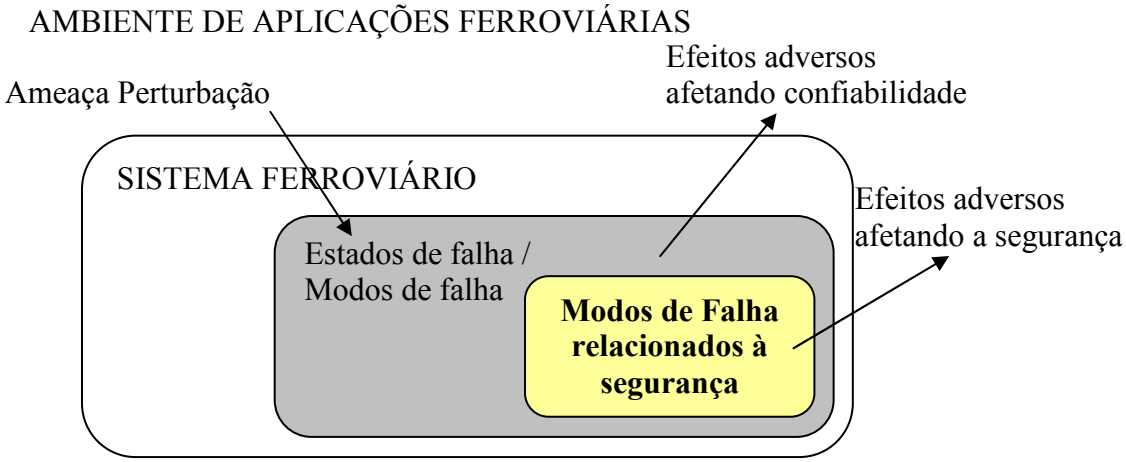

Figura 1 – Efeito de Falhas em um Sistema (CENELEC, 1999)

2.1.3 O Emprego de *Software* em Aplicações de Segurança Crítica

Os primeiros sistemas automáticos de controle e proteção eram baseados em sistemas eletromecânicos, hidráulicos ou pneumáticos, nos quais a segurança era tipicamente obtida por meio do uso de componentes ou arranjos com modos de falha conhecidos, em um projeto que reunia as características necessárias para que não comprometessem a segurança do processo controlado em caso de falhas (LEVESON, 1995).

A necessidade de funções de controle mais complexas e precisas tem aumentado em função do grau de automação necessário para permitir o máximo aproveitamento do investimento feito no sistema a ser controlado. Nestes sistemas de controle de maior complexidade, o emprego de soluções alternativas ao uso de dispositivos eletrônicos programáveis (por exemplo, os microprocessadores) poderiam tornar inviável a sua construção.

Nos dias de hoje, outros motivos podem ser citados e que contribuem para o emprego de microprocessadores nas mais diversas aplicações, tais como alta capacidade de processamento, baixo consumo de energia e dimensões físicas reduzidas.

A complexidade é uma característica intrínseca aos componentes eletrônicos programáveis atuais, em decorrência do avanço da microeletrônica ocorrido nas últimas décadas. Esses componentes, como os mais modernos microprocessadores atuais, chegam a ser formados por dezenas de milhões de transistores (CARLSON; DOYLE, 2002). O levantamento de todos os seus modos de falha torna-se, então, proibitivo, dificultando a obtenção de conclusões sobre a possibilidade da ocorrência de efeitos inseguros em um sistema crítico.

Ainda, o *software* que irá ser executado nos microprocessadores aplicados a sistemas críticos de segurança acrescenta a este cenário um universo de possibilidades de comportamento indesejável ou até mesmo inseguro, caso técnicas adequadas e efetivas de desenvolvimento de *software* não sejam utilizadas.

2.2 Definições Relacionadas com o Software

A formalização de certas definições se faz necessária para o desenvolvimento e compreensão deste trabalho, sendo que alguns conceitos são tão utilizados a ponto de apresentarem interpretações diversas. São apresentados, a seguir, conceitos e termos relacionados com o *software*:

- ***Software***: criação intelectual compreendendo os programas, procedimentos, regras e qualquer documentação correlata à operação de um sistema de processamento de dados. Não depende do meio no qual é registrado (ISO/IEC, 2004b);
- **Produto de *software***: conjunto completo de programas de computador, procedimentos e documentação correlata, assim como dados designados para entrega a um usuário (ISO/IEC, 2004b);

- **Processo de *software***: seqüência de etapas executadas para realizar um determinado objetivo e que envolve métodos, ferramentas e pessoas e pode ser visto como um conjunto de atividades, métodos, práticas e transformações que as pessoas utilizam para desenvolver, manter e evoluir *software* e os artefatos associados (HUMPHREY, 1989). Ou ainda, no universo do CMMI, as atividades que possam ser reconhecidas como implementações de práticas do referido modelo, remetendo a outros itens do próprio modelo; essas atividades podem ser mapeadas a uma ou mais práticas nas áreas de processo do CMMI para possibilitar a melhoria e avaliação de processo por meio de um modelo (CHRISSIS; KONRAD; SHRUM, 2007);

- **Desenvolvimento de *software***: todas as atividades a serem realizadas para a criação de um produto de *software* (ISO/IEC, 2004b);

- **Fase**: segmento definido do trabalho. Não implica no uso de qualquer modelo de ciclo de vida específico, nem implica em um período de tempo durante o desenvolvimento de um produto de *software* (ISO/IEC, 2004b);

- **Modelo**: Um modelo é uma representação de uma entidade ou processo complexo. Ele pode descrever os detalhes de um objeto maior, ou pode ser uma descrição esquemática de um sistema. Um modelo pode capturar um fenômeno de forma a permitir ser analisado e estudado. O valor de um modelo está em sua abstração, e por meio desta simplifica o que pode ser uma realidade complexa – desta forma, poderá ser utilizado pragmaticamente para estudar fenômenos e validar hipóteses (HOFMANN et al., 2007);

- **Modelo de processo de *software***: descreve os processos que são realizados para atingir o desenvolvimento de *software*. Um modelo de processo de *software* pode ser descritivo, geralmente criado como parte de uma análise final de um projeto e

útil na identificação de problemas, ou pode ainda ser prescritivo, utilizado para descrever o processo padrão de desenvolvimento de *software* e como ferramenta de treinamento (GUSTAFSON, 2003);

- **Qualidade**: é a totalidade das características de um produto ou serviço que se baseia na sua habilidade de satisfazer uma dada necessidade (GUSTAFSON, 2003).

2.3 Elementos da Qualidade de Software

A qualidade de *software* deve ser tratada sob duas dimensões: a qualidade dos processos e a qualidade dos produtos. O processo de *software* engloba um conjunto de atividades, métodos, práticas e transformações empregadas no desenvolvimento e manutenção de *software* e seus produtos associados, para os quais normas, métricas e modelos foram definidos e vêm sendo avaliados, buscando melhoria em cada etapa do ciclo (SEPIN/MCT, 2002).

No próximo item é apresentada uma perspectiva da qualidade de *software* conforme apresentada na norma NBR ISO 9000-3 intitulada: "Diretrizes para a aplicação da NBR 19001 ao desenvolvimento, fornecimento e manutenção de *software*, do conjunto de normas de gestão da qualidade e garantia da qualidade" (ISO/IEC, 2004b).

Outra importante perspectiva da qualidade de *software* aderente a este trabalho é apresentada pelo modelo CMU/SEI CMMI-DEV "Modelo de Capacidade e Maturidade para Desenvolvimento" (*Software Engineering Institute / Carnegie Mellon University Capability Maturity Model for Development*). Essa perspectiva também está apresentada no próximo item.

2.4 A Qualidade no Processo de Desenvolvimento de Software

Uma questão fundamental no gerenciamento de projeto de *software* é estabelecer prioridades entre diferentes áreas de processo previstas por normas ou modelos. No gerenciamento orientado ao processo, o controle de pequenas tarefas no ciclo de vida do *software* é enfatizado, enquanto que no gerenciamento orientado ao produto, a obtenção do resultado pela equipe é enfatizada (GUSTAFSON, 2003).

A necessidade de avaliação ou revisão dos processos de *software* de uma organização não teve origem na indústria de desenvolvimento de *software*, mas sim nos setores em que se concentram os grandes compradores de sistemas de uso intensivo de *software*, de missão crítica e outros. Tais setores são principalmente agências de defesa e telecomunicações dos governos de vários países. Podem ser consideradas organizações pioneiras nas iniciativas de métodos de avaliação de *software*, por exemplo, os Departamentos de Defesa americanos e ingleses e as Forças Armadas Alemãs (GUERRA; ALVES, 2004).

2.4.1 Norma ISO 9000-3

A norma ISO 9000-3 (ISO/IEC, 2004b) é aplicada em situações contratuais ao desenvolvimento, fornecimento e manutenção de *software*, envolvendo cliente e fornecedor, que possua as seguintes características:

1. ***Inclui especificamente esforço de projeto, e os requisitos do produto são indicados principalmente em termos de desempenho, ou precisam ser estabelecidos*** (ISO/IEC, 2004b).

Por analogia, a segurança de *software* pode ser considerada como um requisito não funcional tal como um requisito indicado em termos de desempenho. Isso equivale a assumir

que esse atributo seja efetivamente uma característica de determinado produto de *software* resultante da sua consideração em todas as fases de seu desenvolvimento.

Desta forma, é esperado que o "esforço de projeto" esteja presente em todas as fases do desenvolvimento de um produto de *software* com característica de segurança.

2. ***A confiança no produto pode ser obtida por meio da demonstração adequada da capacidade de desenvolvimento, fornecimento e manutenção por um determinado fornecedor*** (ISO/IEC, 2004b).

Os diversos aspectos da qualidade aplicados à obtenção de um produto de *software* podem ser reaplicados em outros projetos realizados por um determinado fornecedor. E, desta forma, pode-se esperar alguma previsibilidade das características de um produto de *software*, se existir informações sobre projetos realizados anteriormente.

É esperado que, para o desenvolvimento de um produto de *software* com característica de segurança, o seu fornecedor tenha experiência acumulada em projetos similares e, no mínimo, esteja apoiado por rigorosos padrões e práticas previamente estabelecidos. A capacidade demonstrada de desenvolvimento com qualidade por um determinado fornecedor seria então preponderante para o desenvolvimento de produtos de *software* com características de segurança.

A norma ISO 9000-3 destina-se a fornecer orientação quando um contrato entre duas partes exigir a demonstração da capacidade de um fornecedor em desenvolver, fornecer e manter produtos de *software* com qualidade (ISO/IEC, 2004b).

As diretrizes apresentadas a seguir destinam-se a descrever os controles e métodos sugeridos para a produção de *software* que atendam aos requisitos do comprador, evitando-se não conformidades em todos os estágios, desde o desenvolvimento até a manutenção.

2.4.1.1 Estrutura ISO 9000-3

A estrutura apresentada pela norma ISO 9000-3 inclui os seguintes itens que estão sucintamente representados para exemplificar atributos de qualidade de processo que poderão contribuir para a obtenção de um *software* com qualidade.

- Responsabilidade da administração do fornecedor
  - Política da qualidade
  - Responsabilidade e autoridade
  - Recursos e pessoal para verificação
  - Representante da administração
  - Análise crítica pela administração
- Responsabilidade da administração do comprador
- Análises críticas conjuntas

O sistema da qualidade inclui, ainda:

- Documentação do sistema da qualidade
- Plano de qualidade
- Auditorias internas do sistema da qualidade
- Ação corretiva

2.4.1.2 Modelo de Ciclo de Vida ISO 9000-3

Um projeto de desenvolvimento de *software* deve ser organizado de acordo com um modelo de ciclo de vida de *software*. Atividades relacionadas à qualidade devem ser planejadas e implementadas de acordo com a natureza do modelo de ciclo de vida utilizado.

O ciclo de vida representado na tabela 1 é detalhado em (ISO/IEC, 2004b). Pode-se observar que as atividades relacionadas permitem conferir qualidade ao produto de *software* por meio da especificação dos processos requeridos para o seu desenvolvimento.

Tabela 1 – Ciclo de Vida (ISO/IEC, 2004b)

Análise crítica de contrato	
Especificação dos requisitos do comprador	
Planejamento do desenvolvimento	Plano de desenvolvimento
	Controle da execução
	Entrada das fases de desenvolvimento
	Saída das fases de desenvolvimento
	Verificação de cada fase
Planejamento da qualidade	
Projeto e implementação	Projeto
	Implementação
	Análises críticas
Ensaios e validação	Planejamento de ensaios
	Ensaios
	Validação
	Ensaios de campo
Aceitação	Ensaios de aceitação
Cópia, entrega e instalação	
Manutenção	Plano de manutenção
	Identificação da situação inicial do produto
	Organização de suporte
	Tipos de atividades de manutenção
	Registros e relatórios de manutenção
	Procedimentos de liberação

2.4.1.3 Atividades de Suporte

O sistema da qualidade proposto pela ISO 9000-3 pressupõe, ainda, atividades de suporte ao processo de desenvolvimento de um produto de *software*, relacionadas na tabela 2:

Tabela 2 – Atividades de suporte (ISO/IEC, 2004b)

Gestão de configuração	Plano de gestão de configuração
	Identificação e rastreabilidade de configuração
	Controle de alterações
	Relatório da situação da configuração
Controle de documentos	Tipos de documentos
	Aprovação e emissão de documentos
	Alterações em documentos
Registros da qualidade	
Medição	Medição de produtos
	Medição de processos
Regras, práticas e convenções	
Ferramentas e técnicas	
Aquisição	Avaliação de sub-fornecedores
	Validação de produtos adquiridos
Produto de *software* incluído	
Treinamento	

2.4.2 Modelo CMU/SEI CMMI-DEV

O *Software Engineering Institute* da *Carnegie Mellon University* (CMU/SEI) é o líder americano na divulgação e promoção da melhoria de processos de *software*, com o desenvolvimento do CMM (*Capability Maturity Model*), um modelo desenvolvido com patrocínio do governo americano para uso em suas agências, especificamente para o Departamento de Defesa (DoD), maior comprador de *software* do mundo (GUERRA; ALVES, 2004).

Os modelos de Capacidade e Maturidade permitem comparar os processos de uma organização aos padrões definidos no modelo, determinando como as práticas diferem do prescrito no modelo, e também determinar o que deve ser feito para alcançar um conjunto de processos completos, exeqüíveis e repetíveis, visando a qualidade do produto final.

Muitas pessoas encontram dificuldade em aplicar o CMM de forma eficiente e efetiva na prática. O desafio em se utilizar o CMM ou qualquer outro modelo está na sua interpretação (HOFMANN et al, 2007).

Por este motivo, neste trabalho serão explorados os principais elementos e as suas organizações na versão 1.2 do modelo CMMI-DEV (*Capability Maturity Model Integration for Development*), a versão mais recente do modelo CMM existente durante a execução deste trabalho.

2.4.2.1 Categorias e Áreas de Processo

O CMMI-DEV consiste em um conjunto de requisitos baseados nas melhores práticas da indústria, organizados em 22 (vinte e duas) diferentes **Áreas de Processo** agrupadas em 4 (quatro) **Categorias de Processo**, conforme apresentado a seguir.

As **Categorias de Processo** são descritas por (COUTO, 2007):

- A categoria **Gerenciamento de Projeto** é constituída por processos que contêm práticas específicas que podem ser usadas por qualquer pessoa que gerencie qualquer tipo de projeto dentro do ciclo de vida do sistema;
- A categoria do **Processo de Engenharia** é constituída de processos que diretamente especificam, implementam ou mantém o produto, a sua relação com o sistema e a documentação do cliente. Em circunstâncias nas quais o

projeto é composto exclusivamente de *software*, o Processo de Engenharia lida somente com a construção e manutenção do mesmo;

- A categoria **Suporte** é constituída por processos que podem ser empregados por qualquer outro processo, incluindo outros processos de suporte, em várias partes do ciclo de vida do sistema;
- A categoria **Gerência de Processo** é constituída por processos que contêm práticas específicas que podem ser usadas por qualquer pessoa que gerencie qualquer tipo de processo dentro do ciclo de vida do sistema.

As **Áreas de Processo** definidas estão relacionadas na tabela 3 (CMU/SEI, 2006):

Tabela 3 – Áreas de Processo do CMMI-DEV

Categoria	**Área de Processo**
Gerenciamento de Projeto	Planejamento de Projeto (PP)
	Monitoração e Controle de Projeto (PMC)
	Gerenciamento de Acordo com Fornecedores (SAM)
	Gerenciamento Integrado de Projeto - IPPD (IPM)
	Gerenciamento de Risco (RSKM)
	Gerenciamento Quantitativo de Projeto (QPM)
Engenharia	Engenharia de Requisitos (REQM)
	Desenvolvimento de Requisitos (RD)
	Solução Técnica (TS)
	Integração de Produto (PI)
	Verificação (VER)
	Validação (VAL)
Suporte	Gerência de Configuração (CM)
	Garantia de Qualidade de Processo e Produto (PPQA)
	Medição e Análise (MA)
	Análise de Decisão e Resolução (DAR)
	Análise de Causas e Resolução (CAR)
Gerenciamento de Processo	Foco em Processos Organizacionais (OPF)
	Definição de Processos Organizacionais - IPPD (OPD)
	Treinamento Organizacional (OT)
	Desempenho de Processos Organizacionais (OPP)
	Implantação e Inovações na Organização (OID)

A cada Área de Processo correspondem Metas Específicas - SG (*Specific Goals*) e Práticas Específicas - SP (*Specific Practices*), que são detalhadas em (CMU/SEI, 2006) e (CHRISSIS; KONRAD; SHRUM, 2007).

2.4.2.2 Níveis de Capacidade

O progresso de uma organização em definir e melhorar os seus processos é medido com o uso dos números de 0 a 5, representando os **Níveis de Capacidade de Processo** definidos como na tabela 4.

Tabela 4 – Níveis de Capacidade do CMMI-DEV

Nível de Capacidade	Característica
0	Os Processos executados são Incompletos
1	Os Processos são Executados ao acaso (*ad hoc*)
2	Os Processos são Gerenciados
3	Os Processos são Institucionalizados
4	Os Processos são Quantitativamente Gerenciados
5	Os Processos são Otimizados

Aos Níveis de Capacidade de Processo, correspondem Metas Genéricas (*Generic Goals*) e Práticas Genéricas (*Generic Practices*) relacionadas na tabela 5 (CMU/SEI, 2006). À cada uma das Áreas de Processos apresentadas na tabela 3 é atribuído um Nível de Capacidade, conforme o atendimento às Metas Genéricas é efetuado.

Tabela 5 – Metas e Práticas Genéricas CMMI-DEV

Metas Genéricas (GG)		
	Práticas Genéricas (GP)	
GG 1	Atingir as Metas Específicas	
	GP 1.1	Executar as Práticas Específicas
GG 2	Institucionalizar um Processo Gerenciado	
	GP 2.1	Estabelecer uma política organizacional
	GP 2.2	Planejar o processo
	GP 2.3	Providenciar recursos
	GP 2.4	Atribuir responsabilidades
	GP 2.5	Treinar pessoas
	GP 2.6	Gerenciar configuração
	GP 2.7	Identificar e envolver os interessados relevantes
	GP 2.8	Monitorar e controlar o processo
	GP 2.9	Avaliar objetivamente a aderência
	GP 2.10	Revisar o andamento com a alta gerência
GG 3	Institucionalizar um Processo Definido	
	GP 3.1	Estabelecer um processo definido
	GP 3.2	Coletar informações de melhoria
GG4	Institucionalizar um Processo Gerenciado Quantitativamente	
	GP 4.1	Estabelecer objetivos quantitativos para o processo
	GP 4.2	Estabilizar o desempenho de sub-processos
GG5	Institucionalizar um Processo em Otimização	
	GP 5.1	Garantir a Melhoria Contínua do Processo
	GP 5.2	Corrigir a Causa Raiz dos Problemas

Existem duas formas de se representar a medição da capacidade de processos: a representação em estágios ou representação "estagiada" (*staged representation*), definida nas primeiras versões do CMM, e a representação contínua (*continuous representation*) (CHRISSIS; KONRAD; SHRUM, 2007).

2.4.2.3 Representação em Estágios do CMMI-DEV

Na representação em estágios são especificados conjuntos de áreas de processo ordenados em quatro Níveis de Maturidade, sendo predefinidas quais áreas de processo devem ser satisfatoriamente avaliadas para atingir cada um dos níveis (do 2 ao 5), apresentados na tabela 6.

Tabela 6 – Níveis de Maturidade CMMI-DEV

Nível de Maturidade	Característica
2	Os Processos são Gerenciados
3	Os Processos são Institucionalizados
4	Os Processos são Quantitativamente Gerenciados
5	Os Processos são Otimizados

Nos Níveis de Maturidade 2 e 3, todas as áreas de Processos relacionadas para esses níveis devem ser avaliadas no Nível de Capacidade correspondente ou superior. Para os Níveis de Maturidade 4 ou 5, todas as Áreas de Processo relacionadas para esses níveis devem estar no Nível de Capacidade 3 ou superior.

A figura 2 representa os elementos do CMMI-DEV na representação em estágios. Nota-se que os níveis de maturidade estão relacionados às Áreas de Processo de interesse (CHRISSIS; KONRAD; SHRUM, 2007).

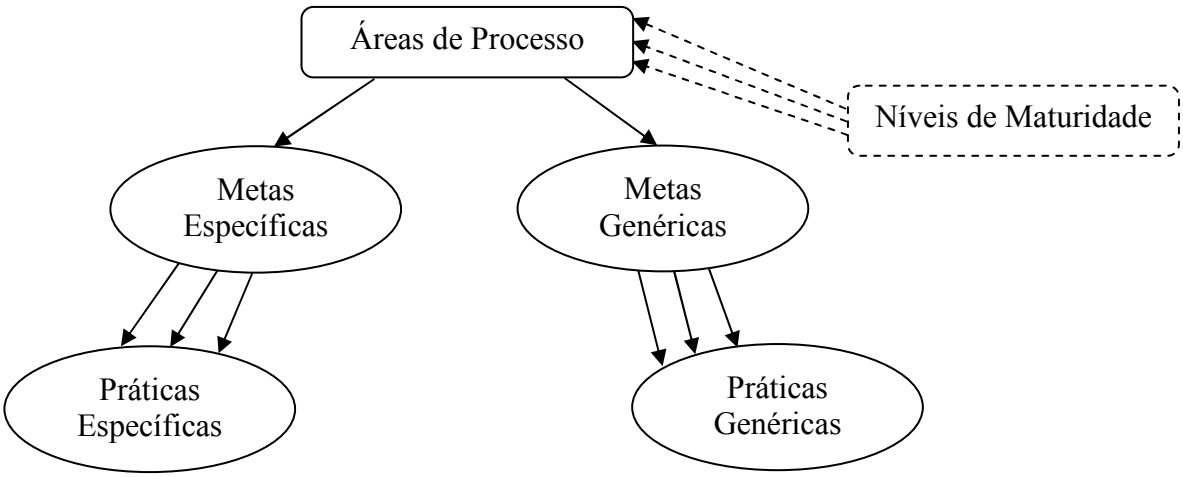

Figura 2 – Representação em Estágios do CMMI-DEV (CHRISSIS; KONRAD; SHRUM, 2007)

2.4.2.4 Representação Contínua do CMMI-DEV

Na representação contínua, é facultada à organização a escolha de quais Áreas de Processo deverão ser avaliadas, com base em seus objetivos de negócio e oportunidades de melhoria. Neste caso, o Nível de Capacidade é avaliado em cada uma dessas áreas.

A figura 3 representa os elementos do CMMI na representação contínua. Os níveis de capacidade estão relacionados às metas genéricas aplicadas a cada área de processo.

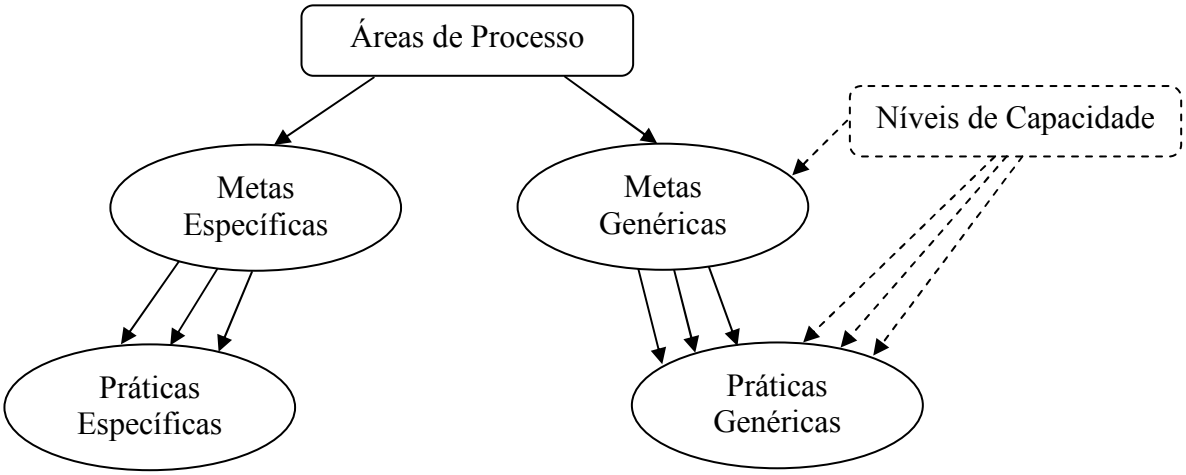

Figura 3 – Representação Contínua do CMMI-DEV (CHRISSIS; KONRAD; SHRUM, 2007)

2.5 Segurança como um Atributo da Qualidade de Produto

O enfoque deste trabalho está diretamente relacionado à qualidade do processo de desenvolvimento de *software*; no entanto, a apresentação da qualidade do produto de *software* é importante para que o contexto do trabalho seja completamente compreendido.

Para ilustrar esta abordagem, serão citadas as características de qualidade conforme classificação presente na norma ISO/IEC 9126-1 "*Information Technology - Software Product Quality - Part 1: Quality Model*" (ISO/IEC, 1991) e também conforme modelos mais sofisticados que incluem a segurança como um atributo da qualidade do produto de *software*.

2.5.1 Norma ISO/IEC 9126-1

Apesar da qualidade de produto de *software* não ser o enfoque principal deste trabalho, não se pode deixar de localizar o contexto da qualidade de produto relativa aos artefatos[1] e ao produto de *software*.

Os modelos de qualidade de *software*, como apresentados na literatura e em normas, utilizam características do *software* para avaliar a sua qualidade. Tipicamente a avaliação da qualidade de *software* é realizada sobre os artefatos de *software*, conforme são obtidos durante o seu processo de desenvolvimento.

Para exemplificação desta abordagem, são citadas as características de qualidade conforme classificadas pela norma ISO/IEC 9126-1 "*Information Technology - Software Product Quality- Part 1: Quality Model*".

Nesta norma são definidas três abordagens para a qualidade de *software* em um modelo de qualidade dividido em duas partes: as abordagens chamadas de **qualidade interna** e **qualidade externa** são definidas na primeira parte, enquanto que na segunda parte é definido um conjunto de características de qualidade referente à abordagem chamada de **qualidade em uso**.

2.5.1.1 Qualidade Interna e Qualidade Externa

A **qualidade interna** é intrínseca ao produto de *software* e pode observada por meio de medidas diretas sobre o código fonte, especificação ou documentação, desde as fases iniciais do desenvolvimento do produto de *software*, apresentando maior consistência conforme se atinge as fases finais do desenvolvimento.

[1] Artefato (*work product*): qualquer informação coesa e persistente produzida como conseqüência da ação de uma ou mais tarefas de engenharia de software (PRESSMAN, 2001). Pode não ser fornecido ao usuário ou contratante, ao contrário do produto de software.

A **qualidade externa** representa o comportamento do *software* e pode ser observada por meio de testes, geralmente nas fases mais avançadas do desenvolvimento do produto de *software*, utilizando recursos mais complexos típicos de ambientes de testes.

As características de qualidade internas e externas definidas por (ISO/IEC, 1991) são relacionadas na tabela 7.

Tabela 7 – Qualidade Interna e Externa (ISO/IEC, 1991)

Características de qualidade	**Sub-características de qualidade**
Funcionalidade	Adequação
	Acurácia
	Interoperabilidade
	Inviolabilidade
	Conformidade com normas de funcionalidade
Confiabilidade	Maturidade
	Tolerância a falhas
	Recuperabilidade
	Conformidade com as normas de confiabilidade
Usabilidade	Inteligibilidade
	Capacidade de aprendizado
	Operacionalidade
	Atratividade
	Conformidade com as normas de usabilidade
Manutenibilidade	Analisabilidade
	Modificabilidade
	Estabilidade
	Testabilidade
	Conformidade com as normas de Manutenibilidade
Portabilidade	Adaptabilidade
	Instalabilidade
	Coexistência
	Capacidade para substituição
	Conformidade com as normas de portabilidade

2.5.1.2 Qualidade em Uso

A **qualidade em uso** é geralmente avaliada pelo contratante ou usuário final do produto de *software*, em conformidade com os objetivos especificados para o *software*. Admite a detecção de necessidades implícitas não observadas pelo desenvolvedor na elaboração da especificação de requisitos de *software*.

As características de qualidade em uso definidas por (ISO/IEC, 1991) são relacionadas na tabela 8.

Tabela 8 – Qualidade em uso (ISO/IEC, 1991)

Características de Qualidade
Efetividade
Produtividade
Segurança
Satisfação

A definição de **segurança** apresentada neste modelo é genérica, incluindo a segurança (*safety*) na abordagem deste trabalho, que está relacionada à ausência de danos às pessoas, propriedade e ambiente, e também a segurança (*security*) presente principalmente nos ambientes de negócios (sistemas bancários e de comércio eletrônico).

Uma observação particular deve ser feita em relação a esta definição de segurança. A norma ISO/IEC 9126-1 admite que os riscos decorram usualmente de deficiências na funcionalidade, confiabilidade, usabilidade ou manutenibilidade, que são características da qualidade interna e qualidade externa do *software*, conforme definidas pela norma e que, portanto, podem ser observadas por meio de indicadores destas características.

2.5.2 Outras Abordagens para Qualidade de Produto

Em modelos mais complexos e detalhados do que o apresentado na norma ISO/IEC 9126-1 pode-se encontrar a segurança novamente representada como um atributo da qualidade, porém melhor detalhada, mas ainda assim como um atributo percebido com o uso do sistema, conforme representado na Figura 4 (FIRESMITH, 2005).

