Gerência de Risco em Processos de Qualidade de Software: uma Análise Comparativa

Cristine Martins Gomes de Gusmão, Hermano Perrelli de Moura
Centro de Informática – Universidade Federal de Pernambuco (UFPE)
CP 7851, Cidade Universitária, Recife, PE, Brasil, 50732-970
E-mail: [cmgg, hermano]@cin.ufpe.br

Resumo

O desenvolvimento de software é geralmente repleto de incertezas, como problemas que ocasionam os atrasos de cronogramas, aumento de custos ou entrega dos produtos de forma insatisfatória. Embora alguns problemas não possam ser totalmente resolvidos, alguns podem ser controlados através de ações preventivas. A área de gerência de projetos que lida com estas incertezas ou problemas mesmo antes que eles ocorram é a gerência de riscos. Nos processos de qualidade de software, a gerência de risco é ponto fundamental para a garantia da qualidade do produto gerado. Este artigo tem a finalidade de proporcionar uma análise detalhada das atividades de gerência de risco presentes nos modelos de qualidade de software.

Palavras-chave: Engenharia de Software, Gerência de Risco, Qualidade do Processo, Modelos de Processo.

Abstract

The software development is generally full of uncertainties and problems that cause the delays of schedules, increase the costs or the delivery of products in an unsatisfactory form. Although some problems cannot be totaly solved, some ones can be controlled through preventive actions. Projects Management area that deals with these uncertainties or problems even before they occur, are Risk Management. In Software Quality Processes, Risk Management is a key to assurance the software quality. This article has the purpose to provide an overview of risk management process in quality models, through the comparative analysis of its activities**.**

Keywords: Software Engineering, Risk Management, Quality Process, Process Models.

1. Introdução

Atualmente, os sistemas de computação estão difundidos em todos os setores da vida moderna e apesar dos avanços nas tecnologias de software, a maioria dos sistemas continua difícil de entender, manter e evoluir [1]. Todo projeto de software enfrenta problemas de qualidade, de cronograma, e de custo que estão sendo afetados por riscos que são inesperados, não planejados ou ignorados simplesmente. Desta forma, à medida que o tamanho e a complexidade dos sistemas de software crescem, aumenta a necessidade da utilização de metodologias para o gerenciamento de riscos, apoiando os projetistas e gerentes de projetos de tecnologia da informação no desenvolvimento e efetivação de suas atividades, garantindo o cumprimento das metas do projeto, custos e prazos, e por fim, a qualidade do produto gerado.

Através de perspectivas globais de negócios muitas organizações estão tornando-se cada vez mais dependentes do sucesso ou do fracasso dos softwares que desenvolvem. Neste contexto, a gerência de riscos não é apenas baseada em boas práticas para o desenvolvimento de software, mas sim, boas práticas para gerir negócios.

Muitas abordagens para gerenciar riscos em projetos de software vêm sendo propostas e usadas desde que Boehm [2] e Charette [3] conseguiram trazer a atenção da comunidade de Engenharia de Software para a necessidade de gerir risco, através de suas propostas de processos da gerência de risco. Embora existam muitos relatórios individuais de sucessos em desenvolvimento de software, através de utilização de técnicas na prática, a indústria de software como um todo, parece ainda não aplicar ativamente e sistematicamente os métodos

da gerência de risco. Desta forma, muito se tem a fazer para permitir que a gerência de risco, como a própria gerência de projetos, seja um processo que flua em todas as fases do desenvolvimento de software.

2. Processo de Gerência de Risco em Engenharia de Software

O desenvolvimento de software pode ser considerado uma atividade de risco e diversos estudos e autores atuais comprovam que muitos dos problemas envolvidos em projetos de grande porte estão muito mais associados a falhas em atividades de gerenciamento do que falhas em atividades técnicas [1].

A gerência de risco é uma prática com processos, métodos, e ferramentas para controlar riscos em um projeto [4]. A gerência de risco em Engenharia de Software tem a finalidade de aumentar a qualidade do produto e do processo de desenvolvimento de software. Observa-se que os projetos de desenvolvimento de software, em geral, apresentam atrasos de cronogramas, custos realizados além do planejado e funcionalidades aquém das expectativas. Esses problemas, embora considerados inerentes ao desenvolvimento de software por muitos autores, podem ser minimizados e controlados pelo contínuo gerenciamento de risco de projetos.

Diversas abordagens que apresentam um processo para Gerência de Risco, são encontradas na literatura da área de Engenharia de Software. Destaca-se o programa de Gerência de Risco do SEI (*Software Engineering Institute*) [4], programas desenvolvidos por organizações que desenvolvem software [5] e abordagens desenvolvidas através da participação de especialistas [5]. Embora tenham características próprias, cada abordagem tem alguns princípios e atividades em comum.

