# Avaliação de Riscos Aplicada à Qualidade em Desenvolvimento de Software

**Alberto Bastos[1], Gustavo Carvalho[2], Leandro Daflon[2], Rafael Espinha[2]**

[1]Módulo – Rio de Janeiro – RJ - Brasil

[2]PrimeUp – Rio de Janeiro – RJ - Brasil

{abastos}@modulo.com.br, {gustavo.carvalho, daflon, rafael.espinha}@primeup.com.br

***Resumo.*** *Atualmente, existem diversos modelos de qualidade (ex. CMMI-DEV e MPS.BR) que indicam uma série de boas práticas que se presentes no dia a dia do desenvolvimento de software contribuem para resultados com a qualidade desejada. Entretanto, devido a grande diversidade dos projetos, equipes, cultura e ambientes de desenvolvimento utilizados, cada organização possui necessidades específicas que demandam estratégias distintas de implementação. Neste artigo é apresentada uma abordagem para o apoio a melhoria de processos de desenvolvimento de software que utiliza como princípio a identificação e gerência de riscos associados à não implementação de boas práticas em uma organização e em seus projetos.*

## 1. Introdução

Com a crescente demanda por qualidade dos produtos de software, a adoção de modelos de maturidade, normas de qualidade e guias de boas práticas na definição de processos tem se tornado cada vez mais freqüente. Modelos como CMMI-DEV e MPS.BR e normas como a ISO/IEC 15504 e 12207 definem um conjunto de boas práticas e características que devem estar presentes em um processo para que este possa ser gerenciado e resulte na entrega de produtos de qualidade. Entretanto, estes modelos ou normas muitas vezes não definem de forma clara como estas boas práticas e características devem ser implementadas e implantadas. Uma das maiores dificuldades de um programa de melhoria de processos é a dificuldade de adaptar este conjunto de boas práticas para a sua realidade, identificando quais áreas são mais relevantes e devem ser abordadas com maior urgência.

Para orientar a adaptação necessária, utilizamos o conceito de risco associado a não utilização das boas práticas de desenvolvimento de software nos projetos e processos da organização. Qualquer risco à qualidade e à institucionalização do processo se reflete em riscos na qualidade do produto que será entregue e, consequentemente, em riscos para a organização Ações de gerência de risco nos processos podem contribuir diretamente para a garantia da qualidade do produto final e fornecem dados que permitem identificar quais ações devem ser tomadas com maior urgência.

Neste artigo apresentamos uma abordagem de análise de processos desenvolvida no ciclo 2007 do Prêmio Dorgival Brandão Júnior da Qualidade e Produtividade em Software, na qual é identificado de forma customizada tanto o nível de conformidade (recomendações do modelo de referência implementadas nos processos da organização) quanto o nível de risco (presente no processo de desenvolvimento devido às recomendações não implementadas) em cada área de processo. Dessa maneira uma análise dos processos da organização fornece duas classes de dados para a tomada de decisão e direcionamento de recursos, indicando o que deve ser feito para melhorar o processo (conformidade) e quais ações devem ser tomadas primeiro (risco).

Uma das formas mais indicadas para a definição e implantação de processos de maneira eficiente é a utilização de um ciclo de melhoria contínua. O modelo IDEAL, desenvolvido pelo Software Engineering Institute (SEI), ilustra a utilização deste conceito. A implantação do ciclo de melhoria faz com que os processos de uma organização sejam constantemente avaliados e melhorados. Neste modelo destacam-se duas fases: Diagnóstico e Estabelecimento. A fase de Diagnóstico consiste em avaliar o ambiente produtivo e identificar as oportunidades de melhoria. Dessa forma, obtém-se a diferença entre o que se espera dos processos da organização e onde eles realmente estão. A partir daí, elaboram-se planos de ação para que esta distância seja diminuída ou eliminada, a partir da priorização e seleção dos planos de ação que serão implantados (fase de Estabelecimento).

Neste sentido, a solução desenvolvida facilita a realização das fases de Diagnóstico e Estabelecimento, identificando claramente os riscos associados aos processos definidos (Diagnóstico) e fornecendo um critério de priorização destes riscos (Estabelecimento). A avaliação verifica tanto a dimensão de conformidade entre o processo e modelos como o MPS.BR ou CMMI, quanto à dimensão dos riscos que a não utilização das boas práticas definidas nestas referências oferecem à qualidade do produto desenvolvido pela a organização e aos seus objetivos de negócio. Esta solução também indica como estes pontos podem ser solucionados de forma que a organização obtenha uma maior qualidade ou resultados a partir deste ciclo.