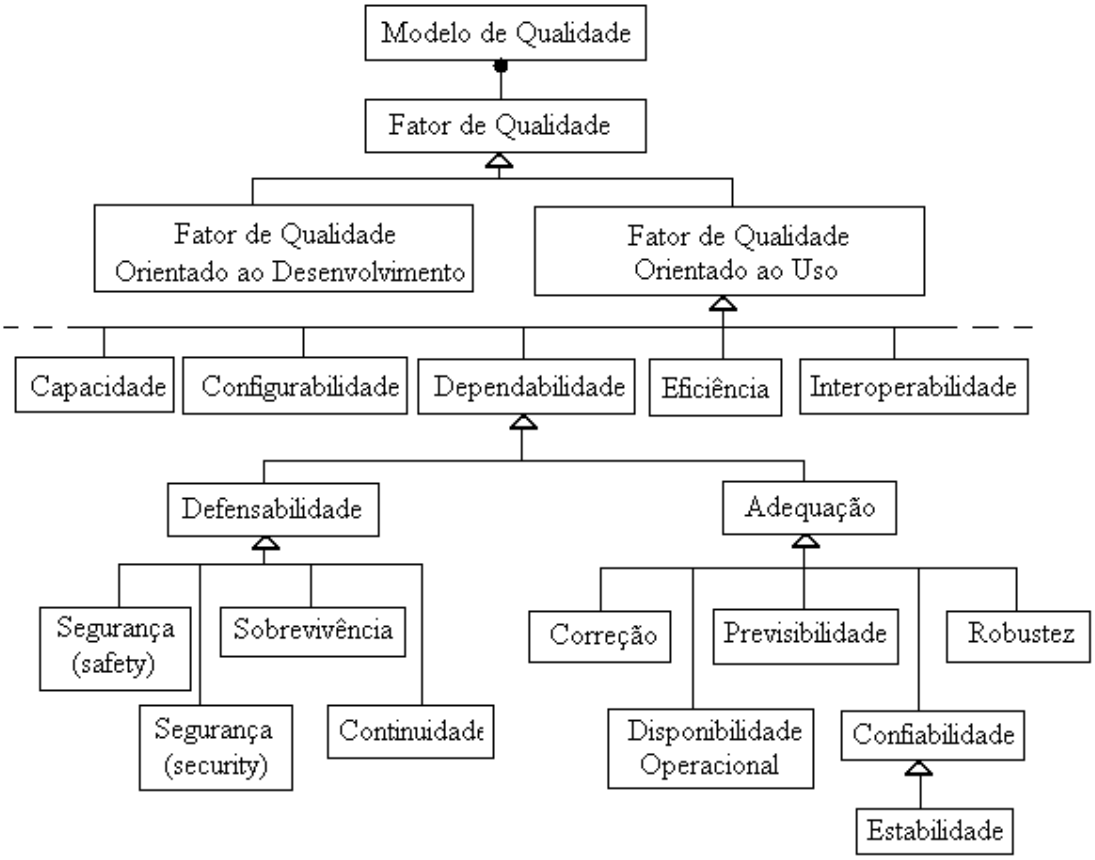

Figura 4 – Segurança como um atributo da qualidade (FIRESMITH, 2005)

Neste caso, a segurança (*safety*) ainda pode ser detalhada nos atributos de interesse deste trabalho, conforme ilustra a figura 5 (FIRESMITH, 2003).

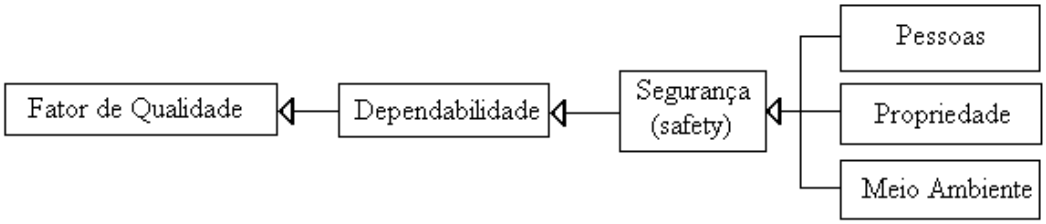

Figura 5 – Atributos da qualidade relativos à segurança (FIRESMITH, 2003)

2.5.3 Uma Abordagem para Qualidade de Produto com Enfoque na Segurança

Uma abordagem apropriada para o emprego de normas e modelos de qualidade de produtos de *software*, para se avaliar a segurança de sistemas críticos, pode ser encontrada em (PÁSCOA, 2002), com o levantamento de fatores e sub-fatores comuns aos modelos de qualidade e aos modelos de segurança.

Nesse trabalho o autor apresenta em detalhe os elementos encontrados em modelos de qualidade e em diversos modelos de segurança, e realiza uma organização padronizada em fatores e sub-fatores, com o objetivo de estabeler uma correlação entre esses elementos.

Por intermédio desse processo, foi possível se demonstrar a implicação direta dos seguintes fatores e sub-fatores de qualidade na segurança de um sistema crítico: (PÁSCOA, 2002)

- Funcionalidade
    - Acurácia
    - Capacidade
    - Comportamento Temporal
    - Inviolabilidade

- Confiabilidade
    - Completeza
    - Consistência
    - Corretude
    - Inteligibilidade
    - Padronização de Comunicação
    - Padronização de Dados
    - Previsibilidade
    - Rastreabilidade
    - Recuperabilidade
    - Simplicidade
    - Tolerância a Falhas
    - Verificabilidade

- Manutenibilidade
    - Analisabilidade
    - Estabilidade
    - Estruturação
    - Instrumentação
    - Modularidade
    - Testabilidade

- Segurança Intrínseca
    - Mecanismos de Segurança

- Exclusão de Riscos
    - Coexistência
    - Generalidade
    - Interoperabilidade
    - Portabilidade
    - Reusabilidade

2.6 Confiabilidade de Software

A confiabilidade de *software* pode ser definida como a "*probabilidade de operação livre de falhas por um período de tempo especificado em um determinado ambiente*" (ANSI/IEEE, 1991). A confiabilidade é um dos atributos da qualidade de *software*, uma propriedade multidimensional que inclui outros fatores de satisfação do cliente tais como funcionalidade, facilidade de uso, desempenho, capacidade e documentação, bem como facilidades de suporte, de instalação e de manutenção (GRADY, CASWELL; 1987) (GRADY, CASWELL; 1992).

A confiabilidade de *software* é geralmente aceita como o fator principal da sua qualidade, pois quantifica as falhas de *software* – que podem tirar de operação um poderoso sistema ou até mesmo trazer riscos às pessoas e patrimônio (LYU, 1996).

Os métodos mais difundidos para a avaliação da confiabilidade de *software*, tal como o descrito em "*Software Reliability Engineering*" (MUSA, 1999), são baseados na observação de falhas do produto terminado, sustentada por análise estatística. Estes métodos constituem uma forma de medir a confiabilidade do produto, pois são baseados na observação direta de seu comportamento. As importantes desvantagens destas abordagens são (DALE, 1990):

- Estão preocupadas puramente com a medida da confiabilidade, enquanto outras informações sobre, por exemplo, os métodos que foram utilizados no desenvolvimento do produto, são ignorados; e
- Podem ser utilizadas sobre módulos de *software*, ou quando o produto final existe, portanto sua aplicação só pode ser iniciada a partir da obtenção de dados durante a fase de testes do desenvolvimento.

Ademais, o tempo necessário para se obter medidas de confiabilidade sobre produtos ou protótipos pode ser muito elevado em função da ordem de grandeza dos requisitos de segurança de sistemas críticos que normalmente superam milhares de anos.

Uma alternativa pesquisada para a obtenção de *software* de alta confiabilidade é a especificação e análise dos processos de desenvolvimento adotados em um projeto, em conformidade com as normas técnicas adequadas a aplicação, além de modelos de ampla aceitação.

Adotando-se uma abordagem deste tipo, a avaliação da confiabilidade deve ser realizada sobre os produtos intermediários ou artefatos de cada fase do processo de desenvolvimento, antes de se obter o produto final. A avaliação, inclusive pode ser feita a partir da análise das especificações do sistema, que não devem apresentar erros para a obtenção de *software* confiável.

2.7 Emprego de Técnicas e Modelos de Engenharia de Software no Desenvolvimento de Sistemas Críticos

Segundo (LAHOZ; BURGARELI; MOURA, 2004), a adoção de boas práticas de gerenciamento de desenvolvimento de *software* pode prover informações importantes relativas à habilidade que uma organização possui para produzir um *software* confiável e de boa qualidade. Por isso, a qualidade do produto de *software* deve estar diretamente relacionada à qualidade dos processos de desenvolvimento que foram utilizados para sua produção. Assim, medidas de processo devem ser tomadas com o intuito de prover informações que revelem a habilidade de uma organização em produzir *software* confiável e de boa qualidade.

Segundo o livro de fundamentos de engenharia de gerenciamento de segurança, denominado "*Yellow Book*" (RAILTRACK, 2000), as organizações devem realizar projetos relacionados à segurança seguindo processos sistemáticos que empregam boas práticas de engenharia. A segurança depende das pessoas que realizam o trabalho de engenharia, mas também depende da forma com que o trabalho é realizado e das ferramentas que são utilizadas.

2.8 Considerações Finais do Capítulo

Os conceitos e definições apresentados neste capítulo, procuraram situar o leitor quanto a definição de segurança utilizada na presente dissertação, e a importância de se considerar todo o processo de desenvolvimento dos *softwares* utilizados em sistemas críticos.

A discussão sobre os desafios e conceitos bem estabelecidos da área de engenharia de segurança oferece uma perspectiva aos profissionais com especialidade em desenvolvimento de *software*. Espera-se que, em uma organização caracterizada por sua cultura de segurança, este conhecimento esteja sedimentado entre os seus profissionais.

Da mesma forma, a apresentação da modelagem de processos de *software* com ênfase em qualidade, para especialistas em sistemas críticos de segurança, possibilita a exploração de uma importante ferramenta em constante evolução.

No próximo capítulo é abordado um modelo específico de qualidade de processos de *software* para o contexto brasileiro.

3 Modelo de Referência MPS.BR

Neste capítulo é apresentado o Modelo de Referência MR-MPS (Melhoria de Processo de *Software* Brasileiro), de acordo com seu Guia Geral na versão 1.2, coordenado pela Associação para Promoção da Excelência do *Software* Brasileiro (SOFTEX), contando com apoio do Ministério da Ciência e Tecnologia (MCT), da Financiadora de Estudos e Projetos (FINEP) e do Banco Interamericano de Desenvolvimento (BID) (WEBER, 2006) (MPS.BR, 2007a).

O MR-MPS é similar e compatível com o modelo CMMI-DEV, e aderente às normas ISO/IEC 12207 "Tecnologia da Informação - Processos do Ciclo de Vida de *Software*" (*Information Technology - Software Life Cycle Processes*) (ISO/IEC, 1995) e ISO/IEC 15504 "Tecnologia da Informação - Validação de Processo" (*Information Technology - Process Assessment*) (ISO/IEC, 2004a).

No período inicial do Projeto MPS.BR (Dezembro de 2003 à Dezembro de 2006), foram alcançados dois grandes resultados (WEBER, 2006):

i) Tecnicamente foram criados e vêm sendo aprimorados, anualmente, um Modelo de Referência (MR-MPS) e um Método de Avaliação (MA-MPS), o que não é algo trivial em qualquer lugar do mundo;

ii) Do ponto de vista do mercado, houve melhoria dos processos de *software* com a implementação do MR-MPS em cerca de 120 empresas em todas as regiões do país, das quais 17 unidades organizacionais foram bem sucedidas em avaliações formais MA-MPS.

As previsões de resultados previstos por (WEBER, 2006) são:

a) Até Dezembro de 2007 cerca de 80 empresas com avaliação oficial MAMPS e até Dezembro de 2008, cerca de 160 empresas avaliadas oficialmente;

b) Até Dezembro de 2006, foram credenciadas 15 Instituições Implementadoras, que atuam como consultorias e facilitadoras, em todas as regiões do país, exceto na Região NO, mediante convênio assinado com a SOFTEX. Até Dezembro de 2008, espera-se exceder muito a meta original: 20 Instituições Implementadoras, em todas as regiões do país; e

c) Até Dezembro de 2006, duas Instituições Avaliadoras demonstraram capacidade para avaliar o MPS.BR em organizações que implementaram o Modelo de Referência MR-MPS, seguindo o Método de Avaliação MA-MPS, conforme convênio assinado com a SOFTEX. Até Dezembro de 2008, espera-se exceder a meta original: 15 (quinze) Instituições Avaliadoras, em todas as regiões do país.

Em (SOFTEX, 2004) são apresentados os sete diferenciais do MR-MPS:

- Os sete níveis de maturidade possibilitam uma implementação mais gradual e adequada à micro, pequena e média empresa; além disto, as avaliações considerando mais níveis permitem uma maior visibilidade dos resultados e melhoria de processo com prazos mais curtos;
- Compatibilidade plena com CMMI e SPICE ISO/IEC 15504 (ISO/IEC, 2004a), (modelo “dois em um”);
- Criado para a realidade da empresa Brasileira (foco na micro, pequena e média empresa de *software*);

- Custo acessível em reais;
- Avaliação periódica das empresas (de dois em dois anos);
- Grande potencial de replicabilidade no Brasil e de exportação de serviços com alto valor agregado; e
- Forte interação Universidade-Empresa, catalisador do desenvolvimento tecnológico e de negócios

3.1 A Representação em Estágios do MR-MPS

Níveis de Maturidade de A ao G estão definidos no MR-MPS, conforme representação apresentada na figura 6. Cada nível de maturidade é identificado por um conjunto de Processos e pelos Atributos de Processos, da mesma forma que o CMMI-DEV na sua representação em estágios. As setas da figura 6 indicam a melhoria progressiva a medida que se passa de um nível de maturidade para o próximo, partindo-se do nível G até se chegar ao nível A.

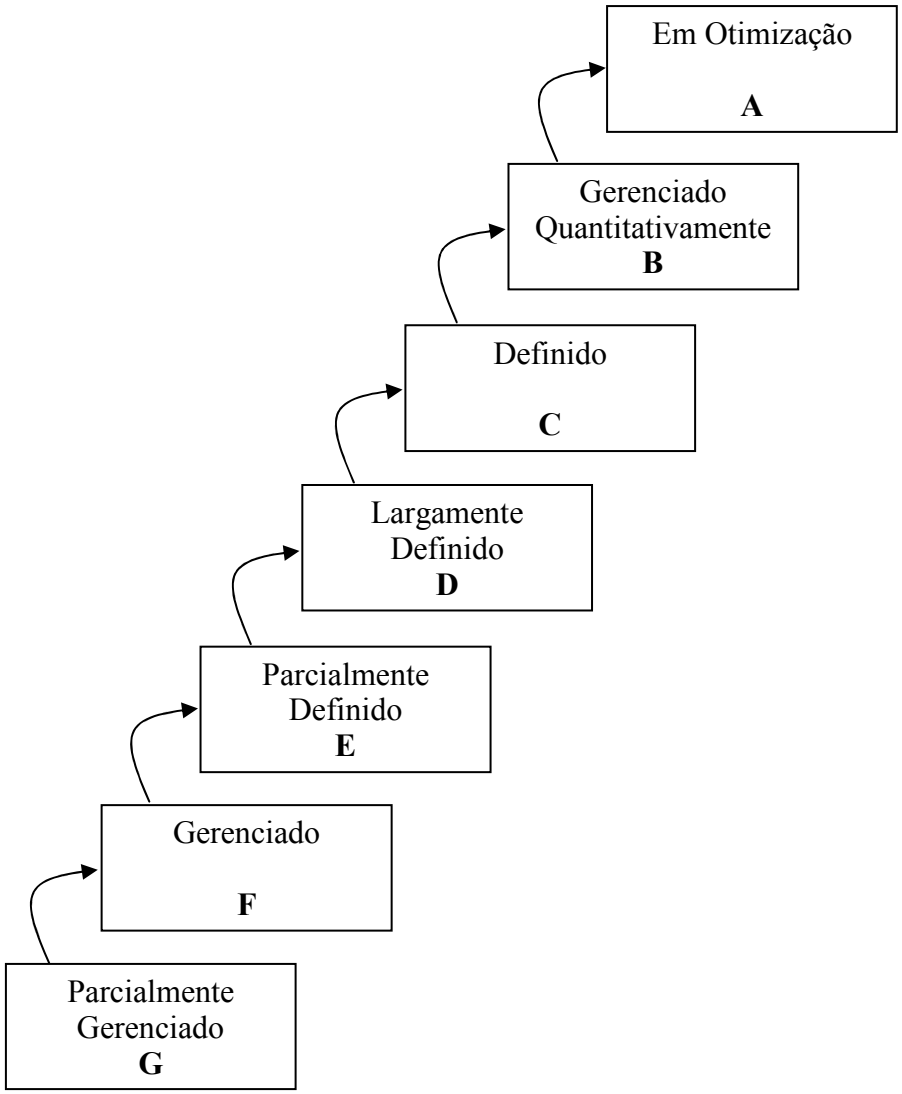

Figura 6 – Níveis de Maturidade do MR-MPS

Assim como no modelo CMMI, os Níveis de Maturidade (*Maturity Levels*) são determinados por um conjunto de Áreas de Processo (*Process Areas*) que devem ter atingido os Níveis de Capacidade (*Capability Levels*) correspondentes.

3.1.1 Níveis de Maturidade do MR-MPS

Os Níveis de Maturidade do MR-MPS são determinados pelo conjunto de **Áreas de Processos** (**PA**) relacionadas a seguir e pelos **Atributos do Processo** (**AP**). Os Atributos de Processo, no MR-MPS, são equivalentes às metas genéricas do CMMI. Deve-se notar que os Atributos de Processo definido para cada Nível de Maturidade devem ser aplicados a todos os conjuntos de Processos dos níveis inferiores.

Na tabela 9 são relacionadas as áreas de processo e seus atributos, para cada nível de maturidade definido pelo MR-MPS. Os Atributos de Processos (AP) presentes nessa tabela são descritos nos próximos itens.

Tabela 9 – Áreas de Processos e Atributos de Processos do MR-MPS

Nível de Maturidade	Áreas de Processos (PA)	Atributos de Processos (AP)
A	Análise de Causas de Problemas e Resolução – ACP	AP 1.1, AP 2.1, AP 2.2, AP 3.1, AP3.2, AP 4.1, AP 4.2, AP 5.1 e AP 5.2
B	Gerência de Projetos – GPR (evolução(*1))	AP 1.1, AP 2.1, AP 2.2, AP 3.1 e AP 3.2, AP 4.1 e AP 4.2
C	Gerência de Riscos – GRI	AP 1.1, AP 2.1, AP 2.2, AP 3.1 e AP 3.2
	Desenvolvimento para Reutilização – DRU	
	Análise de Decisão e Resolução – ADR	
	Gerência de Reutilização – GRU (evolução(*1))	
D	Verificação – VER	AP 1.1, AP 2.1, AP 2.2, AP 3.1 e AP 3.2
	Validação – VAL	
	Projeto e Construção do Produto – PCP	
	Integração do Produto – ITP	
	Desenvolvimento de Requisitos – DRE	
E	Gerência de Projetos – GPR (evolução(*1))	AP 1.1, AP 2.1, AP 2.2, AP 3.1 e AP 3.2
	Gerência de Reutilização – GRU	
	Gerência de Recursos Humanos – GRH	
	Definição do Processo Organizacional – DFP	
	Avaliação e Melhoria do Processo Organizacional – AMP	
F	Medição – MED	AP 1.1, AP 2.1 e AP 2.2
	Garantia da Qualidade – GQA	
	Gerência de Configuração – GCO	
	Aquisição – AQU	
G	Gerência de Requisitos – GRE	AP 1.1 e AP 2.1
	Gerência de Projetos – GPR	

(*1) Para o modelo MR-MPS, o termo "evolução" aqui colocado significa que, para um nível de maturidade superior, espera-se que para a Área de Processo em questão sejam acrescentadas práticas específicas adicionais em relação ao nível de maturidade inferior onde esta área primeiramente aparece.

3.2 A Representação Contínua no MR-MPS

No modelo MR-MPS são definidos **Atributos de Processos** (AP) e **Resultados Esperados dos Atributos de Processos** (RAP) que são, respectivamente, equivalentes às Metas Genéricas e Práticas Genéricas do modelo CMMI.

Em sua representação contínua, no modelo MR-MPS os **Níveis de Capacidade** são determinados para cada uma das **Áreas de Processo (PAs)**, de acordo com os respectivos

Atributos de Processos (APs), da mesma forma que no modelo CMMI. A figura 7 apresenta os 6 (seis) níveis de capacidade definidos pelo modelo MR-MPS.

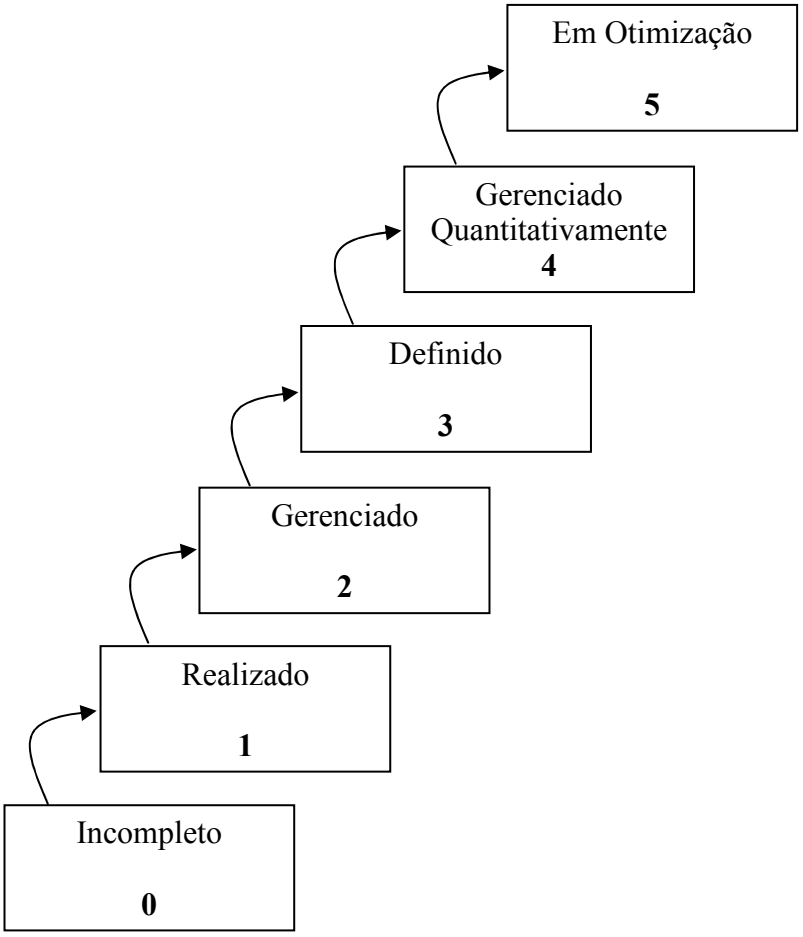

Figura 7 – Níveis de Capacidade do MR-MPS

Assim como no CMMI, a decisão pelo uso da representação contínua implica na seleção das áreas de processo e níveis de capacidade desejados para cada uma dessas áreas (variando de 0 a 5), com base nos objetivos de melhoria de processos da organização, conforme exemplificado na figura 8.

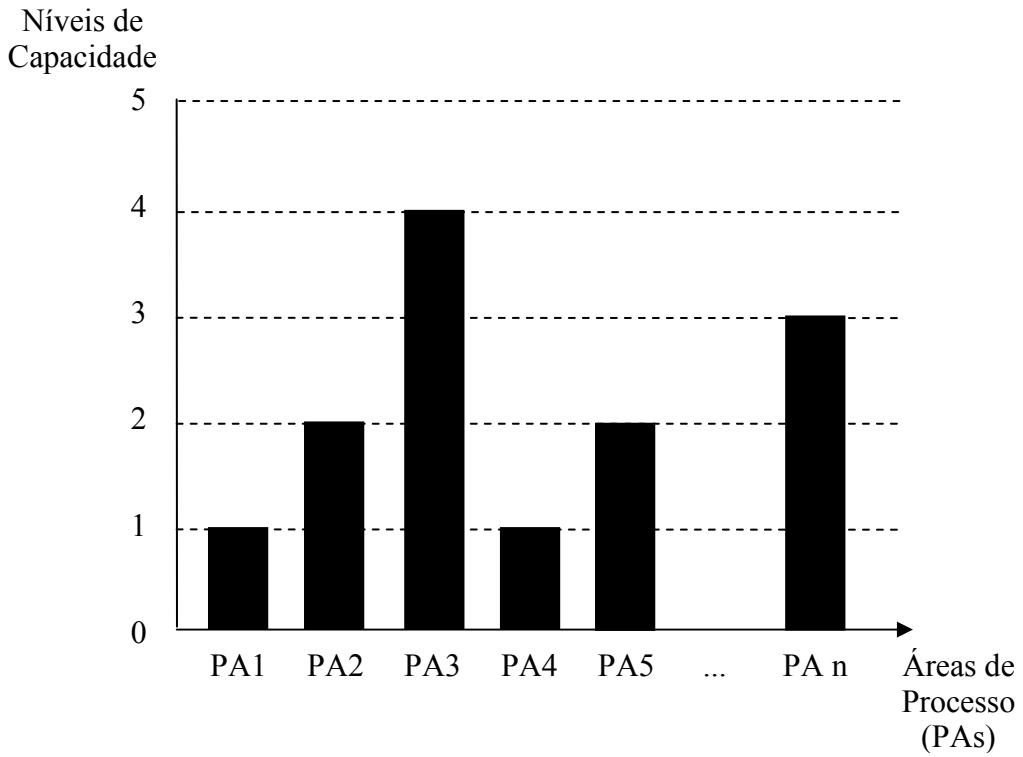

Figura 8 – Níveis de Capacidade por Áreas de Processo (PAs)

O termo Perfil de Capacidade é atribuído a um conjunto de Níveis de Capacidade definidos para cada Área de Processo em que se busca a melhoria ou a avaliação dos processos de *software*.

3.3 Níveis de Capacidade e Atributos de Processos no MR-MPS

Para cada Nível de Capacidade de processo no modelo MR-MPS, em sua representação contínua, correspondem Atributos de Processos, conforme o representado na tabela 10. Nota-se que em um determinado nível de capacidade, estão presentes os Atributos de Processos do próprio nível e dos níveis anteriores. Assim, para o Nível de Capacidade 2, estão presentes os Atributos de Processo do níveis de capacidade 1 (AP1.1) e 2 (AP2.1 e AP2.2). Isso mostra a característica evolutiva dos níveis de capacidade dos processos no modelo MR-MPS.

Tabela 10 – Atributos de Processo (AP) para cada Nível de Capacidade

Nível de Capacidade	Atributos de Processo (APs)
0	Nenhum
1	AP1.1
2	AP1.1, AP2.1, AP2.2
3	AP1.1, AP2.1, AP2.2, AP3.1, AP3.2
4	AP1.1, AP2.1, AP2.2, AP3.1, AP3.2, AP4.1, AP4.2
5	AP1.1, AP2.1, AP2.2, AP3.1, AP3.2, AP4.1, AP4.2, AP5.1, AP5.2

Na tabela 11 estão relacionados os Atributos de Processos (APs) e os Resultados Esperados dos Atributos de Processos (RAPs), conforme o definido no modelo MPS-BR (MPS-BR, 2007a).

Tabela 11 – Resultados Esperados dos Atributos do Processo (RAPs) (MPS-BR, 2007a)

AP 1.1	**O processo é executado:** **Este atributo é uma medida do quanto o processo atinge o seu propósito.**	
	RAP 1	O processo atinge seus resultados definidos.
AP 2.1	**O processo é gerenciado:** **Este atributo é uma medida de quanto a execução do processo é gerenciada.**	
	RAP 2	Existe uma política organizacional estabelecida e mantida para o processo.
	RAP 3	A execução do processo é planejada.
	RAP 4	A execução do processo é monitorada e ajustes são realizados para atender aos planos (*OBS: Na representação por estágios, somente para o Nível G*).
		Medidas são planejadas e coletadas para monitoração da execução do processo (*OBS: Na representação por estágios, a partir do Nível F*).
	RAP 5	Os recursos necessários para a execução do processo são identificados e disponibilizados.
	RAP 6	As pessoas que executam o processo são competentes em termos de formação, treinamento e experiência.
	RAP 7	A comunicação entre as partes interessadas no processo é gerenciada de forma a garantir o seu envolvimento no projeto.
	RAP 8	Métodos adequados para monitorar a eficácia e adequação do processo são determinados.
	RAP 9	A aderência dos processos executados às descrições de processo, padrões e procedimentos é avaliada objetivamente e são tratadas as não conformidades (*OBS: Na representação por estágios, a partir do Nível F*).

AP 2.2	**Os produtos de trabalho do processo são gerenciados:** **Este atributo é uma medida do quanto os produtos de trabalho produzidos pelo processo são gerenciados apropriadamente.**	
	RAP 10	Requisitos para documentação e controle dos produtos de trabalho são estabelecidos.
	RAP 11	Os produtos de trabalho são documentados e colocados em níveis apropriados de controle.
	RAP 12	Os produtos de trabalho são avaliados objetivamente com relação aos padrões, procedimentos e requisitos aplicáveis e são tratadas as não conformidades.
AP 3.1	**O processo é definido:** **Este atributo é uma medida do quanto um processo padrão é mantido para apoiar a implementação do processo definido.**	
	RAP 13	Um processo padrão é definido, incluindo diretrizes para sua adaptação para o processo definido.
	RAP 14	A seqüência e interação do processo padrão com outros processos são determinadas.
AP 3.2	**O processo está implementado:** **Este atributo é uma medida do quanto o processo padrão é efetivamente implementado como um processo definido para atingir seus resultados.**	
	RAP 15	Dados apropriados são coletados e analisados, constituindo uma base para o entendimento do comportamento do processo, para demonstrar a adequação e a eficácia do processo, e avaliar onde pode ser feita a melhoria contínua do processo.
AP 4.1	**O processo é medido:** **Este atributo é uma medida do quanto os resultados de medição são usados para assegurar que o desempenho do processo apóia o alcance dos objetivos de desempenho relevantes como apoio aos objetivos de negócio definidos.**	
	RAP 16	As necessidades de informação requeridas para apoiar objetivos de negócio relevantes da organização e dos projetos são identificadas.
	RAP 17	A partir do conjunto de processos padrão da organização e das necessidades de informação são selecionados os processos e/ou elementos do processo que serão objeto de análise de desempenho.
	RAP 18	Objetivos de medição do processo e/ou sub-processo são derivados das necessidades de informação.
	RAP 19	Objetivos quantitativos de qualidade e de desempenho dos processos e/ou sub-processos são derivados das necessidades de informação.
	RAP 20	Medidas e a freqüência de realização das medições são identificadas e definidas de acordo com os objetivos de medição do processo/sub-processo e os objetivos quantitativos de qualidade e de desempenho do processo.
	RAP 21	Resultados das medições são coletados, analisados e reportados para monitorar o atendimento dos objetivos quantitativos de qualidade e de desempenho do processo/sub-processo.
	RAP 22	Resultados de medição são utilizados para caracterizar o desempenho do processo/sub-processo.