O Instituto de Engenharia de Software (SEI) (1990) define o processo de gerência de risco de software através de um modelo contínuo de gerenciamento de riscos composto por seis fases distintas: *Identificação de Riscos, Análise de Riscos, Plano de respostas aos riscos, Rastreamento de riscos e Controle de riscos*. Todas as fases estão ligadas através dos esforços de comunicação das equipes envolvidas no processo [4].

Boehm (1990) apresentou um processo para gerir riscos, composto por duas grandes fases: *Avaliação de Riscos* (Identificação, Análise e Priorização de riscos) e *Controle dos Riscos* (Plano de gerenciamento de riscos, Resolução dos riscos e Monitoramento dos riscos) [2].

Charette (1990) definiu a engenharia de risco em software, composta por duas fases: *Análise de Riscos* (Identificação de riscos, Estimativas de riscos e Avaliação de riscos) e *Gerência de Risco* (Planejamento de riscos, Controle de riscos e monitoramento de riscos) [3].

Fairley (1994) apresenta o processo de gerência de riscos em projetos de software através de sete passos: (1) Identificar os fatores de risco; (2) Avaliar as probabilidades e efeitos dos riscos; (3) Desenvolver estratégias para mitigar os riscos identificados; (4) Monitorar os fatores de risco; (5) Utilizar planos de contingência; (6) Gerenciar crises; (7) Sair de crises [6].

Chapman e Ward (1997) descreveram um processo genérico, de gerência de riscos de projetos, composto por nove passos: (1) Definir os aspectos chaves do projeto; (2) Focar a estratégia da abordagem de gerência de risco escolhida; (3) Identificar onde os riscos podem surgir; (4) Estruturar as informações sobre riscos e seus relacionamentos; (5) Assinalar o domínio do risco e as respectivas respostas; (6) Estimar a extensão das incertezas; (7) Avaliar a magnitude dos vários riscos; (8) Planejar as respostas; (9) Gerenciar através da execução de controles e monitoramentos [7].

No RUP (*Rational Unified Process*) (1998) o processo de gerência de riscos é apresentado baseado em suas fases de desenvolvimento do produto, de forma sistemática: Concepção – ênfase nos riscos dos requisitos de negócio; Elaboração – foco nos riscos técnicos de definição da arquitetura do software; Construção – tratamento dos riscos lógicos envolvidos na construção do produto e; Transição – os riscos funcionais de utilização do software [8].

O Instituto de Gerenciamento de Projetos (*PMI – Project Management Institute*) (2000) apresenta seis fases para o processo de gerência de riscos: Plano de gerência de riscos, Identificação de riscos, Análise quantitativa de riscos, Análise qualitativa de riscos, Plano de respostas aos riscos e Monitoramento e Controle de riscos [9].

O SEI através dos modelos do CMMI (*Capability Maturity Model Integrated*) (2001) define o processo de gerência de risco em três fases: Avaliação de Riscos, Controle de Riscos e Relatórios de Riscos [10].

Tabela 1. Princípios básicos da gerência de risco [4]

PRINCÍPIO	**CARACTERÍSTICAS**
VISÃO COMPARTILHADA DO PRODUTO	Compartilhamento da visão do produto com base em propósito comum, responsabilidade e comprometimento coletivo com o projeto; Foco em resultados.
TRABALHO EM EQUIPE	Trabalho cooperativo para atingir metas comuns; Concentração e disponibilização de talentos, habilidades e conhecimento.
PERSPECTIVA GLOBAL	Visualização do desenvolvimento de software (definição, projeto e desenvolvimento); Reconhecimento do valor potencial das oportunidades e do impacto dos possíveis fatores adversos.
VISÃO ANTECIPADORA	Pensamento voltado para o futuro, identificação de incertezas, antecipação de possíveis desfechos, gerenciamento dos recursos e atividades do projeto.
COMUNICAÇÃO ABERTA	Facilitação da comunicação formal, informal e espontânea; Utilização de processos decisórios baseados em consenso que permitam valorizar opiniões individuais.
GERENCIAMENTO INTEGRADO	A gerência de risco é parte integral e vital para a gerência de projetos; Adaptação dos métodos e ferramentas de gerência para a infra-estrutura do projeto, respeitando-se a cultura.
CONTINUIDADE DO PROCESSO	Identificação e gerência dos riscos executada rotineiramente em todas as fases do ciclo de vida do projeto.
ACESSO AO CONHECIMENTO	Amplo acesso ao conhecimento sobre gerência de riscos, domínio do problema e sobre o processo de desenvolvimento de software.

A Tabela 1 apresenta oito princípios básicos da gerência de risco que são compostos pela união das características presentes nas abordagens estudadas. Pode-se destacar a abordagem do SEI [4] como a mais representativa da diversidade e abrangência dos fatores apresentados.

