LQPS
Qualidade e Produtividade de Software

Guia de Implantação da Gerência de Riscos em Micro e Pequenas Empresas alinhado ao CMMI-SE/SW

Elton Sanders
Christiane Gresse von Wangenheim

Relatório Técnico LQPS001.06P

Título	Guia de Implantação da Gerência de Riscos em Micros e Pequenas Empresas alinhado ao CMMI-SE/SW
No.	LQPS001.06P
Data	02.05.2006
Versão	Final
Distribuição	Pública

LQPS - Laboratório de Qualidade e Produtividade de Software
Universidade do Vale do Itajaí - UNIVALI - Centro de Educação São José
São José/SC, Brasil

Lista de Acrônimos

GP – Prática Genérica do CMMI-SE/SW (*Generic Practice*)
GG – Objetivo Genérico do CMMI-SE/SW (*Generic Goal*)
SP – Prática Específica do CMMI-SE/SW (*Specific Practice*)
GP – Objetivo Específico do CMMI-SE/SW (*Specific Goal*)
PA – Área de Processo do CMMI-SE/SW (*Process Area*)
RCO – Repositório de Conhecimento da Organização

Sumário

1 Introdução

Muitas empresas de desenvolvimento de software não estão preparadas para lidar com as incertezas que podem acontecer durante um projeto de software, e caso as empresas não lidem de forma apropriada, estas incertezas podem virar certezas. Segundo [HIGUEIRA96], todas as áreas englobadas por desenvolvimento de software são fontes de incerteza, por exemplo, incerteza quanto à tecnologia escolhida, incerteza quanto ao desempenho de hardware, incerteza sobre a funcionalidade do software, incerteza quanto à capacidade e disponibilidade das pessoas ou incerteza quanto ao custo e o cronograma definido do projeto. Estas incertezas são conhecidas como riscos, e caso estes riscos aconteçam, podem influenciar nos objetivos. A gerência de riscos em projetos de software pode auxiliar a empresa a identificar e controlar estes riscos, minimizando o impacto do risco sobre o projeto, ou eliminando a incerteza do projeto.

Em micro e pequenas empresas de software (MPE) brasileiras, pouca atenção é dada à gerência de riscos [MCT05]: apenas 1,4% de micro empresas e 2,2% de pequenas empresas possuem atividades de gerência de risco. Segundo Boehm [BOEHM91], a falta de gerência de risco aumenta a chance de riscos realmente acontecerem, impactando negativamente nos objetivos do projeto e no desempenho da MPE. Muitos destes problemas poderiam ser evitados ou fortemente reduzidos se existisse um comprometimento em identificar e resolver os elementos de alto risco destes projetos, pois frequentemente estes projetos são levados por uma onda de otimismo, deixando passar sinais de riscos que podem levar ao término prematuro do projeto.

A gerência de risco é abordada em modelos de referência de software como o PMBOK [PMI04] e o CMMI-SE/SW [SEI01]. No contexto do CMMI-SE/SW em estágios a área de processo de gerência de riscos faz parte do nível de maturidade 3. No modelo continuo esta área de processo é incluída no grupo de processos da gerência de projetos. As duas representações do CMMI-SE/SW apresentam um conjunto de práticas especificas da gerência de riscos, que abordam cada uma das etapas do processo de gerência de riscos.

Neste contexto, o presente projeto visa o desenvolvimento de um guia de implantação da área gerência de riscos alinhado ao CMMI-SE/SW voltado especificamente a MPEs que permita que estas gerenciem de forma ordenada os seus riscos e criem uma base para planejar, monitorar e controlar os projetos de software. E desta forma oferecendo um suporte para o sucesso e a competitividade destas empresas no mercado.

Este guia apresenta técnicas e ferramentas para ajudar o responsável pela gerência de riscos no projeto de software a tratar os riscos, organizadas por prática específica da gerência de risco segundo o CMMI-SE/SW.

1.1 Estrutura do documento

O capítulo 2 apresenta uma visão geral do CMMI-SE/SW, e as áreas de processo onde o CMMI-SE/SW faz referência a atividades de gerência de riscos.

O capítulo 3 apresenta uma visão geral das micro e pequenas empresas de software no Brasil em relação a gerência de riscos.

O capítulo 4 apresenta as técnicas e métodos da gerência de risco, organizadas por prática especifica do CMMI-SE/SW.

O capítulo 5 apresenta ferramentas que podem auxiliar nas atividades de gerência de risco.

O capítulo 6 apresenta um exemplo de execução da gerência de risco utilizando este guia.

2 Visão Geral sobre o Modelo CMMI-SE/SW

O modelo *Capability Maturity Model Integration* - CMMI foi desenvolvido pelo SEI (*Software Engineering Institute*) [SEI01] sendo uma evolução do modelo CMM. O propósito do CMMI é fornecer um guia para melhorar os processos de uma organização e a sua habilidade de gerenciar o desenvolvimento, a aquisição e a manutenção de produtos ou serviços.

O modelo CMMI-SE/SW apresenta duas representações: a representação em estágios e a representação contínua. Na representação contínua, o modelo CMMI-SE/SW apresenta 22 áreas de processos (*Proces Area* - PA) organizadas em quatro categorias (vide Figura 1).

PAs de Gerência de Processo: OPF: Foco no Processo Organizacional OPD: Definição do Processo Organizacional OT: Treinamento Organizacional OPP: Desempenho do Processo Organizacional OID: Inovação e Melhoria Organizacional	**PAs de Engenharia:** REQM: Gerência de Requisitos RD: Desenvolvimento de Requisitos TS: Solução Técnica PI: Integração de Produto VER: Verificação VAL: Validação
PAs de Gerência de Projeto: PP: Planejamento de Projeto PMC: Monitoração e Controle de Projeto SAM: Gerência de Acordos com Fornecedores IPM: Gerência Integrada de Projeto RSKM: Gerência de Risco QPM: Gerência Quantitativa de Projeto	**PAs de Apoio:** CM: Gerência de Configuração PPQA: Garantia da Qualidade de Processo e Produto MA: Medição e Análise DAR: Análise de Decisão e Resolução CAR: Análise de Causa e Resolução

Figura 1 - Áreas de Processo do CMMI-SE/SW [SEI01]

Na representação em estágios, as áreas de processo são organizadas em cinco níveis de maturidade, indicando quais áreas de processo devem ser implementadas para atingir cada nível de maturidade (Figura 2).

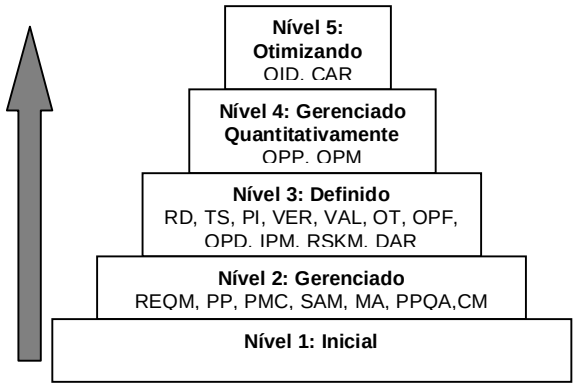

Figura 2 - Níveis de Maturidade da representação em estágios [SEI01]

Os níveis de maturidade representam um caminho de melhoria de processo ilustrando a evolução de melhoria para a unidade de organização visando a melhoria de processo. Nesta representação o resultado de uma avaliação do processo de software apresenta o nível de maturidade de uma unidade de organização como um todo. Quanto maior o nível de uma organização mais madura ela é considerada.

Cada área de processo do CMMI-SE/SW possui objetivos específicos (*Specific goals – SG*) e práticas específicas (*Specific Practices - SP*). Por meio das práticas específicas que são alcançados os objetivos específicos de cada área de processo, capacitando a organização na área de processo. Um objetivo específico (SG) descreve as características que devem estar presentes para satisfazer uma área de processo. Uma prática específica (SP) é a descrição de uma atividade que é considerada importante para se alcançar o objetivo específico a ela associado.

Além dos objetivos e práticas específicas, as áreas de processo possuem objetivos genéricos (GG) e práticas genéricas (SG). São chamadas de genéricas porque possuem características comuns por todas as áreas de processo de um nível de maturidade. Por exemplo, as áreas de processo do nível 2 apresentam o mesmo objetivo genérico GG2 Institucionalizar um processo gerenciado, e as áreas de processo do nível 3 apresentam o mesmo objetivo genérico GG3 Institucionalizar um processo definido. A Figura 3 mostra a relação entre as áreas de processo e as SG, SP, GG e SP na representação por estágios.

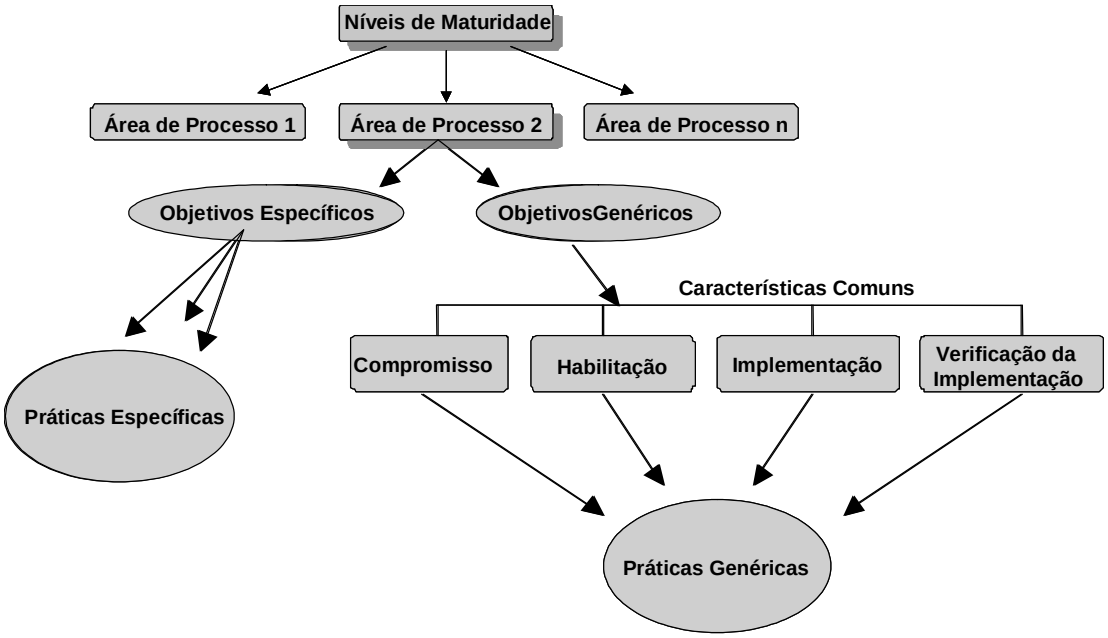

Figura 3 - Componentes da representação por estágios do modelo CMMI-SE/SW [SEI01]

A representação contínua do modelo CMMI-SE/SW utiliza os mesmos elementos da representação por estágios (Figura 4), porém apresenta uma estrutura bidimensional, separando a dimensão do processo (áreas de processo) da dimensão da capacidade (níveis de capacidade).

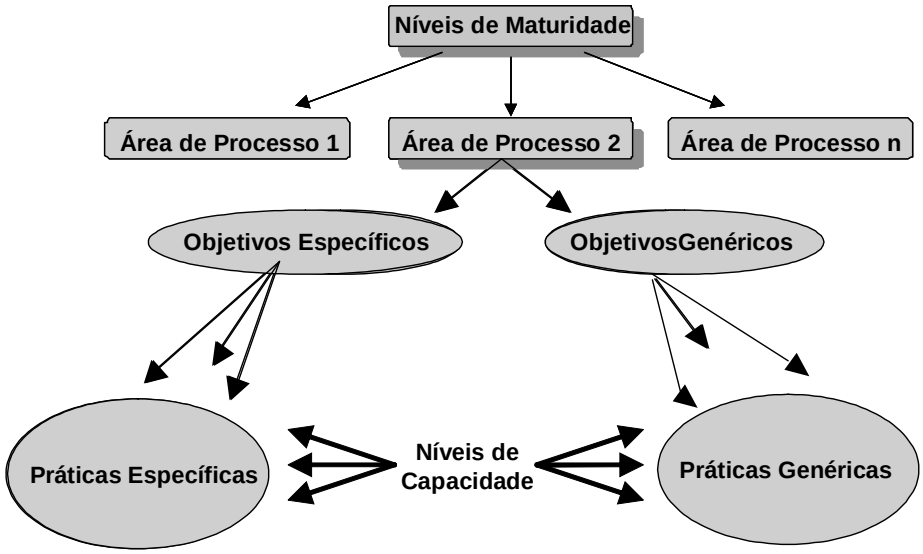

Figura 4 – Componentes da representação contínua do modelo CMMI-SE/SW [SEI01]

Para indicar o nível de capacidade, que cada área de processo se encontra, são utilizados os objetivos genéricos (GG). Para cada nível de capacidade, existe apenas um objetivo genérico.

Assim, o modelo permite selecionar, de forma mais flexível, um subconjunto de áreas de processo e respectivos níveis de capacidade para cada uma.

A dimensão de capacidade é organizada em seis níveis de capacidade (0 – 5), que indicam a habilidade de uma organização executar, controlar e melhorar uma determinada área de processo. Na representação contínua são gerados perfis de processos (Figura 5), contendo as áreas de processo mais relevantes da organização e é indicado o nível de capacidade de cada área de processo específica. Dessa forma é possível direcionar a melhoria apenas para as áreas de processo consideradas mais relevantes no contexto organizacional.

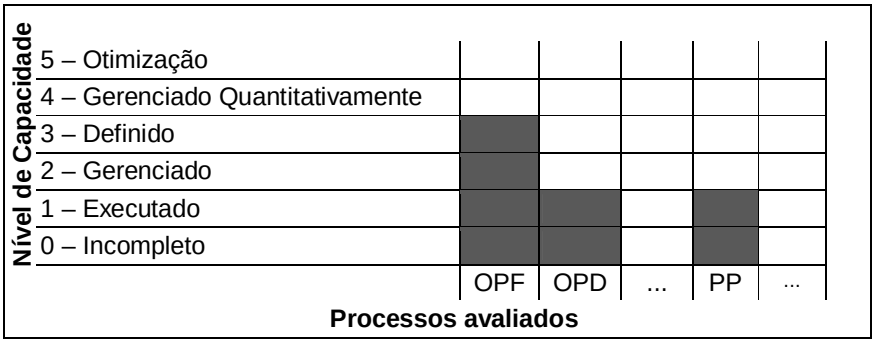

Figura 5 - Perfis de Processo

Além dos GG, GP, SG e SP, as duas representações do modelo CMMI-SE/SW utilizam os seguintes componentes informativos para direcionamento da implementação:

- Sub-práticas (*Subpractices*) – são descrições detalhadas que provêm mais informações sobre as práticas. Por exemplo, a prática pode ser escrever um plano de projeto. E as sub-práticas podem informar o que deve constar dentro do plano.
- Produtos típicos de trabalho (*Typical Work Products*) – cada área de processo provê exemplos de documentos, templates e outras saídas que são típicas na área de processo;
- Diretrizes de adaptação – são utilizadas para possibilitar que as organizações implementem processos padrão de maneira adequada a seus projetos. O conjunto de processos padrão da organização é descrito em um nível geral que não pode ser diretamente útil para executar o processo.
- Exemplos – são apresentados em todas as áreas de processo para auxiliar o entendimento;
- Elaborações das práticas genéricas – oferece informações sobre como a prática genérica deverá ser interpretada para a área de processo. Se não existir uma elaboração, a aplicação da prática genérica é considerada óbvia.