AP 4.2	**O processo é controlado:** **Este atributo é uma medida do quanto o processo é controlado estatisticamente para produzir um processo estável, capaz e previsível dentro de limites estabelecidos.**	
	RAP 23	Técnicas de análise e de controle de desempenho são identificadas e aplicadas quando necessário.
	RAP 24	Limites de controle de variação são estabelecidos para o desempenho normal do processo.
	RAP 25	Dados de medição são analisados com relação a causas especiais de variação.
	RAP 26	Ações corretivas são realizadas para tratar causas especiais de variação.
	RAP 27	Limites de controle são redefinidos, quando necessário, seguindo as ações corretivas.
	RAP 28	Modelos de desempenho do processo são estabelecidos e mantidos.
AP 5.1	**O processo é objeto de inovações:** **Este atributo é uma medida do quanto as mudanças no processo são identificadas a partir da análise de causas comuns de variação do desempenho e da investigação de enfoques inovadores para a definição e implementação do processo.**	
	RAP 29	Objetivos de melhoria do processo são definidos de forma a apoiar os objetivos de negócio relevantes.
	RAP 30	Dados adequados são analisados para identificar causas comuns de variação no desempenho do processo.
	RAP 31	Dados adequados são analisados para identificar oportunidades para aplicar melhores práticas e inovações.
	RAP 32	Oportunidades de melhoria derivadas de novas tecnologias e conceitos de processo são identificadas.
	RAP 33	Uma estratégia de implementação é estabelecida para alcançar os objetivos de melhoria do processo.
AP 5.2	**O processo é otimizado continuamente:** **Este atributo é uma medida do quanto as mudanças na definição, gerência e desempenho do processo têm impacto efetivo para o alcance dos objetivos relevantes de melhoria do processo.**	
	RAP 34	O impacto de todas as mudanças propostas é avaliado com relação aos objetivos do processo definido e do processo padrão.
	RAP 35	A implementação de todas as mudanças acordadas é gerenciada para assegurar que qualquer alteração no desempenho do processo seja entendida e sejam tomadas as ações pertinentes.
	RAP 36	A efetividade das mudanças, levando em conta o seu desempenho resultante, é avaliada com relação aos requisitos do produto e objetivos do processo, para determinar se os resultados são devidos a causas comuns ou a causas especiais.

3.4 Áreas de Processos Definidas no MR-MPS

A descrição das Áreas de Processos (PAs) definidas pelo modelo MR-MPS é necessária para dar subsídio aos julgamentos sobre a relevância de cada uma das áreas em projetos de sistemas críticos de segurança, conforme apresentado no estudo de caso deste trabalho.

No ANEXO A, são relacionadas as Áreas de Processo (PAs), os seus propósitos, e as respectivas Práticas Específicas definidas pelo modelo MR-MPS, de forma sucinta e adequada à emissão de julgamentos por especialistas na área de segurança.

A síntese destes principais componentes do modelo MR-MPS, originalmente distribuídos em seus diversos guias de implantação, utilizando-se a organização em tópicos e tabelas, facilita a ampla visualização do conteúdo de suas áreas de processo, necessária para a realização de comparações paritárias realizadas no estudo de caso deste trabalho.

3.5 Considerações Finais do Capítulo

O modelo MR-MPS apresentado neste capítulo, bem como o detalhamento sucinto de seus elementos, contribuem para a formação de um universo de escolhas para a avaliação e melhoria de processos de desenvolvimento de *software*.

É oportuno destacar resultados práticos para o setor produtivo, adicionalmente ao mérito técnico do modelo MR-MPS, derivados do investimento acadêmico voltado ao crescimento da indústria de *software*.

No Capítulo 4 são apresentados complementos a este modelo, as extensões de segurança originalmente criadas para o CMMI, com uma atenção especial para a uniformização da representação utilizada.

4 Extensões de Segurança para o CMMI

Neste capítulo são abordadas as extensões de segurança propostas por (FONSECA, 2005) em sua tese de doutorado "Uma Extensão de RAMS para o Modelo CMMI baseada nas Normas Ferroviárias CENELEC" e pela FAA "*Federal Aviation Administration*" norte americana, que propõe o FAA "*Safety and Security Extensions for Integrated Capability Maturity Models*" (IBRAHIM et al., 2004).

Em seguida é apresentada e discutida em maior detalhe a extensão do modelo CMMI-DEV +SAFE, desenvolvida pelo ADD/DMO (*Australian Department of Defence / Defence Materiel Organisation*), como base para a extensão ao modelo MR-MPS sugerida neste trabalho. Esta escolha se deve ao fato do CMMI-DEV +SAFE apresentar um escopo reduzido, quando comparado ao trabalho realizado por (FONSECA, 2005), e devido ao fato de apresentar novas áreas de processo aderentes aos aspectos de segurança, ao contrário do modelo da FAA, que amplifica o escopo das áreas existentes.

4.1 Extensão do Modelo CMMI para RAMS

A proposta de (FONSECA, 2005) é aproveitar o grande prestígio internacional alcançado pelo modelo CMMI e incorporar a ele os aspectos de RAMS sem alterar sua estrutura fundamental amplamente aceita.

A extensão do modelo proposta é realizada por meio do levantamento e mapeamento dos requisitos nas normas CENELEC 50126 "*Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety* (RAMS)" (CENELEC, 1999), CENELEC 50128 "*Railway Applications - Communication, Signalling and Processing Systems - Software for Railway Control and Protection Systems*" (CENELEC, 2001) e

CENELEC 50129 "*Railway Applications: Safety Related Electronic System for Signalling*" (CENELEC, 2003).

Na proposta de (FONSECA, 2005) foram criadas quatro novas Áreas de Processo (Gestão de RAMs, Garantia de RAMs, Engenharia de RAMs e Infra-estrutura Organizacional de RAMs), amplificadas três áreas já existentes (Definição de Processo Organizacional, Verificação e Validação) e diversas outras Áreas de Processo do CMMI foram classificadas como de implementação mandatórias.

Observa-se, ainda, que no trabalho de (FONSECA, 2005) é adotada, inicialmente, a representação contínua do CMMI, para flexibilizar a implantação das áreas de processo e promover melhorias nas áreas mais adequadas aos objetivos de negócio da organização. As quatro novas áreas de processo definidas no referido trabalho são apresentadas a seguir com os respectivos objetivos e práticas específicas, na forma adotada neste trabalho de pesquisa.

4.1.1 Gestão de RAMS - RM

Categoria de Processo: Gerenciamento de Projeto

O objetivo da gestão de RAMS é monitorar o processo de desenvolvimento, verificando se as atividades de RAMS são desempenhadas como planejadas, e acompanhar a evolução do projeto (FONSECA, 2005).

Tabela 12 – Práticas Específicas RM

Metas Específicas (SG)		
	Práticas Específicas (SP)	
SG 1	Desenvolver planos de RAMS.	
	SP 1.1	Estabelecer a estratégia para atendimento dos requisitos de RAMS.
	SP 1.2	Estabelecer a organização de RAMS para o projeto.
	SP 1.3	Estabelecer o ciclo de vida de RAMS para o projeto.
	SP 1.4	Estabelecer pontos de auditoria e de avaliação.
	SP 1.5	Planejar a gestão de dados.
	SP 1.6	Planejar os recursos necessários para executar o projeto.
	SP 1.7	Planejar os conhecimentos e habilidades necessárias para executar o projeto.
	SP 1.8	Planejar o envolvimento dos *stakeholders*.
	SP 1.9	Planejar as revisões de segurança.
	SP 1.10	Estabelecer os planos.
SG 2	Obter comprometimento com os planos.	
	SP 2.1	Revisar os planos que afetam o projeto.
	SP 2.2	Reconciliar o trabalho com os níveis de recursos.
	SP 2.3	Obter o comprometimento com os planos.
	SP 2.4	Atribuir responsabilidades.
SG 3	Tratar incidentes.	
	GP 3.1	Tratar incidentes.

4.1.2 Garantia de RAMS - RA

Categoria de Processo: Suporte

O objetivo da Garantia de RAMS é avaliar os produtos gerados pelas atividades de engenharia de RAMS de forma a garantir a integridade do produto (FONSECA, 2005).

Tabela 13 – Práticas Específicas RA

Metas Específicas (SG)		
	Práticas Específicas (SP)	
SG 1	Desenvolver um plano de avaliação.	
	SP 1.1	Estabelecer a estratégia de avaliação.
	SP 1.2	Estabelecer papéis e responsabilidades.
	SP 1.3	Planejar os recursos.
	SP 1.4	Planejar as necessidades de conhecimento e habilidades.
	SP 1.5	Planejar o envolvimento dos *stakeholders*.
	SP 1.6	Identificar o projeto e a dependência de documentos.
	SP 1.7	Estabelecer o plano de avaliação.
SG 2	Realizar avaliações.	
	SP 2.1	Executar avaliações sobre os produtos.
SG 3	Desenvolver um dossiê de segurança.	
	SP 3.1	Coletar evidências da gestão de qualidade.
	SP 3.2	Coletar evidências da gestão de segurança.
	SP 3.3	Coletar evidências sobre a segurança funcional e técnica.
	SP 3.4	Estabelecer um dossiê de segurança.

4.1.3 Engenharia de RAMS - RE

Categoria de Processo: Engenharia

O objetivo da Engenharia de RAMS é definir as atividades que devem ser executadas para que os produtos gerados atendam aos requisitos de RAMS, permitir a verificação,

validação, demonstração e documentação de RAMS, permitir a avaliação sobre os produtos gerados e auditorias sobre o processo e permitir o tratamento e prevenção de problemas de RAMS (FONSECA, 2005).

Tabela 14 – Práticas Específicas RE

Metas Específicas (SG)		
	Práticas Específicas (SP)	
SG 1	Identificar os requisitos de segurança.	
	SP 1.1	Executar a análise de perigos.
	SP 1.2	Executar a avaliação de Riscos.
	SP 1.3	Definir o critério para tolerância de riscos.
SG 2	Refinar os requisitos de segurança.	
	SP 2.1	Alocar os requisitos de segurança aos produtos.
	SP 2.2	Utilizar as recomendações de segurança nos requisitos.
	SP 2.3	Justificar as decisões técnicas de segurança.
SG 3	Estabelecer um registro de perigos.	
	SP 3.1	Estabelecer um registro de perigos para o projeto.
SG 4	Identificar os requisitos de RAM (*reliability, availability, maintainability*).	
	SP 4.1	Executar uma análise preliminar de RAM.
	SP 4.2	Identificar influência externa sobre os requisitos de RAM.
SG 5	Refinar os requisitos de RAM.	
	SP 5.1	Alocar os requisitos de RAM aos produtos.
	SP 5.2	Justificar as decisões técnicas de RAM.
SG 6	Demonstrar a segurança do sistema.	
	SP 6.1	Executar análise sobre os efeitos dos defeitos.
	SP 6.2	Executar análise sobre influências externas.
	SP 6.3	Executar análises sobre as condições de aplicação.
	SP 6.4	Executar testes de qualificação de RAMS.
	SP 6.5	Desenvolver um relatório técnico de segurança.

4.1.4 Infra-Estrutura Organizacional de RAMS - ROI

Categoria de Processo: Suporte

O objetivo da Infra-Estrutura Organizacional de RAMS é criar e manter uma estrutura adequada que englobe pessoas e ferramentas e defina responsabilidades e papéis para a execução das atividades de RAMS na organização e nos projetos.

Tabela 15 – Práticas Específicas ROI

Metas Específicas (SG)		
	Práticas Específicas (SP)	
SG 1	Estabelecer um ambiente apropriado para as atividades de RAMS.	
	SP 1.1	Identificar a organização global de RAMS.
	SP 1.2	Identificar e criar as habilidades necessárias.
	SP 1.3	Qualificar os componentes do ambiente.
	SP 1.4	Obter compromisso da alta gerência.

4.2 Extensão de Segurança FAA para iCMM

O escopo da segurança na extensão do FAA intitulado "*Safety and Security Extensions for Integrated Capability Maturity Models*" (IBRAHIM et al., 2004) para o FAA iCMM ou CMU/SEI CMMI, inclui o conceito de segurança da informação (*security*) e o conceito de segurança definida neste trabalho (*safety*).

Conforme (IBRAHIM; JARZOMBEK; ASHFORD, 2002), a segurança, elemento crítico para o DoD e para a FAA, não é mencionada nos componentes necessários ou esperados do modelo CMMI, mas apenas é mencionada poucas vezes em componentes meramente informativos do CMMI. No entanto, o CMMI é um excelente modelo em que as atividades relacionadas à segurança podem ser inseridas.

O trabalho do CMMI-DEV +SAFE, desenvolvido pelo ADD/DMO (*Australian Department of Defence / Defence Materiel Organisation*) , foi utilizado, em sua primeira versão, para construir a extensão do FAA. No entanto, uma de suas principais características é a correlação direta de suas práticas com as normas de segurança:

Para a segurança (*safety*):

• MIL-STD-882C: *System Safety Program Requirements*, Military Standard, 1993.

• MIL-STD-882D: *Standard Practice for System Safety*, DoD, 2000.

• IEC 61508: *Functional Safety of Electrical/ Electronic/ Programmable Electronic Systems, International Electrotechnical Commission*, 1997 (IEC, 1997).

• DEF STAN 00-56: *Safety Management Requirements for Defence Systems, Ministry of Defence*, 1996.

Para a segurança da informação (*security*):

• ISO/IEC 17799: *Information Technology - Code of practice for information security management, International Organization for Standardization*, 2000.

• ISO/IEC 15408: *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements*, v2.1, *Common Criteria Project Sponsoring Organizations*, 1999.

• ISO/IEC 21827: *Systems Security Engineering Capability Maturity Model* (SSE-CMM), v3.0, SSE-CMM *Project*, 2003.

• NIST 800-30: *Risk Management Guide for Information Technology Systems*, *Special Publication* 800-30, *National Institute of Standards and Technology*, 2001.

4.2.1 Área de Aplicação: Segurança (*Safety and Security*)

Novos conceitos foram desenvolvidos nesta extensão: Área de Aplicação (*Application Area* - AA) e Práticas da Aplicação (*Application Practices* - AP). A Área de Aplicação possui, tal como uma Área de Processo (PA) do CMMI, objetivos e Práticas Específicas,

chamadas Práticas da Aplicação. Para esta extensão é definida uma Área de Aplicação chamada Segurança (*Safety and Security Application Area*). Esta área de aplicação possui as Práticas de Aplicação (APs) presentes na tabela 16.

Tabela 16 – Práticas da Área de Aplicação "Segurança"

Metas da Aplicação	**Práticas da Aplicação (AP(*))**	
1	Uma infra-estrutura para segurança é estabelecida e mantida.	
	AP 1.1	Assegurar competência em segurança.
	AP 1.2	Estabelecer ambiente de trabalho qualificado.
	AP 1.3	Assegurar integridade da segurança e da informação.
	AP 1.4	Monitorar operações e reportar incidentes.
	AP 1.5	Assegurar continuidade de negócios.
2	Riscos de segurança são identificados e gerenciados.	
	AP 1.6	Identificar riscos de segurança.
	AP 1.7	Analisar e priorizar riscos.
	AP 1.8	Determinar, implementar e monitorar o plano de mitigação de riscos.
3	Requisitos de segurança são satisfeitos.	
	AP 1.9	Determinar requisitos regulatórios, leis e normas.
	AP 1.10	Desenvolver e entregar produtos e serviços seguros.
	AP 1.11	Avaliar objetivamente produtos.
	AP 1.12	Estabelecer argumentos de garantia da segurança.
4	Atividades e produtos são gerenciados para atingir os requisitos e objetivos de segurança.	
	AP 1.13	Estabelecer entidade independente.
	AP 1.14	Estabelecer um plano de segurança.
	AP 1.15	Selecionar e gerenciar fornecedores, produtos e serviços.
	AP 1.16	Monitorar e controlar atividades e produtos.

(*) Neste item, AP corresponde a Prática de Aplicação, diferentemente de Atributo de Processo, utilizado no restante deste trabalho.

Essas 16 Práticas da Aplicação (APs) são realizadas por meio de sua sobreposição às Práticas Específicas (SPs) das 22 Áreas de Processo (PAs) existentes no modelo CMMI, com

as diretrizes explícitas pelas normas consideradas na extensão do FAA, e guiadas pelas necessidades da aplicação.

4.2.2 Área de Processo: Ambiente de Trabalho

Esta extensão inclui uma Área de Processo (PA) chamada Ambiente de Trabalho com o objetivo de assegurar que as pessoas disponham da infra-estrutura e procedimentos de trabalho para cumprir suas tarefas de forma eficaz. Esta área de processo possui as Práticas Específicas (SPs) presentes na tabela 17.

Tabela 17 – Práticas Específicas - Ambiente de Trabalho

Metas Específicas (SG)	**Práticas Específicas (SP)**	
SG 1	Um ambiente de trabalho que atende às necessidades dos *stakeholders* é estabelecido e mantido.	
	SP 1.1	Determinar necessidades do ambiente.
	SP 1.2	Determinar padrões de ambiente de trabalho.
	SP 1.3	Estabelecer o ambiente de trabalho.
	SP 1.4	Manter a qualificação dos componentes.
	SP 1.5	Manter a qualificação do pessoal.
	SP 1.6	Manter percepção tecnológica.
	SP 1.7	Assegurar a continuidade do ambiente de trabalho.

4.3 Extensão do Modelo ADD/DMO CMMI-DEV +SAFE

A extensão +SAFE para o modelo CMMI-DEV foi desenvolvida pelo "*Australian Defence Materiel Organisation*", motivado pela necessidade de sua ampliação para incluir áreas especializadas da engenharia de segurança.

O principal propósito do +SAFE é identificar os pontos fortes e fracos de fornecedores de produtos e serviços na área de segurança, e abordar esses pontos fracos no início do processo de aquisição do *software*. Esta extensão foi desenvolvida de forma a possibilitar que usuários

e avaliadores de CMMI possam se familiarizar com a sua estrutura, estilo e conteúdo informativo, reduzindo a dependência de conhecimento especializado no campo de domínio da segurança.

A extensão +SAFE não foi criada com o propósito de ser embutida no modelo CMMI, e não depende de qualquer norma de segurança específica. Deve ser notado, conforme afirmado no próprio documento, que adicionar essa extensão +SAFE ao modelo CMMI não é suficiente para permitir um julgamento consistente com relação à capacidade do fornecedor conceber um sistema com um determinado nível de segurança (ADD/DMO, 2007).

Tendo discutido a motivação e as limitações para a extensão do modelo CMMI voltado à segurança, é possível identificar, segundo a extensão +SAFE, providências necessárias para a obtenção de produtos adequados a sistemas críticos de segurança, não cobertas originalmente pelo modelo.

De interesse especial para esta dissertação, serão apresentados os pontos convergentes do modelo de qualidade MR-MPS com as exigências de segurança consideradas na extensão +SAFE.

4.4 Áreas de Processos Definidas no CMMI-DEV +SAFE

As Áreas de Processos da extensão +SAFE não são definidas em níveis de maturidade. Portanto, essas áreas somente podem ser adotadas juntamente aos modelos CMMI-DEV e MR-MPS em sua representação contínua, sendo necessário atribuir níveis de capacidade, de acordo com o atendimento das Metas Genéricas do CMMI-DEV ou dos Atributos do Processo do MR-MPS.

Uma abordagem mista também seria possível, na qual a organização poderia ter um nível de maturidade com a implementação de todas as áreas de processo relativas ao mesmo, e

adicionar ou incrementar livremente o nível de capacidade de cada área de processo de forma independente e de acordo com os seus objetivos.

A seguir descreve-se as Áreas de Processo definidas na extensão +SAFE do modelo CMMI-DEV.

4.4.1 Gerenciamento de Segurança – GSEG

Categoria de Processo: Gerenciamento de Projeto

O propósito da Área de Processos Gerenciamento de Segurança é garantir que as atividades relacionadas à segurança (incluindo aquelas ligadas a fornecedores) são planejadas, o desempenho e resultados das atividades de segurança são monitorados conforme o planejado, e os desvios do plano são corrigidos (ADD/DMO, 2007).

A tabela 18 apresenta as Práticas Específicas (SPs) da Área de Processo (PA) Gerenciamento de Segurança.

Tabela 18 – Práticas Específicas GSEG

Nível de Maturidade	**Práticas Específicas (SPs)**	
Não se aplica	SG1 / GSEG 1	Desenvolver planos de segurança.
Não se aplica	SG2 / GSEG 2	Monitorar incidentes de segurança.
Não se aplica	SG3 / GSEG 3	Gerenciar fornecedores relacionados à segurança.

4.4.2 Engenharia de Segurança – ESEG

Categoria de Processo: Engenharia

O propósito da Área de Processos Engenharia de Segurança é garantir que a segurança é adequadamente abordada ao longo de todos os estágios do processo de Engenharia e envolve:

- A identificação de riscos, acidentes, e fontes de perigos, e análise destes para avaliar os riscos à segurança;
- O desenvolvimento de requisitos de segurança que atendam aos riscos de segurança;
- A aplicação de princípios de segurança ao longo do ciclo de vida de projeto para garantir que os requisitos de segurança serão satisfeitos;
- Desenvolvimento de uma forma de auditoria que possa atender à aceitação de segurança e prover as informações necessárias para validar as estratégias e planos de segurança, bem como a sua implementação (ADD/DMO, 2007).

A tabela 19 apresenta as Práticas Específicas (SPs) da Área de Processo (PA) Engenharia de Segurança.

Tabela 19 – Práticas Específicas ESEG

Nível de Maturidade	**Práticas Específicas (SPs)**	
Não se aplica	SG1 / ESEG 1	Identificar ameaças, acidentes e fontes de ameaças.
Não se aplica	SG2 / ESEG 2	Analisar ameaças e realizar análise de riscos.
Não se aplica	SG3 / ESEG 3	Definir e manter requisitos de segurança.
Não se aplica	SG4 / ESEG 4	Projeto voltado à segurança.
Não se aplica	SG5 / ESEG 5	Viabilizar aceitação de segurança.

4.5 Relacionamento entre as Áreas de Processos

No documento (ADD/DMO, 2007) é enfatizado que os processos de segurança são altamente dependentes de áreas de processo de suporte, particularmente o Gerenciamento de Configuração, Garantia da Qualidade de Processo e Produto, e Análise de Decisão e Solução. Os processos de segurança são, ainda, dependentes das áreas de processo Análise e Medição e Análise de Causas e Solução. Portanto a implementação efetiva de todas essas áreas de processo é importante para uma melhoria na capacidade de segurança.

Os processos de segurança colocam ênfase significativa na independência das equipes envolvidas nos processos de verificação e validação. Também deve ser considerada a realização de atividades nestas áreas por entidades independentes da organização, o que é considerado como um fator importante de diversidade, entre os profissionais de segurança.

As Áreas de Processos (PAs) originais do CMMI (apresentadas no capítulo 2 deste trabalho) relacionadas ao Gerenciamento de Segurança são as seguintes:

- Gerenciamento de Risco (RSKM);
- Planejamento de Projeto (PP);
- Monitoração e Controle de Projeto (PMC);
- Análise de Decisão e Resolução (DAR); e
- Gerenciamento de Acordo com Fornecedores (SAM).

As Áreas de Processos originais do CMMI relacionadas à Engenharia de Segurança são as seguintes:

- Desenvolvimento de Requisitos (RD);
- Solução Técnica (TS);
- Integração de Produto (PI);
- Verificação (VER);
- Validação (VAL); e
- Garantia da Qualidade de Processo e Produto (PPQA).

4.6 Descrição de Níveis do CMMI-DEV +SAFE

Conforme (ADD/DMO, 2007), a avaliação de um projeto, bem como a sua classificação como de Segurança Crítica, não estão relacionadas com a sua avaliação com base no modelo

CMMI-DEV +SAFE. Portanto, a seleção de processos apresentada a seguir ilustra apenas uma possível classificação desses processos em níveis de segurança.

A classificação em níveis S0 ao S3 está sendo apresentada de maneira similar aos modelos CMMI ou MR-MPS em estágios; no entanto, não tem correlação alguma com a classificação em níveis apresentada naqueles modelos. Deve-se destacar que no nível S0 o projeto não está classificado como de segurança e, portanto, não se aplicam as áreas de processos definidas na extensão CMMI-DEV +SAFE.

A seguir são apresentadas as Áreas de Processos (APs) definidas na extensão CMMI-DEV +SAFE, categorizadas em níveis de segurança.

4.6.1 Gerenciamento de Segurança – GSEG

Nível S1 - Projeto classificado como de segurança, porém a identificação das ameaças indicam que não.

O propósito do Gerenciamento de Segurança é garantir que as atividades relacionadas à segurança (incluindo aquelas ligadas a fornecedores) são planejadas, o desempenho e resultados das atividades de segurança são monitoradas conforme o planejado, e os desvios dos planos são corrigidos (ADD/DMO, 2007). A tabela 20 apresenta as Práticas Específicas (SPs) para a Área de Processo Gerenciamento de Segurança no nível S1.

Tabela 20 – Práticas Específicas GSEG (nível S1)

Nível	**Práticas Específicas**	
S1	GSEG 1	Desenvolver planos de segurança.
S1	GSEG 2	Monitorar incidentes de segurança.
S1	GSEG 3	Gerenciar fornecedores relacionados à segurança.

4.6.2 Engenharia de Segurança – ESEG

Nível S1 - Projeto classificado como de segurança, porém a identificação das ameaças indicam que não.

O propósito da Engenharia de Segurança é garantir que a segurança é adequadamente abordada ao longo de todos os estágios do processo de Engenharia e envolve: a identificação de riscos, acidentes e fontes de perigos, e o desenvolvimento de uma forma de auditoria que possa atender à aceitação de segurança e prover as informações necessárias para validar as estratégias e planos de segurança, e sua implementação (ADD/DMO, 2007). A tabela 21 apresenta as Práticas Específicas (SPs) para a Área de Processo Engenharia de Segurança no nível S1.

Tabela 21 – Práticas Específicas ESEG (nível S1)

Nível	**Práticas Específicas**	
S1	ESEG 1	Identificar ameaças, acidentes e fontes de ameaças.
S1	ESEG 5	Viabilizar aceitação de segurança.

4.6.3 Engenharia de Segurança – ESEG (evolução)

Nível S2 - Projeto classificado como de segurança, porém todas as ameaças são aceitáveis.

O propósito da Engenharia de Segurança é garantir que a segurança seja adequadamente abordada ao longo de todos os estágios do processo de Engenharia e envolve: a análise de riscos, acidentes e fontes de perigos para avaliar os riscos à segurança (ADD/DMO, 2007). A tabela 22 apresenta as Práticas Específicas (SPs) para a Área de Processo Engenharia de Segurança no nível S2.

Tabela 22 – Práticas Específicas ESEG (nível S2)

Nível	**Práticas Específicas**	
S2	ESEG 2	Analisar ameaças e realizar análise de riscos.

4.6.4 Engenharia de Segurança – ESEG (evolução)

Nível S3 - Projeto classificado como de segurança e inclui ameaças não aceitáveis.

O propósito da Engenharia de Segurança é garantir que a segurança é adequadamente abordada ao longo de todos os estágios do processo de Engenharia e envolve: o desenvolvimento de requisitos de segurança que atendam aos riscos à segurança, e a aplicação de princípios de segurança ao longo do ciclo de vida de projeto, para garantir que os requisitos de segurança serão satisfeitos (ADD/DMO, 2007). A tabela 23 apresenta as Práticas Específicas (SPs) para a Área de Processo Engenharia de Segurança no nível S3.

Tabela 23 – Práticas Específicas ESEG (nível S3)

Nível	**Práticas Específicas**	
S3	ESEG 3	Definir e manter requisitos de segurança.
S3	ESEG 4	Projeto voltado à segurança.

4.7 Considerações Finais do Capítulo

As extensões de segurança desenvolvidas para o CMMI, apresentadas neste capítulo, acrescentam possibilidades ao universo de escolhas para a avaliação e melhoria de processos de desenvolvimento de *software* adequado aos sistemas de segurança crítica. Essas extensões, em conjunto com as áreas de processo apresentas no capítulo 3, formam os subsídios necessários para a aplicação do método proposto neste trabalho no capítulo 7.

Nos capítulos seguintes serão descritos o modelo AHP e o método proposto para a priorização das áreas de processo já apresentadas, com o objetivo de formar um conjunto adequado para a aplicação do MR-MPS com a extensão de segurança +SAFE em sua representação contínua.

5 Método de Decisão por Múltiplos Critérios

Nesta dissertação propõe-se a utilização de um modelo de decisão por múltiplos critérios (MDMC) para possibilitar a avaliação subjetiva da importância ou relevância, para a segurança de um sistema, de diferentes processos definidos em normas e modelos de qualidade de *software*.

Apesar da origem de auxílio à decisão utilizando MDMC ser atribuída a obras que datam de meados do século passado, na década de 1950, este tema continua a ser muito explorado por diversos pesquisadores, conforme notado pela vasta bibliografia encontrada a este respeito e apresentada de forma resumida neste capítulo.

5.1 Definições Relacionadas aos MDMC

Os Métodos de Decisão por Múltiplos Critérios (MDMC) constituem poderosas ferramentas para o auxílio a decisão, que objetivam facilitar e justificar escolhas, muitas vezes em cenários complexos.

Para a aplicação de um MDMC, tipicamente é necessário estabelecer o domínio do problema, como a necessidade ou o **objetivo** de se obter as decisões em questão, e relacionar um conjunto de **alternativas** (também referidas como estratégias ou ações) que constituem as possíveis soluções para o problema definido.

Os **critérios de decisão** (referidos ainda como aspectos ou dimensões) escolhidos, devem ser atributos ou características das alternativas, relevantes para o objetivo da decisão, e pelos quais essas serão avaliadas.