Os princípios básicos da gerência de risco são os fatores norteadores das atividades que precisam ser desenvolvidas. Na seção seguinte, apresentam-se as atividades fundamentais da gerência de risco que são consenso na literatura da Engenharia de Software.

3. Atividades da Gerência de Risco

Na literatura de gerência de risco em engenharia de software [4] parece haver um consenso sobre as atividades que compõem o processo de gerência de risco. Deve-se ressaltar que todas as atividades são baseadas e centradas na comunicação, devendo ser realizadas de forma cíclica e contínua dentro do processo de gerência de risco.

Planejar a gerência de risco. Esta atividade tem a finalidade de definir a estratégia do gerenciamento de risco, dos recursos necessários para a realização do processo e por fim, da efetivação das ações consideradas necessárias no plano de gerência de risco.

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

Analisar riscos. Nesta atividade são caracterizados os aspectos mais importantes de cada risco, com a finalidade de explorar as melhores estratégias de mitigação. De uma forma geral, os riscos são categorizados e priorizados, segundo algum critério específico estabelecido, para tornar a gerência concentrada nos riscos considerados prioritários.

Planejar respostas aos riscos. O planejamento é uma atividade da gerência de risco que envolve, em geral, a determinação dos riscos a serem gerenciados, dos planos de ação para os riscos sob controle da gerência e dos planos de contingência para os riscos que se encontram além das capacidades de mitigação.

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

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

Comunicar os riscos. A comunicação entre as equipes e membros do projeto de software é um dos fatores mais importantes para a realização bem sucedida da gerência de riscos. Riscos, problemas e crises podem aparecer, quando a estrutura de comunicação é debilitada em uma organização [11].

4. Gerência de Risco e Modelos de Qualidade do Processo de Software

Qualidade atualmente é um dos maiores fatores de motivação em todas as áreas da atividade humana. Embora seja um consenso, existe a necessidade de definição de uma base de entendimento universal para que se possa desenvolver atividades diárias. Várias normas e modelos foram editados ou estão em desenvolvimento como forma de suprir esta necessidade.

A qualidade de software é diretamente influenciada pela qualidade dos processos utilizados no desenvolvimento de software. Desta forma, a melhoria do processo de qualidade garante a melhoria da qualidade de software. Esta foi a base para a criação dos modelos de definição, avaliação e evolução dos processos de software. Nas seções seguintes abordaremos alguns destes processos sob a visão das atividades da gerência de risco.

4.1 Gerência de Risco na ISO 9000-3

A norma ISO 9000-3 é um guia de aplicação da norma ISO 9001 [12] para o desenvolvimento, fornecimento e manutenção de software. A norma ISO 9001 faz parte da série de normas ISO 9000, voltadas para a gestão e garantia da qualidade. Estas normas especificam os requisitos mínimos para que as empresas possam assegurar a qualidade de seus produtos e serviços, não definindo modelos ou impondo sistemas de qualidade a serem implementados nas organizações. As empresas definem seus próprios modelos de gestão de qualidade, dependendo de seu tipo de negócio e suas características.

As diretrizes propostas na norma ISO 9000-3 cobrem questões como o entendimento comum entre as partes (contratante e contratado) de requisitos funcionais e o uso de metodologias consistentes para o desenvolvimento de software e gerenciamento de projeto como um todo, da concepção até a manutenção.

A norma ISO 9000-3 abrange todo o ambiente de desenvolvimento de software e detém seu foco na garantia da conformidade do produto e serviços associados com as expectativas do cliente. Todas as orientações da ISO 9000-3 dizem respeito à "situação contratual", onde uma empresa contrata a outra empresa para desenvolver um produto de software. A Tabela 2 mostra os processos definidos na norma ISO 9000-3.

Tabela 2. Processos da norma ISO 9000-3

ELEMENTO	DESCRIÇÃO
ESTRUTURA DO SISTEMA DE QUALIDADE	Responsabilidade do Fornecedor; Responsabilidade do Comprador; Análise Crítica Conjunta.
ATIVIDADES DO CICLO DE VIDA	Análise Crítica do Contrato; Especificação dos Requisitos do Comprador; Planejamento do desenvolvimento; Planejamento da qualidade; Projeto e implementação; Testes e validação; Aceitação; Cópia, Entrega e Instalação; Manutenção.
ATIVIDADES DE APOIO	Gerenciamento de configuração; Controle de documentos; Registros da Qualidade; Medição; Regras, Práticas e Convenções; Ferramentas e Técnicas; Aquisição; Produto de Software Incluído; Treinamento.

A norma ISO 9000-3 não aborda explicitamente a gerência de risco, mas em suas práticas, enaltece as atividades de identificação, análise, controle e monitoração de riscos, inerentes a contratos, com a aplicação de ações corretivas e preventivas. Inclusive, com vistas à melhoria contínua do processo de desenvolvimento, fornecimento ou manutenção de software, especificamente na contratação (validação dos requisitos de software especificados pelo comprador). A norma não define processos e sim atividades a serem cumpridas através de uma visão de estrutura, ciclo de vida e atividades de apoio.