O diferencial desta abordagem é a utilização da análise de risco como um instrumento de priorização das ações que devem ser tomadas pelas empresas para mitigar (reduzir as chances de ocorrência) os riscos identificados durante a fase de diagnóstico fornecendo um critério concreto para definição do escopo de cada ciclo de melhoria.

## 2. Objetivos e Justificativa

O objetivo do projeto proposto para o ciclo 2007 foi desenvolver e aplicar a estratégia de análise de risco aplicada à qualidade no desenvolvimento de software. Dentro deste contexto foram estabelecidos três marcos dentro do projeto: Estudo e elaboração da estratégia, desenvolvimento de ferramentas de apoio e aplicação e evolução.

Na primeira etapa o objetivo principal era estudar como a análise de risco podia ser aplicada no âmbito do desenvolvimento de software. A estratégia proposta identifica o risco oferecido pelas boas práticas não implementadas e, a partir daí, indica quais ações deveriam ser tomadas com mais urgência (quanto maior o risco maior a urgência da implementação da prática).

A primeira etapa foi realizada no período de janeiro a março de 2007, em uma dissertação de mestrado realizada com o Laboratório de Engenharia de Software da PUC-Rio (LES), a PrimeUp e a Módulo. A finalidade da criação deste consórcio de instituições foi identificar uma demanda de mercado, propor soluções através da pesquisa acadêmica e promover a transferência imediata de tecnologia da univercidade para o mercado.

Na segunda etapa o objetivo foi desenvolver uma ferramenta de apoio para a utilização da estratégia desenvolvida, facilitando a sua adoção e diminuindo o custo das sucessivas avaliações necessárias em um programa de melhoria contínua. Esta etapa foi realizada em paralelo com a primeira, resultando na customização da ferramenta especialista em análise de risco Risk Manager, desenvolvida pela Módulo.

A terceira etapa tinha como objetivos principais a transferência da tecnologia gerada, através da aplicação da estratégia e da ferramenta em análise de risco em processos de desenvolvimento de software em organizações e a evolução tanto da estratégia quanto da ferramenta desenvolvidas, através do feedback das avaliações realizadas. Esta etapa teve início em março de 2007, sendo finalizada em dezembro do mesmo ano.

## 3. Metodologia de Execução

O objetivo da estratégia de avaliação é complementar métodos como SCAMPI, MA-MPS e ISO/IEC 15504, oferecendo propostas de soluções a alguns potenciais problemas encontrados na aplicação destes métodos. Os princípios que guiam a estratégia são:

<table>
<tr><td>Mapear resultados aos objetivos do negócio da organização</td><td>Tem como objetivo facilitar o convencimento da alta gerência (geralmente não técnica) acerca da importância dos investimentos em engenharia de software ou qualidade, visando obter um maior comprometimento dos patrocinadores. Isto permite dar ênfase às necessidades e prioridades da empresa, ao invés de impor uma estrutura que pode não ser a mais adequada a ela.</td></tr>
<tr><td>Minimizar o esforço de avaliação segundo critérios de importância definidos pela própria organização;</td><td rowspan="2">Inspeções e análises rigorosas, que abrangem todo o modelo de referência, geram relatórios com uma grande quantidade de informações sobre diversas áreas da engenharia de software mas, na maioria dos casos, outra grande quantidade de informações é desperdiçada. Estes dois princípios visam apoiar a reversão deste cenário.</td></tr>
<tr><td>Obter maior aproveitamento dos resultados gerados;</td></tr>
<tr><td>Utilizar duas dimensões de análise: conformidade e risco.</td><td>Este princípio tem como objetivo oferecer dados de um nível de abstração menos granular para a tomada de decisão. Embora a utilização da capacidade de processo e do nível de maturidade seja o parâmetro mais utilizado no direcionamento de recursos na área de desenvolvimento de software, estes conceitos são um tanto abstratos e em muitos casos dificultam esta atividade (se vários processos apresentam a mesma capacidade e o mesmo gap entre a capacidade esperada e a avaliada, qual deve receber os recursos?). A utilização de uma análise de risco oferece um critério de ponderação, desempate ou uma opção para a priorização de investimentos.</td></tr>
</table>

Para auxiliar a realização da avaliação dos processos de uma organização foi customizada uma ferramenta de apoio à execução de avaliações. A metodologia de análise de risco implementada pela ferramenta se baseia na avaliação de características de ativos da organização, que podem representar pessoas da organização, processos utilizados, tecnologias e características do ambiente de desenvolvimento. Cada ativo é mapeado em objetivos do negócio ou de TI da organização e possui uma relevância que está diretamente relacionada à relevância dos objetivos aos quais ele se relaciona. A **Figura 1** ilustra este conceito.