Entre os MDMC bem estabelecidos, podemos citar como exemplos (PAMPLONA, 1999):

- **Método de Análise Hierárquica** (AHP - *Analytic Hierarchy Process*), proposto por Saaty em 1977;
- Método de Análise em Redes (ANP – *Analytic Network Process*), também desenvolvido por Saaty, em 1996;
- ELECTRE (*Elimination and Choice Translating Reality*), uma família de métodos MDMC originados na Europa, em meados de 1960;
- Abordagem de Decisão *Fuzzy* (FDA – *Fuzzy Decision Approach*), baseada em conjuntos *Fuzzy* e proposta por Liang e Wang, em 1992;
- MACBETH (*Measuring Attractiveness by a Categorical Based Evaluation Technique*), proposto por Bana e Costa / Vasnick, em 1994; e
- TOPSIS (*Technique for Order Preference by Similarity to Ideal Solution*), cujo desenvolvimento se deve a Hwang e Yoon em 1981.

Um elemento comum aos MDMC apresentados como exemplo, é o uso de matrizes em que as alternativas são comparadas segundo os critérios de decisão.

5.2 Justificativa do Analytic Hierarchy Process (AHP)

A partir da comparação com outros modelos de decisão por múltiplos critérios (MDMC) apresentada em (PAMPLONA, 1999), na qual os resultados obtidos por diferentes métodos foram considerados similares e diversas vantagens da aplicação do AHP foram observadas em todos os casos, recomenda-se a utilização do AHP para a obtenção de bons resultados, mesmo

quando as alternativas e critérios de decisão não estão diretamente relacionados ou são totalmente independentes.

Outras características favoráveis ao uso do AHP são discutidas em (GOODWIN, 2004).

- A estruturação formal dos problemas que necessitem de escolhas ou julgamento, permite que problemas complexos possam ser decompostos em conjuntos de julgamento mais simples, e oferece uma razão documentada para a escolha ou priorização de uma determinada opção em detrimento a outras:
- A simplicidade da comparação entre pares de alternativas significa que o julgador pode focar uma pequena parte do problema por vez, simplificando a sua tarefa. As comparações verbais também são importantes aos julgadores que poderiam ter dificuldades em expressar suas opiniões numericamente.
- A redundância de julgamentos permite que a consistência do julgamento seja verificada, e é considerada uma boa prática a obtenção das entradas para um modelo de decisão de diferentes formas. Com a utilização do AHP isto é feito de maneira automática.
- A versatilidade do AHP é evidenciada pelos diferentes tipos de aplicação, inclusive envolvendo incertezas e previsões.

5.3 Aplicações do AHP

O campo de aplicação do AHP é muito variado, conforme notado por (VAIDYA; KUMAR, 2004) com a análise de 150 artigos publicados. O AHP foi utilizado como ferramenta por pessoas responsáveis pela tomada de decisão e pesquisadores nas seguintes áreas: social, pessoal, política, educação, fabricação, engenharia, industrial e governamental.

O AHP é amplamente empregado para tomada de decisões de múltiplos critérios, em planejamento e alocação de recursos, e em solução de conflitos (SAATY, 2006).

Na área de Engenharia de *Software* (MIRANDA, 2001) propõe a adoção de um modelo formal, com o emprego do AHP, para melhorar a precisão das estimativas subjetivas realizadas por especialistas, bastante adequada nos estágios iniciais de um projeto de desenvolvimento, quando o conhecimento disponível aos membros da equipe é de natureza principalmente qualitativa.

A seleção de uma ferramenta de projeto de *software*, assim como diversas outras ferramentas, é geralmente abordada sem rigor, baseando-se em preferência pessoal, intuição ou tendência de mercado, podendo gerar resultados errôneos. Uma aplicação correlata do AHP foi apresentada por (AHMAD; LAPLANTE, 2006), considerando doze critérios relevantes para a decisão baseado nas características oferecidas pela maior parte das soluções COTS (*Commercial Off The Shelf*).

5.4 Decomposição de um Problema Usando o AHP

O AHP oferece meios de decompor um problema em uma hierarquia de sub-problemas que podem ser mais facilmente compreendidos e avaliados subjetivamente. As avaliações subjetivas são convertidas em valores numéricos e processados para obter um *ranking* de cada alternativa em uma escala numérica (BHUSHAN, 2004).

Na figura 9, é apresentada a representação tipicamente adotada pelo AHP, ressaltando a decomposição de um problema complexo.

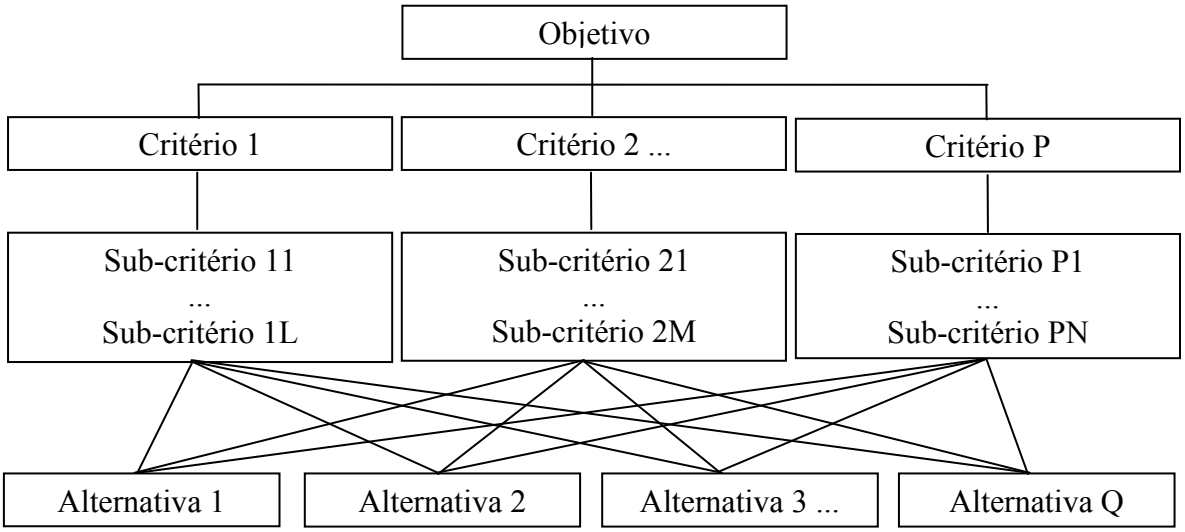

Figura 9 – Análise Hierárquica (BHUSHAN, 2004)

Como um exemplo, pode-se citar um problema cujo **Objetivo** seja seleção de uma ferramenta para Gerenciamento de Projetos, conforme exemplificado por (AHMAD; LAPLANTE, 2006), com base em uma série de **Alternativas** de ferramentas COTS disponíveis no mercado. Esse problema pode ser decomposto na estrutura de **Critérios** relacionados a seguir:

- Agendamento de tarefas;
- Gerenciamento de recursos;
- Facilidades de colaboração;
- Controle da duração das atividades;
- Produção de estimativas;
- Avaliação de riscos;
- Gerenciamento de mudanças;
- Tipos de relatórios e diagramas;
- Possibilidade de anexar arquivos;
- Notificação por *e-mail*;
- Metodologias de processo; e
- Possibilidade de gerenciamento de *portfolio*.

Eventualmente, alguns desses **Critérios** poderiam ser decompostos em séries de **Sub-critérios**. A montagem de uma hierarquia, assim como a estruturação de um problema por qualquer outro método, demanda um conhecimento substancial do sistema em questão (SAATY, 1986). É admissível que os mesmos especialistas que realizam o julgamento tenham uma participação importante na definição da estrutura hierárquica.

5.5 Métricas e Escalas no AHP

O AHP é uma teoria geral de mensuração. Ele é utilizado para obter prioridades relativas em escala absoluta (invariante sob transformação) a partir de comparações aos pares, de forma discreta ou contínua, em estruturas hierárquicas com vários níveis. As comparações podem ser obtidas a partir de medições reais (valores quantitativos) ou de uma escala que reflete os sentimentos de grandeza ou preferência de uma pessoa no assunto (julgamentos qualitativos).

A consistência é uma característica intrínseca ao AHP que pode ser calculada e relacionada ao grupo de elementos ou alternativas e à forma como estão estruturados.

Em sua forma geral, o AHP é uma metodologia não-linear para acomodar o pensamento dedutivo e indutivo do ser humano sem o uso de simbologia. Com isso, o AHP permite levar em consideração, simultaneamente, vários fatores de importância para uma determinada escolha. (SAATY, 2006).

A escala fundamental de valores para representar a intensidade dos julgamentos proposta originalmente (SAATY, 1986) e, empregada atualmente, é mostrada na tabela 24, e foi obtida por meio da teoria de resposta a estímulos e tem sua eficiência validada não somente em muitas aplicações por diversas pessoas, mas também por meio da justificação teórica de seu emprego na comparação de elementos homogêneos (SAATY, 2006).

Tabela 24 – Escala Fundamental de Números Absolutos (SAATY, 2006)

Intensidade da Importância	Definição	Explicação
1	Mesma importância.	As duas alternativas contribuem igualmente para o objetivo.
3	Importância moderada ou pequena.	A experiência e julgamento favorecem sutilmente uma alternativa sobre a outra.
5	Importância forte ou grande.	A experiência e julgamento favorecem fortemente uma alternativa sobre a outra.
7	Importância muito forte ou demonstrada.	A alternativa é fortemente favorecida sobre outra, de acordo com demonstração prática.
9	Importância extrema ou absoluta.	A evidência favorecendo uma alternativa sobre a outra é da mais alta ordem possível de afirmação.
2, 4, 6, 8	Valores inteiros intermediários.	Utilizado para refinamento da escala.
Recíprocos	Inversão da ordem de comparação.	Se a alternativa i tem um dos números acima atribuídos a esta quando comparado com a alternativa j, então a alternativa j tem o valor recíproco quando comparado com a alternativa i.
Racionais	Valores racionais obtidos por meio de operações com a escala.	A consistência é obtida somente pela utilização de valores numéricos racionais.

Existem diversas situações nas quais os elementos ou alternativas a serem comparados são iguais ou quase iguais em medida e, então, uma comparação deve ser feita não para determinar quantas vezes um elemento é maior do que o outro, mas sim para determinar qual fração da medida é maior do que a outra.

O uso de números entre 1 e 9, utilizando valores inteiros, se justifica pela habilidade humana em efetuar julgamentos e distinções entre as afirmações (definições) apresentadas na tabela. Os valores intermediários podem ser utilizados para refinamento dos julgamentos quando a situação assim o permite.

5.6 A Medida de Todas as Coisas – o julgamento humano (SAATY, 1990)

Todas as informações medidas, seja em Física, Engenharia ou Sociologia, devem ser interpretadas para serem compreendidas. Estes números descrevem o grau de uma

propriedade que um objeto ou evento possui, como por exemplo, o quanto é rápido, quanto tempo leva ou quanto é pobre. Os números demonstram a quantidade de uma determinada propriedade que um objeto possui em um dia em relação a outro, ou quanto a mais possui em relação a outro objeto, ou quanto possui a mais ou a menos em relação a um determinado padrão (SAATY, 1990).

A habilidade humana para avaliar o significado das medidas é limitada. Por exemplo, além de certa temperatura observada na experiência diária, não se faz idéia de quanto é mais frio -160 ºC em relação a -140 ºC. Cada um tem um refinamento melhor de que outro, mas não temos a percepção disto. Por outro lado, uma diferença de 20 ºC em nossa faixa perceptível tem muito mais significado. A temperatura ambiente de 30 ºC é mais confortável do que 10 ºC, e de 40 ºC é muito menos confortável que 20 ºC. Mesmo o que é considerada uma temperatura agradável depende de onde se está acostumado a viver (SAATY, 1990).

Compreender medidas depende da experiência e percepção adquirida ao longo da vivência, aprendizado e treinamento. O significado das medidas em diferentes escalas é um fenômeno cultivado por intermédio do condicionamento, não têm significado em si próprio. É possível concluir que sempre interpretamos o significado dos dados subjetivamente, como outros estímulos são percebidos pelos nossos sentidos (SAATY, 1990).

O problema básico é criar um suporte científico para interpretar os dados. O AHP é uma teoria de decisão que interpreta diretamente as informações e dados obtidos com o uso de julgamentos, e efetua a medição destes em escala comparativa em uma estrutura hierárquica sugerida (SAATY, 1990).

5.7 Atribuição de Valores: Julgamentos

A maior parte das dificuldades encontradas quando se utiliza o AHP são relacionadas à necessidade de julgamentos (SAATY, 1986). Se um problema é complexo e requer uma análise cuidadosa, será necessário tempo para justificar os julgamentos. No entanto, conforme observado nos mais complexos problemas, que podem levar até dias para serem concluídos, as pessoas podem descansar e retornar ao processo posteriormente, sem prejuízo ao resultado obtido.

Outro aspecto a ser considerado é a necessidade ocasional da repetição do processo de julgamento para se assegurar de que as pessoas não mudaram drasticamente de opinião. A matemática por trás do método AHP está bem estabelecida e seu uso pode ser simples, mas os julgamentos sob os quais os cálculos são realizados não são. Para se obter resultados satisfatórios, as pessoas que irão efetuar as comparações devem compreender as dimensões funcionais e tecnológicas dos elementos avaliados (MIRANDA, 2001).

5.8 Análise por Várias Pessoas

Uma primeira possibilidade para se obter os julgamentos necessários, quando várias pessoas estão envolvidas no processo, é realizar o estudo do problema, desde o início, contando com todos os participantes e procurar um consenso sobre a atribuição de valores para cada comparação.

No entanto, a aplicação do AHP também é útil quando muitos interesses estão envolvidos e várias pessoas participam do processo de julgamento, em situações nas quais o debate não é possível e muitas respostas para um mesmo questionamento podem surgir.

Os resultados, neste caso, devem ser então ponderados pela prioridade de cada indivíduo, de acordo com a sua relevância para o julgamento do problema. Estas prioridades podem ser obtidas com a extensão da hierarquia para incluir os indivíduos e os respectivos critérios para avaliá-los.

5.9 Descrição Matemática do AHP

Neste item é apresentada uma breve descrição matemática do AHP, na qual procura-se discutir a obtenção e significado das operações envolvidas no método para a obtenção de seus resultados na busca de uma solução para um problema.

A partir de uma matriz, com características próprias advindas de comparações paritárias (aos pares), são estabelecidas as prioridades das alternativas por meio de seu autovalor e autovetor. Em seguida deve ser dado um tratamento à inconsistência desta matriz, devido à redundância dos julgamentos, que poderia levar à conclusões insensatas. O índice de inconsistência é calculado para se obter um indicador dessa situação e, eventualmente, permitir a realização de correção de valores de forma numérica.

Pelo método AHP, pode-se para cada um dos Sub-critérios estabelecer-se uma comparação entre as **Alternativas** com respeito ao Sub-critério considerado. Para cada conjunto de **Sub-critérios** de um determinado Critério, pode-se estabelecer comparações entre esses Sub-critérios, visando a determinação da importância relativa de uns face aos outros. Por fim, considerando-se todos os Critérios escolhidos, pode-se estabelecer novas comparações entre esses **Critérios**, para se obter a importância relativa de cada Critério com relação ao **Objetivo** a ser alcançado.

Por fim, é detalhado formalmente o modo como as prioridades das alternativas em uma hierarquia completa, composta por diversas matrizes de comparação, são obtidas com base na

combinação das prioridades de seus elementos, chegando-se ao resultado final obtido pelo método.

5.9.1 Cálculo das Prioridades em uma Matriz (SAATY, 1991)

Sejam $C_1, C_2, ..., C_n$ os elementos de algum nível em uma hierarquia, e $w_1, w_2, ..., w_n$ os seus pesos relativos no que diz respeito a algum elemento no próximo nível hierárquico superior. Denominam-se a_{ij}, o número que indica a importância de C_i quando comparado C_j.

A matriz A de comparações paritárias é uma matriz quadrada de ordem n dada por:

i \ j	A_1	A_2	...	A_j	...	A_n
A_1	w_1 / w_1	w_1 / w_2	...	w_1 / w_j	...	w_1 / w_n
A_2	w_2 / w_1	w_2 / w_2	...	w_2 / w_j	...	w_2 / w_n
...	...	...	...	...	...	...
A_j	w_j / w_1	w_j / w_2	...	w_j / w_j	...	w_j / w_n
...	...	...	...	...	...	...
A_n	w_n / w_1	w_n / w_2	...	w_n / w_j	...	w_n / w_n

em que: $a_{ij} = w_i / w_j \qquad i, j = 1, ..., n$

Pelas características do método AHP, pode-se afirmar que a matriz de comparação obtida possui todos os seus elementos positivos, e deverá ser recíproca, ou seja:

$a_{ij} > 0 \Rightarrow A$ é matriz positiva, e

$a_{ji} = 1 / a_{ij} \Rightarrow A$ é matriz recíproca.

Uma matriz é chamada de consistente se o julgamento for considerado perfeito em todas as comparações realizadas. Este caso pode ser expresso matematicamente como:

$$a_{ik} = a_{ij} \cdot a_{jk} \text{ para qualquer que seja } i, j, k \quad ; \qquad (1)$$

pois: $a_{ik} = \frac{w_i}{w_j} \cdot \frac{w_j}{w_k} = \frac{w_i}{w_k}$.

Multiplicando-se a matriz A pelo vetor w (vetor coluna composto por $w_1, w_2, ..., w_n$), obtém-se:

$$A \cdot w = n \cdot w \qquad (2)$$

Em teoria matricial, a fórmula (2) expressa o fato de que w é um autovetor de A, com autovalor n. É esta característica que garante que todas as linhas de A são uma combinação linear da primeira.

Considerado-se ainda o traço[1] e o posto[2] de A, tem-se a garantia de que o maior autovalor (λ) de A, denominado $\lambda_{\max}$, será igual a n e é único, como será demonstrado a seguir.

O problema consiste em definir quais os valores das componentes do vetor w. Deve-se, então, resolver o seguinte sistema:

$(A - n \cdot I)w = 0$, sendo I a matriz identidade de ordem n.

Essa equação possui solução não nula se e somente se n for um autovalor de A. Conseqüentemente w será o autovetor associado.

De acordo com a teoria matricial, os autovalores (λ) de uma matriz correspondem às raízes do polinômio característico, que representam a solução de:

---

[1] Em álgebra linear, o traço de uma matriz quadrada A é a soma dos elementos da sua diagonal principal (SANTOS, 2008).

[2] Em álgebra linear, o posto de uma matriz A é o número máxima de linhas e colunas linearmente independentes da matriz A (SANTOS, 2008).

$\det|A-\lambda I|=0$, dado por:

$$P(\lambda)=a_0\lambda^n+a_1\lambda^{n-1}+a_2\lambda^{n-2}+\ldots+a_n$$

As soluções de $P(\lambda)$ são os m autovalores $(\lambda_i, i=1,\ldots,m)$ da matriz A. Caso $m<n$, a equação possui autovalores múltiplos.

Outro fato importante refere-se ao fato da matriz A ter posto unitário, pois todas as linhas da matriz são múltiplas da primeira. Assim só há um autovalor diferente de zero, o que garante a unicidade da solução. Além disto, todos os elementos da diagonal principal são iguais a 1, logo o traço de A ($tr(A)$) é igual a n.

A soma dos autovalores de uma matriz é igual ao seu traço. Neste caso, sabe-se que o traço da matriz é n e só há um autovalor diferente de zero; portanto, este autovalor será igual a n e, uma vez que ele é único (todos os outros são nulos), pode-se afirmar que ele é o máximo autovalor ($\lambda_{\max}$) da matriz.

Tem-se então que, como A só possui um único autovalor, isso implica que:

$$\begin{cases}\lambda_j=0, j=1,2,\ldots,i-1,i,i+1,\ldots,n\\ \lambda_i\neq 0, i\neq j\end{cases}$$

Como: λ_k

e $\sum_{j=1}^{n}\lambda_j=\lambda_i=tr(A)=n$

Pode-se escrever que:

$$\lambda_i=\lambda_{\max}=n$$

E a solução do sistema é qualquer coluna de A, sendo que as colunas de A são formadas por vetores do tipo $(w_1/w_j, w_2/w_j,\ldots,w_n/w_j)^t$. Normalizando o vetor, tem-se uma solução única independente da coluna adotada.

Sendo assim, o problema consiste em determinar o maior autovalor e o autovetor associado, fornecendo desta forma os pesos relativos da matriz correspondente.

5.9.2 Inconsistência de Julgamento

A matriz A possui outra característica: ela é consistente. Define-se a consistência de uma matriz A como a intensidade real com a qual a preferência é expressa ao longo de uma seqüência de objetos em comparação, o que resulta em certa proporcionalidade entre os elementos da seqüência. Inconsistência é a violação desta proporcionalidade. Por exemplo, ao se afirmar que A > B, B > C e C > A, há inconsistência de julgamento.

Na realidade, deseja-se encontrar o autovetor w associado ao autovalor máximo da matriz A, pois se tem uma aproximação destes valores que é dada por a_{ij} e não se pode garantir que a matriz $\widetilde{A} = \left(a_{ij}\right)$ possui necessariamente posto 1. Sendo assim, pode-se ter mais de um autovalor não nulo, o que acarreta $\lambda_{\max} \neq n$. A matriz $\widetilde{A}$ é recíproca, pois $a_{ii} = 1$.

Diz-se que a matriz $\widetilde{A}$ é inconsistente e para se saber o grau de inconsistência deve-se calcular o quão próximo $\lambda_{\max}$ está de n.

No caso ideal tem-se que $a_{ij} = w_i / w_j$ e a condição de consistência (1) é respeitada. Como a_{ij} representa uma aproximação de w_i / w_j pode-se escrever $a_{ij} = \dfrac{w_i}{w_j}\varepsilon_{ij}$, deixando de existir a consistência.

De acordo com a equação (2), e considerando o fato de que no caso ideal $\lambda = n$, então:

$$Aw = \lambda w$$

Logo, pode-se escrever

$$w_i = \frac{1}{n}\sum_{j=1}^{n} a_{ij} w_j \qquad (3)$$

Ao se utilizar as aproximações a_{ij}, perturbaram-se os valores desta equação. Se a perturbação for pequena, ou seja, a_{ij} for próximo de w_i / w_j, há uma solução para (3), w_i e w_j podem ser ajustados desde que acompanhados de uma variação em n.

Seja $n = \lambda_{\max}$ então,

$$w_i = \frac{1}{\lambda_{\max}}\sum_{j=1}^{n} a_{ij} w_j \quad \text{e}$$

$$\lambda_{\max} = \sum_{j=1}^{n} a_{ij} \frac{w_j}{w_i} \qquad (4)$$

Deseja-se que pequenos desvios em a_{ij} acarretem um pequeno desvio em $\lambda_{\max}$.

Primeiramente definiu-se

$$\mu \hat{=} -\frac{1}{n-1}\sum_{i=2}^{n} \lambda_i \qquad (5)$$

Mas

$$\sum_{i=1}^{n} \lambda_i = n \;\Rightarrow n = \lambda_1 + \sum_{i=2}^{n} \lambda_i$$

Logo,

$$\sum_{i=2}^{n} \lambda_i = n - \lambda_1 \qquad (6)$$

Fazendo-se $\lambda_1 = \lambda_{\max}$ e substituindo (6) em (5)

$$\mu = -\frac{1}{n-1}\left(n - \lambda_{\max}\right)$$

$$\mu = \frac{\lambda_{\max} - n}{n-1} \tag{7}$$

De (4) tem-se:

$$\lambda_{\max} = \sum_{j=1}^{n} a_{ij} \frac{w_j}{w_i} = a_{ii} \frac{wi}{wi} + \sum_{\substack{j \\ j \neq i}} a_{ij} \frac{w_j}{w_i}$$

Como $a_{ii} = 1$

$$\lambda_{\max} = 1 + \sum_{j \neq i} a_{ij} \frac{w_j}{w_i}$$

Portanto:

$$\lambda_{\max} - 1 = \sum_{j \neq i} a_{ij} \frac{w_j}{w_i} \tag{8}$$

Desenvolvendo (8):

$i = 1$ $\quad \lambda_{\max} - 1 = a_{12} \frac{w_2}{w_1} + a_{13} \frac{w_3}{w_1} + \Lambda \ + a_{1n} \frac{w_n}{w_1}$

$i = 2$ $\quad \lambda_{\max} - 1 = a_{21} \frac{w_1}{w_2} + a_{23} \frac{w_3}{w_2} + \Lambda \ + a_{2n} \frac{w_n}{w_2}$

$i = 3$ $\quad \lambda_{\max} - 1 = a_{31} \frac{w_1}{w_3} + a_{32} \frac{w_2}{w_3} + \Lambda \ + a_{3n} \frac{w_n}{w_3}$

Λ Λ

$i = n$ $\quad \lambda_{\max} - 1 = a_{n1} \frac{w_1}{w_n} + a_{n2} \frac{w_2}{w_n} + \Lambda \ + a_{nn-1} \frac{w_{n-1}}{w_n}$

E somando as equações anteriores, obtem-se:

$$n\lambda_{\max} - n = \sum_{i \neq j} a_{ij} \frac{w_j}{w_i} \tag{9}$$

Como A é uma matriz recíproca, para $i < j$ pode-se escrever que:

$$\sum_{i<j} a_{ij} \frac{w_j}{w_i} = \sum_{i<j} a_{ji} \frac{w_i}{w_j}$$

E de (9) tem-se

$$n\lambda_{\max} - n = \sum_{1 \leq i < j \leq n} \left(a_{ij} \frac{w_j}{w_i} + a_{ji} \frac{w_i}{w_j} \right) \tag{10}$$

Substituindo (10) em (7), resulta

$$\mu = \frac{1}{n-1} - \frac{n}{n-1} + \frac{1}{n(n-1)} \sum_{1 \leq i < j \leq n} \left(a_{ij} \frac{w_j}{w_i} + a_{ji} \frac{w_i}{w_j} \right) \tag{11}$$

Fazendo-se $a_{ij} = \frac{w_i}{w_j} \varepsilon_{ij}$, tem-se que $\varepsilon_{ij} = a_{ij} \frac{w_j}{w_i}$ e $\frac{1}{\varepsilon_{ij}} = a_{ji} \frac{w_i}{w_j}$.

Substituindo em (11), resulta:

$$\mu = -1 + \frac{1}{n(n-1)} \sum_{1 \leq i < j \leq n} \left(\varepsilon_{ij} + \frac{1}{\varepsilon_{ij}} \right) \tag{12}$$

Analisando-se a equação (12) vê-se que se $\varepsilon_{ij} \to 1$, $\mu \to 0$. O valor de μ aumenta à medida que ε_{ij} se afasta de 1, logo se ε_{ij} for próximo de 1, $a_{ij} \to w_i / w_j$ causando pequenas modificações em $\lambda_{\max}$ e, conseqüentemente, no autovetor associado.

5.9.3 Cálculo da Razão de Consistência

O erro cometido em cada matriz é avaliado pelo grau de inconsistência da mesma (SAATY, 1991). Para tanto, define-se o Índice de Consistência (IC) como:

$$IC = \frac{\lambda_{\max} - n}{n-1}$$

Quando não houver inconsistências, $\lambda_{\max} = n$ e, portanto, $IC = 0$.

Como, quanto maior a matriz, maior deverá ser a inconsistência. (SAATY, 1990) Testou a inconsistência das matrizes de acordo com a ordem das mesmas. Construíram-se 500 amostras de matrizes preenchidas aleatoriamente, utilizando-se a escala de 1 a 9 e a característica de reciprocidade, para matrizes de ordem 3 a 12, e definiu-se o Índice Randômico (IR) que é a média do IC calculado para cada matriz da amostra.

$$IR = \frac{1}{500}\sum_{x=1}^{500}\frac{\lambda_{\max_x} - n_x}{n_x - 1}$$

A tabela 25 fornece os valores de IR encontrados, de acordo com a dimensão n da matriz.

Tabela 25 – Índice Randômico (SAATY, 1990)

n	3	4	5	6	7	8	9	10	11	12
IR	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,48

Para calcular o erro, comparou-se o IC com o IR. Dessa forma, pondera-se a dimensão da matriz de tal forma que se admita um maior erro para matrizes de maior dimensão ($n > 5$) e se é mais rigoroso para matrizes pequenas. Para tanto definiu-se a Razão de Consistência (RC) que é dada por:

$$RC = IC / IR$$

Um erro é considerado aceitável, de acordo com esta ponderação, se $RC < 0{,}10$.

5.9.4 Correção de Valores

Caso a RC seja alta, há duas maneiras de melhorar a consistência da matriz e diminuir a margem de erro. A primeira consiste em rever os pesos atribuídos, discutindo-se com os indivíduos ou obtendo-se um novo consenso com o grupo. A segunda maneira consiste em utilizar cálculos matemáticos (SAATY, 1991).

Como se deseja que a_{ij} se aproxime o máximo possível de w_i / w_j, então calcula-se:

$$\max i \sum_{j=1}^{n} \left| a_{ij} - w_i / w_j \right|$$

Então, substituem-se todos os elementos da linha i ou apenas o $\max a_{ij}$, por w_i / w_j, e recalcula-se então o autovalor e o autovetor.

Este procedimento é eficaz, mas entretanto não pode ser repetido inúmeras vezes, pois oferece o risco de levar a uma solução distorcida. Deve-se neste caso obter novamente os julgamentos.

5.9.5 Cálculo das Prioridades da Hierarquia

Para a solução completa do problema é necessário, além dos pesos relativos da matriz apresentados, obter ainda a solução da hierarquia completa.

Primeiramente define-se $w_{i,j}$ como o autovetor da matriz j do nível i e $v_{i,j}$ o vetor prioridade da matriz j do nível i, considerando a influência dos níveis hierárquicos

inferiores, h o número de níveis da hierarquia e m_k o número de elementos do nível k, $k = 1,...,h$.

Para calcular a prioridade da hierarquia deve-se:

1. Calcular o maior autovalor e o autovetor associado para cada matriz da hierarquia, exceto as do último nível (h): $w_{i,j}$ para $i = 1,2,...,h-1$ e $j = 1,...,m_k$.

2. Fazer $v_{i,j} = w_{i,j}$ para todos os elementos pertencentes ao nível $h-1$.

3. Calcular o vetor prioridade para todos os elementos da hierarquia pertencentes aos níveis do primeiro $A(h-2): v_{i,j}$ para $i = 1,2,...,h-2$, do seguinte modo:

   a. Dado o nó j do nível i, monta-se uma matriz cujas colunas são os vetores prioridades dos elementos do nível $i+1$ que possuem um arco associado ao nó (i, j);

   b. Multiplica-se essa matriz por $w_{i,j}$;

   c. Faz-se $v_{i,j}$ igual ao resultado desta multiplicação; e

Desta forma, a solução da hierarquia será $v_{1,1}$.

Nota-se que $v_{i,j}$ contém as prioridades do nó j do nível i, considerando a influência de todos os níveis hierárquicos inferiores. Desta forma, a prioridade dos elementos do último nível da hierarquia em relação ao seu primeiro nível é o vetor V.