2.1 Gerência de Riscos no CMMI-SE/SW

O CMMI-SE/SW aborda a gerência de riscos principalmente por meio da área de processo de Gerencia de Riscos. No contexto do CMMI-SE/SW em estágios a área de processo de gerência de riscos faz parte do nível de maturidade 3. No modelo continuo esta área de processo é incluída no grupo de processos da gerência de projetos.

Porém, a gerência de riscos está também sendo considerada por meio de uma prática específica na área de processo de Planejamento de Projeto, e na área de processo de Monitoração e Controle, ambas associadas ao nível 2 de maturidade na representação em estágios. A área de processo Planejamento do Projeto, inclui o SG3 Desenvolvimento do Plano do Projeto com a SP2.2 Identificar os Riscos do Projeto, que consiste na identificação e na análise dos riscos para se determinar o impacto, a probabilidade de ocorrência e o período em que podem ocorrer, para que os riscos possam ser priorizados. Na Monitoração e Controle do Projeto, tem-se o SG1 Monitorar o Projeto de Acordo com o Plano, onde está inserida a SP1.3 Monitorar os Riscos do Projeto, que consiste na monitoração de riscos que foram identificados no projeto.

Assim, o modelo CMMI-SE/SW já no nível 2 de maturidade, na gerência de projetos, começa a se preocupar com a gerência de riscos, entretanto numa forma mais simples do que no nível 3 de maturidade, onde o modelo tem um foco bastante mais sistemático nesta área por meio de uma área de processo específica voltado para a gerência de riscos.

2.1.1 Área de processo de Gerência de Risco

A gerência de risco é um processo contínuo e de previsão, que é uma parte importante dos processos de gerenciamento técnico e de negócios. A gerência de riscos deverá tratar as questões que poderiam colocar em perigo o atendimento dos objetivos críticos. Uma abordagem contínua da gerência de risco é aplicada para antecipar e mitigar, de forma efetiva, os riscos que têm um impacto crítico no projeto [SEI01].

A gerência de riscos de riscos inclui uma antecipada e agressiva identificação de riscos através da colaboração e envolvimento dos *stakeholders* relevantes. Uma forte liderança entre todos os *stakeholders* relevantes é necessária para estabelecer um ambiente para uma exposição e discussão livres e abertas sobre os riscos [SEI01].

Embora as questões técnicas sejam preocupações importantes tanto nas etapas iniciais quanto em todas as fases do projeto, a gerência de riscos deve considerar as fontes internas e externas de riscos técnicos, de custos e de cronograma. Uma detecção de riscos antecipada e agressiva é importante porque, normalmente, é mais fácil, barato e causa menos interrupções fazer mudanças e corrigir esforços de trabalho durante as fases iniciais, que em fases posteriores do projeto [SEI01].

Conforme descrito no modelo CMMI-SE/SW, a gerência de riscos pode ser dividida em três partes: definir uma estratégia de gerência de riscos, identificar e analisar os riscos e tratar os riscos identificados, incluindo a implementação de planos de mitigação de riscos, quando necessário.

A Figura 6 mostra o relacionamento entre as áreas de processo do CMMI-SE/SW com atividades de gerência de risco.

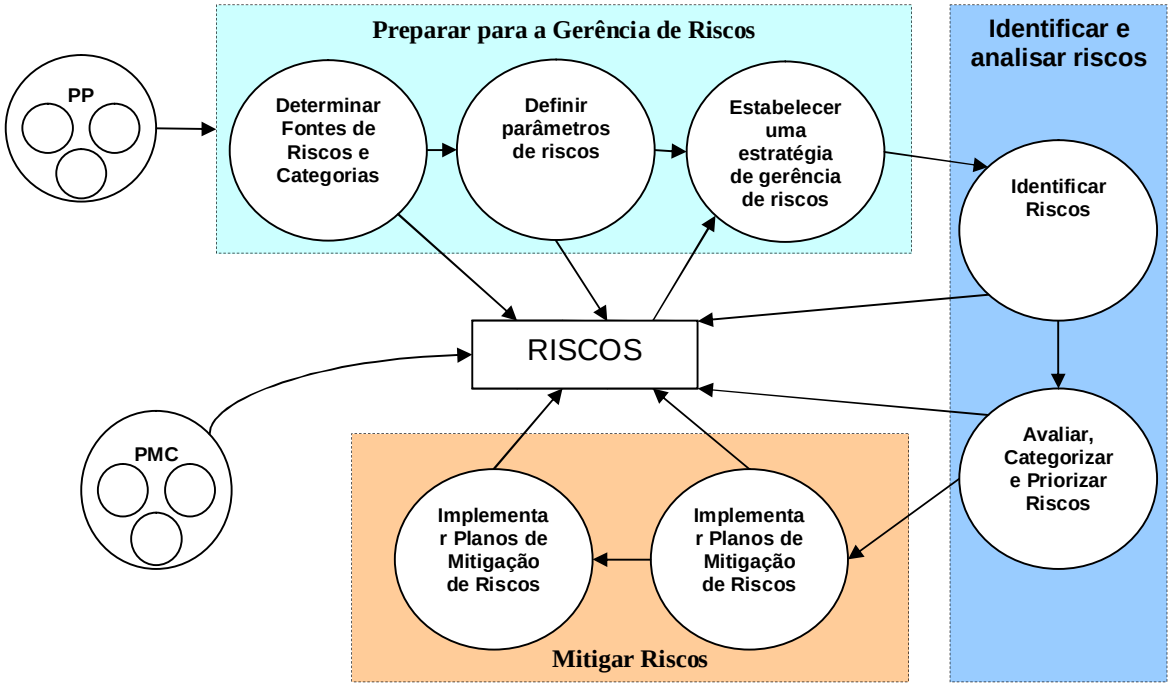

Figura 6 – Relacionamento entre as áreas de processo PP e PMC com RSKM (Adaptado de [AHERN03])

As áreas de processo Planejamento do Projeto, e Monitoração e Controle do Projeto, nível 2, tratam o gerenciamento de riscos de uma forma reativa, focando simplesmente na identificação dos riscos para a conscientização, e reação à medida que ocorram. Já o foco da área de processo Gerência de Risco, nível 3, é voltado ao tratamento o gerência de riscos de uma forma pro-ativa, descrevendo a evolução das práticas específicas para sistematicamente planejar, antecipar, e mitigar riscos com o objetivo de minimizar seu impacto no projeto.

Além das áreas de planejamento de projeto e monitoração e controle de projeto, a área de Análise e Resolução de Decisões (associado ao nível 3 de maturidade) provê um processo formal de avaliação para todas as áreas de processo, que garante que todas as alternativas foram avaliadas e a melhor foi usada. Este processo de escolha é usado na mitigação de

riscos. E a área de processo de Solução Técnica provê soluções técnicas alternativas com a finalidade também de mitigar riscos.

A Figura 7 mostra as atividades de gerência de riscos nas áreas de processo relacionadas.

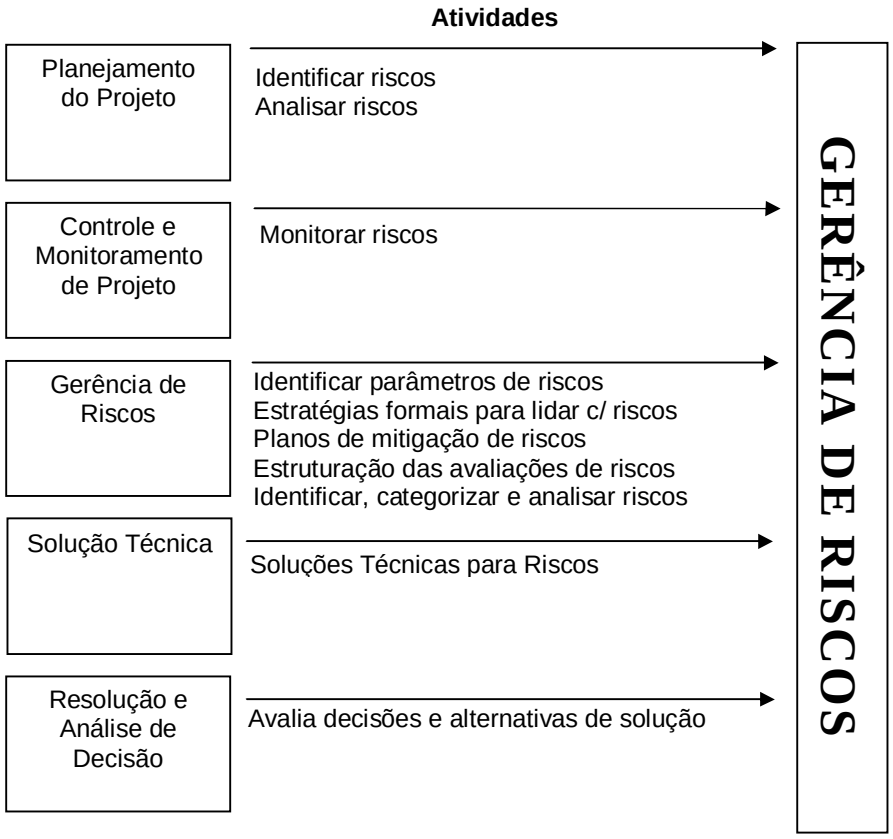

Figura 7 - Atividades de gerência de riscos nas áreas de processo do CMMI-SE/SW [SEI01]

A área de processo de Gerência de Risco tem por finalidade identificar potenciais problemas antes que ocorram. Desta forma, as atividades de tratamento destes riscos podem ser planejadas e realizadas, de acordo com suas necessidades, ao longo do ciclo de vida do produto ou projeto, para mitigar possíveis impactos adversos.

A

Tabela 1 mostra os objetivos específicos e as práticas específicas e genéricas da área de processo de gerência de risco.

Tabela 1 – Objetivos e práticas específicas e genéricas da área de processo da Gerência de Risco

SG1	Preparação para a gerência de riscos	
	SP1.1	Determinar fontes de riscos e categorias
	SP1.2	Definir parâmetros
	SP1.3	Estabelecer uma estratégia de gerência de riscos
SG2	Identificar e analisar riscos	
	SP2.1	Identificar riscos
	SP2.2	Avaliar, categorizar e priorizar riscos
SG3	Mitigar riscos	
	SP3.1	Desenvolver planos de mitigação de riscos
	SP3.2	Implementar planos de mitigação de riscos
GG3	Institucionalizar um processo definido	
	GP2.1	Estabelecer uma política organizacional
	GP3.1	Estabelecer um processo definido
	GP2.2	Planejar o processo
	GP2.3 GP2.4	Fornecer recursos Atribuir responsabilidades
	GP2.5	Treinar as pessoas
	GP2.6	Gerenciar configurações
	GP2.7	Identificar e envolver os *stakeholders* relevantes
	GP2.8	Monitorar e controlar o processo
	GP3.2	Coletar informações e melhorias
	GP2.9	Avaliar objetivamente a aderência
	GP2.10	Revisar o status com o nível mais alto de gerência

3 Contexto: Micro e Pequenas Empresas

As MPEs são, hoje, em todo o mundo e destacadamente no Brasil, um segmento dos mais importantes, visto serem agentes de inclusão econômica e social pelo acesso às oportunidades ocupacionais e econômicas, tornando-se sustentáculo da livre iniciativa e da democracia, sendo responsável pela esmagadora maioria dos postos de trabalho gerados no País [SEBRAE05]. A Legislação Básica da Micro e Pequena Empresa [SEBRAE06] define uma MPE em relação à receita bruta atual. Também existe a classificação do SEBRAE [SEBRAE05] relativa a empresas de serviços, que associa MPEs ao número de empregados da empresa (Tabela 2). Este será o critério adotado por este trabalho para definir uma MPE devido à facilidade de se obter essa informação.

Tabela 2 - Classificação das empresas por porte [SEBRAE05]

Porte	Número de Empregados
Micro	Até 9 pessoas
Pequena	Até 49 pessoas
Média	Até 99 pessoas
Grande	Acima de 99 pessoas

MPEs na economia brasileira representam 99% das empresas formalmente estabelecidas, gerando 60% dos empregos formais e cerca de 20% do PIB [SEBRAE05]. No período de 1995 a 2000, foram criadas mais de 400 mil novas microempresas e que em relação a novos postos de trabalho nos pequenos negócios o crescimento, no mesmo período, foi de 25,9%, correspondendo a 1,4 milhões de novos empregos, enquanto nas grandes empresas o incremento foi de apenas 0,3%, não atingindo 30 mil novas contratações [SEBRAE05].

De acordo com pesquisa realizada pelo [MCT05] com as empresas associadas ao SOFTEX, cerca de 77% da força efetiva das empresas de software no Brasil são micro e pequenas empresas (Figura 8), demonstrando a importância das MPEs no mercado nacional.

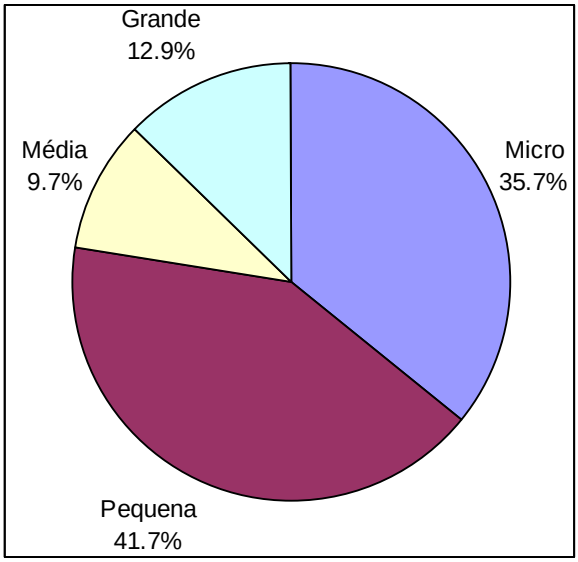

Figura 8 - Porte de empresas de software no Brasil [MCT05]

Quanto a idade, MPEs de Software são geralmente empresas muito novas, a maior parte com menos de 15 anos de vida [MCT05], desta forma com pouca experiência acumulada.