4.2 Gerência de Risco na ISO 12207 e ISO 15504

A ISO/IEC 12207 formaliza dos Processos do Ciclo de Vida do Software através de um *framework* com terminologias de processos bem definidos, ao invés de forçar a utilização de um determinado modelo de ciclo de vida ou método de desenvolvimento de software [13].

A ISO/IEC 12207 é a primeira norma internacional que descreve em detalhes os processos, atividades e tarefas que envolvem o fornecimento, desenvolvimento, operação e manutenção de produtos de software. A principal finalidade desta norma é servir de referência para os demais padrões que venham a surgir. Lançada em agosto de 1995, ela é citada em quase todos os trabalhos relacionados à engenharia de software desde então, inclusive àqueles relativos à qualidade.

Esta norma divide os processos em três grandes classes: Processos Fundamentais, Processos de Apoio e Processos Organizacionais [13].

- Processos fundamentais são compostos pelos processos de manutenção, aquisição, fornecimento, desenvolvimento e operação, responsáveis pelo início e execução do desenvolvimento, operação ou manutenção do software durante o seu ciclo de vida.
- Processos de apoio são compostos pelos processos de documentação, gerência de configuração, garantia da qualidade, verificação, validação, revisão conjunta, auditoria, e resolução dos problemas que têm o papel de auxiliar um outro processo.
- Processos organizacionais são compostos pelos processos de gerência, de infra-estrutura, de melhoria e de treinamento que implementam uma estrutura constituída de processos de ciclo de vida e de pessoal associados, melhorando continuamente a estrutura e os processos.

A ISO/IEC 12207 apresenta um detalhamento de cada um dos processos acima. Define como podem ser usados de diferentes maneiras por diferentes organizações (ou parte destas), representando diversos pontos de vista para esta utilização. Estas visões representam a forma como uma organização pode utilizar estes processos, agrupando-os de acordo com suas finalidades e necessidades:

- Visão de Contrato – dentro dos processos fundamentais, na visão do cliente e fornecedor, a integração dos processos de aquisição e fornecimento.
- Visão Operacional – ainda dentro dos processos fundamentais, esta visão enfoca o operador e os usuários, através do processo de operação.
- Visão de Engenharia – esta visão proporciona a integração dos processos de manutenção e desenvolvimento, favorecendo as equipes responsáveis por estes processos, dentro dos processos fundamentais.
- Visão de Equipe de Apoio – Integração dos processos de apoio.

A ISO/IEC 12207 está sendo alterada para ficar de acordo com a ISO/IEC 15504-5 (*SPICE – Software Process Improvement and Capability dEtermination*) – An Assessment Model and Indicator Guindance [14]. Desta forma, a ISO/IEC 12207 substituirá os processos da norma ISO/IEC 15504, que estarão incluídos em seu anexo ISO/IEC PDAM 12207 [15].

O projeto SPICE objetivou a criação de normas para a avaliação de processos e a contínua melhoria desses processos, baseando-se nas melhores características de modelos de avaliação como CMM (*Capability Maturity Model*).

A melhoria de processos é realizada através de avaliações, que descrevem práticas usuais da organização, de uma unidade organizacional ou de um projeto. A análise dos resultados é feita em relação às necessidades do negócio da organização, levantando aspectos negativos e positivos, como também os riscos envolvidos no processo em avaliação.

O processo de gerência de risco, de acordo com a norma ISO 15504 [16], é composto pelas seguintes atividades:

- Definição do escopo da gerência de risco – determinar o escopo da gerência de risco que será utilizada pelo projeto, de acordo com as políticas de gerência de risco organizacional[1].
- Identificação de riscos – identificar riscos para o projeto, no início e durante sua execução.
- Análise e priorização de riscos – avaliar a probabilidade de ocorrência, o impacto, o tempo de ocorrência, a causa e as relações entre os riscos para determinar a prioridade de aplicação dos recursos para a redução desses riscos.
- Definição da estratégia para gerir risco – definir uma estratégia apropriada para gerenciar um risco ou um conjunto de riscos, em nível de projeto e em nível organizacional.
- Definição das métricas – para cada risco ou conjunto de riscos, definir as métricas[2] para aferição da mudança na situação do risco e do progresso das atividades de redução.
- Implementação da estratégia da gerência de risco – executar a estratégia definida para a gerência de risco, em nível de projeto e em nível organizacional.
- Avaliação dos resultados – em pontos de controle pré-determinados, aplicar as métricas definidas para avaliar o progresso esperado e o nível de sucesso da estratégia da gerência de risco.
- Execução das ações corretivas[3] – quando o progresso esperado na redução do risco não é alcançado, executar ações corretivas para corrigir ou evitar o impacto do risco.