5.10 Considerações Finais do Capítulo

O método de decisão por múltiplos critérios AHP, descrito neste capítulo, e selecionado para este trabalho, constitui uma base para permitir a ponderação entre as áreas de processo proposta pelo método que será descrito no capítulo 6 desta dissertação.

6 Método Proposto

Segundo (RAILTRACK, 2000), uma organização deve iniciar as atividades de gerenciamento de engenharia de segurança cedo, enquanto é mais fácil construir a segurança, e todas as atividades relacionadas devem ser planejadas antes de serem colocadas em prática.

Dessa forma, para o desenvolvimento de *software* adequado à aplicação em sistemas críticos de segurança, é oportuna a determinação e o planejamento de um processo adequado e alinhado aos modelos de processo de *software* de ampla aceitação.

O emprego desses modelos é, muitas vezes, considerado oneroso, apesar dos benefícios potenciais já demonstrados pela prática na indústria. Ainda, por serem genéricos, esses modelos reúnem as melhores práticas e recomendações aplicáveis a uma vasta gama de projetos.

Pelos motivos expostos, será apresentada agora uma proposta de um método para auxílio à importante decisão sobre a adoção de processos, buscando priorizá-los em função de sua relevância em relação à segurança, obtida por meio do consenso de profissionais experientes na área de sistemas críticos de segurança.

6.1 Premissas para a Aplicação do Método

Neste primeiro item do capítulo, são apresentadas as principais condições e premissas que devem ser observadas e consideradas para a aplicação do método proposto visando a sua aplicação de forma efetiva.

6.1.1 Visibilidade do Processo de Desenvolvimento de *Software*

A falta de visibilidade durante o desenvolvimento dos produtos de *software* dificulta o gerenciamento do projeto. Segundo (GUSTAFSON, 2003), em várias outras áreas da engenharia é mais fácil visualizar os progressos do desenvolvimento de um projeto. No entanto, muitos projetos de *software* são abandonados quando falta pouco para terminá-los. Muitas das técnicas de gerenciamento de *software* estão baseadas na visibilidade do processo, como por exemplo, a qualidade do processo em si.

Uma prática muito comum de se tentar melhorar a qualidade de um *software* baseia-se somente em encontrar e corrigir problemas em seus artefatos. Isso tem como resultado natural que a indústria em geral não acredita que seja possível entregar um *software* específico, com relativa complexidade, dentro do prazo e orçamento. A relação entre os fatores tempo, custo e funcionalidade faz com que o desenvolvimento de *software* freqüentemente deixe de atender a estes três requisitos simultaneamente (DANIELS *et al*., 2003).

O chamado paradigma do desenvolvimento de *software* "caixa preta", que consiste em apenas gerar, testar e re-trabalhar o *software*, sem preocupação com os detalhes do processo de desenvolvimento de *software*, pode não ser adequado ao desenvolvimento de sistemas críticos, pois seriam necessárias inúmeras interações para a obtenção do *software* sem erros que possam levar o sistema a uma condição insegura.

No entanto, é necessário preocupar-se com essa prática, comum na indústria de *software* não voltados para aplicações críticas e, portanto, sem atributos de segurança, e que podem levar a se obter resultados caóticos no produto final.

O método proposto prevê situações nas quais:

- A preocupação com a segurança esteja presente no planejamento da qualidade, ainda que implicitamente;

- O plano de desenvolvimento de *software* seja definido; e
- A visibilidade do processo de desenvolvimento de *software* seja suficiente para a obtenção de evidências quanto à aderência aos planos.

6.1.2 Validação do Processo de Desenvolvimento de *Software*

O Plano de Garantia da Qualidade de *Software* deve ser o ponto de partida para a obtenção de evidências quanto ao atendimento aos requisitos de segurança pelos itens de *software* desenvolvidos.

A validação do processo com relação às práticas estabelecidas por normas, modelos e melhores práticas, de uso geral ou ainda interno à organização, contribui para a obtenção de um nível de segurança apropriado.

Não se deve esquecer que o propósito de qualquer ferramenta de auxílio à decisão é prover a percepção e entendimento do problema, ao invés de simplesmente prescrever uma solução "correta". Muitas vezes o processo de buscar a estruturação de um problema é mais útil para alcançar este objetivo do que o próprio resultado numérico oriundo de um modelo (GOODWIN, 2004).

6.1.3 Defeitos Inseridos no Desenvolvimento de *Software*

A afirmação falsa, mas muito comum, de que "*programação é uma arte, e não uma ciência*" é um bom ponto para se iniciar a discussão a respeito de como surgem os defeitos de *software*. Na maior parte dos casos o fracasso de projetos de *software* não pode ser atribuído à codificação ruim ou a problemas no gerenciamento de projeto. Este fato sugere que o

problema esteja entre estas duas atividades, sendo este o lugar da Engenharia de *Software* (DANIELS *et al.*, 2003).

As atividades de análise de segurança realizadas sobre as etapas finais da obtenção de *software*, ou mesmo sobre o produto final, tipicamente deverão ser pessimistas quanto ao funcionamento correto do *software* em situações adversas. Entretanto, enquanto se está trabalhando no desenvolvimento do sistema, não se pode desprezar a oportunidade do emprego de esforços e disciplinas da Engenharia de *Software* para minimizar a possibilidade de se inserir erros que possam levar o sistema a uma situação insegura.

Os artefatos produzidos de acordo com o plano de desenvolvimento de *software* devem fornecer evidências de que as atividades realizadas estão em conformidade com o plano de garantia da qualidade de *software*.

A produção de relatórios de verificação sobre estes artefatos será de utilidade para o ajuste das expectativas iniciais em relação à segurança do sistema sob análise. Se o plano de garantia da qualidade de *software* não sofrer alterações durante o processo de desenvolvimento, as justificativas para desvios do plano podem ser apresentadas e ter seu impacto avaliado.

6.1.4 Representação da Segurança em Níveis

Um nível de segurança, no contexto deste trabalho, deve apenas indicar uma expectativa em relação à segurança de um sistema, no qual um item de *software* construído com enfoque em segurança esteja sendo aplicado. A modelagem da segurança de um sistema deve levar em conta todos os seus aspectos e as características do ambiente em que será empregado.

A definição numérica da segurança não é usual na definição de processos de desenvolvimento de *software*; portanto, esta avaliação deve estar a cargo de especialistas e em função das particularidades de cada projeto.

No entanto, a aplicação do método proposto neste trabalho busca oferecer uma percepção da segurança do *software* a ser obtido, a partir do emprego de práticas recomendadas por modelos de melhoria do processo de desenvolvimento e os seus mecanismos de implementação e avaliação. Desta forma, espera-se que o método possa ser empregado desde a etapa de definições do projeto, até a avaliação do processo de desenvolvimento de *software* já concluído.

Na verdade, a generalidade do método permite que ele seja utilizado inclusive no auxílio à decisão de políticas de qualidade de empresas responsáveis pelo desenvolvimento de *software* para sistemas críticos, até a análise de processos de desenvolvimento de *software* já superados ou abandonados.

6.2 Descrição do Método Proposto

A aplicação do método descrito neste trabalho deve ser iniciada pela consolidação de todas as Áreas de Processo (PAs) descritas pelo modelo MR-MPS e também as descritas na extensão de segurança +SAFE do modelo CMMI, que forem de interesse para a organização.

O passo seguinte compreende a adequação das informações para a aplicação do método AHP, envolvendo as seguintes etapas:

a) a formalização de um objetivo a ser alcançado;

b) a definição dos critérios/sub-critérios a serem utilizados para a comparação das Áreas de Processo (PAs) entre si;

c) a definição de uma escala de valores a serem atribuídos no processo de comparação; e

d) o estabelecimento de uma hierarquia própria envolvendo o objetivo, critérios/sub-critérios e alternativas.

A seguir, é necessário obter os julgamentos de especialistas na área de sistemas críticos de segurança, com base nas comparações paritárias (aos pares) das alternativas, a respeito dos critérios/sub-critérios, que podem ser apresentados em um questionário, ou de outra forma adequada à compreensão, como matrizes numéricas ou por meio de ferramentas especiais.

Finalmente, com a obtenção das prioridades com a aplicação do método AHP, sugere-se a criação de um perfil de capacidade (*capability profile*), conforme definido no capítulo 2, adequado para a implementação da melhoria ou avaliação do processo de desenvolvimento de *software*, com base na representação contínua definida no modelo CMMI.

Desta forma, os passos previsto no método proposto neste trabalho de pesquisa são agora representados no diagrama da figura 10, e detalhados nos próximos itens deste capítulo.

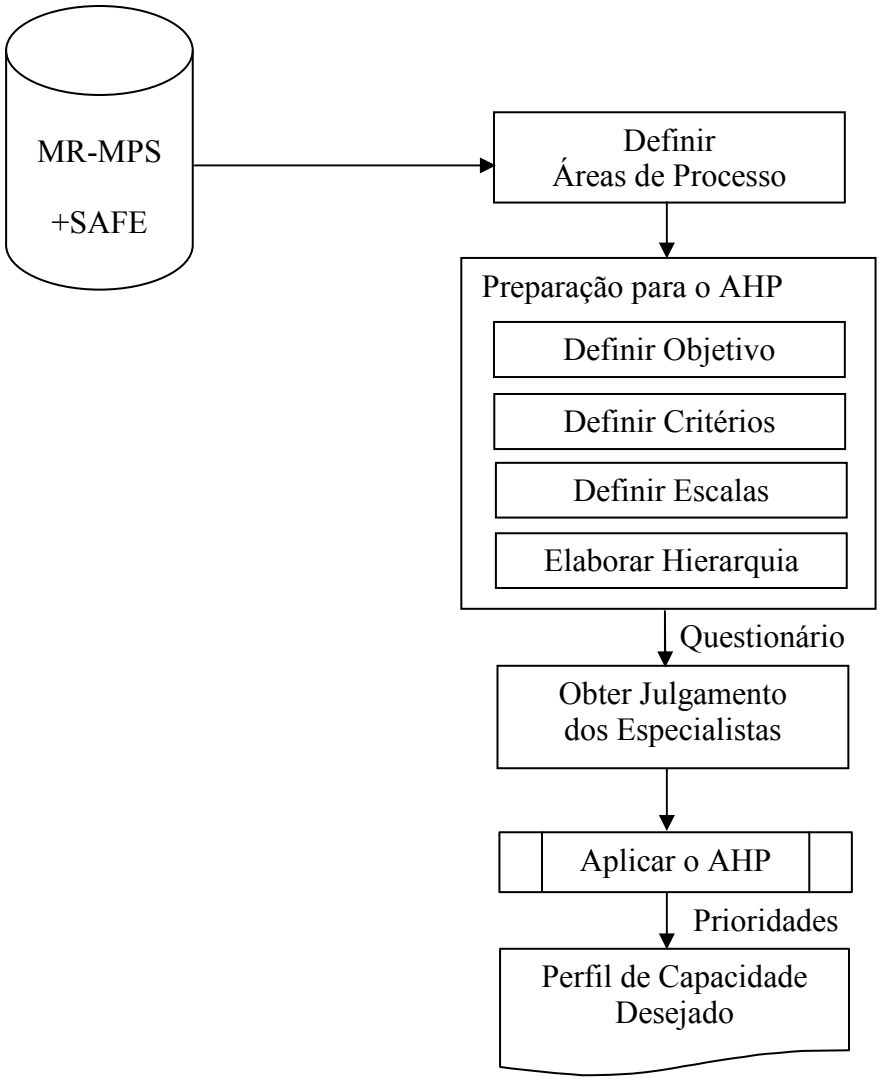

Figura 10 – Passos do Método Proposto Usando o AHP

Com o perfil de capacidade definido é possível realizar uma avaliação da organização utilizando, por exemplo, os métodos de avaliação descritos pelo MA-MPS (Método de Avaliação para Melhoria de Processo de *Software*) (MPS.BR, 2007i), SCAMPI (*Standard CMMI Appraisal Method for Process Improvement*) (CMU/SEI, 2006b) ou ISO-15504 (ISO/IEC, 2004a), ainda que de forma resumida (informal), possibilitando a implementação da melhoria de processo detalhada nos modelos MPS-BR e CMMI +SAFE nas áreas nas quais for detectada necessidade.

Novos perfis podem ser definidos com o aumento dos níveis de capacidade ponderados pelas prioridades obtidas pela aplicação do AHP, possibilitando a evolução da organização segundo as informações obtidas pelo processo inicial ou aplicando novamente o método descrito neste trabalho, se desejável. Uma representação simples desta iteração é apresentada na figura 11.

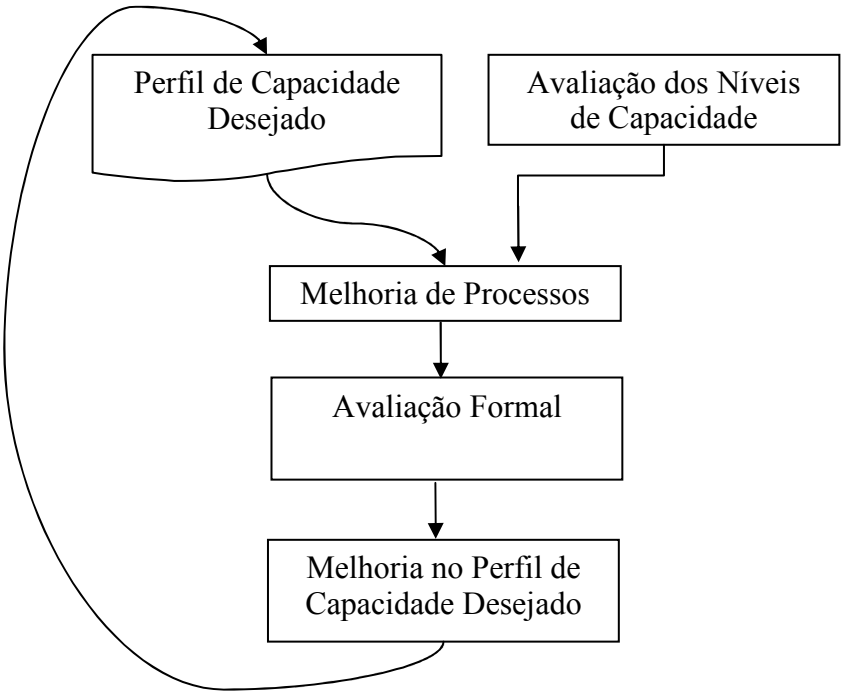

Figura 11 – Melhoria do Processo de Software

Este ciclo pode ser implementado utilizando-se diversas abordagens para melhoria de processo de *software*, tais como o IDEAL do SEI, Six Sigma, QIP e DLI, ou outros métodos derivados do PDCA (*Plan-Do-Check-Act*), conforme apresentado em (GARCIA; TURNER, 2007).

Por permitir uma evolução dos requisitos sugeridos para a melhoria de processos, sem a mudança dos dados fundamentais obtidos na primeira aplicação deste método, é possível promover a melhoria sem a necessidade de refazer a aplicação completa do mesmo.

6.2.1 Definição das Áreas de Processo (PAs)

Nesta etapa, todas possibilidades de melhoria de Processos de Desenvolvimento de *Software*, com as mais diversas abordagens, deve ser explorada. No caso de utilização do método por um grupo reunido, pode ser atrativa a possibilidade da participação coletiva na obtenção das alternativas, que podem ser obtidas por meio de pesquisa bibliográfica ou até mesmo de sugestões por indivíduos experientes.

Nesta etapa é importante a exploração de processos, tecnologias, ou até mesmo práticas e técnicas que podem não constituir o conhecimento comum do grupo, mas que possam ser apresentadas e descritas com clareza. Isto representa um benefício indireto da utilização deste método.

Na presente dissertação, as áreas de processo definidas no modelo MR-MPS e na extensão de segurança CMMI +SAFE estão descritas sucintamente nos capítulos três e quatro, respectivamente.

6.2.2 Preparação para o AHP

Esta etapa tem como objetivo a obtenção de toda a fundamentação necessária para a aplicação da ferramenta AHP, conforme descrito no capítulo 5.

6.2.2.1 Definição do Objetivo

O nível mais alto de qualquer hierarquia para o auxílio à decisão, utilizando o processo AHP, é o **objetivo**. Todos os julgamentos realizados devem sempre considerá-lo.

Especificamente, o método apresentado neste trabalho, implica no emprego do AHP com a finalidade de se obter uma lista de prioridades, para a implantação, avaliação ou melhoria de processos de desenvolvimento de *software*, com relação à sua importância ou relevância para a aplicação em sistemas críticos de segurança.

Pode-se postular, desta forma, o Objetivo como simplesmente "*Priorizar Processos*".

6.2.2.2 Definição dos Critérios/Sub-critérios

A seguir é necessário definir os **critérios** para a avaliação qualitativa das alternativas a serem priorizadas. Sendo o AHP um método de decisão por múltiplos critérios, é possível, para o refinamento da decisão, desmembrar, para efeito da priorização de processos, os critérios pelos quais estes processos devem ser julgados. No caso do uso de múltiplos critérios, é ainda possível estabelecer a importância relativa dos critérios para a solução do problema.

Devido ao fato de se pressupor o julgamento das alternativas por indivíduos especialistas em engenharia de *software*, engenharia de segurança, desenvolvimento de *software* adequado à segurança ou em projeto de sistemas críticos, será proposto o julgamento em uma única dimensão: a importância ou relevância para a segurança do sistema construído. A aplicação mais direta deste método admite o uso de um único critério, e se a escolha for esta, possivelmente será denominado: "*Adequado à Segurança*".

Da mesma forma que proposto por (AHMAD; LAPLANTE, 2006), incluir o custo como critério nesta etapa pode não ser inicialmente uma boa escolha. Apesar da inclusão do fator custo ser comum em diversas aplicações do AHP, ele pode ser incluído após a obtenção dos resultados, com a construção de uma representação de custo-benefício que seja mais apropriada para a tomada de decisão.

No entanto, incluir o custo como um critério para obter a relevância das alternativas é uma possibilidade e pode ser benéfica, partindo-se do princípio de que a maturidade dos especialistas e da organização admita fazer esta ponderação.

6.2.2.3 Definição da Escala

O método proposto neste trabalho, por capturar o julgamento sobre a importância ou relevância relativa entre as diversas alternativas que estão analisadas, sugere que a escala fundamental recomenda no AHP, descrita no capítulo 5 (1, 2, 3, 4, 5, ...), é adequada para uso neste método.

Eventualmente pode utilizar diferentes escalas numéricas na aplicação do método AHP, ou até mesmo conjuntos nebulosos (*fuzzy*), como encontrados na bibliografia (WANG; WANG; HU, 2005) (WANG; LUO; HUA, 2007). Neste trabalho, o estudo de caso utiliza a escala fundamental.

6.2.2.4 Construção da Hierarquia

A organização das alternativas em uma hierarquia concentra a maior parte do esforço da aplicação do método proposto. Reunir elementos de natureza distintas em uma representação hierárquica é uma tarefa que pode se tornar complicada sem o estudo cuidadoso de fatores ou características que possam classificá-los de acordo com sua afinidade.

Para organizar os elementos em conjuntos, deve-se considerar ainda o número de elementos na matriz de comparação, para evitar a necessidade de uma quantidade excessiva

de julgamentos, o que poderá tornar esta tarefa cansativa e, em casos extremos, até mesmo invalidar os resultados obtidos.

Com a definição e organização de alternativas em grupos, será possível esboçar a hierarquia, como pode ser observado na figura 12.

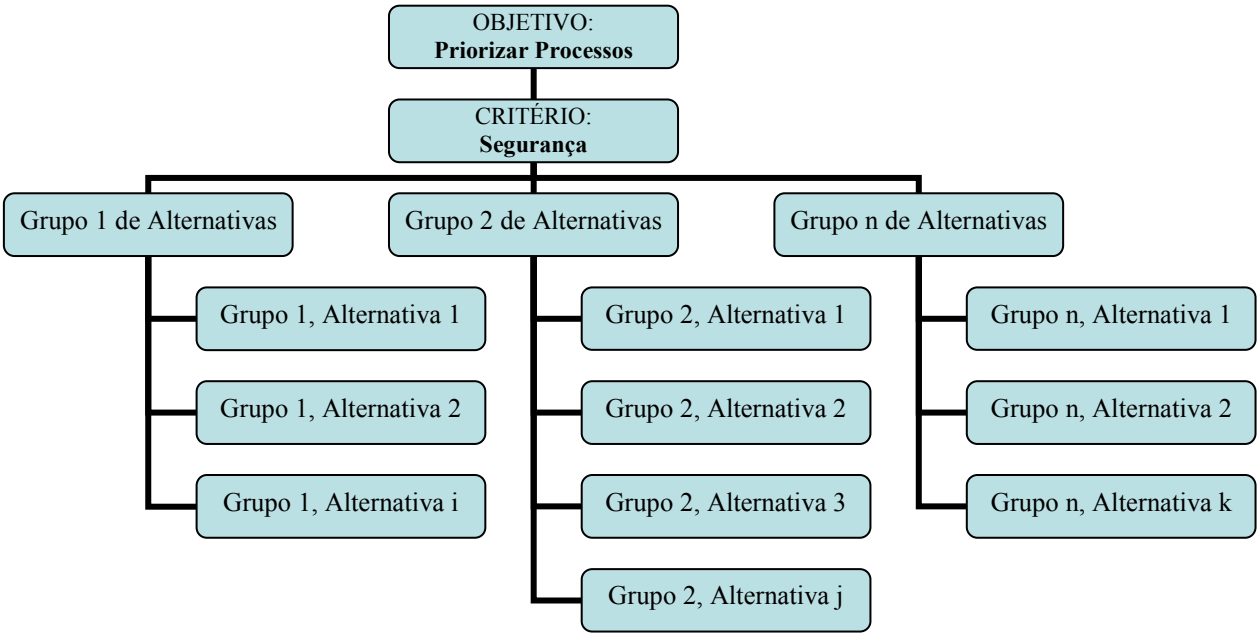

Figura 12 – Representação da Hierarquia

Nota-se que o método AHP permite utilizar um número grande de níveis hierárquicos. No entanto, para facilitar a compreensão e aplicação do método proposto, apenas este exemplo típico será apresentado.

6.2.3 Realização de Julgamentos

A melhor estratégia para buscar as opiniões e julgamentos dos especialistas irá depender de diversos fatores como, por exemplo, o tempo disponível para os julgamentos, a possibilidade da realização de reuniões em que se apresentem e se discutam as alternativas, ou

ainda a disponibilidade de uma ferramenta de *software* para oferecer uma realimentação rápida e visual relacionada com os julgamentos efetuados.

Efetivamente, as diferentes abordagens irão apresentar vantagens e desvantagens na forma como os resultados poderão ser obtidos, bem como na oportunidade de se obter ganhos indiretos decorrentes da aplicação desta etapa do método proposto. Desta forma, é adequado não prescrever uma forma particular.

São apresentados a seguir modos pelos quais os indivíduos ou grupos poderão expressar e registrar suas opiniões e julgamentos para cada conjunto de alternativas.

6.2.3.1 Modo Questionário

No modo questionário, os julgamentos são realizados no formato seqüencial. Esta é possivelmente a forma mais intuitiva, e que provavelmente requer menor domínio sobre o processo utilizado.

Este modo é bastante intuitivo e está exemplificado na figura 13. No questionário apresentado devem ser assinaladas as colunas da tabela com os números correspondentes ao grau de importância relativa da Alternativa apresentada na coluna da esquerda comparada com a Alternativa apresentada na coluna da direita.

Na figura, nota-se que a Alternativa 1, quando comparada com a Alternativa 2, recebe a classificação 5, que é favorável a Alternativa 1 e indica que esta é "*fortemente favorecida sobre a outra*" (vide classificação na escala fundamental apresentada no capítulo 5).

	Importância Relativa																
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
Alternativa 1					x													Alternativa 2
Alternativa 1																		Alternativa 3
Alternativa 1																		...
Alternativa 1																		Alternativa n
Alternativa 2																		Alternativa 3
Alternativa 2																		...
Alternativa 2																		Alternativa n
Alternativa 3																		...
Alternativa 3																		Alternativa n
...																		...
...																		Alternativa n

Figura 13 – Julgamentos Modo Questionário

Por ser de aplicação direta, esta é uma forma adequada para obter julgamentos de um grupo não habituado ao método utilizado, sendo o foco dado na importância de se descrever as alternativas de forma direta e inequívoca, sem a necessidade do especialista entender o funcionamento detalhado do método AHP.

6.2.3.2 Modo Matricial

Outra possibilidade de obtenção de julgamentos é apresentar para o especialista as alternativas em modo matricial, para o preenchimento da matriz diretamente com os números correspondentes à escala de julgamento. Por exemplo, na escala fundamento, os valores de preenchimentos seriam os seguintes: {1/9, 1/8, 1/7, 1/6, 1/5, 1/4, 1/3, 1/2, 1, 2, 3, 4, 5, 6, 7, 8, 9}.

A figura 14 apresenta o mesmo exemplo do item anterior, em que afirma-se que a alternativa 1 é *fortemente favorecida* em relação a alternativa 2, o que é determinado pelo

valor 5 escolhido. Nota-se ainda, o reduzido número de campos que devem ser preenchidos – pois para a aplicação do método AHP é admitido que o julgamento das alternativas é recíproco (por exemplo, se a alternativa 1 tem o valor 5 comparada à alternativa 2, a alternativa 2 tem automaticamente o valor 1/5 comparada à alternativa 1 e, portanto, este valor não precisa ser preenchido. Naturalmente, uma alternativa quando comparada com ela mesma apresenta valor de julgamento igual a 1.

Importância	Alternativa 1	Alternativa 2	Alternativa 3	...	Alternativa n
Alternativa 1	1	5			
Alternativa 2		1			
Alternativa 3			1		
...				1	
Alternativa n					1

Figura 14 – Julgamentos Modo Matricial

Obter julgamentos com uso de pesos ou valores numéricos é adequado para a obtenção de resultados quando adquire-se maior experiência com o uso do método, e é necessário, além do conhecimento das alternativas, o domínio da escala adotada e o significado de seus valores. Julgamentos obtidos por intermédio de questionários podem ser representados com o uso de matrizes, de modo a sintetizar as informações obtidas para simplificar sua análise.

6.2.3.3 Outras Ferramentas

Além do uso de formulários para se obter os julgamentos, é possível ainda realizar entrevistas com os especialistas, descrevendo verbalmente as alternativas e os elementos da escala utilizada, de modo que seja possível obter uma afirmação em relação à importância relativa entre cada par de alternativas.

Outra alternativa é utilizar uma representação gráfica dos julgamentos com auxílio de ferramentas de *software* mais elaboradas, quando disponível. Neste caso a interação, direta ou assistida, com a ferramenta permite muitas possibilidades, como por exemplo permitindo a participação de pessoas geograficamente dispersas.

6.2.4 Análise de Sensibilidade

Esta etapa do processo é opcional, podendo ser implementada como refinamento do método proposto. Um resultado prático possível, com a obtenção de julgamentos individuais, é realizar uma análise de sensibilidade dos valores atribuídos a cada julgamento, para investigar tendências nos resultados.

Os indivíduos podem ser classificados em grupos, segundo diversos critérios, e os resultados de suas avaliações combinados. Com este resultado será possível determinar as preferências de cada grupo e realizando uma análise crítica, podem ser extraídas conclusões importantes sobre possíveis recomendações.

Da mesma forma, ao se combinar os julgamentos dos especialistas é possível ponderar, de acordo com critérios diversos relativos à sua experiência prática ou acadêmica, por exemplo, no desenvolvimento de sistemas de segurança, de modo a obter diferentes resultados que possibilitem uma discussão mais ampla deste problema. É possível, a título de exemplo, dar maior peso a especialistas com maior experiência na referida área.

6.2.5 Aplicação do Método AHP

Com o uso do método de análise hierárquica AHP são obtidos, como resultados, os elementos do vetor w (peso relativo dos elementos com relação ao nível hierárquico superior) das matrizes de comparação paritária, e o índice de consistência RC (vide item 5.9). No último nível da hierarquia (objetivo) é possível obter, ainda, o vetor V (prioridade dos elementos do último nível da hierarquia em relação ao seu primeiro nível), contendo os valores numéricos para cada área de processo com relação ao objetivo. Com estes valores, é possível classificar as áreas de processo em relação à sua importância.

Sendo as alternativas os processos de desenvolvimento de *software*, e os julgamentos obtidos com relação ao critério "*importância para a segurança*", tem-se em mãos, como o resultado direto, a classificação dos processos (objetivo do método).

Certamente existem diversas formas de se tratar os resultados obtidos – seja na priorização de investimento de recursos e esforços, na avaliação da efetividade de um programa de melhoria de processos, ou até mesmo na definição de uma política organizacional.

As discussões em torno dos resultados obtidos diretamente da aplicação do método proposto, bem como uma análise crítica da sensibilidade dos resultados em relação à variação dos parâmetros, constituem também uma contribuição obtida com a utilização do método proposto.

6.2.6 Obtenção do Perfil de Capacidade

Após o cálculo das prioridades das alternativas geradas pelo uso do método AHP, pode-se criar um perfil de capacidade, isto é, a representação de uma expectativa em relação aos níveis de capacidade, para cada Área de Processo (PA) analisada.

O método proposto neste trabalho permite a obtenção matemática de um perfil de capacidade a partir do vetor prioridades V resultante do uso do método AHP.

Após a aplicação do método AHP, é necessário estipular um Valor de Ganho arbitrário k, que pode ser manipulado livremente, e é proporcional ao nível de esforço ou à expectativa de melhoria de processos na organização, com o objetivo de normalizar os resultados e permitir a escolha de um perfil adequado aos diferentes estágios de melhoria de processos admissíveis pela organização.

Desta forma, o vetor de prioridades V será multiplicado pelo **Valor do Ganho** k e seus valores arredondados para números inteiros compreendidos entre 0 e 5, correspondentes aos níveis de capacidade das Áreas de Processo definidos na representação contínua dos modelos de melhoria e avaliação de processos de *software*, gerando o vetor *P*, conforme descrito a seguir.

$$P = \min\{n = k \cdot V \in \mathbb{N} \mid n \leq 5\}$$

6.3 Considerações Finais do Capítulo

Uma vez apresentado o método proposto, o próximo capítulo apresenta um estudo de caso para a sua experimentação, objetivando a obtenção de resultados práticos na área de

aplicação específica de modelos de melhoria e avaliação do processo de desenvolvimento de *software* para sistemas críticos de segurança.

7 Estudo de Caso

A aplicação para uso do método proposto neste estudo de caso visa obter um perfil de capacidade de processos de desenvolvimento de *software* adequado para a aplicação do modelo MR-MPS com a extensão de segurança CMMI +SAFE, exemplificando e ressaltando suas possibilidades.