Quanto ao tipo de produto, cerca de 98,6% de micro empresas e 99,4% das pequenas empresas de software brasileiras desenvolvem software [MCT05], que podem chegar ao mercado em pacote, serviço ou embarcado [FREIRE02]:

- **Software pacote:** É geralmente padronizado e se caracteriza por não haver interação direta entre o usuário e aqueles que desenvolvem o software durante a confecção do produto. Desse modo, não existe um cliente exclusivo, o que significa que o software deve estar apto a atender uma demanda bastante genérica, fazendo com que o produto seja capaz de viver por si só, de forma independente. A comercialização é usualmente feita como produto de prateleira, sendo que as estratégias de marketing e vendas podem ser similares às utilizadas pelos equipamentos de hardware. A competitividade é dada pela capacidade de desenvolvimento técnico e de distribuição em massa, sendo que os dispêndios para a criação e o lançamento são altos, tendo realmente um caráter mais "industrial". Assim, as empresas líderes investem pesadamente em estratégias agressivas de marketing, aproveitando as vantagens de economias de escala, rede de vendas, suporte abrangente e marca reconhecida.
- **Software serviço (ou por encomenda):** aqueles programas desenvolvidos sob encomenda, fruto normalmente de projetos solicitados por usuários, os quais antecipadamente definem os traços gerais e específicos do desenvolvimento, desse modo, possuindo um caráter mais de serviço do que de produto. Assim, a interatividade entre usuário e os que o desenvolvem é intrínseca ao processo de produção, diferentemente do que acontece no software pacote. Como fator competitivo preponderante estão não só o conhecimento das atividades como também das necessidades dos clientes. Os riscos de mercado são menores, pois as vendas são efetuadas antes, porém os custos de desenvolvimento são mais significativos.
- **Software embarcado:** chegar ao mercado embutido em um equipamento. Atualmente, todo equipamento automatizado traz consigo um software – mesmo que simplificado – para operacionalizá-lo, o que torna a atividade de desenvolvimento desse tipo de software uma das mais importantes e dinâmicas.

Na Figura 9 e na Figura 10 é apresentado um breve panorama do tipo de software produzido por MPEs. São desenvolvidos diversos tipos de software, tanto em pacote, sob encomenda e os embarcados.

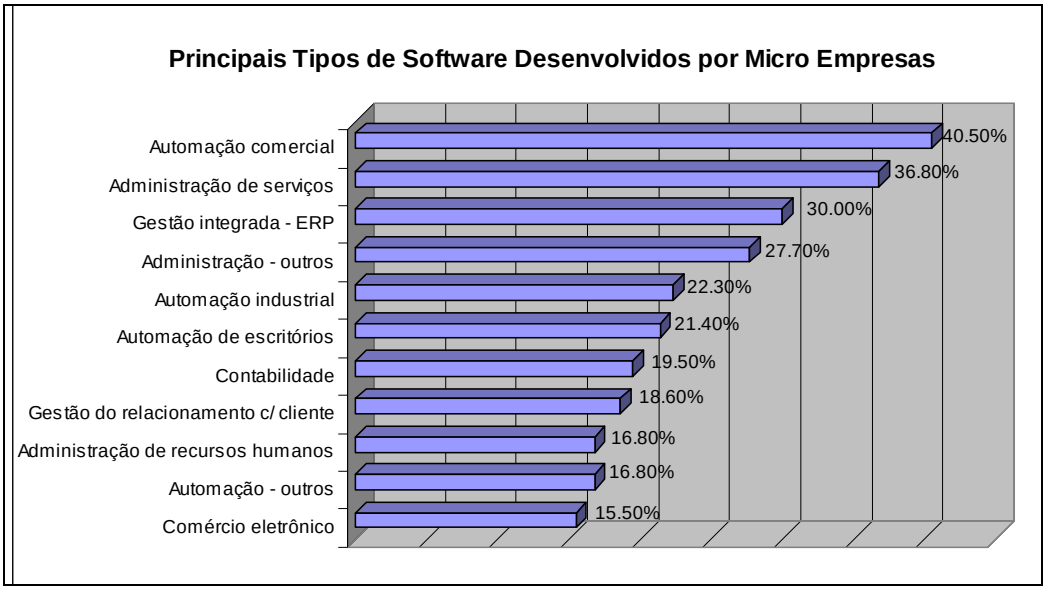

Figura 9 - Principais Tipos de Software Desenvolvidos por Micro Empresas [MCT05]

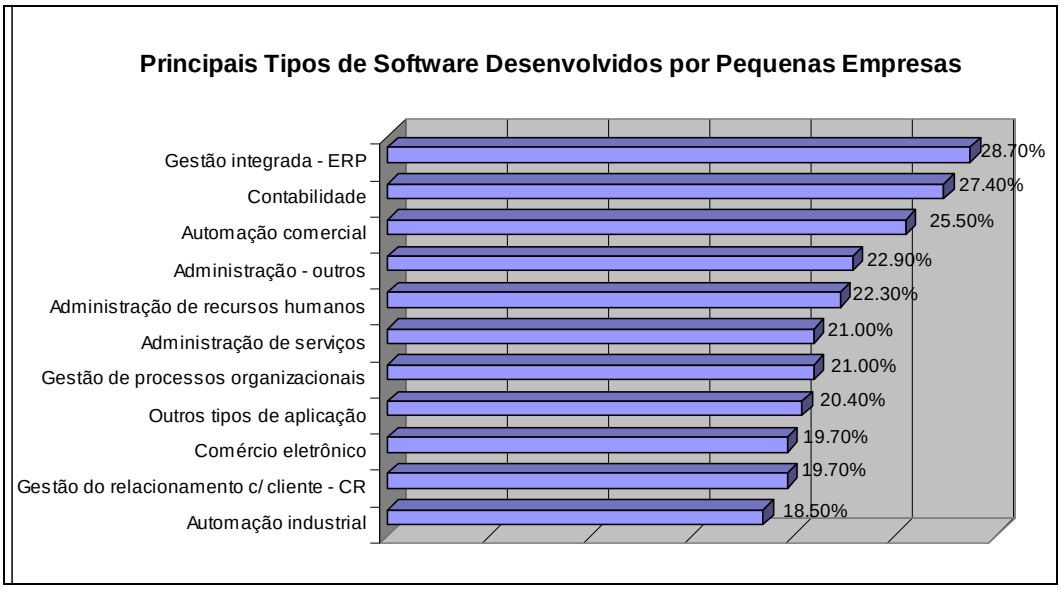

Figura 10 - Principais Tipos de Softwares Desenvolvidos em Pequenas Empresas [MCT05]

Ainda segundo FREIRE [FREIRE02] os softwares podem ser agrupados conforme o tipo de mercado em que se insere, dividindo-se em duas grandes categorias horizontal e vertical:

- **Segmento horizontal**: produtos com contéudo geralmente proviniente da área de informática, com pouco conteúdo específico de outra área de conhecimento. Vendido em forma de pacotes, precisa ser flexível, pois tem como objetivo resolver problemas informacionais básicos comuns às mais diversas áreas. São exemplos de produtos do

segmento horizontal os sistemas operacionais, as planilhas, os bancos de dados, processadores de texto, entre outros.

- **Segmento vertical**: produtos de uso restrito, abrangendo conhecimentos específicos de outras áreas além da informática, como saúde, transportes, pesquisa, educação, logística, compras, estoques, entre outras, podendo ser vendido em forma de pacotes ou, e principalmente, sob encomenda.

Considerando o conceito de segmento horizontal/vertical no mercado de softwares e o os tipos de software desenvolvidos por MPEs é possível observar que há um concentração no mercado vertical, uma vez que as principais áreas de atuação das MPEs são automação, ERP e administração, onde é necessária embutir o conhecimento das empresas nos softwares. Para Freire [FREIRE02] o baixo custo de desenvolvimento de programas para estas áreas e a menor complexidade relativa exigida para estes produtos, somados à fragmentação e crescimento constantes nessas áreas, podem dar uma idéia do por quê dessa concentração. Essas áreas proporcionam o aparecimento de segmentos de mercado específicos (automação de consultórios médicos, livrarias, farmácias, videolocadoras), abrindo oportunidades de atuação para as MPEs. Além disso, a própria estrutura que as MPEs possuem, faz com que estas desenvolvam produtos de baixa complexidade que necessitam de pouca mão de obra e tempo curto de projeto.

Nestes segmentos de mercado, os projetos se iniciam de maneira tímida, atendendo a algumas funcionalidades iniciais requisitadas pelo cliente, facilitando a entrada da MPE no mercado com pequenas equipes, baixo custo e um curto tempo de entrega da 1ª versão do produto. Depois são feitas constantes atualizações incrementais no produto de forma a atender a novas necessidades do cliente, e possibilitando amadurecer o produto e fornecê-lo a outras empresas do mesmo segmento [FREIRE02]

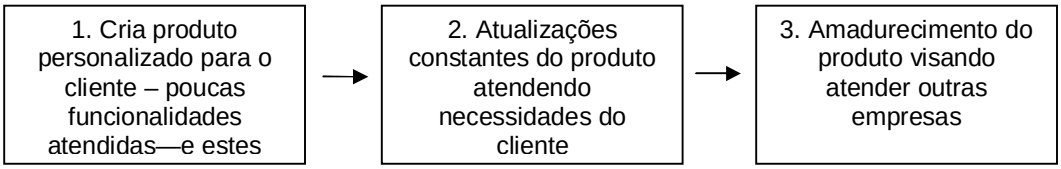

Figura 11 - Atuação de MPEs no mercado de Desenvolvimento de Software para empresas de pequeno porte

Em consulta aos profissionais do Laboratório de Qualidade e Pesquisa [LQPS06], algumas MPEs fazem projetos de desenvolvimento de software sob encomenda, algumas fazem pacotes, outras tem um produto padrão customizável, que é adaptado para um cliente específico em pequenos projetos. Outras MPEs possuem projetos de manutenção contínua ou desenvolvem software, porém vendem apenas o serviço de manutenção.

Tipicamente, MPEs por terem um número reduzido de funcionários, possuem equipes pequenas, onde cada integrante da equipe assume diversos papéis dentro do processo de desenvolvimento e administração da empresa, dividindo ora seu tempo em atividades técnicas, ora em atividades de administração ou atividades organizacionais.

MPEs também apresentam uma série de problemas de organização interna causado por excesso de informalidades de estrutura de organização e do fluxo de informações. Devido à falta de recursos, a empresa tem um enfoque em atividades externas, tais como terminar o produto o quanto antes, promover o produto em atividades de marketing e vendas, criar alianças estratégicas etc., não se dedicando com a atenção devida ao aperfeiçoamento do

processo de desenvolvimento, gerência e qualidade. São ainda muito susceptíveis a influências, sejam elas de investidores, clientes ou do próprio mercado. Desta forma, a empresa se mantém em constante processo de ajuste daquilo que ela faz e de como faz.

Em relação à gerência de riscos, foco deste trabalho, pouca atenção é dedicada a este tipo de atividade em MPEs [MCT05]: apenas 1,4% de micro empresas e 2,2% de pequenas empresas possuem atividades de gerência de risco. Esta falta de gerência de risco aumenta a chance de riscos realmente acontecerem, impactando negativamente nos objetivos do projeto e no desempenho da MPE. Muitos destes problemas poderiam ser evitados ou fortemente reduzidos se existisse um comprometimento em identificar e resolver os elementos de alto risco destes projetos, pois freqüentemente estes projetos são levados por uma onda de otimismo, deixando passar sinais de riscos que podem levar ao término prematuro do projeto [BOEHM91]. Além disto, as seguintes características das MPEs podem levá-las a não executarem a gerência de riscos [MARTENS01], [SEBRAE05], [ROVERE01] [ROUILLER01], [KASSE04], [COLEMAN98]:

- **Dificuldade em inserção no mercado –** As MPEs enfrentam dificuldades de inserção nos mercados que disputam, ambientes extremamente competitivos e globalizados; e para conquistá-los, precisam atender, simultaneamente, exigência de preços, prazos, qualidade e confiabilidade [MARTENS01]. Assim, as MPEs podem deixar de lado a gerência de riscos e demais processos, com o objetivo de gastar menos tempo e ter um custo menor, correndo o risco de o produto não ter qualidade e confiabilidade.
- **A falta de recursos financeiros das MPEs -** O uso de máquinas obsoletas é generalizado entre as MPEs devido às dificuldades que estas empresas encontram em obter crédito, ficando mais sensíveis aos ciclos econômicos, inibindo os esforços de atualização tecnológica [SEBRAE05]. Assim, as MPEs podem não conseguir simular os ambientes onde seus produtos estão instalados, com a finalidade de realizar testes de benchmarketing para mitigar riscos, ou mesmo alocar recursos para gerenciar riscos.
- **Ambiente familiar -** a baixa capacitação gerencial, que decorre do fato de que estas empresas são em sua maioria familiares [ROVERE01]. Assim, as MPEs podem se arriscar a não ter uma gerência capacitada em resolver riscos, ou até mesmo que encubra riscos em potenciais, por estarem relacionados a recursos de mão de obra da própria família.
- **Falta de capacitação gerencial -** Além disso, o tamanho reduzido das empresas faz com que seus proprietários/administradores tenham um horizonte de planejamento de curto prazo, ficando presos num círculo vicioso onde a resolução de problemas diários impede a definição de estratégias de longo prazo e de inovação [ROVERE01]. Assim, as MPEs não enxergam oportunidades à longo prazo, focando em ações de curto prazo, por exemplo, demissão de mão de obra ou compra de equipamentos de menor custo, porém com menor desempenho. Além disso, esta característica faz com que as MPEs não possuam capacidade de avaliação de riscos de forma pró-ativa.
- **Falta de maturidade para atuar com novas tecnologias -** A adoção de novas tecnologias da informação pode provocar mudanças no comportamento e na estrutura da MPE, no sistemas gerenciais, nas técnicas e no domínio de processos adotados pela empresa, causando grande impacto nas organizações, devido a situações novas situações a serem enfrentadas, que, muitas vezes, deixam os gerentes sem saber como lidar com elas [MARTENS01]. Assim como novas tecnologias, novos processos de gerência de projetos também não são bem vistos em MPEs, tal como a própria gerência de riscos, justamente por não estar no domínio dos gerentes, que normalmente se limitam a ser o “dono” do negócio, realizando tarefas de alocação de recursos ou relacionadas a pagamentos.

- **Multi-funcionalidade da mão de obra em MPEs** – A empresa não conta com pessoal habilitado com conhecimentos técnicos específicos na área de TI, o que dificulta ainda mais um melhor aproveitamento da tecnologia. Desta forma, o próprio empresário torna-se polivalente, passando a atender problemas de produção, de compras, de marketing de vendas e de recursos humanos [MARTENS01]. Essa característica faz com que o gerente de projetos (que pode ser o próprio empresário) possa não dispor de tempo suficiente para aplicar a gerência de riscos.
- **Precariedade na gerência de projetos -** os seguintes fatores agravam os problemas da gerência de projetos de software em MPEs [ROULLER01]: (1) Falta de formalização de procedimentos para gerência e controle de projetos; (2) Inexistência de um processo definido; (3) Recursos pessoais e financeiros limitados; (4) Falta e/ou pouca cultura em processos; (5) Pouco treinamento em engenharia de software; (6) Imaturidade metodológica; (7) Crescimento ocorrido por demanda; (8) Falta de experiência administrativa por parte dos gerentes e diretores; (9) Falta de definição das metas organizacionais. Todos estes fatores fazem com a execução da gerência de riscos seja mais complicada pela falta da cultura organizacional em procedimentos definidos, e a falta de planejamento pró-ativo, essencial para a gerência de riscos.
- **Precariedade na gerência de riscos -** A falta de preparo para os momentos de impasse demonstra que os gerentes das MPEs possuem dificuldades em gerenciar riscos, e possivelmente enxergar novas oportunidades. Kasse [KASSE04] lista os seguintes problemas na gerência de riscos por parte dos gerentes: (1) Tendência a gerenciar os riscos que eles vêem, e não todos os riscos ou os riscos críticos; (2) Tendência a gerenciar os riscos onde eles têm experiência; (3) Tendência a realmente gerenciar para custo e prazo – os sintomas; (4) São normalmente recompensados por suas habilidades em gerência em situação de crise.
- **Tempo de entrega ao mercado -** Segundo Kulpa & Johnson [KULPA03] o primeiro dirigenciador do negócio para MPEs é tempo de resposta ao mercado. Decisões precisam ser tomadas de forma rápida e dentro do prazo. Enquanto que o CMMI-SE/SW promove a qualidade com o alongamento do processo usado para desenvolver e entregar sistemas, as MPEs precisam entregar seus sistemas no tempo estimado do mercado, preferindo a velocidade de entrega de qualidade ou funcionalidades do sistema, deixando de lado a gerência de riscos.
- **Ausência de padrão no ciclo de vida dos projetos -** Segundo Coleman & Verbruggen [COLEMAN98] as pequenas empresas possuem os seguintes problemas quanto a ausência de padrões durante o ciclo de vida dos projetos: (1) Ausência de um documento padrão de requisitos; (2) Ausência de um documento padrão para o projeto; (3) Ausência de padrões para programação; (4) Ausência de planos de programadores para testes de unidade; (5) Ausência de testes independente dos módulos; (6) Ausência de documentação formal de erros; (7) Ausência de documentação de solicitações de correções de erro e alterações. Estes fatores dificultam a gerência de riscos em MPEs, uma vez que encontrar riscos na documentação gerada, conforme as melhores práticas relatadas no CMMI-SE/SW, se torna um trabalho não repetitivo ao longo da vida da empresa já que os projetos não possuem padrão.
- **Estimativas irreais -** Os gerentes de projetos em MPEs ao estimar, costumam basear-se em estimativas passadas, mesmo sabendo que elas podem estar incorretas, e também há gerentes que se recusam a estimar somente por julgarem perda de tempo, uma vez que correm o risco de obterem resultados incorretos e, portanto, acharem que estão desperdiçando tempo [ROULLIER01]. Prazos irreais fazem com que processos como a gerência de risco, sejam descartados em função da obtenção do produto no

prazo estipulado (ou com pouco atraso), independente dos riscos à volta do projeto, resultando em uma baixa qualidade do produto final.