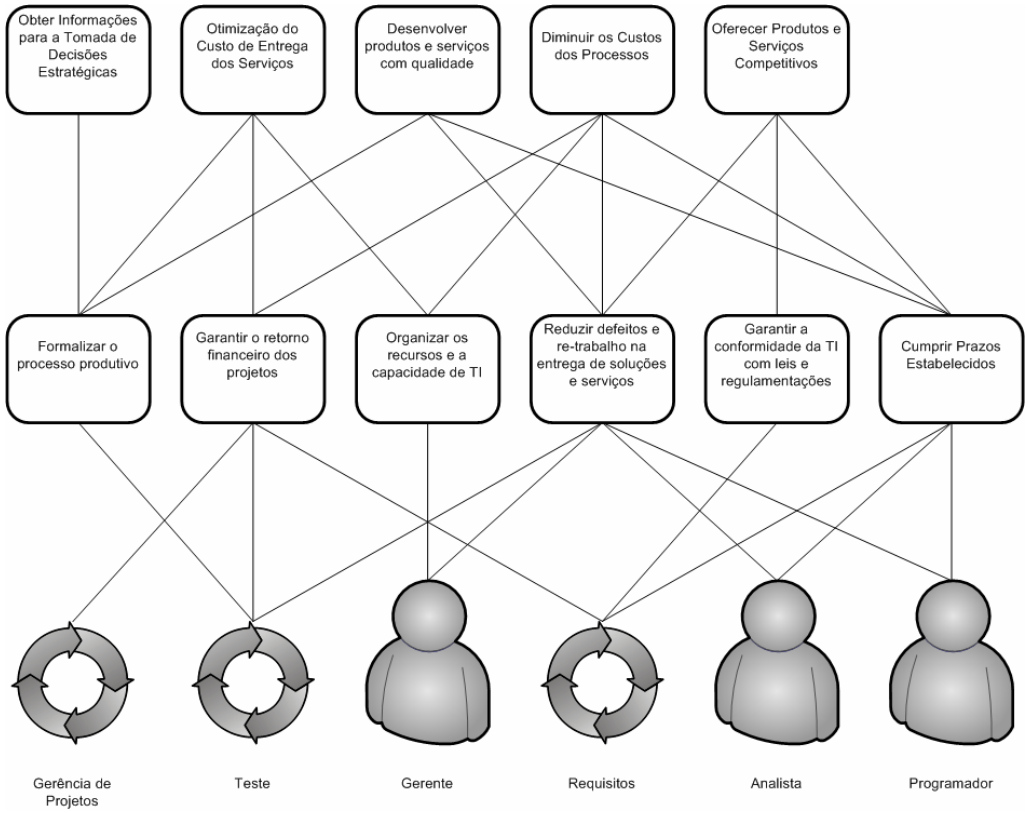


Figura 1. **Mapeamento dos ativos em objetivos do negócio da organização**

Um ativo é um coletor de dados que indica o estado de implementação de um conjunto de boas práticas na organização. Um projeto de avaliação pode utilizar diferentes checklists. Um *checklist* é composto por um ou mais controles, que representam os itens atômicos de verificação da implementação das boas práticas. Cada controle possui uma estrutura com os elementos exemplificados na **Tabela 1**.

**Nome do Controle** indica uma boa prática ou requisito que deve estar presente no ativo para que o controle seja considerado implementado e seu risco associado seja eliminado.

**Justificativa** define termos e conceitos e fornece uma justificativa que explique o porque aquele controle deve ser implementado. São apresentadas as vantagens que se obtém com a implementação do controle e as conseqüências da sua não implementação.

**Ameaças** indicam quais elementos podem se aproveitar da não implementação do controle para se manifestar e causar danos ao negócio da organização.