As informações para aplicação do método foram obtidas com a definição da hierarquia e das alternativas considerando as Áreas de Processos (PAs) definidas na extensão de segurança CMMI +SAFE e as áreas relacionadas definidas no modelo MR-MPS. O questionário piloto utilizado foi preenchido com o auxílio de um profissional especialista na área de sistemas críticos de segurança, atuando em sistemas metro-ferroviários.

7.1 Emprego do Método Proposto

As etapas definidas formalmente no capítulo anterior são rigorosamente seguidas neste capítulo de estudo de caso para exemplificar a aplicação do método proposto.

7.1.1 Escolha das Áreas de Processo

A escolha das Áreas de Processo (PAs), provenientes dos capítulos 3 e 4, ficou restrita, neste estudo de caso, naquelas definidas pela extensão de segurança CMMI +SAFE e nas áreas relacionadas definidas no modelo MR-MPS.

O detalhamento sucinto das áreas selecionadas encontra-se nos capítulos 3 e 4, bem como no anexo A deste trabalho, sendo as seguintes:

- AQU Aquisição (nível de maturidade 2 do CMMI-DEV e F do MR-MPS);
- DRE Desenvolvimento de Requisitos (nível de maturidade 3 do CMMI-DEV e D do MR-MPS);
- ESEG Engenharia de Segurança (área de processo do CMMI +SAFE);
- GQA Garantia da Qualidade (nível de maturidade 2 do CMMI-DEV e F do MR-MPS);
- GSEG Gerenciamento de Segurança (área de processo do CMMI +SAFE);
- GPR Gerenciamento de Projetos (nível de maturidade 2 do CMMI-DEV e G do MR-MPS);
- ITP Integração de Produto (nível de maturidade 3 do CMMI-DEV e D do MR-MPS);
- PCP Projeto e Construção do Produto (nível de maturidade 3 do CMMI-DEV e D do MR-MPS);
- VAL Validação (nível de maturidade 3 do CMMI-DEV e D do MR-MPS); e
- VER Verificação (nível de maturidade 3 do CMMI-DEV e D do MR-MPS)

7.1.2 Preparação para o AHP

Esta etapa tem como objetivo a obtenção de todas as informações e definições necessárias para a aplicação do método AHP, conforme descrito no capítulo 5.

7.1.2.1 Definição do Objetivo

Pode-se postular para o estudo de caso, e genericamente para a aplicação do método proposto, o objetivo como "*Priorizar Processos*".

7.1.2.2 Definição dos Critérios

No estudo de caso foi realizada a aplicação mais direta deste método com o uso de um único critério denominado: "*Adequado à Segurança*".

7.1.2.3 Definição da Escala

O método proposto, por capturar o julgamento sobre a importância ou relevância relativa entre as alternativas, considera que a escala fundamental proposta no AHP seja adequada para uso.

7.1.2.4 Construção da Hierarquia

Para o presente estudo de caso, e a obtenção do questionário piloto, a hierarquia selecionada apresenta um único nível. Devido ao estreitamento do escopo com a limitação do número de Áreas de Processo selecionadas (10), é possível realizar a comparação paritária com um tempo e esforço razoável, permitindo a concepção deste estudo de caso.

Em uma aplicação mais complexa utilizando o método proposto, toda a potencialidade do método AHP poderia ser explorada. No entanto, esta redução de escopo não compromete a validação deste método por meio deste estudo de caso.

Assim, todas as alternativas possíveis serão reunidas em um único nível abaixo do objetivo e do critério selecionados, como apresentado na figura 15.

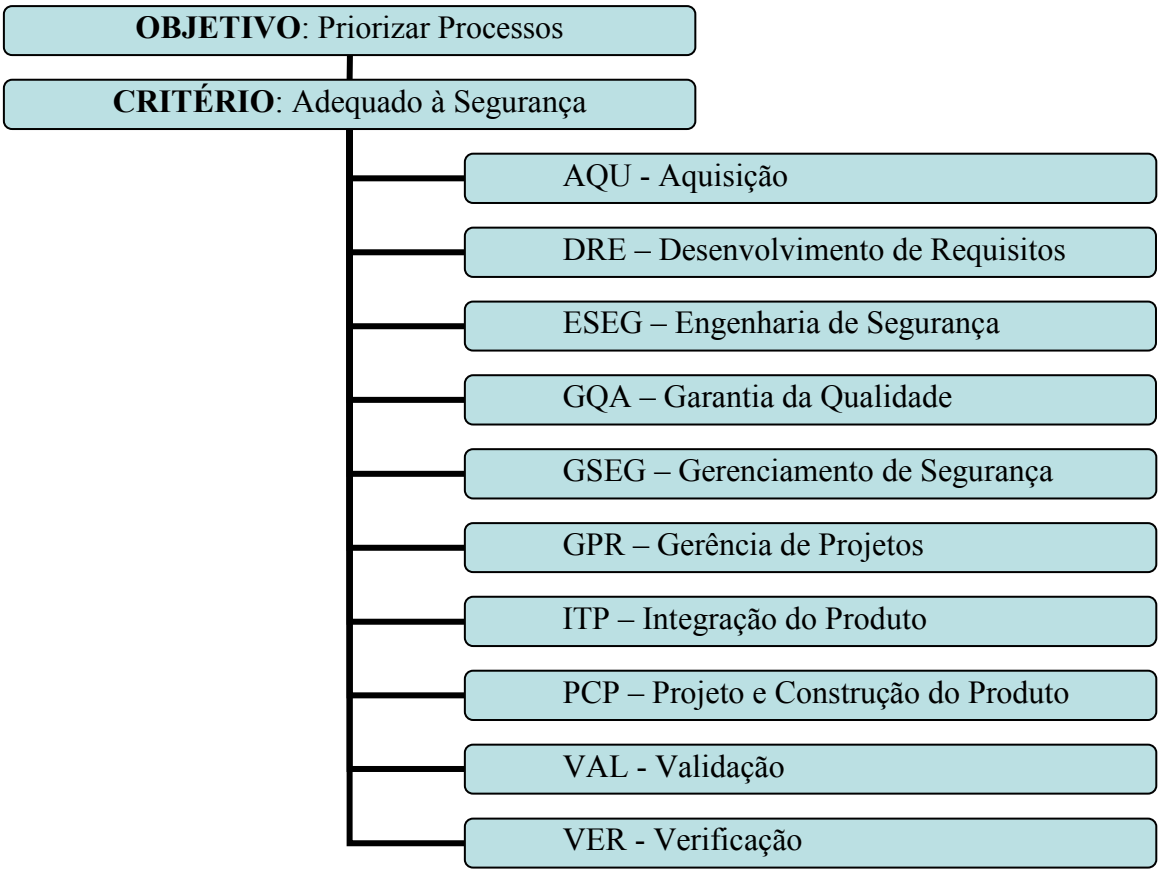

Figura 15 – Estudo de caso - Hierarquia

7.1.3 Realização do Julgamento

Nesta dissertação de mestrado, a escolha pela aplicação do questionário a um único especialista na área de segurança justifica-se por se priorizar uma maior ênfase no método proposto do que nos resultados inicialmente obtidos. Um julgamento piloto foi promovido com o uso de um questionário, e as informações obtidas são apresentadas em seguida, em formato matricial, para ilustrar a sua aplicação.

7.1.3.1 Obtenção de Julgamentos por meio de Questionário

O questionário aplicado, com as informações obtidas de julgamentos pelo processo piloto, é apresentado a seguir.

	Importância Relativa																
	9	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	
AQU													5					DRE
AQU														6				ESEG
AQU									1									GQA
AQU										2								GPR
AQU										2								GSEG
AQU									1									ITP
AQU											3							PCP
AQU										2								VAL
AQU											3							VER
DRE									1									ESEG
DRE								2										GQA
DRE							3											GPR
DRE								2										GSEG
DRE						4												ITP
DRE						4												PCP
DRE								2										VAL
DRE									1									VER
ESEG							3											GQA
ESEG						4												GPR
ESEG								2										GSEG
ESEG						4												ITP
ESEG						4												PCP
ESEG							3											VAL
ESEG								2										VER
GQA									1									GPR
GQA										2								GSEG
GQA								2										ITP
GQA										2								PCP
GQA									1									VAL
GQA										2								VER
GPR										2								GSEG
GPR									1									ITP
GPR										2								PCP
GPR										2								VAL
GPR											3							VER
GSEG								2										ITP
GSEG										2								PCP
GSEG										2								VAL
GSEG											3							VER
ITP										2								PCP
ITP										2								VAL
ITP											3							VER
PCP										2								VAL
PCP											3							VER
VAL											3							VER

Figura 16 – Questionário Piloto

7.1.3.2 Representação de Julgamentos no Modo Matricial

As mesmas informações obtidas pelo questionário são agora representadas na forma matricial para a exemplificação desta outra forma de se obter resultados.

Importância	AQU	DRE	ESEG	GQA	GPR	GSEG	ITP	PCP	VAL	VER
AQU		1/5	1/6	1	1/2	1/2	1	1/3	1/2	1/3
DRE			1	2	3	2	4	4	2	1
ESEG				3	4	2	4	4	3	2
GQA					1	1/2	2	1/2	1	1/2
GPR						1/2	1	1/2	1/2	1/3
GSEG							2	1/2	1/2	1/3
ITP								1/2	1/2	1/3
PCP									1/2	1/3
VAL										1/3
VER										

Figura 17 – Representação na Forma Matricial

7.1.4 Aplicação do Método AHP

Até o momento foi estabelecida a hierarquia e realizados os julgamentos das alternativas. Tipicamente, devido à possibilidade de uma modelagem mais avançada, e conseqüentemente maior complexidade dos cálculos envolvidos (GOODWIN, 2004), os próximos passos podem se beneficiar da utilização de ferramentas de *software* que implementam o método AHP.

No presente estudo de caso, a escolha pelo uso de uma ferramenta de *software* justifica-se pela exploração das soluções disponíveis no mercado e pela maior agilidade na realização de experimentos.

Pode-se citar alguns exemplos de ferramentas que implementam o método AHP, como o "*Super Decisions*", desenvolvido por William J. L. Adams para a *Creative Decisions Foundation*, e disponível em http://www.superdecisions.com, ou o "*Expert Choice*",

desenvolvido a partir de 1983 pelo Dr. Ernest Forman, utilizada em larga escala, e com uma versão de avaliação disponível em http://expertchoice.com .

As figuras a seguir correspondem a cópias de tela do *software Super Decisions*, utilizados no processo piloto de avaliação do método AHP para auxílio à decisão sobre as Áreas de Processo de *Software* mais importantes ou relevantes para a Segurança de um sistema.

Na figura 18, a janela principal do aplicativo é mostrada com o esboço da hierarquia elaborada neste estudo de caso. Nota-se os elementos Objetivo (*Goal*), Critérios (*Criteria*) e Alternativas (*Alternatives*), bem como os seus relacionamentos, visualizados por meio de setas.

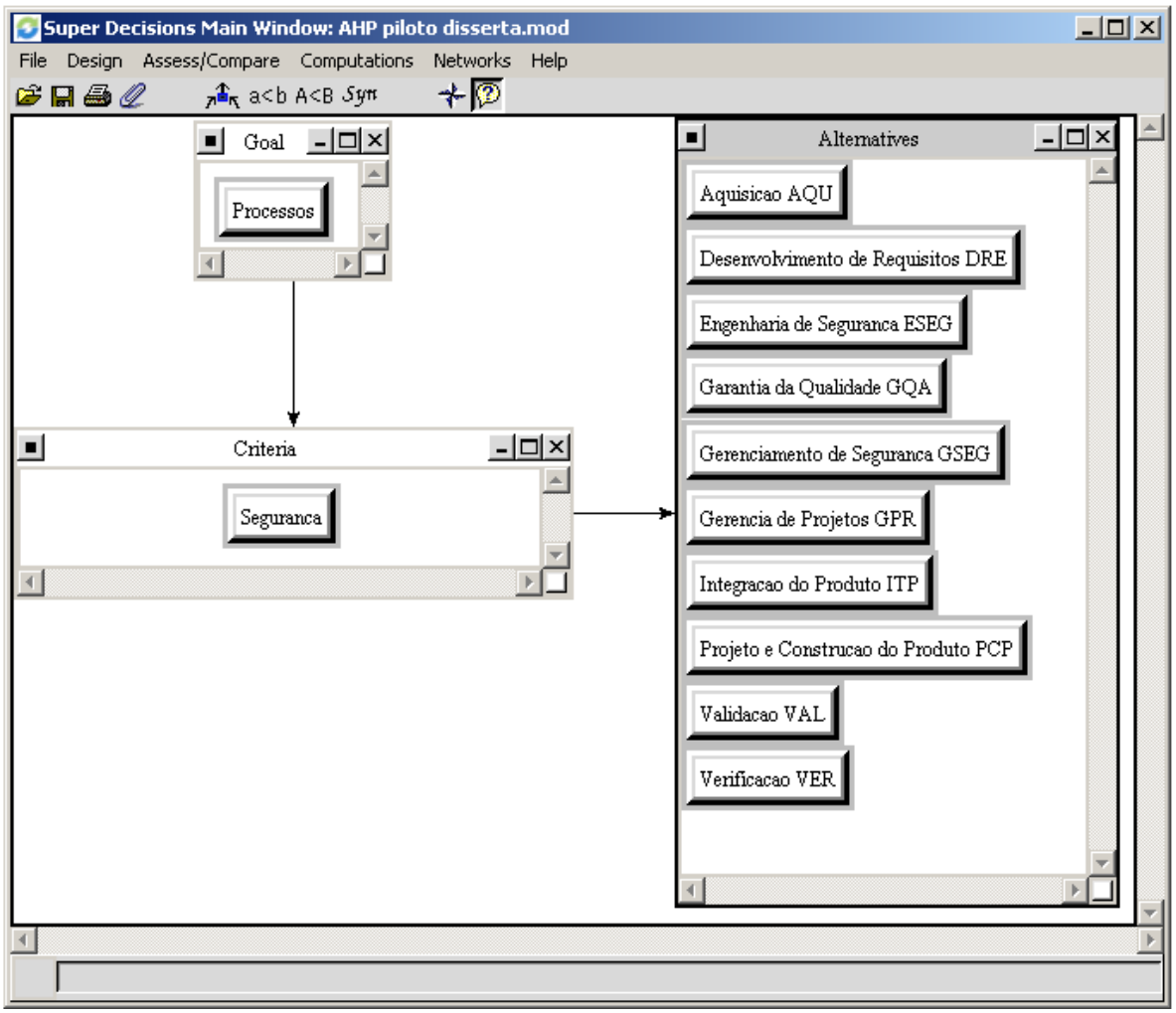

Figura 18 – Software Super Decisions – Hierarquia

Na figura 19, a janela de julgamentos (*comparisons*) no modo questionário é apresentada. Nesta etapa, as alternativas são apresentadas aos pares (45) para os quais são atribuídos valores relacionados com suas prioridades relativas, de acordo com a escala fundamental (de 1 a 9). No exemplo, é possível notar na linha 10 que o valor "1" selecionado indica que "*Desenvolvimento de Requisitos DRE*" é *igualmente importante* a "*Engenharia de Segurança ESEG*", de acordo com o critério "Segurança" (denominado "*Especialista 2*" na figura).

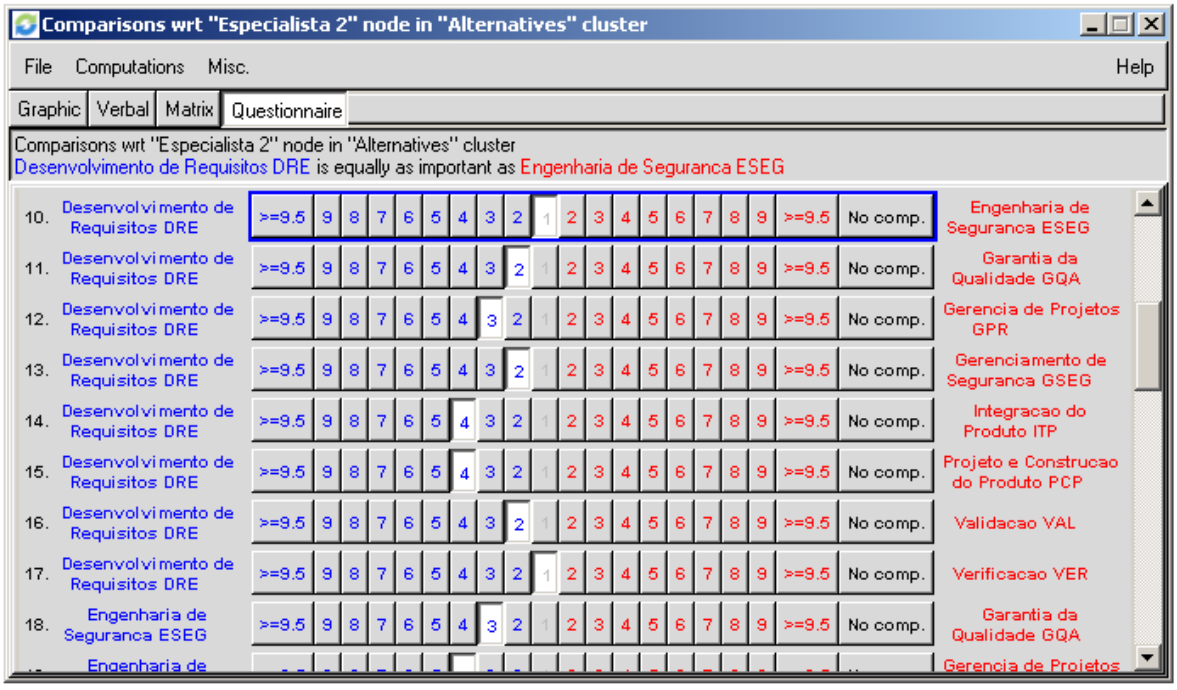

Figura 19 – Software Super Decisions - Julgamentos

Após a obtenção dos julgamentos, é possível obter as prioridades das alternativas referentes a este formulário, e o respectivo Índice de Consistência (IC), importante para uma pré-avaliação das resultados parciais obtidos até o momento obtidos, por meio desta comparação.

A figura 20 apresenta o IC para a matriz apresentada, o que pode ser observado pelo texto "*inconsistency index is 0.0339*". Além disso, podem ser observados os valores das prioridades relativas referentes a cada uma das 10 alternativas utilizadas neste estudo de caso.

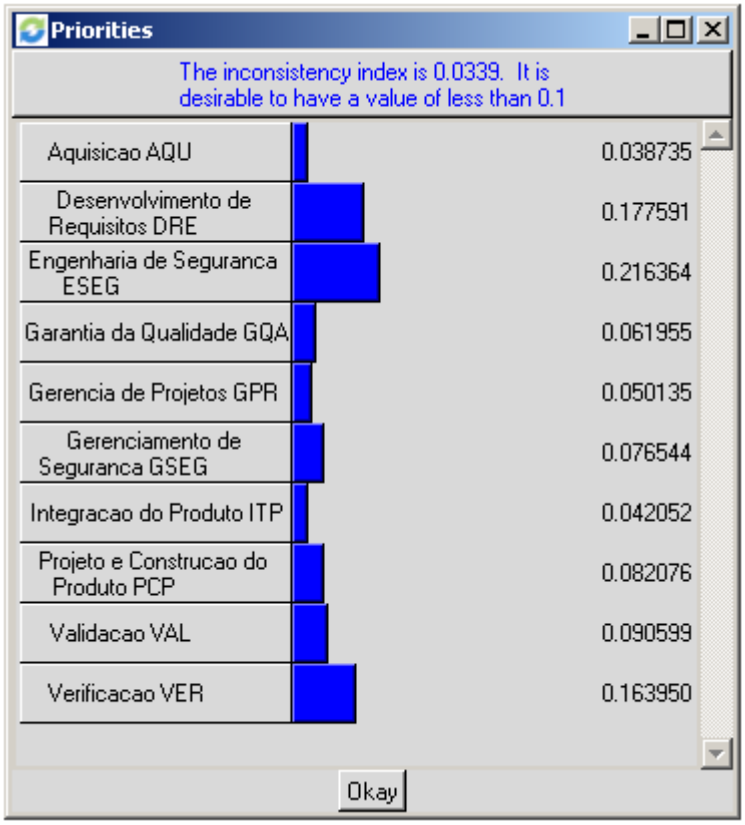

Figura 20 – Software Super Decisions – Índice de Consistência

Nota-se que o IC obtido está dentro do esperado (é menor do que 0,1, conforme apresentado no item 5.9), sendo aceitável afirmar que as comparações paritárias foram realizadas pelo julgador (especialista) de forma coerente.

Por fim, pode-se visualizar uma das possíveis representações dos resultados obtidos pelo *software Super Decisions*, que são as prioridades obtidas para cada alternativa representadas em modo gráfico e numérico, conforme apresentado na figura 21. Por exemplo, a coluna "*Normals*" apresenta os valores correspondentes às prioridades para cada alternativa de forma normalizada, com a soma das prioridades de todas as alternativas totalizando 1.

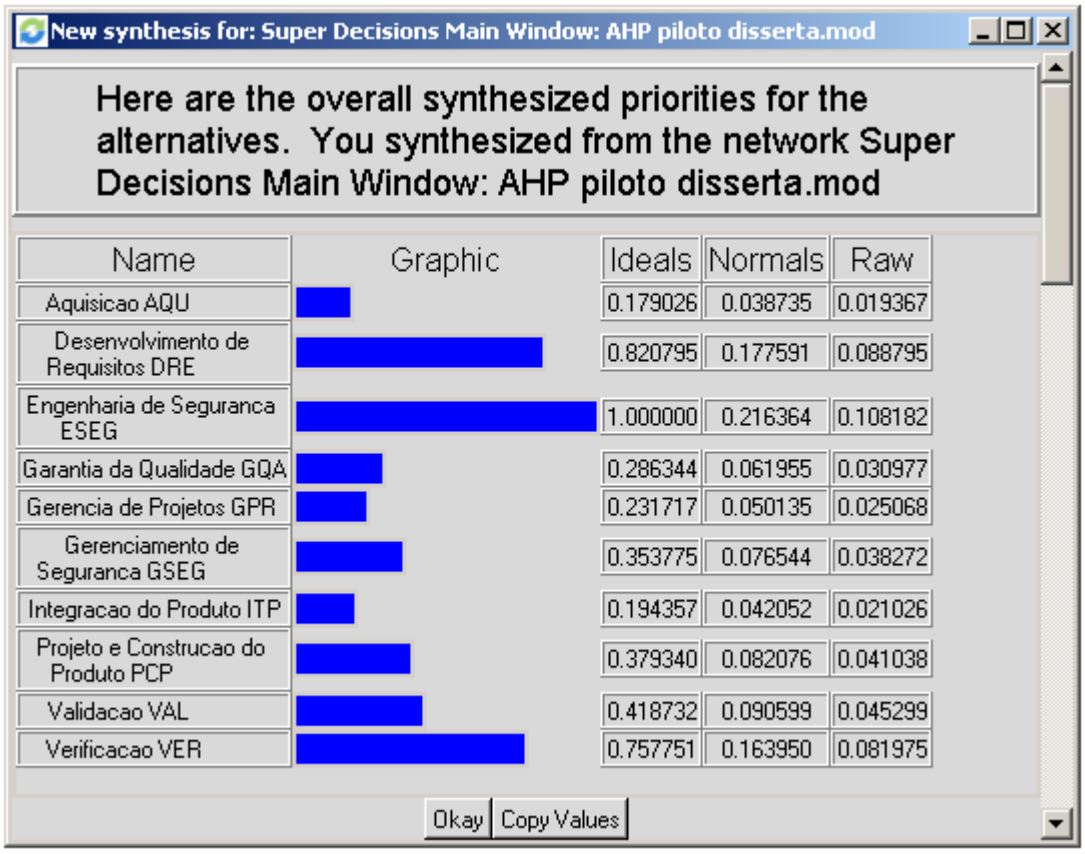

Figura 21 – Software Super Decisions - Resultados

A solução da hierarquia realizada pela ferramenta *software Super Decisions* permite obter as prioridades das alternativas mesmo quando existem muitos critérios e vários níveis hierárquicos, o que estaria adequado para aplicações mais apuradas de situações reais.

Os resultados obtidos nesta etapa são utilizados no item seguinte para a obtenção dos perfis de capacidade.

7.1.5 *Obtenção de Diferentes Perfis de Capacidade*

Após a obtenção das prioridades com o uso do método AHP, as Áreas de Processo (PAs) são dispostas de forma a se obter um perfil de capacidade, com cada área apresentando um nível de capacidade de 0 a 5. Com o método proposto, é possível obter-se resultados distintos

para cada Valor do Ganho k utilizado (definido no item 6.2.6), buscando-se com isso atingir a melhoria de processos de uma organização de forma incremental, de acordo com o valor k.

A seguir são apresentados, como exemplo, três perfis de capacidade adequados a organizações em diferentes estágios de capacidade de seus processos, por meio da seleção de Valores do Ganho k apropriados para cada caso.

7.1.5.1 Descrição da Planilha e Gráficos

Os perfis de capacidade neste estudo de caso foram obtidos com o uso de planilhas eletrônicas e seus elementos são ilustrados na figura 22.

Obtenção do Perfil de Capacidade			
Valor do Ganho k:		20	
		Perfil de Capacidade:	
PA	**AHP**	**objetivo**	**atual**
AQU	0,038735	0	0
DRE	0,177591	3	0
ESEG	0,216364	4	0
GQA	0,061955	1	0
GPR	0,050135	1	0
GSEG	0,076544	1	0
ITP	0,042052	0	0
PCP	0,082076	1	0
VAL	0,090599	1	0
VER	0,16395	3	0

Figura 22 – Planilha para Obtenção do Perfil de Capacidade – Caso 1

Na coluna PA (Áreas de Processo) da tabela presente na figura 22, são relacionadas todas as Áreas de Processo selecionadas para este estudo de caso. As siglas empregadas para cada área são depois utilizadas como legenda para a elaboração dos gráficos de "Perfil de Capacidade" apresentados para cada um dos estudos de casos deste capítulo.

Na coluna AHP, estão os dados correspondentes ao vetor V (prioridade das áreas de processo em relação ao objetivo) obtido com a aplicação do AHP no passo anterior.

A célula denominada "*Valor do Ganho k*" corresponde ao Valor do Ganho k escolhido para a obtenção de um determinado perfil de capacidade. Este valor pode ser livremente ajustado, de forma interativa, para se obter um perfil de capacidade adequado à maturidade atual da organização, e ao montante de recursos disponíveis para a melhoria dos processos.

Com estas informações, a coluna denominada "*objetivo*" é calculada de acordo com o método proposto descrito no capítulo 6, e contém os níveis de capacidade das áreas de processo objetivados. Ou seja, o vetor de prioridades V (coluna AHP) é multiplicado pelo Valor do Ganho k e os valores resultantes na coluna "*objetivo*" são arredondados para números inteiros compreendidos entre 0 e 5, correspondentes aos níveis de capacidade das Áreas de Processo definidos na representação contínua dos modelos de melhoria e avaliação de processos de *software*.

A coluna seguinte, denominada "*atual*", descreve o perfil de capacidade inicial da organização – que pode ser obtido por meio de avaliações segundo os modelos MR-MPS ou CMMI-DEV.

Para a planilha utilizada no Estudo de Caso 1 – Perfil Inicial, é admitido que os processos de desenvolvimento de software existentes não seguem estes modelos, ou ainda não exista uma avaliação, ainda que preliminar, sobre a maturidade da empresa. Neste caso, o valor zero é atribuído como forma de obter-se o perfil inicial.

Esta é uma situação esperada quando uma organização inicia o investimento na melhoria de processos por meio da aplicação de modelos de capacidade e maturidade.

7.1.5.2 Estudo de Caso 1 – Perfil Inicial

Para este primeiro estudo de caso foi escolhido um valor de k (igual a 20, como mostra a figura 22 no item anterior) de modo a se atingir um perfil de capacidade, considerando que a

organização ainda não dispõe de uma avaliação inicial de capacidade de suas áreas de processo de desenvolvimento de *software* ou ainda não adotou um modelo de capacidade e maturidade.

O Valor do Ganho escolhido arbitrariamente permite o levantamento de diferentes perfis de capacidade, adequados ao volume de recursos que estima-se ser suficiente para representar um alvo para esta situação.

O perfil de capacidade obtido para este estudo de caso está representado na figura 23.

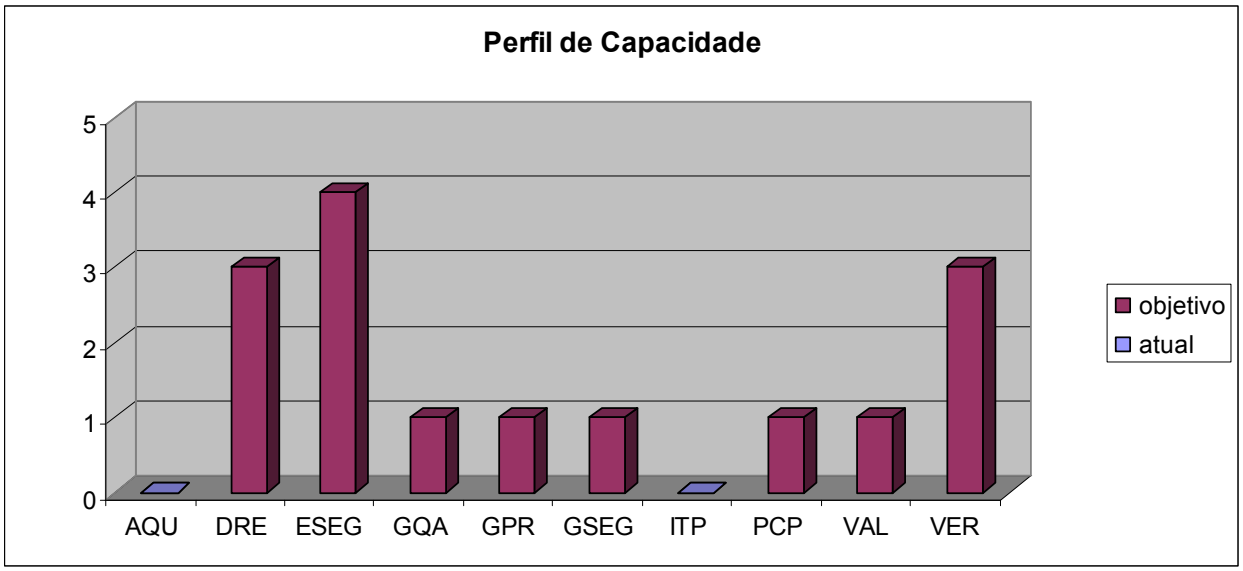

Figura 23 – Perfil de Capacidade 1

No Perfil de Capacidade 1, tem-se a situação atual em que todas as áreas de processos estão no nível de capacidade 0 (incompleto) do modelo MR-MPS. Pode-se verificar, então, uma proposta de implantação inicial, em que a maior parte das áreas de processo estão nos níveis 0 (incompleto) e 1 (realizado), que correspondem, respectivamente, à adoção parcial das práticas específicas (SPs) no nível 0 e a satisfação completa destas no nível 1, ainda que de forma não gerenciada.