Um dos aspectos positivos da ISO 15504 é a expansão e flexibilização dos modelos de qualidade (TQM, PDCA, SW-CMM, etc.), mas devido a grande quantidade de informação necessita de treinamento e capacitação para sua efetiva aplicação.

4.3 Gerência de Risco no SW-CMM (Capability Maturity Model for Software)

Em 1987, o SEI – *Software Engineering Institute*, sob a coordenação de Watts Humphrey, gerou a primeira versão do que veio a se chamar modelo CMM – *Capability Maturity Model*. O modelo era composto pelos documentos de maturidade de processos [5] e pelo questionário de maturidade [17]. Em 1991, o SEI evoluiu a estrutura de maturidade de processo para o SW-CMM – *Capability Maturity Model for Software* [18].

O SW-CMM foi o primeiro modelo desenvolvido na área de maturidade e capacidade organizacional, na área de desenvolvimento de software. Foi uma requisição do Departamento de Defesa do Estados Unidos ao Instituto de Engenharia de Software (*SEI - Software Engineering Institute*) da Universidade Carnegie Mellon (*Carnegie Mellon University*).

O SW-CMM estabelece cinco níveis de maturidade sendo que cada um desses níveis indica a capacidade do processo. Cada nível é caracterizado pela existência de determinados processos, chamados de KPA – *Key Process Areas* (Áreas-Chave de Processo). A qualidade na execução do processo, o nível de acompanhamento desta execução e a adequação dos processos aos projetos são alguns dos fatores medidos para a determinação do nível de maturidade da organização.

---

[1] Assuntos que são considerados no escopo incluem severidade, probabilidade e tipo de risco.
[2] As métricas deveriam cobrir mudanças na probabilidade, no impacto e temporalidade da ocorrência do risco.
[3] Ações corretivas podem envolver o desenvolvimento ou implementação de novas estratégias de redução ou ainda, o ajuste das estratégias existentes.

O SW-CMM tem cinco níveis de maturidade onde o nível mais avançado corresponde a uma maior maturidade do processo que está associado a uma maior produtividade e qualidade, e a um menor risco. A Tabela 3 apresenta os níveis de maturidade e as áreas chaves dos processos do SW-CMM versão 1.2.

Tabela 3. Níveis de maturidade e áreas chaves de processo – SW-CMM versão 1.2 [18]

NÍVEIS	ÁREAS CHAVES DE PROCESSO	RESULTADO
NÍVEL 5 – OTIMIZADO	Prevenção de Defeitos Gerenciamento de mudanças tecnológicas Gerenciamento de mudanças de processo	***Maior produtividade e qualidade, menor risco***
NÍVEL 4 - GERENCIADO	Gerenciamento quantitativo do processo Gerenciamento de Qualidade de Software	
NÍVEL 3 – DEFINIDO	Foco no processo organizacional Definição do processo organizacional Programa de treinamento Engenharia do produto de software Gerenciamento integrado do software Coordenação entre grupos Revisões	
NÍVEL 2 - REPETITIVO	Gestão de requisitos Planejamento de Projeto de Software Acompanhamento e Supervisão de Projeto de Software Gestão de Subcontratação de Software Garantia da Qualidade de Software Gestão de Configuração	***Menor produtividade e qualidade, maior risco***
NÍVEL 1 - INICIAL	N/A	

A atividade de gerência de risco está localizada no nível 2, na KPA de Planejamento de Projeto de Software:

- Analisar os riscos do software associados a custo, recursos, cronograma e aspectos técnicos do projeto identificados, avaliados e documentados.

Onde na realidade, existe um conjunto de tarefas associadas:

- Análise dos riscos do projeto com a priorização dos mesmos de acordo com o impacto; e
- Definição dos planos de contingências para os riscos identificados que não tenham condições de serem eliminados.

O SW-CMM é um modelo aplicável às organizações que desejam uma avaliação de seus processos e enquadramento em um dos seus níveis de maturidade, mas uma das grandes limitações é a pouca ênfase dada à diversidade das organizações, dificultando sua aplicações em organizações de pequeno porte.

4.4 Gerência de Risco no CMMI (Capability Maturity Model Integration)

Em decorrência da evolução do modelo SW-CMM (*Software – Capability Maturity Model*), em 2000 foi lançado o modelo CMMI – *Capability Maturity Model Integration*, que agrega, além da representação por estágios (SW-CMM), a representação contínua [10].

O CMMI foi desenvolvido com objetivos específicos, voltados para a substituição de todos os modelos CMM:

- eliminar inconsistências e diminuir as redundâncias;
- maior visibilidade e entendimento do uso de uma terminologia comum; e
- assegurar a conformidade com a norma ISO/IEC 15504.