No próximo capítulo é apresentado o guia de implantação da gerência de riscos em MPEs. Este guia é contextualizado com base nas características apresentadas das MPEs, de forma a facilitar a implantação da gerência de riscos em MPEs.

4 Guia de Implantação da Gerência de Riscos em MPEs

Alinhado aos objetivos específicos e práticas específicas da área de processo de gerência de riscos, este guia descreve a implantação da área de processo de gerência de riscos especificamente voltado ao contexto de em Micro e Pequenas Empresas (MPEs).

Desta forma o presente guia fornece técnicas, diretrizes, exemplos e *templates* de produtos de trabalhos para a implementação de um processo de gerência de riscos em conformidade com as práticas específicas da áreas de processo (PA) de Gerência de Riscos do modelo CMMI-SE/SW de forma adaptada para MPEs.

4.1 Conceitos fundamentais

A gerência de riscos do projeto inclui os processos que tratam da realização de identificação, análise, respostas, monitoramento e controle e planejamento da gerência de riscos em um projeto; a maioria desses processos é atualizada durante todo o projeto [PMI04].

O objetivo da gerência de risco é identificar os problemas em potencial antes que eles ocorram, de forma que as atividades de tratamento de riscos possam ser planejadas e invocadas, conforme necessário, durante o ciclo de vida do projeto, para mitigar os impactos adversos no atendimento dos objetivos do projeto [SEI01].

Risco é a possibilidade de perigo, incerto, mas previsível, que ameaça de dano à pessoa ou a coisa [MICHAELIS02]. No contexto de projetos de softwares, **riscos** são eventos ou ocorrências que impedem um projeto de alcançar seus objetivos de custo, cronograma e desempenho [ENGERT99].

A gerência de risco no contexto do CMMI-SE/SW é considerada uma atividade contínua, que deve ser executada durante todo o ciclo de vida de um projeto. Tipicamente a gerência de riscos é composta das seguintes atividades [PMI04]:

- Planejamento da gerência de riscos
- Identificação dos riscos
- Análise de riscos
- Análise qualitativa e quantitativa de riscos
- Planejamento de resposta a riscos
- Monitoramento e controle de riscos.

Desta forma, todas as atividades apresentadas neste guia formam uma única iteração, mas que devem ser repetidas durante todo o ciclo de vida do projeto, e seus resultados devem ser armazenados em um Repositório de Conhecimento da Organização (RCO) para consulta nas iterações seguintes ou mesmo para consulta por outros projetos (vide Figura 12). O RCO pode ser elaborado, por exemplo, a partir de registros e documentos de projetos, todas as informações e a documentação relativas ao encerramento do projeto, informações sobre os resultados de decisões a respeito da seleção de projetos anteriores e informações sobre o desempenho de projetos anteriores e informações de esforço aplicado para a gerência de riscos.

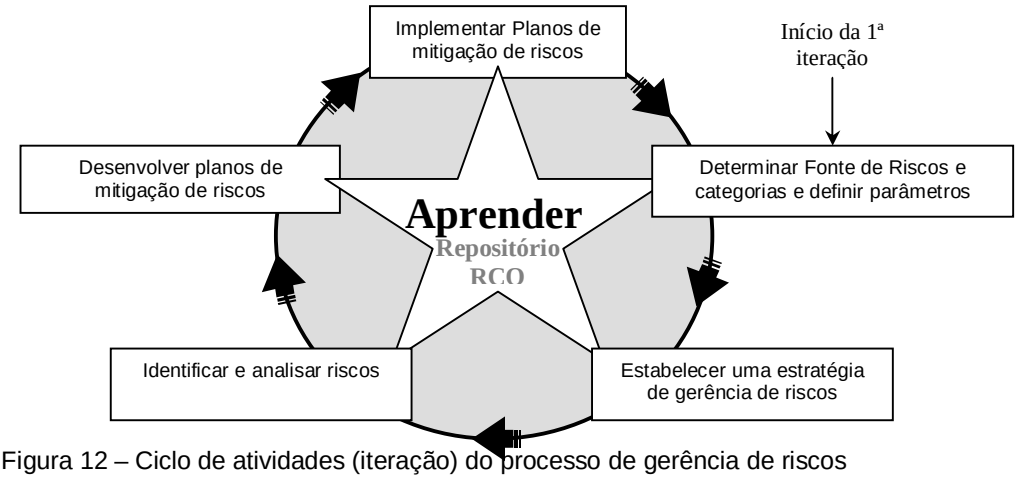

Figura 12 – Ciclo de atividades (iteração) do processo de gerência de riscos

A seguir, são apresentados todos os objetivos específicos e práticas específicas do CMMI-SE/SW da área de gerência de riscos. Para cada uma das práticas, o guia descreve além de técnicas e ferramentas alternativas que podem ser utilizadas para implementar estas práticas de forma adaptada ao contexto de uma MPE.

SG 1 – Preparar para a gerência de risco

A preparação para a gerência de risco é conduzida.

SP 1.1 – Determinar as fontes de riscos e categorias

Objetivo

O objetivo desta SP é gerar um repositório de fontes e categorias de risco [SEI01]:

- **Fontes de riscos** – são itens ou atividades com potencial para um impacto nos objetivos do projeto. Fontes de riscos podem ser internas ou externas ao projeto. Exemplos são: Requisitos incertos, esforços sem precedentes, *design* impossível de ser implementado, equipe com não capacitada etc.
- **Categorias de riscos –** fornecem um mecanismo para a coleta e organização dos riscos. Categorias podem ser baseadas nas fases do modelo de ciclo de vida do projeto (por exemplo, riscos de requisitos, de design, de produção, de teste ou entrega), nos tipos de processo (processo de desenvolvimento ou processo e métodos de gerência), produtos utilizados (ferramentas de desenvolvimento), ou riscos do próprio projeto (riscos de contrato, orçamento, cronograma, desempenho).

A Figura 13 mostra o relacionamento entre as fontes e as categorias de riscos. As fontes estão dentro das categorias de riscos, e dentro de uma mesma categoria podem ter fontes internas e externas de riscos, e a Tabela 3 apresenta exemplos de categorias e fontes de riscos.

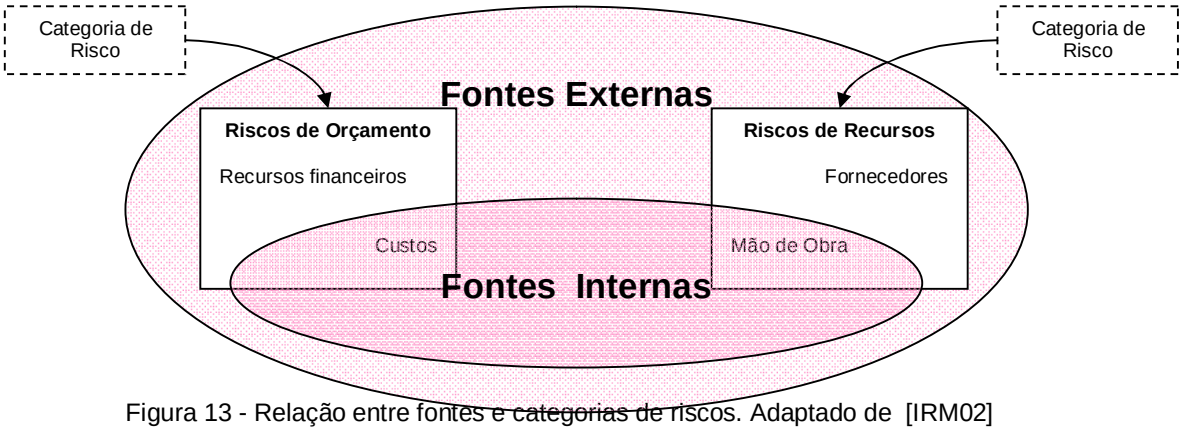

Figura 13 - Relação entre fontes e categorias de riscos. Adaptado de [IRM02]

Tabela 3 - Categorias de Riscos de Software [CARR93]

A. Engenharia de Produto	**B. Ambiente de Desenvolvimento**	**C. Definições do Programa**
1. Requisitos a) Estabilidade b) Completos c) Clareza d) Validade e) Implementável f) Histórico g) Grau de Dificuldade 2. Design a) Funcionalidade b) Dificuldade c) Interfaces d) Desempenho e) Testável f) Restrições de Hardware g) Non-Developmental Software[1] 3. Codificação e Teste de Unidade a) Implementável b) Testes c) Codificação / Implementação 4. Integração e Teste a) Ambiente b) Produto c) Sistema 5. Especialidades da Engenharia a) Manutenibilidade b) Disponibilidade c) Proteção contra falhas d) Segurança de Acesso e) Fatores humanos f) Especificações	1. Processo de Desenvolvimento a) Formalidade b) Adequabilidade c) Controle de Processo d) Experiência e) Controle de Produto 2. Ferramenta de Desenvolvimento a) Capacidade b) Adequabilidade c) Usabilidade d) Experiência e) Disponibilidade f) Suporte à Ferramenta g) Entrega 3. Processo de Gerenciamento a) Planejamento b) Organização do Projeto c) Experiência em Gerência d) Interfaces do Projeto 4. Métodos de Gerenciamento a) Monitoração b) Gerenciamento de Pessoal c) Garantia de Qualidade d) Gerência de Configuração 5. Ambiente de Trabalho a) Atitude de Qualidade b) Cooperação c) Comunicação d) Estado de Espírito	1. Recursos a) Programação b) Equipe c) Orçamento d) Facilidades 2. Contratos e) Tipo de Contrato f) Restrições g) Dependências 3. Interfaces de Programas h) Cliente i) Parceiros j) Fornecedores k) Contratos Principais l) Gerência da Organização m) Fornecedores n) Política

[1] Non-Developmental Software também é conhecido como softwares Drill-and-Practice, que é um termo que advém de uma teoria de aprendizado conhecida como “comportamental”. O foco desta teoria está na repetição de novas habilidades até que essa habilidade seja incorporada ao indivíduo. Feedback é essencial, mas oferecido de forma bem simples. Se o usuário que está aprendendo responder corretamente, e o feedback será “ok” ou uma luz verde, caso o usuário responder errado, não será dado nenhum feedback, o usuário simplesmente tem que tentar outra alternativa até o acerto.

A organização poderá determinar as fontes e categorias de risco durante a etapa de planejamento do projeto. O planejamento do projeto visa definir e refinar os objetivos do projeto, e planeja a ação necessária para alcançar os objetivos e o escopo para os quais o projeto foi realizado. Mais informações sobre o planejamento de projetos de software em micro e pequenas empresas alinhado ao CMMI-SE/SW podem ser encontrado, por exemplo, em [KUNTZE06].

As informações do plano do projeto serão fundamentais para a identificação de fontes e categorias de riscos que envolvem o projeto. Além da consulta ao plano de projeto, a organização deverá se basear nas próprias experiências anteriores, que podem ser consultadas no Repositório de Conhecimentos da Organização (RCO), para obter mais informações sobre fontes e categorias de riscos utilizadas previamente por outros projetos na organização.

Este repositório é o local onde a organização armazena as taxonomias de riscos, planos de riscos (SP1.3), registro de riscos (SP2.1) e outros artefatos produzidos pela atividade de gerência de riscos dos projetos já executados ou em execução.

Como ponto de partida para identificação de fontes e categorias de riscos de um projeto, a organização pode usar uma taxonomia de riscos. **Taxonomias de riscos** sintetizam experiências passadas na execução do processo de gerência de riscos, com fontes e categorias de riscos já caracterizadas. Estas taxonomias categorizam riscos ou em forma de questionários, com perguntas sobre o projeto (recursos humanos e materiais, fornecedores, características da organização, financeiros etc) ou em forma de *checklist* de riscos**.** Várias taxonomias genéricas estão disponíveis para consulta pública. Algumas destas taxonomias são apresentadas em anexo incluindo [DIR06], [CARR93], [JONES04], [BOEHM91], [THOMSETT02], [LEOPOLDINO04] e [MACHADO02]. Estas taxonomias são genéricas para qualquer contexto, e podem ser usadas por qualquer projeto de software. Além destas taxonomias genéricas, existem taxonomias voltadas para tipos específicos de projeto, como, por exemplo, a taxonomia definida por [OLIVEIRA03], apresentada no anexo G, que classifica áreas de risco comuns em projetos de manutenção de software, e o anexo H, com uma taxonomia que identifica riscos na modernização de sistemas legados [SANTOS04]. É importante ressaltar que estes taxonomias genéricas foram desenvolvidas com base nas experiências de várias organizações na prática, mas que, mesmo assim, precisam ser adaptadas ao contexto de uma organização específica para representar uma boa base para a identificação de riscos, de forma totalmente adaptada ao contexto e as características especificas de uma organização, seus produtos, modelo de negócio e processos. Desta forma, estas taxonomias podem ser utilizadas como ponto de partida, sendo revisadas cuidadosamente e, com o passar do tempo, baseadas em dados objetivos coletados na própria organização, acrescentando novas fontes de riscos ou eliminando fontes não aplicáveis.

Entretanto, é importante que a organização continuamente customize as próprias taxonomias considerando suas características especificas, com base em dados históricos sobre riscos observados em projetos passados na própria organização. Revisar a taxonomia tem o objetivo de selecionar os riscos que são relevantes ao projeto especifico. Desta forma, pode ser desenvolvido pela organização, uma taxonomia de riscos para cada tipo de projeto, visando facilitar a identificação de riscos específicos de um projeto, ou uma taxonomia genérica da organização, aplicável a todos os projetos.