Em uma organização que se proponha a aumentar radicalmente o nível de capacidade de uma área de processo – neste exemplo ESEG, de 0 diretamente para 4 – aplicando os atributos de processo do modelo MR-MPS ou práticas genéricas do CMMI-DEV pertinentes, observa-

se uma significativa otimização com o direcionamento de recursos, e espera-se uma obtenção de resultados mais rápida e uma preparação mais ágil para se atingir níveis altos de capacidade em outras áreas de processo relevantes no futuro.

7.1.5.3 Estudo de Caso 2 – Organização CMMI-DEV nível 2

Neste estudo de caso, busca-se apresentar um exemplo em que as áreas correspondentes ao CMMI-DEV nível 2 já estejam implementadas na organização, e deseja-se ampliar a capacidade dos processos de acordo com os resultados obtidos por meio do método proposto.

Para tanto, foi selecionado um valor de k mais elevado (igual a 35), de modo a permitir uma substancial melhoria das áreas de processo de desenvolvimento de *software* por parte da organização, considerando as mesmas prioridades já estabelecidas após a aplicação do método AHP.

A nova planilha apresentada na figura 24, apresenta as mesmas prioridades obtidas pelos julgamentos realizados inicialmente, e além do novo valor de k e os novos objetivos calculados, a representação do estágio atual da capacidade das áreas de processo selecionadas que correspondem ao nível 2 do CMMI-DEV.

Obtenção do Perfil de Capacidade			
Valor do Ganho k:		**35**	
		Perfil de Capacidade:	
PA	**AHP**	**objetivo**	**atual**
AQU	0,038735	1	**2**
DRE	0,177591	5	0
ESEG	0,216364	5	0
GQA	0,061955	2	**2**
GPR	0,050135	1	**2**
GSEG	0,076544	2	0
ITP	0,042052	1	0
PCP	0,082076	2	0
VAL	0,090599	3	0
VER	0,16395	5	0

Figura 24 – Planilha para Obtenção do Perfil de Capacidade – Caso 2

Na figura 25 apresenta-se o estado atual das áreas de processo da organização avaliadas e o objetivo a ser atingido, de acordo com os critérios estabelecidos pelo método proposto neste trabalho.

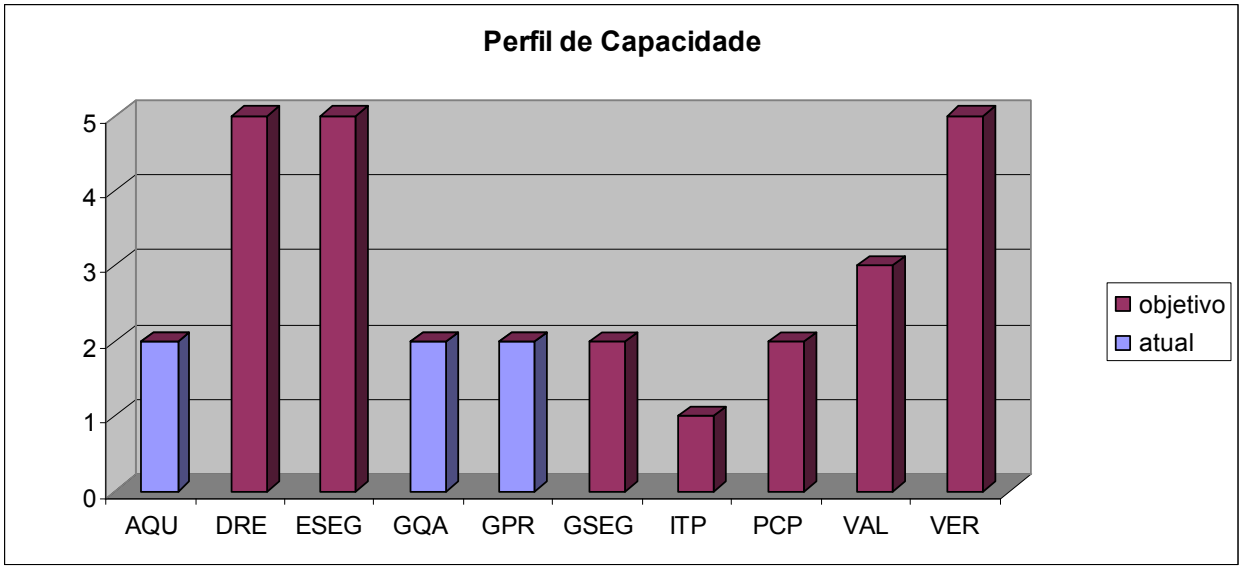

Figura 25 – Perfil de Capacidade 2

Neste exemplo, a organização já tem um nível de maturidade equivalente ao CMMI-DEV nível 2 (ou MR-MPS nível F), ou seja, suas áreas de processos AQU, GQA e GPR já possuem no estado inicial o nível de capacidade 2. Neste caso, verifica-se uma possibilidade de

melhoria substancial de capacidade da organização. Esta melhoria implica a execução de todas as práticas específicas recomendadas na área de processo ITP (nível de capacidade 1 a ser atingido) e a implementação gerenciada das áreas GSEG e PCP (nível de capacidade 2), enquanto que as demais áreas apresentam níveis mais altos de capacidade, pois são consideradas mais relevantes à segurança de um sistema crítico, de acordo com os julgamentos realizados no estudo de caso deste trabalho (áreas DRE, ESEG, VAL e VER, que apresentam níveis de capacidade 3 ou 5).

7.1.5.4 Estudo de Caso 3 – Organização de Alta Maturidade

Para este terceiro estudo de caso, aumentou-se ainda mais a expectativa em relação à melhoria de processos de *software* de uma organização. Neste terceiro perfil de capacidade, admite-se uma organização que tenha atingido um nível de maturidade equivalente ao CMMI-DEV nível 3 (ou MR-MPS nível C), e que esteja caminhando para um nível de capacidade mais elevado. Adotou-se, para tanto, um valor de k ainda mais elevado (igual a 65).

Para Valores do Ganho k mais elevados, será alcançada a saturação do modelo, com a prescrição de níveis de capacidade máximos em todas as áreas de processo – o que não é interessante para a tarefa de priorização proposta, e tampouco indicada para organizações de alta maturidade, equivalente aos níveis 4 e 5 do CMMI ou B e A do MR-MPS.

A nova planilha apresentada na figura 26, apresenta prioridades idênticas aos casos apresentados anteriormente, e a representação do estágio atual da capacidade das áreas de processo selecionadas que correspondem ao nível 3 do CMMI-DEV.

Obtenção do Perfil de Capacidade			
Valor do Ganho k:		**65**	
		Perfil de Capacidade:	
PA	**AHP**	**objetivo**	**atual**
AQU	0,038735	2	**3**
DRE	0,177591	5	**3**
ESEG	0,216364	5	0
GQA	0,061955	4	**3**
GPR	0,050135	3	**3**
GSEG	0,076544	4	0
ITP	0,042052	2	**3**
PCP	0,082076	5	**3**
VAL	0,090599	5	**3**
VER	0,16395	5	**3**

Figura 26 – Planilha para Obtenção do Perfil de Capacidade – Caso 3

Na figura 27 apresenta-se o estado atual das áreas de processo da organização avaliadas e o objetivo a ser atingido, de acordo com os critérios estabelecidos pelo método proposto neste trabalho.

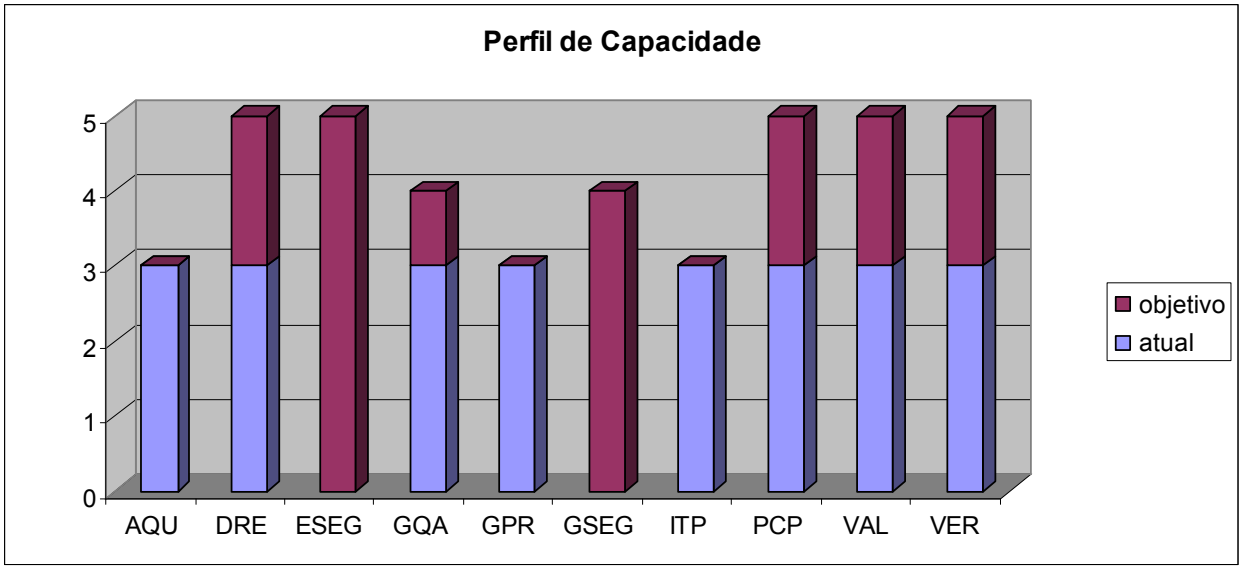

Figura 27 – Perfil de Capacidade 3

Vale notar que a aplicação de um método como o AHP é imposta pela área de processo DAR (*Decision Analysis and Resolution*) do CMMI-DEV, prescrita em seu nível de

maturidade 3. Como esta área não foi escolhida neste estudo de caso como uma área diretamente relacionada com aspectos de segurança, não aparece nas figuras apresentadas.

Acrescenta-se, ainda, que nos níveis de maturidade 4 e 5 definidos pelo modelo CMMI-DEV não há necessidade de todas as áreas de processo estarem simultaneamente nos níveis de capacidade 4 e 5, respectivamente.

A escolha das áreas de processo que devem atingir os níveis de capacidade 4 e 5, utilizando a priorização por especialistas na área de segurança, é uma característica de organizações dos altos níveis de maturidade CMMI-DEV 4 e 5 (ou MR-MPS níveis B e A), e implica ainda em um forte indício da prevalência de uma cultura de segurança.

Pode-se concluir a partir deste terceiro estudo de caso que o método proposto é adequado para organizações que desejam atingir os elevados níveis de maturidade 4 e 5 contribuindo, ainda, para a definição das áreas de processos mais adequadas à segurança, segundo o julgamento de especialistas na área.

7.2 Considerações Finais do Capítulo

A flexibilidade do método proposto no Capítulo 6 e utilizado neste capítulo permite o suporte à importante decisão sobre a melhoria de processos de desenvolvimento de *software* sob diferentes circunstâncias. O emprego de um modelo de decisão por múltiplos critérios aumenta as possibilidades de uma organização obter subsídios para a sua auto-avaliação no tocante aos aspectos de melhoria dos seus processos de desenvolvimento de *software*.

Os resultados obtidos apontam para a aplicação do método proposto considerando hipóteses diversas de níveis de capacidade dos processos da organização, obedecendo às prioridades obtidas pelos julgamentos.

Nos três estudos de caso apresentados, admitindo organizações com diferentes níveis de maturidade em seu processo de desenvolvimento de *software*, a aplicação do método proposto para a priorização da melhoria da capacidade das áreas de processo, em concordância com a opinião dos especialistas em sistemas críticos, é um indicativo da cultura de segurança da empresa.

A determinação de níveis de capacidade apropriados para habilitar uma organização a desenvolver sistemas críticos não poderá ser alcançada sem a realização de um vasto conjunto de avaliações e uma análise profunda dos resultados obtidos, e ainda assim possivelmente não será suficiente.

No entanto, a possibilidade de envolver especialistas em segurança nesta importante decisão é um forte indício da cultura de segurança da organização – e este é um atributo preponderante para a obtenção de *software* adequado a sistemas críticos.

8 Conclusão e Considerações Finais

A oportunidade de melhoria dos processos de desenvolvimento de *software* utilizando modelos, orientada pelas fortes necessidades impostas pela sua aplicação intensiva em sistemas críticos de segurança, indica que este é um caminho a ser percorrido para se obter *software* adequado a estes sistemas. Espera-se com este trabalho de pesquisa promover um aumento da compreensão e percepção da relação entre os processos de *software* e os objetivos de segurança, e sinalizar em direção às práticas recomendadas para a obtenção de sistemas seguros.

Este trabalho de pesquisa apresenta um conjunto de informações necessárias para uma abordagem coerente de aspectos genéricos da qualidade de *software* e de sua aplicação em sistemas críticos de segurança, propondo um método para a melhoria e avaliação de processos de *software*, baseado em modelos de referência adequadamente priorizados a favor da segurança.

O método proposto neste trabalho demonstrou-se viável para aplicação em organizações em diferentes estágios de maturidade com relação aos processos de desenvolvimento de *software*, permitindo realizar a prescrição de aspectos supostamente mais relevantes à segurança, considerando os julgamentos dos especialistas nesta área.

8.1 Conclusões

Espera-se que, com a sua utilização, o método proposto neste trabalho de pesquisa possa servir como base para um *benchmark* de segurança, com a obtenção de informações objetivas de projetos de sistemas críticos e as práticas empregadas para o cumprimento de suas características de segurança especificadas no domínio de aplicação.

As discussões de especialistas acerca do tema da segurança, em decorrência da aplicação do método proposto neste trabalho no tocante ao julgamento de prioridades, pode permitir sinalizar para a obtenção de *softwares* mais adequados a sistemas críticos, em seu contexto de projeto. Pode-se ainda se utilizar deste método para um registro dos resultados das discussões dos especialistas, permitindo um avanço de opiniões na área.

A proposta de uso de um processo analítico com obtenção de valores numéricos para apoio às decisões inerentes à modelagem de processos de *software*, com base em julgamentos subjetivos e qualitativos, representa uma contribuição interessante para as etapas de especificação e avaliação de engenharia de *software*, com a produção de resultados relevantes, e no campo científico, representa uma valiosa oportunidade para a consolidação do conhecimento abrangente.

A aposta no desenvolvimento de sistemas críticos com foco na qualidade de *software*, para se obter um produto adequado em relação à segurança na operação dos sistemas controlados, é uma importante contribuição para o progresso tecnológico.

O uso de ferramental específico para o auxílio a tomada de decisão se mostra adequado para a solução de problemas complexos e de natureza qualitativa, conforme empregado para o método proposto, acomodando uma vasta gama de alternativas e critérios, dispostos de forma organizada.

A descrição sucinta do método AHP realizada neste trabalho, e o estudo de seus elementos e aplicações, indica que este modelo de decisão por múltiplos critérios é importante e adequado para sintetizar as opiniões de especialistas através de julgamentos qualitativos, para a obtenção das prioridades numéricas sobre as alternativas escolhidas.

Os resultados obtidos nos estudos de caso indicam a flexibilidade do método proposto, e a possibilidade de aplicação em diversos estágios de maturidade das organizações,

prescrevendo benefícios com a melhoria dos processos de desenvolvimento de software prioritários.

8.2 Propostas de Trabalhos Futuro

Com base nos resultados obtidos na realização deste trabalho de pesquisa, pode-se propor as seguintes continuidades para este trabalho:

- A aplicação do método proposto, considerando os julgamentos por especialistas de diversas áreas de aplicação dos sistemas críticos de segurança, e a análise dos resultados obtidos, podem servir como base para a comparação e obtenção de conclusões sobre diferentes abordagens possíveis;
- A análise de sensibilidade dos resultados, frente aos julgamentos de um grande número de especialistas – com experiências diferentes nas áreas prática e acadêmica, pode revelar tendências a preferência por diferentes formas de abordar a melhoria de processos de desenvolvimento de *software*;
- Aplicação da lógica nebulosa (*fuzzy*) pode ser estudada para permitir uma flexibilidade ainda maior na obtenção dos julgamentos qualitativos, quando comparada à escala fundamental do AHP, com números inteiros, e o estudo aprofundado do comportamento deste método;
- A análise das diferentes possibilidades de evolução da capacitação dos processos de desenvolvimento de *software* em uma organização considerando além de sua priorização, os custos decorrentes da melhoria dos processos de forma a obter uma matriz de custo x benefício;
- A aplicação deste método em outras áreas de desenvolvimento de *software*, não associadas aos sistemas críticos, exercitando um aspecto genérico deste método, pode trazer benefícios às organizações que escolham a representação contínua dos modelos de melhoria de maturidade e capacidade.

8.3 Considerações Finais

O método para aplicação de modelos de melhoria e avaliação do processo de desenvolvimento de *software* em sistemas críticos de segurança, apresentado no presente trabalho, mostra-se adequado para a aplicação direta em uma organização, assim como revela uma grande oportunidade de discussões e trabalhos futuros.

A disseminação de informações sobre os avançados modelos de processo de desenvolvimento de *software* disponíveis na atualidade, entre especialistas em sistemas críticos de segurança, possibilita um maior domínio sobre práticas valiosas da indústria de *software* e formas comuns de sua implementação em uma organização.

Ademais, o envolvimento de especialistas em sistemas críticos de segurança na definição de uma abordagem adequada para a melhoria do processo de desenvolvimento de *software* em uma organização pode ser considerado um bom indício, e uma excepcional prática, da construção de sua cultura de segurança.

Outro importante aspecto a ser salientado, é a potencialização do trabalho realizado por pesquisadores e profissionais da área de Engenharia de *software*, com a possibilidade de ponderar e priorizar a introdução de novos conceitos e práticas adequadas ao desenvolvimento de sistemas críticos de segurança.

Por fim, a aplicação do método apresentado admite uma forte interação entre os especialistas em segurança de sistemas críticos, e os pesquisadores e profissionais da área de Engenharia de *software*. O autor espera, humildemente, contribuir com o seu trabalho desta forma.

REFERÊNCIAS BIBLIOGRÁFICAS

ADD/DMO *Australian Department of Defence*, *Defence Materiel Organisation,* "+SAFE, V1.2 *A Safety Extension to* CMMI-DEV, V1.2", *Software Engineering Institute*, Carnegie Mellon University, 2007.

<www.sei.cmu.edu/pub/documents/07.reports/07tn006.pdf> acessado em 03/09/2007.

AHMAD, Norita; Laplante, Phillip A., *Penn State University, "Software Project Management Tools: Making a Practical Decision Using AHP"*, Proceedings of the 30th Annual IEEE/NASA *Software* Engineering Workshop SEW-30, IEEE, 2006.

ALBUQUERQUE, R., Ribeiro, B, "Segurança no Desenvolvimento de *Software*", Editora Campus, 2002.

ANSI/IEEE, "*Standard Glossary of Software Engineering Terminology*", STD-729-1991, ANSI/IEEE, 1991.

CARLSON, J. M.; Doyle, John; "Complexity and robustness", *Proceedings of the National Academy os Sciences of the United States of America, 2002.*

CENELEC BS EN 50126:1999, "*Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety* (RAMS)", CENELEC, 2001.

_____. BS EN 50128:2001, "*Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems*", CENELEC, 2001.

_____. BS EN 50129:2003 "*Railway Applications: Safety Related Electronic System for Signalling*", CENELEC, 2003.

CHRISSIS, M. B., Konrad, M., Shrum, S., "*CMMI: guidelines for process integration and product improvement*", *SEI Series in Software Engineering*, Addison Wesley, 2007.

CMU/SEI *Software* Engineering Institute, Carnegie Mellon University CMMI Product Development Team, "*CMMI for Development, Version 1.2*" (CMU/SEI-2006-TR-008, ESC-TR-2006-08), August 2006. <http://www.sei.cmu.edu/publications/documents/06.reports/06tr008.html> acessado em 17/09/2007

CMU/SEI *Software* Engineering Institute, Carnegie Mellon University CMMI Product Development Team, "*Standard CMMI Appraisal Method for Process Improvement (SCAMPI), Version 1.2 Method Definition Document*" (CMU/SEI-2006-HB-002), August 2006. <http://www.sei.cmu.edu/publications/documents/06.reports/06hb002.html> acessado em 17/09/2007

COUTO, Ana Brasil, "CMMI – Integração dos Modelos de Capacitação e Maturidade de Sistemas", Ed. Ciência Moderna, 2007.

DALE, C.; Paul Rook (ed.) – "*Software Reliability Handbook*" – Elsevier Applied Science, 1990.

FIRESMITH, Donald G., "*Common Concepts Underlying Safety, Security, and Survivability Engineering*", *Software Engineering Institute*, Carnegie Mellon University, 2003. <http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03tn033.pdf> acessado em 11/06/2006.

_____., "*Engineering Safety-Related Requirements for Software-Intensive Systems, 13th IEEE International Requirements Engineering Conference"*, Tutorial, 2005. <http://www.sei.cmu.edu/programs/acquisition-support/presentations/firesmith/safetyrelated/safetyrelated.pdf> acessado em 11/06/2006.

FONSECA, José Antonio, "Uma Extensão de RAMS para o modelo CMMI baseada nas normas ferroviárias CENELEC", Escola Politécnica da Universidade de São Paulo, 2005.

GARCIA, S.; Turner, R., "*CMMI Survival Guide – Just Enough Process Improvement*", *SEI Series in Software Engineering*, Addison Wesley, 2006.

GUERRA, A. C., Alves, A. M., "Aquisição de Produtos e Serviços de *Software*", Elsevier, 2004.

GRADY, Robert B.; Caswell, Deborah L.- "*Software Metrics: Establishing a Company-Wide Program*." Prentice Hall, 1987.

_____. - "*Practical Software Metrics for Project Management and Process Improvement*". Prentice Hall, 1992.

GUSTAFSON, D. A., Trad. Campos, F. C. A., "Teoria e problemas de engenharia de *software*", (Coleção Schaum), Bookman, 2003.

HOFMANN, Hubert F., Yedlin, Deborah K., Mishler, John W., Kushner, Susan, "*CMMI for Outsourcing: Guidelines for Software Systems, and IT Acquisition*", SEI *Series in Software Engineering*, Addison Wesley, 2007.

HUMPHREY, Watts S., "Managing the Software Process", Addison-Wesley, 1989.

IBRAHIM, Linda, Jarzombek, J., Ashford, M., "*Integrity Assurance: Extending the CMMI & iCMM for Safety and Security*", The Federal Aviation Administration FAA, 2002.

IBRAHIM, Linda, Jarzombek, J., Ashford, M., Bate, R., Croll, P., Horn, M., LaBruyere, L., Wells, C., "*Safety and Security Extensions for Integrated Capability Maturity Models*", The Federal Aviation Administration FAA, 2004.

IEC 61508, "*Functional safety of electrical/electronic/programmable electronic safety related systems - Part 5: Examples of methods for the determination of safety integrity levels*", International Electrotechnical Commission (IEC), 1998.

IEC 2002, "*Functional safety and IEC 61508: A basic guide*", International Electrotechnical Commission (IEC), 2002

IEEE Std 1483-2000, "*IEEE Standard for Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control*", IEEE, 2000.

ISO/IEC 12207, "Information Technology – Software Life Cycle Processes", International Organization for Standardization, International Electrotechnical Commission, 1995.

ISO/IEC 15504, "*Information Technology - Process Assessment",* International Organization for Standardization, International Electrotechnical Commission, 2004a.

ISO/IEC 90003, "*Software engineering – Guidelines for the application of ISO 9001:2000 to computer software*", International Organization for Standardization, International Electrotechnical Commission, 2004b.

ISO/IEC 9126-1, "*Information technology - Software quality characteristics and metrics - Part 1: Quality characteristics and sub characteristics, International Organization for Standardization*", International Electrotechnical Commission, 1991.

JOHNSON, Barry W. –"*Design and Analyses of fault-Tolerant Digital Systems*" – Addison-Wesley, 1989.

LAHOZ, Carlos H. N., Burgareli, L. A., Moura, Carlos A. T., "Melhoria e confiabilidade em desenvolvimento de *software* para projetos espaciais", II workshop de segurança (Safety Workshop): Sistemas Eletro-Eletrônicos e Programáveis, EPUSP, 2004.

LEVESON, N. G., "*SAFEWARE: System Safety and Computers*", Addison-Wesley, 1995.

LYU, Michael R. (ed.) – "*Handbook of Software Reliability Engineering*", McGraw-Hill, 1996.

MIL-Std-882C:1996, "*System Safety Program Plan Requirements*."

MIRANDA, Eduardo, Ericsson Research Canada, "*Improving Subjective Estimates Using Paired Comparisons*", IEEE *Software* fl. 87-91, 2001

MOUETTE, Dominique, "Utilização do método de análise hierárquica no processo de tomada de decisão no planejamento de transporte urbano: uma análise voltada aos impactos ambientais", Universidade Estadual de Campinas, 1993.

MPS.BR, ASSOCIAÇÃO PARA PROMOÇÃO DA EXCELÊNCIA DO *SOFTWARE* BRASILEIRO – SOFTEX, MPS.BR – Guia Geral, versão 1.2, junho 2007. <http://www.softex.br/mpsbr/_guias/MPS.BR_Guia_Geral_V1.2.pdf> acessado em 20/09/2007.

_____., MPS.BR – Guia de Implementação – Parte 1, versão 1.1, junho 2007. <http://www.softex.br/mpsbr/_guias/ MPS.BR_Guia_de_Implementacao_Parte_1_V1.1.pdf> acessado em 20/09/2007.

_____., MPS.BR – Guia de Implementação – Parte 2, versão 1.1, junho 2007. <http://www.softex.br/mpsbr/_guias/ MPS.BR_Guia_de_Implementacao_Parte_2_V1.1.pdf> acessado em 20/09/2007.

_____., MPS.BR – Guia de Implementação – Parte 3, versão 1.1, junho 2007. <http://www.softex.br/mpsbr/_guias/ MPS.BR_Guia_de_Implementacao_Parte_3_V1.1.pdf> acessado em 20/09/2007.

_____., MPS.BR – Guia de Implementação – Parte 4, versão 1.1, junho 2007. <http://www.softex.br/mpsbr/_guias/ MPS.BR_Guia_de_Implementacao_Parte_4_V1.1.pdf> acessado em 20/09/2007.

_____., MPS.BR – Guia de Implementação – Parte 5, versão 1.1, junho 2007. <http://www.softex.br/mpsbr/_guias/ MPS.BR_Guia_de_Implementacao_Parte_5_V1.1.pdf> acessado em 20/09/2007.

_____., MPS.BR – Guia de Implementação – Parte 6, versão 1.0, junho 2007. <http://www.softex.br/mpsbr/_guias/ MPS.BR_Guia_de_Implementacao_Parte_6_V1.0.pdf> acessado em 20/09/2007.

_____., MPS.BR – Guia de Implementação – Parte 7, versão 1.0, junho 2007. <http://www.softex.br/mpsbr/_guias/ MPS.BR_Guia_de_Implementacao_Parte_7_V1.0.pdf> acessado em 20/09/2007.

_____., MPS.BR – Guia de Avaliação, versão 1.1, junho 2007. <http://www.softex.br/mpsbr/_guias/ MPS.BR_Guia_de_ Avaliacao_V1.1.pdf> acessado em 20/09/2007.

MUSA J.D. – "*Software Reliability Engineering*", McGraw-Hill, 1999.

MUTAFELIJA, B. - "ISO 9001:2000 – CMMI v1.1 *Mappings*", 2003. <http://www.sei.cmu.edu/cmmi/adoption/pdf/iso-mapping.pdf> acessado em 20/09/2007.

PAMPLONA, Edson de O., "Justificativas para Aplicação do Método de Análise Hierárquica", 19.o ENEGEP, Rio de Janeiro RJ, 1999.

PÁSCOA, João Eduardo Proença, "Fatores e subfatores para avaliação da segurança em *software* de sistemas críticos", Escola Politécnica da Universidade de São Paulo, 2002.

PSM, Safety & Security Technical Work Group, "*Safety Measurement White Paper*", Practical *Software* and Systems Measurement, 2006. http://www.psmsc.com/Downloads/TechnologyPapers/SafetyWhitePaper_v3.0.pdf acessado em 20/09/2007.

PRESSMAN, Roger S., "*Software Engineering, A Practitioner's Approach*", McGraw-Hill, 2001.

RAILTRACK, "*Engineering Safety Management – Yellow Book 3 volume I Fundamentals*", Railtrack PLC, Praxis Critical Systems, 2000.

SAATY, Thomas L., "*Axiomatic Foundation of the Analytic Hierarchy Process*", Management Science, vol. 32, n. 7, Julho 1986.

_____., "*Physics as a Decision Theory*", European Journal of Operational Research, n. 48, fls. 98-104, 1990.

_____., "*How to make a decision: The Analytic Hierarchy Process*", European Journal of Operational Research, n. 48, fls. 9-26, 1990b.

_____., "Método de análise hierárquica", Silva, Wainer da Silveira, trad. e rev. técnica, McGraw-Hill, Makron 1991.

_____., "*Decision Making with the Analytic Network Process – Economic, Political, Social and Technological Applications with Benefits, Opportunities, Costs and Risks*", Springer Science and Business Media LLC, 2006.

SANTOS, Reginaldo J.; "Introdução à Álgebra Linear". Universidade Federal de Minas Gerais, 2008. <http://www.mat.ufmg.br/~regi> acessado em 01/04/2008.

SEPIN/MCT, "Qualidade e Produtividade no Setor de *Software* Brasileiro", Ministério da Ciência e Tecnologia, Secretaria de Política de Informática, 2002.

SOFTEX, "Workshop do Projeto de melhoria de processo do *software* Brasileiro (mps Br), Curso Oficial: Introdução ao Modelo de Referência para melhoria de processo de *software*", Sociedade para Promoção da Excelência do *Software* Brasileiro, 2004.

STOREY, N., "*Safety Critical Computer Systems*", New York: Addison-Wesley, 1996.

WANG, Y.M., Luo, Y.,Hua, Z., "On the extent analysis method for fuzzy AHP and its applications", European Journal of Operational Research, Janeiro de 2007.