O CMMI oferece uma avaliação e melhoria de processos organizacionais de forma efetiva e eficiente; reduz os custos de formação e avaliação; promove uma visão integrada da melhoria dos processos organizacionais; e um novo meio de representação da informação de disciplinas específicas, através do uso de modelos de melhoria testados [10].

De acordo com a Tabela 4, pode-se visualizar os níveis e as áreas de processos equivalentes. As atividades de gerência de risco estão definidas no nível 3 – Definido, na área de processo de gerenciamento de riscos.

Tabela 4. CMMI – Áreas de Processos

NÍVEL	FOCO	ÁREA DE PROCESSO
5 OTIMIZADO	MELHORAMENTO CONTÍNUO DO PROCESSO	Inovação Organizacional Análise de causas e resoluções.
4 GERENCIADO QUANTITATIVAMENTE	GERENCIAMENTO QUANTITATIVO	Performance organizacional do processo Gerenciamento quantitativo de projetos
3 DEFINIDO	PADRONIZAÇÃO DO PROCESSO	Requisitos de desenvolvimento Soluções técnicas Integração de produtos Verificação Validação Foco no processo organizacional Definição do processo organizacional Treinamento organizacional Gerenciamento de projeto integrado Gerenciamento de riscos Integração da equipe de trabalho Gerenciamento integrado de suprimentos Análise de decisões Ambiente organizacional para integração
2 GERENCIADO	GERENCIAMENTO BÁSICO DE PROJETOS	Gerenciamento de requisitos Planejamento do projeto Controle e monitoração do projeto Gerenciamento de suprimentos Avaliação e análise Garantia da qualidade do processo e produto Configuração do gerenciamento
1 INICIAL	N/A	N/A

Este modelo é subdividido em áreas de processos, com quatro categorias: Processos de Gerência de Processo, Processos de Gerência de Projeto, Processos de Engenharia e Processos de Apoio. A Tabela 5 mostra as áreas-chave de processos dentro das categorias do CMMI.

Tabela 5. Distribuição das áreas-chave nos processos do CMMI [10]

CATEGORIA DE PROCESSO	GRUPO DE ÁREA DE PROCESSO	PROCESSOS
Gerência de Processo	Básico	Foco no Processo Organizacional, Definição do Processo Organizacional, Treinamento Organizacional
	Avançado	Execução do Processo Organizacional, Entrega e inovação organizacional
Gerência de Projeto	Básico	Planejamento de Projeto Monitoramento e Controle de Projeto Gerência de "Contratos" com Fornecedores
	Avançado	Gerência integrada de projeto Gerência de risco Gerência quantitativa de projeto
Engenharia		Desenvolvimento de requisitos Gerência de requisitos Solução técnica Integração do Produto Verificação Validação
Processo de Apoio	Básico	Gerência de Configuração Gerência de Qualidade de Produto e de Processo Análise e Medição
	Avançado	Resolução e análise de decisão Resolução e análise de causa

A gerência de risco pode ser iniciada já no nível 2, dentro da área de processo de Planejamento de Projeto e Monitoramento e Controle de Projeto, com a simples identificação dos riscos, tendo como objetivo o conhecimento e tratamento quando ocorrerem. A categoria de processo de Gerência de Risco é uma evolução dessas práticas para: planejamento sistemático, antecipação e minimização de riscos para a redução proativa de seus impactos no projeto.

5. Análise Comparativa dos Processos de Gerência de Risco

As definições dos processos apresentados na seção anterior, diferenciam-se em relação à nomenclatura utilizada para a descrição das atividades, à subdivisão dessas atividades em tarefas e na definição do escopo de determinadas atividades.

Através da Tabela 6 pode-se melhor visualizar a similaridade entre os processos de gerência de risco analisados, tendo como referência as atividades apresentadas na Seção 3. Todos os processos estudados pregam que as atividades devem ser executadas de forma contínua e cíclica, promovendo a análise de riscos que durante os levantamentos iniciais não tenham sido percebidos ou que tenham apresentado sinais de ocorrência quando o projeto já tenha sido iniciado.