**Recomendação** fornece razões e dados para a elaboração de um plano de ação após a realização da avaliação, através de uma sugestão de como o controle pode ser implementado para diminuir a exposição da organização aos riscos e atingir a conformidade desejada com o modelo ou norma de referência.

**Referências** relacionam referências bibliográficas para que mais informações acerca do controle e da sua implementação possam ser obtidas.

**Probabilidade** representa a probabilidade de uma ameaça se manifestar caso o controle não esteja implementado na organização. Este elemento é representado por um número de 1 (menor) a 5 (maior probabilidade).

**Severidade** indica o grau do impacto negativo na organização, caso uma ou mais ameaças se manifestem. Este elemento é representado por um número de 1 (menor) a 5 (maior severidade).

**Agrupamento** indica a qual agrupamento o controle pertence. Os agrupamentos são comuns a todos os checklists, permitindo verificar o estado da implementação de características espalhadas em vários checklists.

| | | | |
|---|---|---|---|
| **Controle** | As versões anteriores de um item de configuração devem ser passíveis de recuperação. | | |
| **Justificativa** | Deve ser possível recuperar versões anteriores de um item de configuração para reverter casos como modificações implementadas incorretamente, corrompimento de arquivos e realização de junções (merge) incorretamente entre um ramo e a linha principal de desenvolvimento. | | |
| **Recomendação** | Este controle pode ser implementado através dos seguintes procedimentos:<br>- Documentar e Disponibilizar as versões dos itens de configuração (ICs).<br>- Reportar os procedimentos para: (1) recuperar uma versão anterior, (2) verificar as revisões de um IC e (3) analisar as diferenças entre a versão anterior e a atual. Essas informações devem constar no plano de gerência de configuração e nos procedimentos de controle de versões.<br>- Garantir a integridade e a disponibilidade dos repositórios de configurações.<br>Observação: A ferramenta de controle de versões deve facilitar a visualização e recuperação das versões dos itens de configuração. Exemplos de Artefatos Produzidos:<br>- Lista de versões de itens de configurações<br>- Procedimentos para controle de versões | | |
| **Probabilidade** | 4 | **Severidade** | 3 |
| **Referências** | Std 1042 - IEEE Guide to Software Configuration Management, Institute of Electrical and Electronics Engineers, 1987.<br>ISO/IEC 12207 - Information technology - Software life cycle processes, International Organization for Standardization, 1995.<br>CMMI-Dev / MPS.Br: Área de Processo: Gerência de Configuração | | |
| **Ameaças** | Baixa manutenibilidade ; Perda de controle de solicitações de mudança | | |
| **Agrupamento** | Gerência de Configuração | | |

Tabela 1. **Exemplo de controle**

A avaliação consiste em responder aos checklists associados aos ativos do projeto de avaliação. Estes podem ser respondidos diretamente ou através de questionários enviados via WEB, onde o conteúdo dos controles pode ser interpretado para um domínio específico, por exemplo, para os diversos papéis de uma organização. A utilização dos questionários permite um ganho de escala e de cobertura da avaliação, ao mesmo tempo em que diminui o impacto da avaliação e aumenta a aceitação das melhorias no processo de desenvolvimento uma vez que todos se sentem parte da avaliação e podem contribuir com comentários e sugestões.

Após a coleta dos dados, é gerado um conjunto de relatórios contendo tabelas e gráficos que indicam o estado da implementação das boas práticas e os riscos presentes na organização e fornecem dados para a tomada de decisão (o que e como deve ser feito). Cada controle não implementado ou implementado parcialmente, contribui com um índice de risco (PSR) que é obtido pela multiplicação da relevância do ativo avaliado (R), da probabilidade da concretização das ameaças possíveis (P) e da severidade desta concretização (S) . Além do PSR, os seguintes indicadores são utilizados:

$$\text{Índice de Segurança} = \frac{PSR_{\substack{controles \\ implementados}}(elemento)}{PSR(Total)}$$

$$\text{Índice de Conformidade} = \frac{Num.Controles.implementados}{Num.ControlesTotal}$$

A partir destes índices, pode-se gerar um grande número de interpretações, através da filtragem e agrupamento de dados das áreas de processo, ameaças, departamentos ou objetivos.

## 4. Resultados Obtidos

Nesta seção apresentaremos os resultados gerados por este projeto no ciclo 2007 do Prêmio Dorgival Brandão Júnior da Qualidade e Produtividade em Software.