WANG, K., Wang, C. K., Hu, C., "Analytic Hierarchy Process With Fuzzy Scoring in Evaluating Multidisciplinary R&D Projects in China", IEEE Transactions on Engineering Management, Fevereiro de 2005.

WEBWER, K. C., "Avaliação do Modelo MPS em Empresas em 2005 e 2006", SOFTEX – Associação para Promoção da Excelência do *Software* Brasileiro, PBQP, 2006.

VAIDYA, Omkarprasad S.; Kumar, Sushil, "*Analytic Hierarchy Process: An overview of applications*", European Journal of Operational Research, 169 (2006) 1-29, 2004.

ANEXO A

Neste anexo são relacionadas as Áreas de Processos (PAs) organizadas por níveis de maturidade – conforme a sua definição nos Guias de Implementação do MR-MPS (MPS.BR, 2007b), (MPS.BR, 2007c), (MPS.BR, 2007d), (MPS.BR, 2007e), (MPS.BR, 2007f), (MPS.BR, 2007g), (MPS.BR, 2007h).

Para cada Área de Processo (PA), é apresentado o nível de maturidade correspondente à sua aplicação na representação em estágios do modelo MR-MPS, o seu propósito e sua classificação em categorias de forma análoga ao apresentado pelo modelo CMMI. Tabelas são apresentadas com as respectivas Práticas Específicas para cada Área de Processo, conforme definição presente nos Guias de Implementação do modelo MR-MPS.

As Áreas de Processo que possuem Práticas Específicas exclusivas ou modificadas para Níveis de Maturidade específicos, são identificadas pelo termo “evolução”, e divididas em itens diferentes para adequar à sua aplicação no estudo de caso.

A.1 Gerência de Projetos – GPR

Nível G – Parcialmente Gerenciado (MPS.BR, 2007b)

Categoria de Processo: Gerenciamento de Projeto

O propósito da Área de Processo Gerência de Projetos é estabelecer e manter planos que definem as atividades, recursos e responsabilidades do projeto, bem como prover informações sobre o andamento do projeto que permitam a realização de correções quando houver desvios significativos no desempenho do projeto.

Tabela 26 – Práticas Específicas GPR

Nível	Práticas Específicas	
G	GPR 1	O escopo do trabalho para o projeto é definido.
G	GPR 2	As tarefas e os produtos de trabalho do projeto são dimensionados utilizando métodos apropriados.
G	GPR 3	O modelo e as fases do ciclo de vida do projeto são definidas.
G	GPR 4	O esforço e o custo para a execução das tarefas e dos produtos de trabalho são estimados com base em dados históricos ou referências.
G	GPR 5	O orçamento e o cronograma do projeto, incluindo marcos e/ou pontos de controle, são estabelecidos e mantidos.
G	GPR 6	Os riscos do projeto são identificados e o seu impacto, probabilidade de ocorrência e prioridade de tratamento são determinados e documentados.
G	GPR 7	Os recursos humanos para o projeto são planejados considerando o perfil e o conhecimento necessários para executá-lo.
G	GPR 8	As tarefas, os recursos e o ambiente de trabalho necessários para executar o projeto são planejados.
G	GPR 9	Os dados relevantes do projeto são identificados e planejados quanto à forma de coleta, armazenamento e distribuição. Um mecanismo é estabelecido para acessá-los, incluindo, se pertinente, questões de privacidade e segurança.
G	GPR 10	Planos para a execução do projeto são estabelecidos e reunidos no Plano do Projeto.
G	GPR 11	A viabilidade de atingir as metas do projeto, considerando as restrições e os recursos disponíveis, é avaliada. Se necessário, ajustes são realizados.
G	GPR 12	O Plano do Projeto é revisado com todos os interessados e o compromisso com ele é obtido.
G	GPR 13	O progresso do projeto é monitorado com relação ao estabelecido no Plano do Projeto e os resultados são documentados.
G	GPR 14	O envolvimento das partes interessadas no projeto é gerenciado.
G	GPR 15	Revisões são realizadas em marcos do projeto e conforme estabelecido no planejamento.
G	GPR 16	Registros de problemas identificados e o resultado da análise de questões pertinentes, incluindo dependências críticas, são estabelecidos e tratados com as partes interessadas.
G	GPR 17	Ações para corrigir desvios em relação ao planejado e para prevenir a repetição dos problemas identificados são estabelecidas, implementadas e acompanhadas até a sua conclusão.

A.2 Gerência de Requisitos – GRE

Nível G – Parcialmente Gerenciado (MPS.BR, 2007b)

Categoria de Processo: Engenharia

O propósito da Área de Processo Gerência de Requisitos é gerenciar os requisitos dos produtos e componentes do produto e identificar inconsistências entre os requisitos, os planos do projeto e os produtos de trabalho do projeto.

Tabela 27 – Práticas Específicas GRE

Nível	Práticas Específicas	
G	GRE 1	O entendimento dos requisitos é obtido junto aos fornecedores de requisitos.
G	GRE 2	Os requisitos de software são aprovados utilizando critérios objetivos;
G	GRE 3	A rastreabilidade bidirecional entre os requisitos e os produtos de trabalho é estabelecida e mantida.
G	GRE 4	Revisões em planos e produtos de trabalho do projeto são realizadas visando identificar e corrigir inconsistências em relação aos requisitos.
G	GRE 5	Mudanças nos requisitos são gerenciadas ao longo do projeto.

A.3 Aquisição – AQU

Nível F – Gerenciado (MPS.BR, 2007c)

Categoria de Processo: Gerenciamento de Projeto

O propósito da Área de Processo Aquisição é gerenciar a aquisição de produtos e/ou serviços que satisfaçam a necessidade expressa pelo adquirente.

Tabela 28 – Práticas Específicas AQU

Nível	Práticas Específicas	
F	AQU 1	As necessidades de aquisição, as metas, os critérios de aceitação do produto e/ou serviço, os tipos e a estratégia de aquisição são definidos;
F	AQU 2	Os critérios de seleção do fornecedor são estabelecidos e usados para avaliar os potenciais fornecedores;
F	AQU 3	O fornecedor é selecionado com base na avaliação das propostas e dos critérios estabelecidos;
F	AQU 4	Um acordo que expresse claramente a expectativa, as responsabilidades e as obrigações de ambas as partes (cliente e fornecedor) é estabelecido e negociado entre elas;
F	AQU 5	Um produto e/ou serviço que satisfaça a necessidade expressa pelo cliente é adquirido baseado na análise dos potenciais candidatos;
F	AQU 6	Os processos do fornecedor que são críticos para o sucesso do projeto são identificados e monitorados, gerando ações corretivas, quando necessário;
F	AQU 7	A aquisição é monitorada de forma que as condições especificadas sejam atendidas, tais como custo, cronograma e qualidade, gerando ações corretivas quando necessário;
F	AQU 8	O produto e/ou serviço de *software* é entregue e avaliado em relação ao acordado e os resultados da aceitação são documentados;
F	AQU 9	O produto adquirido é incorporado ao projeto, caso pertinente.

A.4 Gerência de Configuração – GCO

Nível F – Gerenciado (MPS.BR, 2007c)

Categoria de Processo: Suporte

O propósito da Área de Processo Gerência de Configuração é estabelecer e manter a integridade de todos os produtos de trabalho de um processo ou projeto e disponibilizá-los a todos os envolvidos.

Tabela 29 – Práticas Específicas GCO

Nível	Práticas Específicas	
F	GCO 1	Um Sistema de Gerência de Configuração é estabelecido e mantido;
F	GCO 2	Os itens de configuração são identificados;
F	GCO 3	Os itens de configuração sujeitos a um controle formal são colocados sob *baseline*;
F	GCO 4	A situação dos itens de configuração e das *baselines* é registrada ao longo do tempo e disponibilizada;
F	GCO 5	Modificações em itens de configuração são controladas e disponibilizadas;
F	GCO 6	Auditorias de configuração são realizadas objetivamente para assegurar que as *baselines* e os itens de configuração estejam íntegros, completos e consistentes;
F	GCO 7	O armazenamento, o manuseio e a liberação de itens de configuração e *baselines* são controlados.

A.5 Garantia da Qualidade – GQA

Nível F – Gerenciado (MPS.BR, 2007c)

Categoria de Processo: Suporte

O propósito da Área de Processo Garantia da Qualidade é assegurar que os produtos de trabalho e a execução dos processos estejam em conformidade com os planos e recursos predefinidos.

Tabela 30 – Práticas Específicas GQA

Nível	Práticas Específicas	
F	GQA 1	A aderência dos produtos de trabalho aos padrões, procedimentos e requisitos aplicáveis é avaliada objetivamente, antes dos produtos serem entregues ao cliente e em marcos predefinidos ao longo do ciclo de vida do projeto;
F	GQA 2	A aderência dos processos executados às descrições de processo, padrões e procedimentos é avaliada objetivamente;
F	GQA 3	Os problemas e as não-conformidades são identificados, registrados e comunicados;
F	GQA 4	Ações corretivas para não-conformidades são estabelecidas e acompanhadas até as suas efetivas conclusões. Quando necessário, o escalonamento das ações corretivas para níveis superiores é realizado, de forma a garantir sua solução;

A.6 Medição – MED

Nível F – Gerenciado (MPS.BR, 2007c)

Categoria de Processo: Suporte

O propósito da Área de Processo Medição é coletar, analisar e relatar os dados relativos aos produtos desenvolvidos e aos processos implementados na organização e em seus projetos, de forma a apoiar os objetivos organizacionais.

Tabela 31 – Práticas Específicas MED

Nível	Práticas Específicas	
F	MED 1	Objetivos de medição são estabelecidos e mantidos a partir dos objetivos da organização e das necessidades de informação de processos técnicos e gerenciais;
F	MED 2	Um conjunto adequado de medidas, orientado pelos objetivos de medição, é identificado e/ou definido, priorizado, documentado, revisado e atualizado;
F	MED 3	Os procedimentos para a coleta e o armazenamento de medidas são especificados;
F	MED 4	Os procedimentos para a análise da medição realizada são especificados;
F	MED 5	Os dados requeridos são coletados e analisados;
F	MED 6	Os dados e os resultados de análises são armazenados;
F	MED 7	As informações produzidas são usadas para apoiar decisões e para fornecer uma base objetiva para comunicação aos interessados.

A.7 Melhoria do Processo Organizacional – AMP

Nível E – Parcialmente Definido (MPS.BR, 2007d)

Categoria de Processo: Gerenciamento de Processo

O propósito da Área de Processo Avaliação e Melhoria do Processo Organizacional é determinar o quanto os processos padrão da organização contribuem para alcançar os objetivos de negócio da organização e para apoiar a organização a planejar, realizar e implantar melhorias contínuas nos processos com base no entendimento de seus pontos fortes e fracos.

Tabela 32 – Práticas Específicas AMP

Nível	Práticas Específicas	
E	AMP 1	A descrição das necessidades e os objetivos dos processos da organização são estabelecidos e mantidos;
E	AMP 2	As informações e os dados relacionados ao uso dos processos padrão para projetos específicos existem e são mantidos;
E	AMP 3	Avaliações dos processos padrão da organização são realizadas para identificar seus pontos fortes, pontos fracos e oportunidades de melhoria;
E	AMP 4	Registros das avaliações realizadas são mantidos acessíveis;
E	AMP 5	Os objetivos de melhoria dos processos são identificados e priorizados;
E	AMP 6	Um plano de implementação de melhorias nos processos é definido e executado, e os efeitos desta implementação são monitorados e confirmados com base nos objetivos de melhoria;
E	AMP 7	Ativos de processo organizacional são implantados na organização;
E	AMP 8	Os processos padrão da organização são utilizados em projetos a serem iniciados e, se pertinente, em projetos em andamento;
E	AMP 9	A implementação dos processos padrão da organização e o uso dos ativos de processo organizacional nos projetos são monitorados;
E	AMP 10	Experiências relacionadas aos processos são incorporadas aos ativos de processo organizacional.

A.8 Definição do Processo Organizacional – DFP

Nível E – Parcialmente Definido (MPS.BR, 2007d)

Categoria de Processo: Gerenciamento de Processo

O propósito da Área de Processo Definição do Processo Organizacional é estabelecer e manter um conjunto de ativos de processo organizacional e padrões do ambiente de trabalho utilizáveis e aplicáveis às necessidades de negócio da organização.

Tabela 33 – Práticas Específicas DFP

Nível	Práticas Específicas	
E	DFP 1	Um conjunto definido de processos padrão é estabelecido e mantido, juntamente com a indicação da aplicabilidade de cada processo;
E	DFP 2	Uma biblioteca de ativos de processo organizacional é estabelecida e mantida;
E	DFP 3	Tarefas, atividades e produtos de trabalho associados aos processos padrão são identificados e detalhados, juntamente com as características de desempenho esperadas;
E	DFP 4	As descrições dos modelos de ciclo de vida a serem utilizados nos projetos da organização são estabelecidas e mantidas;
E	DFP 5	Uma estratégia para adaptação do processo padrão para o produto ou serviço é desenvolvida considerando as necessidades dos projetos;
E	DFP 6	O repositório de medidas da organização é estabelecido e mantido;
E	DFP 7	Os ambientes padrões de trabalho da organização são estabelecidos e mantidos.

A.9 Gerência de Recursos Humanos – GRH

Nível E – Parcialmente Definido (MPS.BR, 2007d)

Categoria de Processo: Gerenciamento de Processo

O propósito da Área de Processo Gerência de Recursos Humanos é prover a organização e os projetos com os recursos humanos necessários e manter suas competências consistentes com as necessidades do negócio.

Tabela 34 – Práticas Específicas GRH

Nível	Práticas Específicas	
E	GRH 1	Uma revisão das necessidades estratégicas da organização e dos projetos é conduzida para identificar recursos, conhecimentos e habilidades requeridos e, de acordo com a necessidade, desenvolvê-los ou contratá-los;
E	GRH 2	Indivíduos com as habilidades e competências requeridas são identificados e recrutados;
E	GRH 3	As necessidades de treinamento que são responsabilidade da organização são identificadas;
E	GRH 4	Uma estratégia de treinamento é planejada e implementada com o objetivo de atender às necessidades de treinamento dos projetos e da organização;
E	GRH 5	Os treinamentos identificados como sendo responsabilidade da organização são conduzidos e registrados;
E	GRH 6	A efetividade do treinamento é avaliada;
E	GRH 7	Critérios objetivos para avaliação do desempenho de grupos e indivíduos são definidos e monitorados para prover informações sobre este desempenho e melhorá-lo;
E	GRH 8	Uma estratégia apropriada de gerência de conhecimento é planejada, estabelecida e mantida para compartilhar informações na organização;
E	GRH 9	Uma rede de especialistas na organização é estabelecida e um mecanismo de apoio à troca de informações entre os especialistas e os projetos é implementado;
E	GRH 10	O conhecimento é prontamente disponibilizado e compartilhado na organização.

A.10 Gerência de Reutilização – GRU

Nível E – Parcialmente Definido (MPS.BR, 2007d)

Categoria de Processo: Suporte

O propósito da Área de Processo Gerência de Reutilização é gerenciar o ciclo de vida dos ativos reutilizáveis.

Tabela 35 – Práticas Específicas GRU

Nível	Práticas Específicas	
E	GRU 1	Uma estratégia de gerenciamento de ativos é documentada, contemplando a definição de ativo reutilizável, além dos critérios para aceitação, certificação, classificação, descontinuidade e avaliação de ativos reutilizáveis;
E	GRU 2	Um mecanismo de armazenamento e recuperação de ativos reutilizáveis é implantado;
E	GRU 3	Os dados de utilização dos ativos reutilizáveis são registrados;
E	GRU 4	Os ativos reutilizáveis são periodicamente mantidos, segundo os critérios definidos, e suas modificações são controladas ao longo do seu ciclo de vida;
E	GRU 5	Os usuários de ativos reutilizáveis são notificados sobre problemas detectados, modificações realizadas, novas versões disponibilizadas e descontinuidade de ativos.

A.11 Gerência de Projetos – GPR (evolução)

Nível E – Parcialmente Definido (MPS.BR, 2007d)

Categoria de Processo: Gerenciamento de Projeto

A partir do nível E, alguns resultados evoluem e outros são incorporados, de forma que a gerência de projetos passe a ser realizada com base no processo definido para o projeto e nos planos integrados.

Tabela 36 – Práticas Específicas GRU (nível E)

Nível	Práticas Específicas	
E	GPR 4	O planejamento e as estimativas das atividades do projeto são feitos baseados no repositório de estimativas e no conjunto de ativos de processo organizacional;
E	GPR 10	Um plano geral para a execução do projeto é estabelecido com a integração de planos específicos;
E	GPR 13	O projeto é gerenciado utilizando-se o Plano do Projeto e outros planos que afetam o projeto. Os resultados são documentados;
E	GPR 18	Um processo definido para o projeto é estabelecido de acordo com a estratégia para adaptação do processo da organização;
E	GPR 19	Produtos de trabalho, medidas e experiências documentadas contribuem para os ativos de processo organizacional;

A.12 Desenvolvimento de Requisitos – DRE

Nível D – Largamente Definido (MPS.BR, 2007e)

Categoria de Processo: Engenharia

O propósito da Área de Processo Desenvolvimento de Requisitos é estabelecer os requisitos dos componentes do produto, do produto e do cliente.

Tabela 37 – Práticas Específicas DRE

Nível	Práticas Específicas	
D	DRE 1	As necessidades, expectativas e restrições do cliente, tanto do produto quanto de suas interfaces, são identificadas;
D	DRE 2	Um conjunto definido de requisitos do cliente é especificado a partir das necessidades, expectativas e restrições identificadas;
D	DRE 3	Um conjunto de requisitos funcionais e não-funcionais, do produto e dos componentes do produto que descrevem a solução do problema a ser resolvido, é definido e mantido a partir dos requisitos do cliente;
D	DRE 4	Os requisitos funcionais e não-funcionais de cada componente do produto são refinados, elaborados e alocados;
D	DRE 5	Interfaces internas e externas do produto e de cada componente do produto são definidas;
D	DRE 6	Conceitos operacionais e cenários são desenvolvidos;
D	DRE 7	Os requisitos são analisados para assegurar que sejam necessários, corretos, testáveis e suficientes e para balancear as necessidades dos interessados com as restrições existentes;
D	DRE 8	Os requisitos são validados.

A.13 Integração do Produto – ITP

Nível D – Largamente Definido (MPS.BR, 2007e)

Categoria de Processo: Engenharia

O propósito da Área de Processo Integração do Produto é compor os componentes do produto, produzindo um produto integrado consistente com o projeto, e demonstrar que os requisitos funcionais e não-funcionais são satisfeitos para o ambiente alvo ou equivalente.

Tabela 38 – Práticas Específicas ITP

Nível	Práticas Específicas	
D	ITP 1	Uma estratégia de integração, consistente com o projeto e com os requisitos do produto, é desenvolvida para os componentes do produto;
D	ITP 2	Um ambiente para integração dos componentes do produto é estabelecido e mantido;
D	ITP 3	A compatibilidade das interfaces internas e externas dos componentes do produto é assegurada;
D	ITP 4	As definições, o projeto e as mudanças nas interfaces internas e externas são gerenciados para o produto e os componentes do produto;
D	ITP 5	Cada componente do produto é verificado, utilizando-se critérios definidos, para confirmar que estes estão prontos para a integração;
D	ITP 6	Os componentes do produto são integrados, de acordo com a seqüência determinada e seguindo os procedimentos e critérios para integração;
D	ITP 7	Os componentes do produto integrados são avaliados e os resultados da integração são registrados;
D	ITP 8	Uma estratégia de regressão é desenvolvida e aplicada para uma nova verificação do produto, caso ocorra uma mudança nos componentes do produto (incluindo requisitos, projeto e códigos associados);
D	ITP 9	O produto e a documentação relacionada são preparados e entregues ao cliente.

A.14 Projeto e Construção do Produto – PCP

Nível D – Largamente Definido (MPS.BR, 2007e)

Categoria de Processo: Engenharia

O propósito da Área de Processo Projeto e Construção do Produto é projetar, desenvolver e implementar soluções para atender aos requisitos.

Tabela 39 – Práticas Específicas PCP

Nível	Práticas Específicas	
D	PCP 1	Alternativas de solução e critérios de seleção são desenvolvidos para atender aos requisitos definidos;
D	PCP 2	Soluções são selecionadas para o produto ou componentes do produto, com base em cenários definidos e em critérios identificados;
D	PCP 3	O produto ou componente do produto é projetado e documentado;
D	PCP 4	As interfaces entre os componentes do produto são projetadas com base em critérios predefinidos;
D	PCP 5	Uma análise dos componentes do produto é conduzida para decidir sobre sua construção, compra ou reutilização;
D	PCP 6	Os componentes do produto são implementados e verificados de acordo com o projeto (*design*);
D	PCP 7	A documentação é identificada, desenvolvida e disponibilizada de acordo com os padrões identificados;
D	PCP 8	A documentação é mantida de acordo com os critérios definidos.

A.15 Validação – VAL

Nível D – Largamente Definido (MPS.BR, 2007e)

Categoria de Processo: Engenharia

O propósito da Área de Processo Validação é confirmar que um produto ou componente do produto atenderá a seu uso pretendido quando colocado no ambiente para o qual foi desenvolvido.

Tabela 40 – Práticas Específicas VAL

Nível	Práticas Específicas	
D	VAL 1	Produtos de trabalho a serem validados são identificados;
D	VAL 2	Uma estratégia de validação é desenvolvida e implementada, estabelecendo cronograma, participantes envolvidos, métodos para validação e qualquer material a ser utilizado na validação;
D	VAL 3	Critérios e procedimentos para validação dos produtos de trabalho a serem validados são identificados e um ambiente para validação é estabelecido;
D	VAL 4	Atividades de validação são executadas para garantir que os produtos de *software* estejam prontos para uso no ambiente operacional pretendido;
D	VAL 5	Problemas são identificados e registrados;
D	VAL 6	Resultados de atividades de validação são analisados e disponibilizados para as partes interessadas;
D	VAL 7	Evidências de que os produtos de *software* desenvolvidos estão prontos para o uso pretendido são fornecidas.

A.16 Verificação – VER

Nível D – Largamente Definido (MPS.BR, 2007e)

Categoria de Processo: Engenharia

O propósito da Área de Processo Verificação é confirmar que cada serviço e/ou produto de trabalho do processo ou do projeto atende apropriadamente os requisitos especificados.

Tabela 41 – Práticas Específicas VER

Nível	Práticas Específicas	
D	VER 1	Produtos de trabalho a serem verificados são identificados;
D	VER 2	Uma estratégia de verificação é desenvolvida e implementada, estabelecendo cronograma, revisores envolvidos, métodos para verificação e qualquer material a ser utilizado na verificação;
D	VER 3	Critérios e procedimentos para verificação dos produtos de trabalho a serem verificados são identificados e um ambiente para verificação é estabelecido;
D	VER 4	Atividades de verificação, incluindo testes e revisões por pares, são executadas;
D	VER 5	Defeitos são identificados e registrados;
D	VER 6	Resultados de atividades de verificação são analisados e disponibilizados para as partes interessadas.

A.17 Gerência de Reutilização – GRU (evolução)

Nível C – Definido (MPS.BR, 2007f)

Categoria de Processo: Suporte

O propósito da Área de Processo Gerência de Reutilização é gerenciar o ciclo de vida dos ativos reutilizáveis.

Tabela 42 – Práticas Específicas GRU (nível C)

Nível	Práticas Específicas	
C	GRU 3	Os dados de utilização dos ativos de domínio são registrados;

A.18 Análise de Decisão e Resolução – ADR

Nível C – Definido (MPS.BR, 2007e)

Categoria de Processo: Suporte

O propósito da Área de Processo Análise de Decisão e Resolução é analisar possíveis decisões usando um processo formal, com critérios estabelecidos, para avaliação das alternativas identificadas.

Tabela 43 – Práticas Específicas ADR

Nível	Práticas Específicas	
C	ADR 1	Guias organizacionais para a análise de decisão são estabelecidos e mantidos;
C	ADR 2	O problema ou questão a ser objeto de um processo formal de tomada de decisão é definido;
C	ADR 3	Critérios para avaliação das alternativas de solução são estabelecidos e mantidos em ordem de importância, de forma que os critérios mais importantes exerçam mais influência na avaliação;
C	ADR 4	Alternativas de solução aceitáveis para o problema ou questão são identificadas;
C	ADR 5	Os métodos de avaliação das alternativas de solução são selecionados de acordo com sua viabilidade de aplicação;
C	ADR 6	Soluções alternativas são avaliadas usando os critérios e métodos estabelecidos;
C	ADR 7	Decisões são baseadas na avaliação das alternativas utilizando os critérios de avaliação estabelecidos.

A.19 Desenvolvimento para Reutilização – DRU

Nível C – Definido (MPS.BR, 2007f)

Categoria de Processo: Suporte

O propósito da Área de Processo Desenvolvimento para Reutilização é identificar oportunidades de reutilização sistemática na organização e, se possível, estabelecer um programa de reutilização para desenvolver ativos a partir de engenharia de domínios de aplicação.

Tabela 44 – Práticas Específicas DRU

Nível	Práticas Específicas	
C	DRU 1	Domínios de aplicação em que serão investigadas oportunidades de reutilização ou nos quais se pretende praticar reutilização são identificados, detectando os respectivos potenciais de reutilização;
C	DRU 2	A capacidade de reutilização sistemática da organização é avaliada e ações corretivas são tomadas, caso necessário;
C	DRU 3	Um programa de reutilização, envolvendo propósitos, escopo, metas e objetivos, é planejado com a finalidade de atender às necessidades de reutilização de domínios;
C	DRU 4	O programa de reutilização é implantado, monitorado e avaliado;
C	DRU 5	Propostas de reutilização são avaliadas de forma a garantir que o resultado da reutilização seja apropriado para a aplicação alvo;
C	DRU 6	Formas de representação para modelos de domínio e arquiteturas de domínio são selecionadas;
C	DRU 7	Um modelo de domínio que capture características, capacidades, conceitos e funções comuns, variantes, opcionais e obrigatórios é desenvolvido e seus limites e relações com outros domínios são estabelecidos e mantidos;
C	DRU 8	Uma arquitetura de domínio descrevendo uma família de aplicações para o domínio é desenvolvida e mantida por todo seu ciclo de vida;
C	DRU 9	Ativos do domínio são especificados; adquiridos ou desenvolvidos, e mantidos por todo seu ciclo de vida.

A.20 Gerência de Riscos – GRI

Nível C – Definido (MPS.BR, 2007f)

Categoria de Processo: Gerenciamento de Projeto

O propósito da Área de Processo Gerência de Riscos é identificar, analisar, tratar, monitorar e reduzir continuamente os riscos em nível organizacional e de projeto.

Tabela 45 – Práticas Específicas GRI

Nível	Práticas Específicas	
C	GRI 1	O escopo da gerência de riscos é determinado;
C	GRI 2	As origens e as categorias de riscos são determinadas, e os parâmetros usados para analisar riscos, categorizá-los e controlar o esforço da gerência do risco são definidos;
C	GRI 3	As estratégias apropriadas para a gerência de riscos são definidas e implementadas;
C	GRI 4	Os riscos do projeto são identificados e documentados, incluindo seu contexto, condições e possíveis conseqüências para o projeto e as partes interessadas;
C	GRI 5	Os riscos são priorizados, estimados e classificados de acordo com as categorias e os parâmetros definidos;
C	GRI 6	Planos para a mitigação de riscos são desenvolvidos;
C	GRI 7	Os riscos são analisados e a prioridade de aplicação dos recursos para o monitoramento desses riscos é determinada;
C	GRI 8	As medições do risco são definidas, aplicadas e avaliadas para determinar mudanças na situação do risco e no progresso das atividades para seu tratamento;
C	GRI 9	Ações apropriadas são executadas para corrigir ou evitar o impacto do risco, baseadas na sua prioridade, probabilidade, conseqüência ou outros parâmetros definidos.

A.21 Gerência de Projetos – GPR (evolução)

Nível B – Gerenciado Quantitativamente (MPS.BR, 2007g)

Categoria de Processo: Gerenciamento de Projeto

No nível B, a gerência de projetos passa a ter um enfoque quantitativo, refletindo a alta maturidade que se espera da organização. Novamente, alguns resultados evoluem e outros são incorporados.

Tabela 46 – Práticas Específicas GPR (nível B)

Nível	Práticas Específicas	
B	GPR 18	Os subprocessos mais adequados para compor o processo definido para o projeto são selecionados com base na estabilidade histórica, em dados de capacidade e em outros critérios previamente estabelecidos;
B	GPR 20	Os objetivos para a qualidade e para o desempenho do processo definido para o projeto são estabelecidos e mantidos;
B	GPR 21	Subprocessos do processo definido para o projeto e que serão gerenciados estatisticamente são escolhidos e são identificados os atributos por meio dos quais cada subprocesso será gerenciado estatisticamente;
B	GPR 22	O projeto é monitorado para determinar se seus objetivos para qualidade e para o desempenho do processo serão atingidos. Quando necessário, ações corretivas são identificadas;
B	GPR 23	O entendimento da variação dos subprocessos escolhidos para gerência quantitativa, utilizando medidas e técnicas de análise estatística previamente selecionadas, é estabelecido e mantido;
B	GPR 24	O desempenho dos subprocessos escolhidos para gerência quantitativa é monitorado para determinar a sua capacidade de satisfazer os seus objetivos para qualidade e para o desempenho. Ações são identificadas quando for necessário tratar deficiências dos subprocessos;
B	GPR 25	Dados estatísticos e de gerência da qualidade são incorporados ao repositório de medidas da organização.

A.22 Análise de Causas de Problemas e Resolução – ACP

Nível A – Em Otimização (MPS.BR, 2007h)

Categoria de Processo: Suporte

O propósito da Área de Processo Análise de Causas de Problemas e Resolução é identificar causas de defeitos e de outros problemas e tomar ações para prevenir suas ocorrências no futuro.

Tabela 47 – Práticas Específicas ACP

Nível	Práticas Específicas	
A	ACP 1	Defeitos e outros problemas são registrados, identificados, classificados e selecionados para análise;
A	ACP 2	Defeitos e outros problemas são analisados para identificar sua causa raiz e soluções aceitáveis para evitar sua ocorrência futura;
A	ACP 3	Ações para resolução do problema são selecionadas e implementadas;
A	ACP 4	As ações implementadas para resolução de problemas são acompanhadas com medições, para verificar se as mudanças no processo corrigiram o problema e melhoraram o seu desempenho;
A	ACP 5	Dados das ações para análise de causas de problemas e resolução são armazenados para uso em situações similares.