Tabela 6. Análise comparativa das atividades do processo de gerência de risco

ATIVIDADES	PROCESSOS			
	ISO-9000-3	**ISO-12207 / ISO-15504**	**CMM**	**CMMI**
PLANEJAR A GERÊNCIA DE RISCO	Planejar o desenvolvimento do projeto	Definição do escopo da gerência de risco	*Não existe menção a esta atividade*	Determinar as origens e as categorias de riscos Definir parâmetros Estabelecer estratégia
IDENTIFICAR RISCOS	Identificar Riscos	Identificar Riscos	Identificação dos riscos	Identificar Riscos
ANALISAR RISCOS	Analisar problemas potenciais	Analisar e priorizar riscos	Análise dos riscos do projeto com a priorização dos mesmos de acordo com o impacto	Priorizar, estimar e classificar riscos Avaliar e classificar cada risco.
PLANEJAR RESPOSTAS AOS RISCOS	Definir planos de contingência	Definir a estratégia para a gerência de risco	Definição dos planos de contingências para os riscos identificados que não tenham condições de serem eliminados	Desenvolver planos para reduzir riscos
MONITORAR RISCOS	Verificar a execução dos procedimentos do plano de desenvolvimento do projeto	Definir métricas para riscos Implementar a estratégia da gerência de risco Avaliar os resultados da estratégia da gerência de risco Executar ações corretivas	*Não existe menção a esta atividade*	Implementar planos para reduzir riscos
CONTROLAR RISCOS	Controlar a execução do projeto	*Não existe menção a esta atividade*	*Não existe menção a esta atividade*	*Não existe menção a esta atividade*
COMUNICAR OS RISCOS	Comunicação implícita	Comunicação implícita	Comunicação implícita	Comunicação implícita

Os únicos processos estudados que apresentam a atividade *Planejar a Gerência de Risco* são os das normas ISO 9000-3 [12], ISO 12207 [13], ISO 15504 [16] e CMMI [10]. As vantagens de apresentar esta atividade são as definições dos recursos de hardware, software e pessoal necessário à realização da gerência de risco, baseado no plano de escopo. Determinar as origens e as categorias desses recursos e definir indicadores. Para acompanhar a produtividade, proporcionam uma estratégia de utilização e otimização dos recursos efetivamente alocados no projeto. Como desvantagem apresenta-se o custo e o tempo atrelado ao desempenho desta atividade e tarefas complementares.

A atividade *Identificar Riscos* aparece em todos os processos estudados, onde sua principal finalidade é levantar os riscos associados ao projeto. Esta atividade é vital para o processo, pois promove a identificação dos prováveis fatores e eventos associados a esses riscos, bem como o impacto do risco no projeto.

De uma forma geral, todos os processos estudados têm em comum a atividade *Analisar Riscos*. As abordagens do SW-CMM [18] e CMMI [10] apresentam explicitamente as necessidades de avaliar e estimar os esforços para eliminar os riscos levantados.

A atividade *Planejar Respostas aos Riscos* tem o objetivo de definir os planos de ações corretivas, preventivas e de contingência para o efetivo controle dos riscos. Esta atividade aparece em todas as abordagens, com variações de nomenclatura, tais como: no CMMI estabelece-se como redução de riscos; já o CMM frisa a definição dos planos de contingências para os riscos que não serão eliminados, com o intuito de mitiga-los. De todas as atividades estudadas, nos processos analisados, esta atividade é a mais importante, pois é a partir dela que os planos e ações serão traçados para conter os riscos.

A atividade *Monitorar Riscos* aparece com o mesmo significado, em todos os processos, com exceção das normas ISO 12207 [13] , ISO 15504 [16] e CMMI [10]. As normas ISO condensam muitas atividades que poderiam ter suas definições no Planejamento das respostas aos riscos, como por exemplo, à definição das métricas. Já o CMMI associa a atividade à redução dos riscos, que é uma forma de controle.

Todos os processos de uma forma geral, colocam implicitamente as ações corretivas como forma de replanejamento e correção dos desvios encontrados ao longo do acompanhamento da execução do projeto. Esta atividade apresenta a vantagem de garantir a aplicação das definições do plano de gerência de riscos pelo monitoramento contínuo do projeto.

A atividade *Controlar Riscos* envolve a avaliação da situação atual para determinação de possíveis desvios do plano inicial de gerência de risco. Com exceção do processo apresentado pela norma ISO 9000-3 [12], a atividade de controle de risco é tratada implicitamente na atividade de monitorar riscos.

A necessidade da atividade de *Comunicação* não é explicitada em nenhum dos processos analisados, embora seja implícita em todo projeto de software, independentemente de abordagem ou modelo utilizado.

A comunicação entre os membros do projeto de software é um dos fatores mais importantes para a realização bem sucedida da gerência de risco. Riscos, problemas e crises podem aparecer, quando a estrutura de comunicação é falha em uma organização.

6. Considerações Finais

A gerência de risco adiciona à gerência de projetos uma abordagem estruturada para identificação e análise de riscos no início do planejamento do projeto e no decorrer das fases de desenvolvimento de software. O planejamento de respostas aos riscos cria a perspectiva de se obter alternativas e planos de contingências para se mitigar os riscos, enquanto as funções de monitoração e controle dos processos de gerência de risco se combinam com a função de controle da gerência de projetos.