Atividades

Por meio das taxonomias de riscos é possível identificar quais fontes e categorias de riscos pertencem. O primeiro passo da organização é selecionar todos os *stakeholders* que irão

participar das atividades de identificação de riscos (SP2.1), que pode incluir o gerente de projetos, membros da equipe do projeto, equipe de gerenciamento de riscos (se designada), especialistas no assunto de fora da equipe do projeto, clientes, usuários finais, outros gerentes de projetos, partes interessadas e especialistas em gerenciamento de riscos [PMI04].

Com os *stakeholders* selecionados, é realizada uma reunião [PMI04] com o objetivo de identificar as fontes e categorias de riscos pertinentes ao projeto e à organização. Nesta reunião pode ser realizada uma revisão na taxonomia da organização ou em taxonomias disponíveis para consulta pública, de forma a obter mais informações sobre novas categorias e fontes de riscos aplicáveis ao projeto ou à organização. Além de também descobrir categorias e fontes de riscos que deixaram de ser aplicáveis ao projeto ou à organização. A Figura 14 mostra um exemplo de apresentação da taxonomia de riscos para o projeto.

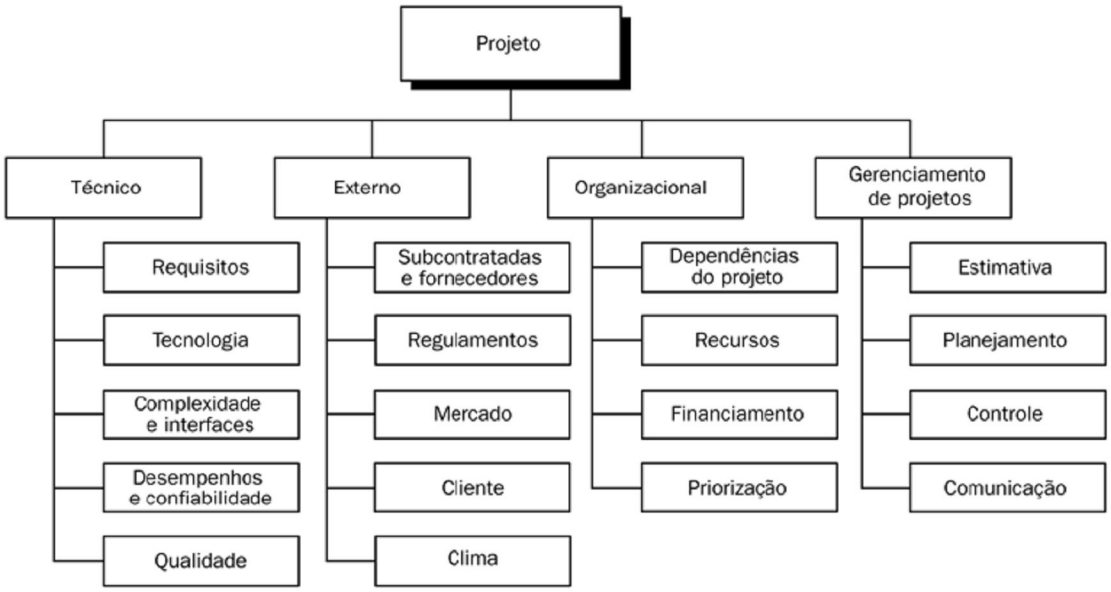

Figura 14 - Exemplo de apresentação da taxonomia de riscos para o projeto [PMI04]

Algumas taxonomias (por exemplo, [THOMSETT02], [DIR06]), além de categorias e fontes de riscos, apresentam indicadores ou indícios de riscos que ajudam a identificar se a fonte de risco ou a categoria é ou não é pertinente ao projeto, além de também indicar o status geral do risco no contexto do projeto (ver SP2.2). A Figura 15 mostra um exemplo de uma taxonomia de riscos onde são apresentados indícios das fontes de risco. As fontes de riscos encontradas são consolidadas em categorias existentes, ou novas categorias.

A definição das fontes e categorias de riscos a serem usadas na taxonomia de riscos deve ser feita na 1ª iteração. Porém, a revisão e atualização da taxonomia deve ser feita em todas as iterações, com o objetivo de adequar melhor a taxonomia ao contexto da organização.

		Indícios			Classificação			
#	Fontes de Risco	Baixo	Médio	Alto	Baixo	Médio	Alto	Não Aplicável
Missão e Objetivo								
1	Projeto é adequado a organização cliente	Diretamente suporta as missões e objetivos da organização cliente	Indiretamente impacta nos objetivos ou missão da organização cliente	Não suporta ou não está relacionado a organização cliente				
2	Projeto é adequado a organização patrocinadora	Diretamente suporta missões e objetivos da organização patrocinadora	Indiretamente impacta nos objetivos ou missão da organização patrocinadora	Não suporta ou não está relacionado a organização patrocinadora				

Figura 15 - Taxonomia de Riscos [THOMSETT02]

Para manter a taxonomia de riscos atualizada, a organização deve atualizar a taxonomia de riscos sempre que:

- Novas fontes de riscos, que não forem específicas do projeto, forem descobertas;
- Fontes de riscos deixam de serem aplicáveis a organização;
- Fontes de riscos mudam suas características.

A Figura 16 mostra um exemplo de *template* de taxonomia de risco que pode ser usado pela organização.

Taxonomia de riscos da organização					
Categoria	**Fonte de Risco**	**Justificativa**	**Técnicas de tratamento de riscos**	**Limites para monitoração**	**Procedimento de medição**
<< categoria do risco>>	<< fonte de risco dentro da categoria>>	<< justificativa para ter incluído o risco dentro desta categoria >>	<< técnicas que podem ser aplicadas para tratar riscos desta fonte de riscos >>	<< limites que podem ser monitorados para verificar se o risco está próximo, ou aconteceu >>	<< procedimentos de coletar dados para as métricas que podem ser usadas para verificar se os limites foram atingidos >>

Figura 16 – Exemplo de Template de taxonomia de riscos

SP 1.2 – Definir parâmetros de riscos

Objetivo

O objetivo desta SP é definir os parâmetros utilizados para analisar e categorizar os riscos (vide SP 2.2), e os parâmetros utilizados para controlar o esforço da gerência de riscos (vide SP 3.1) [SEI01]. Estes parâmetros são usados para comparar os riscos. Os parâmetros para a avaliação, categorização e priorização de riscos incluem:

- **Probabilidade de Riscos**: Chance de um evento de risco acontecer [COOPER04]. Por exemplo, a probabilidade pode ser medida em uma escala numérica de 0 a 1, ou em percentuais (0%, 10%, 70% etc.), ou por meio de um escala ordinal, por exemplo: remota, improvável, provável, altamente provável, quase certa.
- **Impacto dos Riscos**: Conseqüência de um evento de risco ao influenciar nos objetivos do projeto [COOPER04]. O impacto pode ser medido da mesma forma que a probabilidade, em uma escala numérica de 0 a 1, em percentuais (0%, 10%, 70% etc), ou por meio de uma escala ordinal, por exemplo: Baixo, Médio e Alto ou Crítico, Sério, Menor, Desprezível.
- **Limites para disparar atividades de gerência de riscos**: Indicação de eventos que, quando aconteçam, indiquem o momento de iniciar uma atividade de gerência de riscos [SEI01]. Por exemplo, quando o custo de um projeto exceder 10% do custo determinado no orçamento, disparar uma ação de contenção de despesas menos significativas para o projeto, como por exemplo, material de escritório.

Geralmente, a organização deve revisar com cuidado a escala de impacto e probabilidade que deseja utilizar para cada projeto, para garantir que a escala reflita os objetivos da organização [COOPER04].

Atividades

A organização é responsável por definir critérios para a avaliação e quantificação da probabilidade e dos impactos dos riscos. Desta forma, deve ser selecionado uma forma de representar os parâmetros de probabilidade e impacto. Pode ser muito difícil para as empresas definirem matematicamente esses parâmetros, pois não possuem experiência suficiente e registro numérico do histórico destas informações, alem de criar a impressão que sabem estimar estes fatores com um maior grau de precisão do que realmente podem [KASSE04]. Desta forma, pode ser mais adequado usar uma escala ordinal. Isto também vale tipicamente para MPEs que em geral se caracterizam por falta de dados históricos sistematicamente coletados e disponíveis para uma classificação mais precisa. As categorias usadas dependem de cada contexto. A Tabela 4 e a Tabela 5 apresentam exemplos de escala ordinais relativa para indicar os riscos.

Além do impacto e da probabilidade, é necessário identificar a forma de priorização dos riscos, que tem como objetivo identificar a importância de cada um dos riscos levantados no projeto, identificando assim aqueles que necessitam de mais atenção da organização, produzindo uma lista ordenada dos riscos identificados [BOEHM91]. A priorização dos riscos pode ser feita através da composição entre a probabilidade e o impacto (**Fator de Exposição**), por meio de uma matriz de relacionamento entre probabilidade e impacto (Figura 17). Com o resultado desta relação, obtém o fator de exposição, que define o nível

de exposição do projeto ao risco, possibilitando a organização de priorizar os riscos com base no fator de exposição encontrado.

Tabela 4 – Exemplo de Critérios de probabilidade de riscos baseada em uma escala ordinal

	Nível	Descrição
A	Quase Certo	Um evento simular aconteceu na organização várias vezes durante o ano na mesma atividade, locação ou operação
B	Alto	Um evento similar aconteceu na organização várias vezes durante o ano na organização
C	Possível	Um evento similar aconteceu alguma vez na organização
D	Baixo	Um evento similar aconteceu alguma vez antes em uma organização simular
E	Raro	Um evento similar aconteceu alguma vez em outras empresas, porém nunca nesta organização

Tabela 5 – Exemplo de critérios de impacto de riscos baseados em uma escala ordinal

	Nível	Descrição
A	Catastrófico	Evento extremo, podendo gerar grandes custos ou atrasos, ou prejudicar a reputação da organização
B	Maior	Evento crítico, podendo gerar custos maiores custos ou atrasos, ou produtos não apropriados
C	Moderado	Grande impacto, mas pode ser gerenciado com algum esforço usando procedimentos padrões
D	Menor	Impacto minimizável com procedimentos de gerência padrão
E	Insignificante	Impacto pode ser simplesmente ignorado

O fator de exposição pode ser representando por uma escala ordinal de termos relativos, tal como a probabilidade e impacto. Com a definição do grau de exposição, os riscos, com maior grau de exposição terão prioridade de atenção sobre os demais riscos.

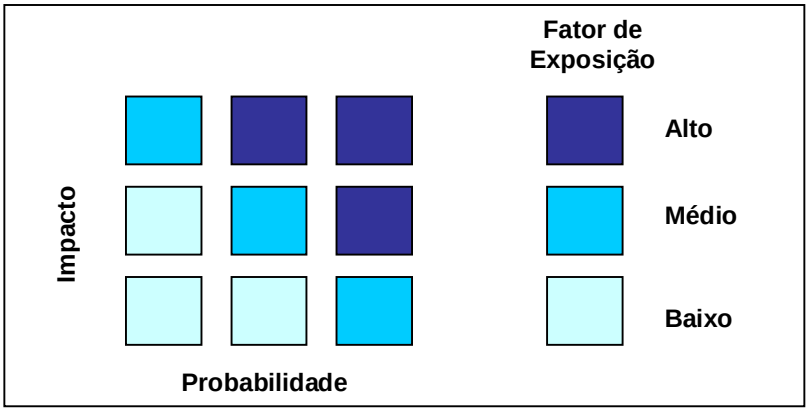

Figura 17 – Matriz de Probabilidade x Impacto: Cálculo do Fator de Exposição

É importante, caso for possível, que a organização use uma mesma escala ordinal de termos relativos em todos os projetos executados pela organização, de forma a facilitar a consulta ao RCO por outros projetos.

A definição de parâmetros de probabilidade e impacto deve ser realizada na 1ª iteração da gerência de projeto, e revisada nas demais iterações do ciclo do projeto.

Além dos parâmetros de probabilidade e impacto, a organização, para cada fonte de risco aplicável ao projeto deve estabelecer limites para determinar a aceitabilidade do risco, a priorização, e gatilhos para disparar uma ação de gerência [SEI01]. Limites são indicadores de que o risco está próximo ou que aconteceu (caso os limites sejam ultrapassados). As ações podem ser elaboradas com base na experiência da organização, por meio da consulta ao RCO ou reuniões de *brainstorming*, ou consultando taxonomias que apresentem esta informação. Exemplos de limites são: desempenho abaixo de 0.80, processamento superior a 120%, indicador de faltas de funcionários de 15%. A Tabela 6 mostra outros indicadores de risco que podem ser usados na definição de limites.

Para mais informações sobre a definição e uso de medidas como base para acompanhar os limites, deve ser feito um programa de medição, usando, por exemplo, o método GQM (*Goal-Question-Metric*) [BASILI94] ou PSM (Practical Software and System Software Measurement) [PSM06]. Estes métodos são descritos no contexto de MPEs no Guia para Medição e Análise de Projetos de Software em Micro e Pequenas Empresas Alinhado ao CMMI-SE/SW [RUBIK06].

Tabela 6 - Indicadores de risco (Adaptado de [SOMMERVILLE03])

Tipo do Risco	Indicadores possíveis
Tecnologia	Dias de atraso na entrega de hardware ou software de suporte Problemas de tecnologia reportados
Pessoas	Moral baixa da equipe Baixo relacionamento entre os integrantes da equipe Disponibilidade de trabalho
Organizacional	Problemas organizacionais Falta de ação da gerência sênior
Ferramentas	A equipe não quer usar as ferramentas Reclamações sobre as ferramentas Pedidos de computadores melhores
Requisitos	Reclamações do cliente Muitos pedidos de mudança de requisitos
Estimativas	Não conseguir cumprir o prazo estabelecido Não conseguir eliminar os defeitos encontrados

Segundo [SEI01], a definição de limites pode ser refinada mais tarde, para cada risco identificado, para estabelecer pontos em que o monitoramento de riscos mais agressivo é empregado ou para sinalizar a implementação de planos de mitigação de riscos. Este procedimento pode ser realizado pela organização durante a identificação de riscos, na SP2.1. Faz parte da definição de limites identificar as fontes de riscos pertinentes ao projeto, para evitar que sejam monitoradas fontes de riscos muito improváveis, e assim sejam realizadas atividades de gerência de riscos para categorias que não estão presentes no projeto. Esta análise pode ser suportada pelo uso de um *template*, como, por exemplo, o apresentado no Anexo A, que mostra uma taxonomia de riscos, em forma de lista de fontes de riscos, com a opção de identificar quais riscos são aplicáveis ou não ao projeto. E para documentação dos limites, podem ser usados os próprios formulários de registro de risco, que serão abordados na SP2.1.