**Produto de software gerado - Módulo Risk Manager Para a Avaliação de Processos de Desenvolvimento de Software:** Customização da ferramenta especialista em análise de risco Módulo Risk Manager para o contexto de desenvolvimento de software. A ferramenta, inicialmente desenvolvida para análise de risco em segurança da informação, foi customizada através da criação de uma nova taxonomia de ameaças e agrupamentos de checklists e da elaboração de uma base de conhecimento (checklists, questionários e relatórios) para análise de risco baseada nos modelos CMMI, MPS.BR e em práticas de programação neuro linguistica e People-CMM (verificação do risco associado a aspectos pessoais do ambiente de desenvovimento).

**Outro produto gerado - Base de Conhecimento de Recomendações:** Elaboração de uma base de conhecimento de recomendação de implementação das práticas dos modelos CMMI-DEV e MPS.BR. Estas recomendações são utilizadas como base na elaboração de um plano de ação para correção das não conformidades de maior risco associado. Esta base de conhecimento mostrou-se fundamental na implantação de melhoria de processos, principalmente nas organizações com menor maturidade e menor conhecimento dos modelos de referência.

**Método desenvolvido - Estratégia de Análise de Risco Aplicada à Qualidade em Desenvolvimento de Software:** Estratégia de análise de risco para identificação do risco oferecido pelas boas práticas de um modelo de referência não implementadas, indicando quais ações devem ser tomadas com mais urgência (quanto maior o risco maior a urgência da implementação da prática).

### 4.1. Artigos e Relatórios Técnicos publicados


Espinha, R.S.L; Sousa, J.M.S; Melhorando Processos Através da Análise de Risco e Conformidade; Revista Engenharia de Software Magazine.

Carvalho et al.; Avaliação de equipes e processos de desenvolvimento de software baseada em risco e conformidade; 1º. Simpósio sobre qualidade e certificação em TI.

Espinha, R.S.L; Lucena, C.J.P; Staa, A.V.; Uma Abordagem para a Avaliação de Processos de Desenvolvimento de Software Baseada em Risco e Conformidade; Dissertação de mestrado aprovada

Participação de integrantes do projeto no comitê da Associação Brasileira de Normas Técnicas (ABNT) para tradução da norma ISO 15505 (CE-21:007.10 Comissão de Estudo de Avaliação de Processos de Software)


### 4.2. Recursos humanos capacitados

| | |
|---|---|
| ESPECIALISTAS (graduação): | 05 |
| ESPECIALISTAS (pós-graduação): | 01 |
| MESTRADO: | 05 |
| DOUTORADO: | 03 |

### 4.3. Dissertações e/ou teses geradas

Rafael de Souza Lima Espinha. Uma Abordagem para a Avaliação de Processos de Desenvolvimento de Software Baseada em Risco e Conformidade, Mestre em Informática. Orientadores: Arndt von Staa e Carlos José Pereira de Lucena. 27/03/2007

### 4.4. Eventuais parcerias ou programas de transferência de tecnologia efetuados

- Criação de um consórcio entre o Laboratório de Engenharia de Software da PUC-Rio, PrimeUp e Módulo para desenvolvimento e comercialização da estratégia e da ferramenta de análise de risco no desenvolvimento de software.
- Visita ao Centro de Pesquisa Renato Archer (CenPRA) para identificação e formalização de oportunidades de parceria.

### 4.5. Participação em Cursos, Seminários e Palestras

- *Gustavo Robichez de Carvalho,* Seminário de Tecnologias Emergentes : Desafios em Tecnologias de Software Emergentes. RIO INFO 2007 – Hotel Glória, Rio de Janeiro.
- *Rafael de Souza Lima Espinha, Reduzindo Riscos no Desenvolvimento de Software: Qualidade no Desenvolvimento de Software, Apresentação no Fórum de Assessores de Informática do estado do Rio de Janeiro, 17/07/2007*
- *Rafael de Souza Lima Espinha, Avaliação de Riscos Aplicada à Qualidade em Desenvolvimento de Software, Apresentação de parte dos resultados do projeto no Encontro da Qualidade e Produtividade em Software, 27/09/2007*

### 4.6. Prêmios

- RIO INFO 2007 – Vencedor do Prêmio na Categoria Empresa Semente, com a solução de análise de risco no desenvolvimento de software – Hotel Glória, Rio de Janeiro.