A partir desta análise comparativa das atividades dos processos de qualidade, sob a visão do processo de gerência de riscos, pode-se concluir que:

- não existe um processo padrão para gerenciar riscos. O que existem são práticas consolidadas na gerência de projetos: identificar, analisar, priorizar e controlar riscos;
- não existe a indicação de processos e métodos que possam ser utilizados na execução das atividades para o gerenciamento de riscos;
- as organizações ajustam seus processos às atividades de gerência de risco, de acordo com a sua realidade;
- nenhum dos processos apresenta um detalhamento das tarefas que possivelmente compõem as atividades propostas; e

- nenhum dos processos apresenta a necessidade da efetiva realização de avaliações de riscos sob a ótica qualitativa[4] e quantitativa[5], uma vez que o ambiente organizacional, pela competitividade no ambiente de negócios, coloca os gerentes e as empresas em contato com escassez de recursos, estreitas oportunidades e constantes mudanças ocasionadas por demandas de clientes internos e externos.

Neste estudo, procurou-se mostrar que a gerência de risco é fator de grande importância e utilidade no alcance da maturidade organizacional. As atividades de identificação, análise e monitoração de riscos devem ser realizadas de forma sistematizada e controlada, durante todo o processo. Salienta-se a necessidade de avaliações constantes e contínuas dos fatores e eventos associados a cada risco priorizado, como uma forma de implementar a melhoria e garantir a qualidade do processo de desenvolvimento de software.

Finalmente, as avaliações propostas devem levar em consideração métodos de coleta de dados qualitativos e quantitativos, subsidiando os gestores na tomada de decisão, pois os riscos associados a cada projeto devem ser visualizados de acordo com suas particularidades.

[4] Abordagem Qualitativa: análise baseada em experiência e visão subjetiva.
[5] Abordagem Quantitativa: indica a análise de quantidades numéricas ou valoradas.

Referências Bibliográficas

1. HALL, E. M. 1998. *Managing Risk*. 2ª Ed. USA: Addison Wesley. p 88-103.
2. BOEHM, B. W. 1991. Software Risk Management: principles and practices, *IEEE Software*, Volume 8. No1. p 32-40.
3. CHARETTE, R. 1990. *Application strategies for risk analysis*. New York: MultiScience Press. p 17-21.
4. HIGUERAG, P.R. 1994. An Introduction to Team Risk Management, Technical Report. *Software Engineering Institute, Carnegie Mellon University*. USA.
5. HUMPHREY, W. 1987. Characterizing the software process: a maturity framework, Technical Report. *Software Engineering Institute, Carnegie Mellon University*, USA.
6. FAIRLEY, R., 1994. Risk Management For Software's Projects. *IEEE Software*. p 54-66.
7. CHAPMAN, C. e WARD, S. 1997. *Project Risk Management: Processes, Techniques and Insights*. John Wiley & Sons. p 30-41.
8. KRUCHTEN, P. 2003. *Introdução ao Rup: Rational Unified Process*. 2ª Ed. Ciência Moderna. São Paulo. p 25-36.
9. PMI - PROJECT MANAGEMENT INSTITUTE. 2000. *A Guide to the Project Management Body of Knowledge*. Disponível na URL: <http://www.pmi.org/pmi/publictn/pmboktoc.htm>. Acesso em: 25.07.2003.
10. SOFTWARE ENGINEERING INSTITUTE, 2001. CMMI - Capability Maturity Model Integration version 1.1 Pittsburgh, PA. *Software Engineering Institute*, Carnegie Mellon University. USA.
11. HUMPHREY, W.S. 1990. *Managing the Software Process*. Addison – Wesley. p 9-17.
12. NBR ISO 9001, 2000. ISO 9001 - Sistema de Gestão de Qualidade Requisitos. *Associação Brasileira de Normas Técnicas* – ABNT. Rio de Janeiro.
13. NBR ISO 12207. 1998. ISO 12207 – Tecnologia de Informação – Processos de ciclo de vida de software. *Associação Brasileira de Normas Técnicas* – ABNT. Rio de Janeiro.
14. ISO/IEC 15504. 1999. ISO 15504 Part 5: An Assessmente Model and Indicator Guidance, ISO/IEC JTC1 SC7. *International Standard Organization* – ISO/IEC.
15. ISO/IEC PDAM 12207. 2002. ISO/IEC 12207 Information Tecnology – Ammendment to ISO/IEC 12207, ISO/IEC JTC1 SC7. *International Standard Organization* – ISO/IEC.
16. ISO/IEC 15504. 1999. ISO 15504 Software Process, ISO/IEC JTC1 SC7. *International Standard Organization* – ISO/IEC.
17. HUMPHREY, W. 1987. A method for assessing the software engineering capability of contractors. Pittsburgh, PA. *Software Engineering Institute*, Carnegie Mellon University. USA.
18. PAULK, M. 1993. Capability Maturity Model for Software version 1.1. Pittsburgh, PA. *Software Engineering Institute*, Carnegie Mellon University. USA.