SP 1.3 – Estabelecer uma Estratégia de Gerência de Riscos

Objetivo

O objetivo desta SP é estabelecer e manter a estratégia a ser utilizada para a gerência de riscos. A estratégia de gerência de risco deve incluir os seguintes itens [SEI01] [PMI04]:

- Escopo do esforço da gerência de riscos: Determinar o escopo da gerência de risco que será utilizado pelo projeto, de acordo com as políticas de gerência de risco organizacional. Neste escopo estão incluídos recursos de hardware, software e pessoal necessário à realização da gerência de risco, baseando no escopo do projeto.
- Métodos e ferramentas a serem utilizadas para a identificação, análise, mitigação, monitoramento e comunicação de riscos. Estes métodos são apresentados ao longo deste guia, tais como taxonomia de riscos, cálculo do fator de exposição, entrevistas, *brainstorming*, *delphi*, estratégias de tratamento de riscos, emissão de relatórios de risco etc.
- Fontes de riscos e categorias específicas do projeto, como mostrado na SP1.1
- Como estes riscos são organizados (por exemplo, por meio de uma taxonomia), categorizados, comparados e consolidados (por exemplo, riscos menores que fazem parte de outros riscos podem ser incluídos nos riscos maiores);
- Parâmetros, incluindo a probabilidade, impacto, fator de exposição e limites;
- Técnicas de mitigação de riscos a serem utilizadas. Estas técnicas são formas de evitar ou resolver a fonte do risco [BOEHM91]. São exemplo destas técnicas: prototipação, simulação, *designs* alternativos ou desenvolvimento incremental. O Anexo C apresenta a lista dos 10 maiores riscos elaborada por [BOHEM91], e com as respectivas técnicas de mitigação, usadas por diversos projetos, para cada um dos 10 riscos. A Figura 18 mostra parte desta lista de riscos;
- Definição de procedimentos de medição de riscos para monitorar o status dos riscos. Estas medidas são formas de verificar a evolução do risco (como mostrado na identificação de limites na SP1.2);
- Intervalos de tempo para monitoramento e reavaliação dos riscos.

Item de risco	Técnica de Gerência de Risco
Mão de obra abaixo do esperado	Equipe com talento e qualificado para o trabalho, desenvolvimento do time, treinamento e acordos pessoais
Cronograma e orçamento irreais	Estimativa de orçamento e cronograma detallhadas, projetos com base no custo, desenvolvimento incremental, re-utilização de software e limpeza dos requisitos
Desenvolvimento de funções ou propriedades erradas;	Análise da organização, análise da missão, formulação do conceito de operação, pesquisa com o usuário, participação do usuário, prototipação, manual para os usuários, análise de desempenho, analise do fator de qualidade
Desenvolvimento de uma interface com o usuário errada	Protótipos, cenários, análise de tarefas, participação do usuário
Projetar funcionalidades sem requisitos incluídos por analistas, ou por preciosismo (*Gold-Plating*);	Limpeza dos requisitos, prototipação, análise de custo benefício, projetar com base no custo

Figura 18 - Riscos e técnicas de gerência de riscos [BOEHM91] (parcial)

Atividades

O primeiro passo para estabelecer uma estratégia de gerência de riscos é a organização determinar o escopo da gerência de risco, identificando quais são os recursos de hardware, software e pessoas para o projeto. Este passo busca evitar que sejam gastos recursos excessivos com a gerência de riscos, com base no escopo do projeto e na política da organização. Para cada uma das atividades da gerência de riscos deve ser identificado um grupo de pessoas responsáveis por cada etapa das atividades da gerência de risco, recursos de hardware de softwares necessários.

Com base nos recursos definidos no escopo da gerência de risco, a organização deve identificar:

- Métodos e ferramentas a serem utilizadas para a identificação, análise, mitigação, monitoração e comunicação;
- Fontes de riscos, que podem ser informados no registro de riscos (SP2.1);
- Organização dos Riscos;
- Parâmetros utilizados para utilizados para definir o nível de probabilidade, impacto e limite para os riscos (apresentados na SP1.2);
- Técnicas que serão utilizadas para mitigação de riscos;
- Procedimentos de medição que serão analisadas para monitoração de riscos. Estes procedimento podem ser atualizados na própria taxonomia de riscos da organização, para facilitar a consulta por outros projetos;
- Intervalo de tempo para a monitoração e reavaliação de riscos.

Desta forma, a organização que deseja identificar poucos recursos de software, hardware e pessoas, poderá adequar as atividades de risco com base nestes recursos, escolhendo:

- Métodos e ferramentas que demandem menor esforço;
- Parâmetros de probabilidade, impacto e limites mais simples;
- Técnicas de mitigação de riscos que não exigem um alto custo de hardware, software ou pessoal;
- Medidas para monitoração de riscos menos precisas, porém funcionais;
- Intervalo de tempo maior para a monitoração e reavaliação de riscos.

Com isto, a organização vai ter uma gerência de riscos menos precisa, porém adequada à política da organização e ao projeto.

Para manter a estratégia de gerência de risco acessível para consulta, a organização deve ter um documento que consolide todas as informações pertinentes a estratégia de gerência de riscos adotada. O Anexo J apresenta o *template "Estratégia de Gerência de Riscos"* para a documentação da estratégia de gerência de riscos do projeto.

A organização pode utilizar template apresentado na Figura 19 para gerar *a "Estratégia de Gerência de Riscos"*, baseando-se nas informações do RCO e do plano do projeto. Este documento pode ser armazenado no RCO, para consulta por outros projetos.

As fontes de riscos pertinentes ao projeto podem ser documentadas na própria taxonomia usada pelo projeto, e as medidas podem documentadas no próprio registro de riscos (como

mostrado na SP2.1). Porém, é importante indicar qual a taxonomia e o documento de registro de riscos que será usado pelo projeto na estratégia de gerência de riscos.

ESTRATÉGIA DA GERÊNCIA DE RISCOS

1 Escopo da Gerência da Risco

<<Determinar o escopo da gerência de risco que será utilizado pelo projeto, de acordo com as políticas de gerência de risco organizacional. Nesta atividade serão definidos recursos de hardware, software e pessoal necessário à realização da gerência de risco, baseando no escopo do projeto.>>

2 Tempo de reavaliação e monitoração de riscos

<<Intervalo de tempo para monitoramento e reavaliação dos riscos>>

3 Métodos e ferramentas

<<Métodos e ferramentas a serem utilizadas para a identificação, análise, mitigação, monitoramento e comunicação de riscos. Estes métodos são apresentados ao longo deste guia, tais como taxonomia de riscos, cálculo do fator de exposição, entrevistas, brainstorming, delphi, estratégias de tratamento de riscos, emissão de relatórios de risco etc.>>

4 Organização dos riscos

<<Como estes riscos são organizados (por exemplo, por meio de uma taxonomia), categorizados, comparados e consolidados (por exemplo, riscos menores que fazem parte de outros riscos podem ser incluídos nos riscos maiores) >>

5 Parâmetros

<<Parâmetros, incluindo a probabilidade, impacto e limites>>

Figura 19 – Exemplo de *template* para a estratégia de gerência de riscos

SG 2 – Preparar para a gerência de risco

Os riscos são identificados e analisados para determinar sua importância relativa

SP 2.1 – Identificar Riscos

Objetivo

O objetivo desta SP é identificar e documentar os riscos [SEI01]. A identificação de potenciais questões, perigos, ameaças e vulnerabilidades, com base na taxonomia que a organização definiu na estratégia de gerência de risco, que poderiam afetar negativamente os esforços ou plano de trabalho é a base para a gerência de risco.

Os riscos devem ser identificados e descritos de uma forma fácil de entender, antes que possam ser analisados e gerenciados de forma apropriada. Os riscos são documentados em uma declaração concisa que inclui o contexto, as condições e as conseqüências da ocorrência do risco.

Atividades

O primeiro passo, segundo o CMMI-SE/SW [SEI01], é identificar os riscos associados a custo, cronograma e desempenho em todas as fases apropriadas do ciclo de vida do projeto para verificar a extensão do seu impacto nos objetivos do projeto. Porém a organização pode ter outras categorias de riscos identificadas na taxonomia que sejam prioritários. Com base nestas categorias, a organização deve buscar informações que podem ser usadas para identificar riscos. São exemplos de fontes de informação [PMI04] [SEI01]:

- **Fatores ambientes da organização** - As informações publicadas, inclusive bancos de dados comerciais, estudos acadêmicos, *benchmarking* ou outros estudos do setor podem também ser úteis para a identificação de riscos;
- **Histórico de riscos em outros projetos** - As informações sobre projetos anteriores podem estar disponíveis em arquivos de projetos anteriores, inclusive dados reais e lições aprendidas. Este histórico pode ser disponibilizado no RCO da organização;
- **Declarações do escopo do projeto** - A incerteza nas premissas do projeto deve ser avaliada como causa potencial de riscos do projeto;
- **Plano de Gerência de Riscos** - as atribuições de funções e responsabilidades, provisão para atividades de gerência de riscos no orçamento e no cronograma e categorias de risco podem ser fontes de riscos;
- **Plano de Gerência do Projeto -** As saídas dos processos de outras áreas de conhecimento devem ser revisadas para identificar possíveis riscos em todo o projeto;
- **WBS – *Work Breakdown Structure* do projeto –** Cada elemento da estrutura de decomposição do trabalho (WBS) deve ser revisado para descobrir riscos;
- **Especialistas no assunto –** Especialistas nos assuntos relacionados ao projeto;
- **Especificações de design e requisitos de acordos -** Examinar especificações de design e requisitos

Para coletar informações nestas fontes, podem ser usadas as seguintes técnicas [PMI04] [MACHADO02]:

- **Revisão da documentação -** Pode ser realizada uma revisão estruturada da documentação do projeto, incluindo planos, premissas, arquivos de projetos anteriores, taxonomias e outras informações. A qualidade dos planos e também a consistência entre esses planos e com as premissas e requisitos do projeto podem ser indicadores de risco do projeto;
- **Brainstorming -** A meta do *brainstorming* é obter uma lista abrangente de riscos do projeto. A equipe do projeto normalmente realiza o *brainstorming*, freqüentemente com um conjunto multidisciplinar de especialistas que não fazem parte da equipe. Idéias sobre o risco do projeto são geradas sob a liderança de um facilitador, que pode ser o gerente do projeto ou o gerente de riscos, ao depender do porte. A taxonomia de riscos, definida pela organização, pode ser usada como uma referência. Em seguida, os riscos são identificados e categorizados por tipo de risco e suas definições são refinadas;
- **Técnica Delphi -** A técnica Delphi é um meio de alcançar um consenso entre especialistas. Nesta técnica, os especialistas em riscos de projetos participam anonimamente. Um facilitador usa um questionário para solicitar idéias sobre os riscos importantes do projeto. As respostas são resumidas e então redistribuídas para os especialistas para comentários adicionais. O consenso pode ser alcançado após

algumas rodadas desse processo. A técnica Delphi ajuda a reduzir a parcialidade nos dados e evita que alguém possa indevidamente influenciar o resultado;

- **Entrevistas -** As entrevistas com participantes experientes do projeto, partes interessadas no projeto e especialistas no assunto podem identificar os riscos. As entrevistas são uma das principais fontes de coleta de dados sobre identificação de riscos;
- **Taxonomias de risco –** A organização pode se basear na taxonomia de riscos para coletar informações necessárias para a identificação de riscos;
- **Análise das premissas (cenários) -** Todos os projetos são concebidos e desenvolvidos com base em um conjunto de hipóteses, cenários ou premissas. A análise das premissas é uma ferramenta que explora a validade das premissas conforme elas se aplicam ao projeto. Ela identifica os riscos do projeto causados pelo caráter inexato, inconsistente ou incompleto das premissas;
- **Comparação Análoga –** Esse método identifica riscos com base na idéia que nenhum projeto representa um sistema totalmente novo, independente do quão avançado ou único ele seja. Para tanto, o método prevê a identificação de projetos similares, de modo que os dados destes projetos possam ser utilizados pelo projeto atual para a sua revisão ou para a sua própria elaboração.
- **Análise causal – Estes método** mostra a relação entre um efeito e sua possível causa para que seja, verificada a origem e o risco. Entre os métodos empregados na análise causal estão: o diagrama de causa e efeito e os 6 W.
    - **Diagrama de causa e efeito** - também conhecido como Espinha de peixe ou Diagrama de Ishiwaka (Figura 20). A filosofia da análise causal é que se um erro ocorrer, ele irá acontecer novamente, ao menos que se faça alguma coisa para evitá-lo.
    - **6 Ws** - baseada também em encontrar a origem das incertezas do projeto, e endereça-las por meio de 6 questões básicas: Who (Quem são os *stakeholders?*), Why (O que os stakeholders querem alcançar?), What (No que os stakeholders estão interessados?), Which way (De que maneira será feito?), Where whital (Quais recursos serão necessários?) e When (Quando terá que ser feito?).

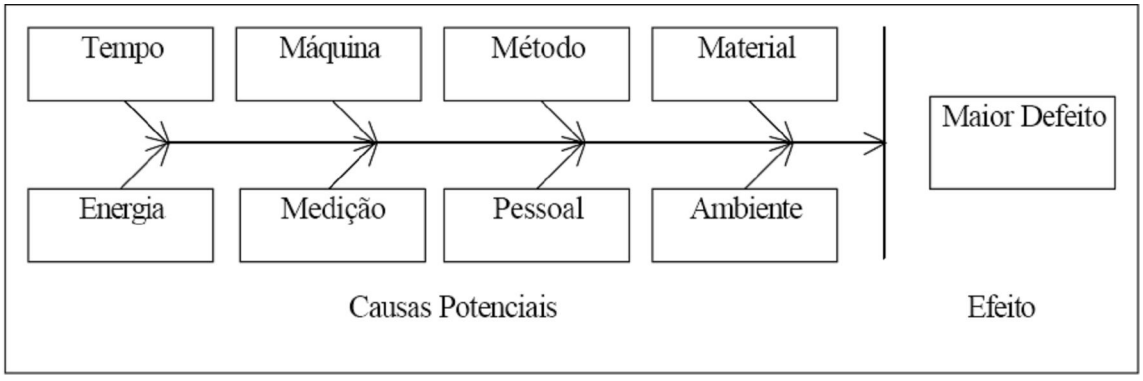

Figura 20 - Diagrama de Causa e Efeito [MACHADO02].

Com base nestas técnicas, os *stakeholders* selecionados para a identificação de riscos na SP1.1, devem coletar informações sobre riscos e então identificar os riscos pertinentes ao

projeto. Para evitar que seja realizada uma outra reunião, esta SP pode ser executada durante a reunião de revisão das fontes de riscos e categorias.

Os riscos são incertezas relacionadas às fontes de risco. Por exemplo, uma incerteza sobre o perfil da mão de obra, ou sobre a data de entrega firmada com o cliente. Os riscos **não** necessariamente são iguais às fontes de riscos encontradas. As fontes de riscos e categorias servem como base para identificar os riscos. É necessário detalhar os riscos conforme as situações específicas encontradas pelos *stakeholders* durante a reunião. A Tabela 7mostra exemplos de riscos em projetos de software.

Tabela 7 - Exemplo de fontes de riscos, categorias e riscos

Categoria	Fontes de Risco	Risco
Equipe	Novas tecnologias	A equipe do projeto pode não se adaptar a tempo a tecnologia Java Web
Prazo	Falta ou insuficiência de tempo para assegurar a implementação das mudanças	Não há tempo suficiente para entregar o módulo 5
Técnico	Dependência do sistema	Não pode dar suporte a ferramenta MobileCom, pois não apresenta rodar em sistemas operacionais UNIX
Projeto	Tamanho do projeto	Projeto grande (maior que 1 ano), com atividades complexas (Mais de 20 pessoas)

A identificação de riscos deve ser feita em todas as iterações. Novos riscos podem surgir ao longo do ciclo de vida do projeto.