### 4.7. Avaliações Realizadas

| | |
|---|---|
| Projetos Piloto | 15 |
| Projetos Comerciais | 5 |
| Tamanho das Equipes Avaliadas | 10 a 60 colaboradores |
| Tempo Médio das Avaliações (alocação parcial da equipe de avaliação) | 10 dias |

## 5. Aplicabilidade dos Resultados

Considerando que o objetivo principal da estratégia e da ferramenta desenvolvidos não é a certificação das organizações avaliadas, mas sim o apoio à identificação e implementação de melhorias, os resultados obtidos são relevantes, uma vez que atendem a uma demanda do mercado de desenvolvimento de software.

Os resultados obtidos no ciclo 2007 já estão sendo amplamente aplicados em projetos comerciais direcionando, através do conceito de risco, as ações de melhoria e a implementação de modelos de qualidade. Comparando o esforço das avaliações realizadas com avaliações e auditorias tradicionais (ex. SCAMPI, MA-MPS) podemos notar que a estratégia desenvolvida, utilizada em conjunto com a ferramenta de apoio, demanda menos recursos, possibilitando a realização de diversas avaliações em um ciclo de melhoria e em projetos de implantação e certificação de modelos de qualidade.

## 6. Características Inovadoras

A inovação da solução proposta consiste na utilização do conceito de análise de risco associada a avaliações de conformidade, com o objetivo de identificar o impacto das não conformidades encontradas na qualidade do produto desenvolvido e nos objetivos da organização. Sabendo como estas não conformidades afetam a organização e seus produtos, fica mais fácil determinar quais não conformidades merecem maior atenção, ou seja, quais práticas e recomendações do modelo de referência precisam ser implementadas com maior urgência.

No cenário atual, onde as organizações que desenvolvem software precisam otimizar e justificar a utilização de seus recursos, o conceito de risco associado a não conformidades fornece dados fundamentais para direcionar e justificar ações de melhoria no processo de desenvolvimento.

## 7. Conclusão e Perspectivas Futuras

O trabalho proposto para o ciclo de 2007 foi concluído, gerando um produto comercial que vem sendo utilizado em projetos de melhoria de processo. O consórcio formado por representantes da academia e da indústria mostrou-se fundamental para a rápida transferência tecnológica da solução.

A utilização de uma abordagem baseada em análise de risco mostrou-se eficaz no direcionamento de projetos de melhoria de processos, permitindo a visibilidade de problemas relacionados com a não utilização de boas práticas de desenvolvimento para a alta gerência e facilitando a justificativa e direcionamento de recursos para a área de qualidade de software.

Como perspectivas futuras temos a utilização da solução em cenários cada vez mais variados e a constante evolução da estratégia, da ferramenta e da base de conhecimento através do feedback das avaliações realizadas.

## 8. Referências Bibliográficas


BOEHM,B.W. **Software Risk Management: Principles and Practices**. IEEE Software, v.8(1), p. 32-41, 1991.

CHRISSIS, M.B.; KONRAD, M.; SHRUM, S. **CMMI: Guidelines for Process Integration and Product Improvement**. Boston: Addison-Wesley, 2003.

DEMARCO, T; LISTER, T. **Waltzing with Bears: Managing Risks on Software Projects**. New York: Dorset House Publishing, 2003.

GREMBA, J.;MYERS, C. **The IDEAL$^{SM}$ Model: A Practical Guide for Improvement**. 1997.

ISO/IEC. **International Standard 12207.** Information Technology – Software Life Cycle Processes, Reference No. ISO/IEC 12207: 1995(E): First Edition 1995.

____. **International Standard 15504.** Information Technology – Proces Assessment, Reference No. ISO/IEC 15504:2004(E).

POULIN, A. **Reducing Risk with Software Process Improvement.** Boca Raton: Auerbach Publications, 2005.

SOFTEX.. **MPS.BR – Melhoria de Processo do Software Brasileiro.** Guia de Avaliação. Versão 1.0, 2006a.

**____. MPS.BR – Melhoria de Processo do Software Brasileiro.** Guia Geral. Versão 1.1, 2006b.

SEI. **Standard CMMI Appraisal Method for Process Improvement (SCAMPI[SM]) A, Version 1.2: Method Definition Document**. Software Engineering Institute, CMU, Pittsburgh, 2006a