Uma forma de descrever riscos é através de frases SE-ENTÃO (*if-then*) [ENGERT99]. Ao invés de apenar citar o problema ou causa, é criada uma descrição onde é apresentado o problema que pode ocorrer, e a consequência do problema caso ocorra. Como por exemplo:

- SE o contrato não for fechado antes do dia 30 de setembro, ENTÃO o programa perde $8 milhões em investimentos;
- SE notebooks comerciais sem customizações forem utilizados, ENTÃO a disponibilidade operacional não será adequada ao ambiente;
- SE a versão 1.1 do programa X não for entregue com 1 mês de atraso, ENTÃO o projeto sofrerá um atraso significativo.

Após a identificação dos riscos, deve-se documentar o contexto, condições e impactos potenciais dos riscos identificados, de forma que os riscos possam ser facilmente entendidos. Nesta documentação do contexto do risco, deve ser considerado o intervalo de tempo relativo do risco, as circunstâncias ou condições em torno do risco e quaisquer dúvidas ou incertezas [SEI01]. Além disso, os *stakeholders* devem ser identificados e associados a cada risco. Com base nas informações coletadas até o momento da identificação de riscos, a

Tabela 8 mostra um exemplo de risco identificado. Os riscos podem ser documentados no registro de riscos.

Tabela 8 - Exemplo de Risco (SP 2.1)

Id	1
Risco	Falta de Envolvimento do usuário
Descrição do Risco	Se o usuário não se envolver no projeto, então os requisitos podem não atender ao próprio usuário
Categoria	Cliente/Usuário
Fonte de Risco	Envolvimento do usuário

A Figura 21 apresenta um exemplo de registro de riscos usado pela organização para documentação dos riscos em uma lista.

Riscos identificados							
Id	**Categoria**	**Fonte de Risco**	**Se...**	**Então...**	**Probabilidade**	**Impacto**	**Fator de Exposição**
<< identificador único do risco >>	<< categoria do risco encontrado >>	<< fonte de risco >>	<< se determinada condição acontecer >>	<< então determinado impacto acontecerá >>	<< probabilidade do risco acontecer com base na escala definida >>	<< impacto caso o risco aconteça com base na escala definida >>	<< cálculo baseado na probabilidade e no impacto definido >>

Figura 21 - Exemplo de *template* para o registro dos riscos

SP 2.2 – Avaliar, Categorizar e Priorizar Riscos

Objetivo

A avaliação de riscos é necessária para atribuir a importância relativa para cada risco identificado. É utilizada para determinar quando a atenção apropriada da gerência de risco é exigida [SEI01].

Atividade

Inicialmente, cada risco é avaliado e são atribuídos valores de acordo com os parâmetros de riscos definidos, que incluem probabilidade, impacto, fator de exposição e limites, conforme foram definidos na SP1.2.

A probabilidade e o impacto são avaliados para cada risco identificado. Os riscos podem ser avaliados em entrevistas ou reuniões com *stakeholders* selecionados por sua familiaridade com as categorias de risco da pauta, usando técnicas de *brainstorming*, Delphi ou revisão documentação, tal como na identificação de riscos. São incluídos os membros da equipe do projeto e, talvez, especialistas de fora do projeto. A opinião especializada é necessária, pois podem existir poucas informações sobre riscos no RCO da organização. Um facilitador experiente pode liderar a discussão, pois os participantes podem ter pouca experiência em avaliação de riscos. Esta etapa pode ser realizada na mesma reunião em que os riscos são identificados na SP2.1, pelos *stakeholders* identificados pela organização na SP1.1 [PMI04].

Outra opção de avaliar a probabilidade e impacto dos riscos é usar técnicas de estimativas de três pontos e simulação de Monte Carlos [PMI04]. Nas estimativas de três pontos são coletadas três estimativas de custo ou duração para representar os cenários otimista, mais provável e pessimista. A partir da média destes três valores será fornecido uma estimativa de duração ou custo da atividade mais exato do que a estimativa mais provável, de apenas um dado coletado. A Tabela 9 mostra um exemplo da aplicação da técnica de estimativas de três pontos. Com base na distribuição de valores encontrada, é aplicada a técnica de Monte Carlo para realizar uma simulação de um cenário futuro, e assim calcular a probabilidade de um determinado custo ou prazo para o projeto. A Figura 22 apresenta a aplicação da análise de Monte Carlo, com base nos dados obtidos na Tabela 9, onde o projeto tem 12% de chance de ter um custo de $41. Desta forma, o projeto tem um risco de 88% do orçamento de $41 não ser suficiente. Caso o projeto deseje diminuir este risco, deverá trabalhar com um orçamento maior.

Tabela 9 - Faixas de estimativas de custo do projeto [PMI04]

Elemento do WBS	Baixo	Mais provável	Alta
Projeto	4	6	10
Construção	16	20	35
Teste	11	15	23
Projeto Total		41	

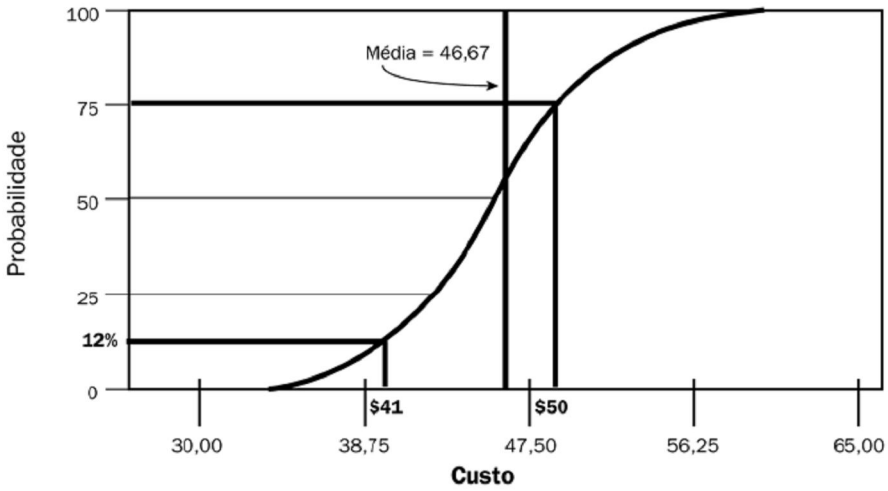

Figura 22 - Aplicação da análise de Monte Carlo [PMI04]

A partir da avaliação de probabilidade e impacto, o próximo passo é o cálculo do fator de exposição de cada um dos riscos, como foi estabelecido na SP1.2 pela organização, desta forma é possível priorizar os riscos baseado no fator de exposição encontrado: quanto maior o fator de exposição, maior a prioridade. Desta forma, será produzida uma lista de riscos ordenada do maior fator de exposição, ao menor fator de exposição.

A avaliação de riscos deve ser feita em todas as iterações da gerência de risco, pois os riscos podem diminuir ou aumentar sua probabilidade e impacto ao longo do ciclo de vida do projeto.

Depois de realizada a avaliação do risco, os riscos podem ser categorizados para um tratamento mais eficiente. Esta categorização pode ser realizada durante a identificação e avaliação dos riscos, com base na taxonomia definida pela organização.

A probabilidade, impacto, fator de exposição e a categoria devem ser informados no registro de riscos, complementando as informações sobre o risco, registradas na SP 2.1. A Tabela 10 mostra um exemplo de risco, com o impacto, probabilidade e fator de exposição atualizado.

Tabela 10 - Exemplo de Risco (SP 2.2)

Id	1
Risco	Falta de Envolvimento do usuário
Descrição do Risco	Se o usuário não se envolver no projeto, então os requisitos podem não atender ao próprio usuário
Categoria Fonte de Risco	Cliente/Usuário Envolvimento do usuário
Probabilidade	Baixa
Impacto	Alto
Fator de exposição	Médio

SG 3 – Mitigar Riscos

Os riscos são tratados e mitigados, quando apropriado, para reduzir os impactos adversos no atendimento dos objetivos.

SP 3.1 – Desenvolver planos de mitigação de riscos

Objetivo

Um componente crítico de um plano de mitigação de riscos é desenvolver cursos alternativos de ação, caminhos alternativos e posições de retomada, com um curso de ação recomendado para cada risco crítico [SEI01].

O plano de mitigação de riscos para um dado risco inclui técnicas e métodos utilizados para evitar, reduzir e controlar a probabilidade de ocorrência do risco, a extensão do dano gerado, caso o risco ocorra (plano de contingência) ou ambos, garantindo respostas em temo hábil [SEI01] [RAMP03] [PMI04].

Os riscos são monitorados com base nos limites estabelecidos, e os planos de mitigação de riscos são implantados para fazer com que o risco fique em um nível aceitável (abaixo do limite). Caso o risco não possa ser mitigado, um plano de contingência pode ser invocado.

Os planos de mitigação de riscos e de contingência são freqüentemente gerados somente para riscos selecionados, onde as conseqüências dos riscos são definidas como altas ou inaceitáveis; outros riscos podem ser aceitos e simplesmente monitorados [SEI01].

As opções de tratamento de risco normalmente incluem alternativas como [SEI01] [PMI04]:

- **Evitar o risco –** Evitar o risco implica em mudar ou diminuir requisitos, mantendo o atendimento às necessidades do usuário. Por exemplo, o esclarecimento dos requisitos, obtenção de informações, melhoria da comunicação ou aquisição de especialização podem prevenir alguns riscos que surgem no início do projeto;
- **Controlar ou mitigar o risco -** A mitigação de riscos exige a redução da probabilidade e/ou impacto de um evento de risco adverso até um limite aceitável. Por exemplo, a realização de ações no início para reduzir a probabilidade e/ou o impacto de um risco que está ocorrendo no projeto é freqüentemente mais eficaz do que a tentativa de reparar os danos após a ocorrência do risco; A adoção de processos menos complexos, realizando mais testes, ou a escolha de um fornecedor mais estável. A mitigação pode exigir a elaboração de protótipos para reduzir o risco decorrente do incremento de escala a partir de um modelo de bancada, para um dado processo ou produto. Quando não for possível reduzir a probabilidade, uma resposta de mitigação poderá abordar o impacto do risco se concentrando nas ligações que determinam a gravidade. Por exemplo, o projeto de redundância em um subsistema pode reduzir o impacto de uma falha do componente original;
- **Transferir o risco –** Exige a passagem do impacto negativo de uma ameaça para terceiros, juntamente com a propriedade da resposta. Por exemplo, a contratação de um fornecedor para desenvolvimento de um componente pode transferir o risco envolvido na construção do componente para um fornecedor externo. Essa transferência de riscos simplesmente confere a uma outra parte a responsabilidade por seu gerenciamento; ela não elimina os riscos.
- **Monitorar o risco -** Observar e periodicamente reavaliar os riscos com relação a mudanças nos parâmetros de riscos atribuídos. Por exemplo, observar se a quantidade de requisitos novos por semana é superior a 1 ou se um risco mudou sua probabilidade de baixa para média;
- **Aceitar o risco -** Reconhecer o risco, mas não tomar nenhuma ação. Uma estratégia adotada porque raramente é possível eliminar todos os riscos do projeto. Esta estratégia indica que a equipe do projeto decidiu não mudar o plano de gerenciamento do projeto para tratar um risco ou que não consegue identificar qualquer outra estratégia de resposta adequada. Por exemplo, um requisito adicional ao sistema devido a mudança na lei que pode acontecer antes do projeto concluir.

Atividades

Uma vez determinado os principais riscos do projeto, a organização deve desenvolver um conjunto de funções para manter os riscos sobre controle.

O primeiro passo a ser realizado, é determinar os níveis e limites que definem quando um risco se torna inaceitável e dispara a execução de um plano de mitigação de riscos ou um plano de contingência. Com base nos limites e alternativas definidos na estratégia de gerência de risco, cabe a organização selecionar qual limite e opção de tratamento de riscos deve ser associado aos riscos, com base na prioridade do risco e categoria. Quando a situação atingir o ponto identificado pelo limite, uma das opções de tratamento de risco ou plano de contingência, associados ao risco, deve ser executado.

A partir da revisão dos riscos, uma lista de possíveis opções de tratamento e limites é gerada. São possíveis escolhas de tratamento de riscos: evitar, mitigar, transferir, monitorar ou aceitar o risco. O método para gerar esta lista é semelhante à identificação e avaliação de riscos. Por meio de *brainstorming* com os *stakeholders* selecionados pela organização serão geradas idéias, o histórico de atividades de mitigação de riscos da organização será analisado, serão usadas idéias que já foram usadas anteriormente, ou serão usadas taxonomias de riscos com opções de tratamento de riscos [COOPER04]. Com as novas opções de tratamento de riscos definidas, a organização pode atualizar a taxonomia de riscos da organização.

As atividades de mitigação de riscos deverão ser examinadas com relação às vantagens e desvantagens que elas oferecem versus os recursos que são gastos. Como em qualquer outra atividade do projeto, pode ser necessário desenvolver planos alternativos e avaliar os benefícios de cada alternativa. O plano mais apropriado é, então, selecionado para execução. Às vezes, o risco pode ser significativo e os benefícios pequenos, mas o risco deve ser mitigado para reduzir a probabilidade de ocorrer um impacto [SEI01][COOPER04].

Os planos de mitigação de riscos devem ser revistos a cada iteração da gerência de risco, uma vez que os status dos riscos podem ter se alterado, e os planos definidos anteriormente não terem um custo-benefício apropriado.

O plano de mitigação de riscos pode ser definido durante as atividades de identificação e avaliação de riscos. Com isto, a organização pode estabelecer uma reunião de riscos, de acordo com o prazo pré-definido na estratégia de gerência de riscos, para a execução de todas estas atividades. O registro de riscos pode ser atualizado com o plano de mitigação, ou pode ser desenvolvido um plano de mitigação mais detalhado para cada risco. Estas atividades extras poderão ser incorporadas ao WBS do projeto.

Para cada atividade de tratamento de risco, deve ser definido uma data inicial, uma data final, os recursos necessários para a execução da atividade e o responsável por executar as ações de tratamento de risco [SEI01]. Estas atividades de mitigação de riscos, ao serem incluídas no projeto podem impactar o plano inicial do projeto, com um aumento de recursos e tempo necessário [RAMP03], por isto a gerência de risco deve ser integrada às atividades de monitoração e controle de projeto.

A Tabela 11 mostra um exemplo de risco atualizado com o plano de mitigação, limite e plano de contingência.

Tabela 11 - Exemplo de Risco (SP 3.1)

Id	1
Risco	Falta de Envolvimento do usuário
Descrição do Risco	Se o usuário não se envolver no projeto, então os requisitos podem não atender ao próprio usuário
Categoria	Cliente/Usuário
Fonte de Risco	Envolvimento do usuário
Probabilidade	Baixa
Impacto Fator de exposição	Alto Médio
Responsável	Gerente do Projeto
Estratégia	Mitigar

Plano de mitigação Limite	Aumentar o número de reuniões formais entre o usuário e a equipe de desenvolvimento Apenas 1 encontro entre o usuário e a equipe de desenvolvimento por semana
Plano de contingência	Contratação de consultor/especialista na área de domínio do sistema

A Figura 23 mostra um exemplo de *template* que pode ser usado para registrar os planos de mitigação de riscos.

Plano de Mitigação de Riscos					
Id	**Responsável**	**Estratégia**	**Prevenção**	**Limite**	**Plano de Contingência**
<< identificador único do risco >>	<< responsável pela prevenção dos riscos >>	<< mitigar, transferir, aceitar, etc. >>	<< técnica de prevenção escolhida para tentar mitigar o risco >>	<< limite a ser monitorado para verificar se o risco aconteceu ou está próximo de acontecer >>	<< ação a ser executada caso o risco aconteça >>

Figura 23 - Exemplo de *template* de Planos de mitigação de risocs

SP 3.2 – Implementar planos de Mitigação de Riscos

Objetivo

Com base no período definido na estratégia de gerência de riscos, a organização deve regularmente monitorar os limites definidos para os riscos. Esta atividade pode resultar na descoberta de novos riscos ou de novas opções de tratamento de riscos, que podem exigir um replanejamento ou uma reavaliação. Em cada caso, os limites associados com o risco deverão ser comparados contra o *status*, para determinar a necessidade de implementar um plano de mitigação de riscos [SEI01].

Além disso, o monitoramento e controle de riscos determina se [PMI04]:

- As premissas do projeto continuam válidas;
- O risco, conforme avaliado, mudou seu estado anterior, usando análise das tendências;
- Os procedimentos e políticas de gerência de riscos adequados estão sendo seguidos;
- As reservas para contingências dos custos ou do cronograma devem ser modificadas de acordo com os riscos do projeto.

Neste momento também é garantido que todos aqueles que precisam estar envolvidos na gerência de riscos recebam as informações necessárias sobre o desenvolvimento dos riscos, e as medidas tomadas para lidar com eles [KASSE04].

Atividades

A organização deve acompanhar o progresso dos riscos acompanhando probabilidade, impacto, fator de exposição etc. para verificar a prioridade de tratamento dos riscos ou se novos riscos, que estavam sendo apenas monitorados, aparecem. A organização também

deve coletar medidas de desempenho do sucesso da execução da atividade de tratamento de risco, que podem ser baseadas em limites. Medidas baseadas em limites são usadas quando valores planejados ou esperados se mantêm relativamente constantes com o tempo [NATWICK03]. A análise de uma medida baseada em limites requer determinar quando o desempenho ultrapassa os limites estabelecidos. Estes limites estabelecidos podem ser normas, valores esperados ou restrições, e podem ser acompanhados por meio de um gráfico de controle.

Para criar um gráfico de controle [DORNER97] podem ser usadas ferramentas de planilha eletrônica, onde deverá ser informado os dados coletados, o limite superior e o limite inferior. Por exemplo, a organização deseja acompanhar o risco “Não disponibilidade das equipes”, por meio do indicador “ média de atraso semana (em horas)”. Para esta situação hipotética, foi identificado que o limite para acusar a ocorrência do risco seria de um atraso médio de 2 horas dos colaboradores do time, com um erro de 15% para baixo ou para cima. A Tabela 12 mostra uma tabela onde foi apontada a média semana de atraso, em horas, de 3 times (A, B e C). Nesta tabela também foi informado qual é o limite superior e o limite inferior, neste caso o limite estabelecido foi de 2 horas de atraso semanais, podendo variar 15% (Limite superior = 1.7 e Limite inferior = 2.3).

Tabela 12 - Dados coletados em relação a média de atraso semanal de 3 times

A	B	C	Limite	LS	LI
0	1	1	2	1.7	2.3
0	1.5	1.3	2	1.7	2.3
0.5	1.3	1.4	2	1.7	2.3
0.75	1.4	1.9	2	1.7	2.3
0.7	1.8	2.2	2	1.7	2.3
0.8	1.9	2.5	2	1.7	2.3
0.6	1.2	2.7	2	1.7	2.3
0.9	1.4	2.6	2	1.7	2.3

Com a tabela criada, foi possível elaborar o gráfico de controle para acompanhamento do progresso do risco. (Figura 24). O risco para a equipe B conseguiu ser controlado após a 6ª semana, porém o atraso médio da equipe C, na mesma 6ª semana, ultrapassou o limite superior, indicando que as atividades de mitigação de risco não tiveram sucesso, e um plano de contingência teve que ser executado.

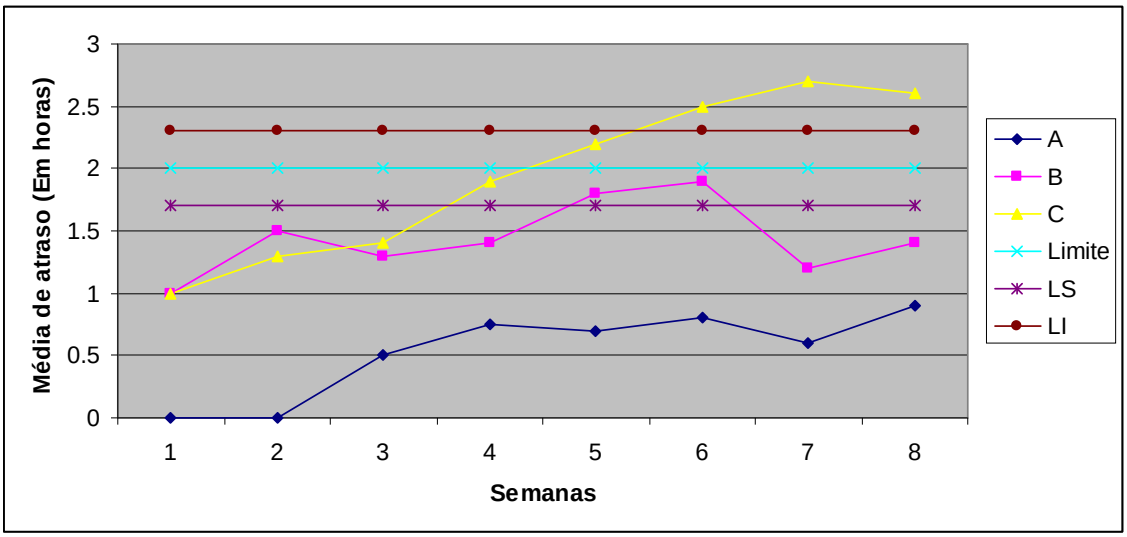

Figura 24 - Monitoramento do risco "Não disponibilidade da mão de obra" por meio da variável "Média de Atraso (Em horas)"

Após executar um plano de mitigação de riscos deve-se continuar monitorando o status do risco, analisando os limites associados ao risco para verificar a necessidade de execução de um plano de contingência. Enquanto um plano de mitigação de riscos está sendo executado, o *status* do risco pode ser alterado, diminuindo o risco, ou agravando o risco, podendo gerar a necessidade de invocar outras opções de tratamento de riscos para lidar com o novo *status*.

O responsável pela gerência de risco pode realizar reuniões com os *stakeholders* para avaliar o progresso dos principais riscos do projeto. Nesta reunião, pode ser informado o tempo em que o risco está na lista dos principais riscos, o *ranking* do risco em relação aos principais riscos na reunião anterior, e uma síntese do progresso do risco. A Tabela 13 mostra como esta lista dos principais riscos pode ser elaborada.

Tabela 13 - Lista dos principais riscos do projeto (Adaptado de [BOEHM91])

	Ranking			
Risco	Atual	Última Reunião	Número de Reuniões	Progresso
Estagiários estão com muitas responsabilidades no projeto	1	2	3	Está sendo avaliada a possibilidade de contratação de um dos estagiários
Documentação pobre do sistema	2	1	3	A documentação está sendo elaborada com a ajuda de um dos desenvolvedores do sistema
Desempenho de hardware abaixo do estimado no projeto	3	3	2	Será adquirido um hardware para avaliação de desempenho

Além disso, pode ser indicado no registro de riscos se o plano de mitigação de riscos não está funcionando e ações são requeridas. Esta indicação pode ser feita por meio de um alerta, que poderia ser um semáforo, onde: verde representa sucesso nas atividades de mitigação de risco, e vermelho indica falha nas atividades de mitigação de risco [MACHADO02], e os riscos que forem sendo eliminados, podem ter o seu status alterado para eliminado, e os riscos que acontecerem podem passar a ter um status de aconteceu. Riscos sem avaliação de progresso podem ficar sem status. A Tabela 14 mostra o status possíveis para o risco.

Tabela 14 - Status do progresso da ação de tratamento dos riscos

Status do Progresso	Descrição
Vazio	Ainda não foi avaliado o progresso
Verde	Ação de tratamento do risco está tendo progresso
Vermelho	Ação de tratamento do risco não está tendo progresso
Aconteceu	Risco aconteceu
Eliminado	Risco foi eliminado

A Figura 25 mostra um exemplo de *template* que pode ser usado pela organização para acompanhar o progresso dos riscos.

Progresso dos Riscos								
Id	**Prob. Inicial**	**Imp. Inicial**	**F.E. Inicial**	**Prob. Atual**	**Imp. Atual**	**F.E. Atual**	**Progresso**	**Observações**
<< identificador único do risco >>	<< probabilidade inicial >>	<< impacto inicial >>	<< fator de exposição inicial >>	<< probabilidade atual >>	<< impacto atual >>	<< fator de exposição atual >>	<<verde, vermelho, eliminado ou aconteceu >>	<< observações sobre o prorgresso ou sobre o motivo dos riscos terem acontecido >>

Figura 25 - Exemplo de *template* de relatório de progresso dos riscos

A organização pode também criar um relatório de status do risco como uma parte do relatório padrão de gerência do projeto, ou um relatório separado, incluindo [KASSE04] [GOLDPRACTICES06]:

- Os 10 riscos principais;
- Novos riscos desde o último relatório;
- Número de itens que foram mitigados, evitados ou tiveram seu impacto reduzido para uma prioridade menor com sucesso;
- Número de planos de contingência que tiveram que ser usados;
- Riscos que aconteceram e quando aconteceram;
- Status dos riscos existentes:
    - Descrição do risco;
    - Antiga e nova prioridade;
    - Antiga e nova probabilidade e impacto;
    - Antiga e nova responsabilidade;
    - Razão da mudança de status.

O relatório de status dos riscos pode ser apresentado por etapa do processo de desenvolvimento (Figura 26), com base no valor de exposição dos riscos que compõe cada fase, onde verde significa baixo nível de risco, amarelo significa médio, vermelho significa alto e em branco quando os riscos ainda não foram avaliados.

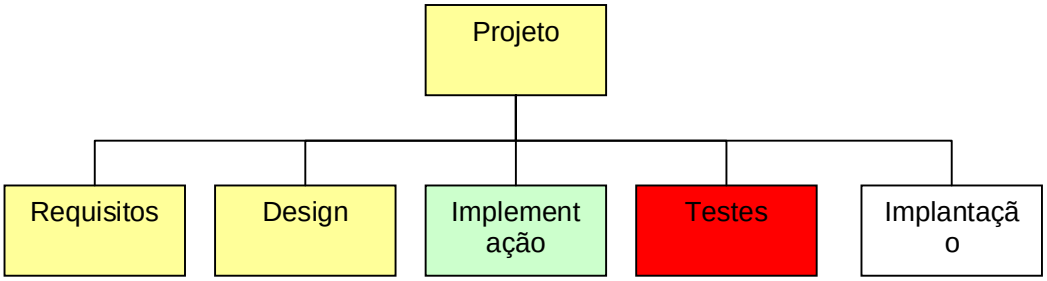

Figura 26 - Status dos riscos por fase do projeto (Adaptado de [GOLDPRACTICES06])

A Figura 27 apresenta a quantidade de riscos agrupados por fator de exposição. Onde 4 riscos apresentam probabilidade e impacto baixos, 2 riscos apresentam probabilidade média e impacto baixo, e apenas 1 risco apresenta probabilidade alta e impacto médio. A Figura 28 apresenta os riscos graficamente na matriz de probabilidade versus impacto.

A Figura 29 mostra um painel de controle (*Dashboard*) com informações sobre a quantidade de riscos encontradas ao longos das semanas do projeto, os 5 principais riscos, a status do tratamento de todos os riscos do projeto, a situação inicial dos riscos no projeto, e a situação atual (com base no fator de exposição).

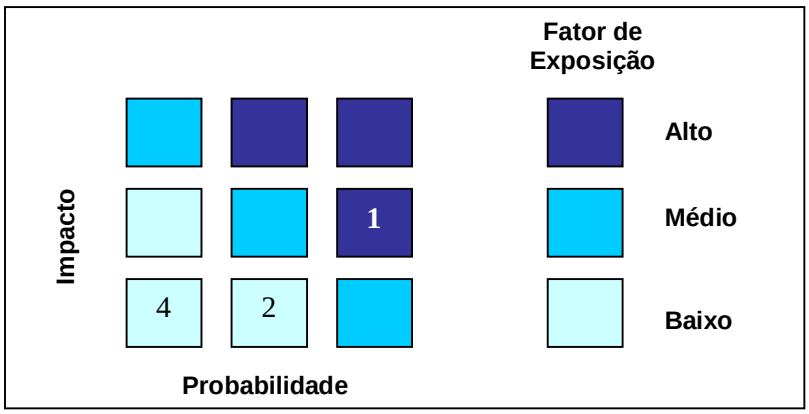

Figura 27 - Status geral do projeto em relação aos riscos (Adaptado de RADAR06])

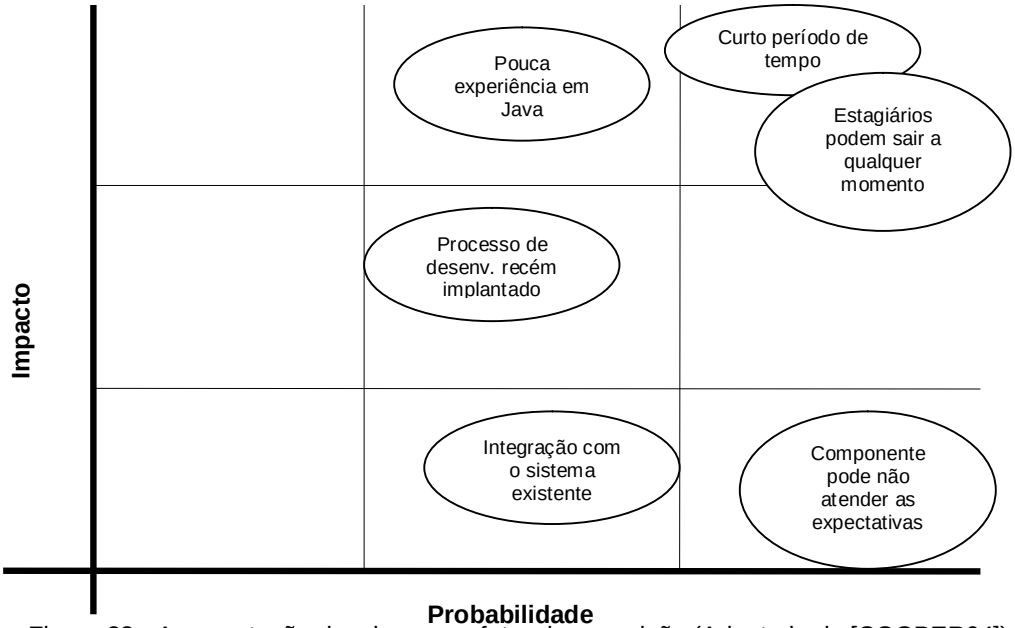

Figura 28 - Apresentação dos riscos por fator de exposição (Adaptado de [COOPER04])

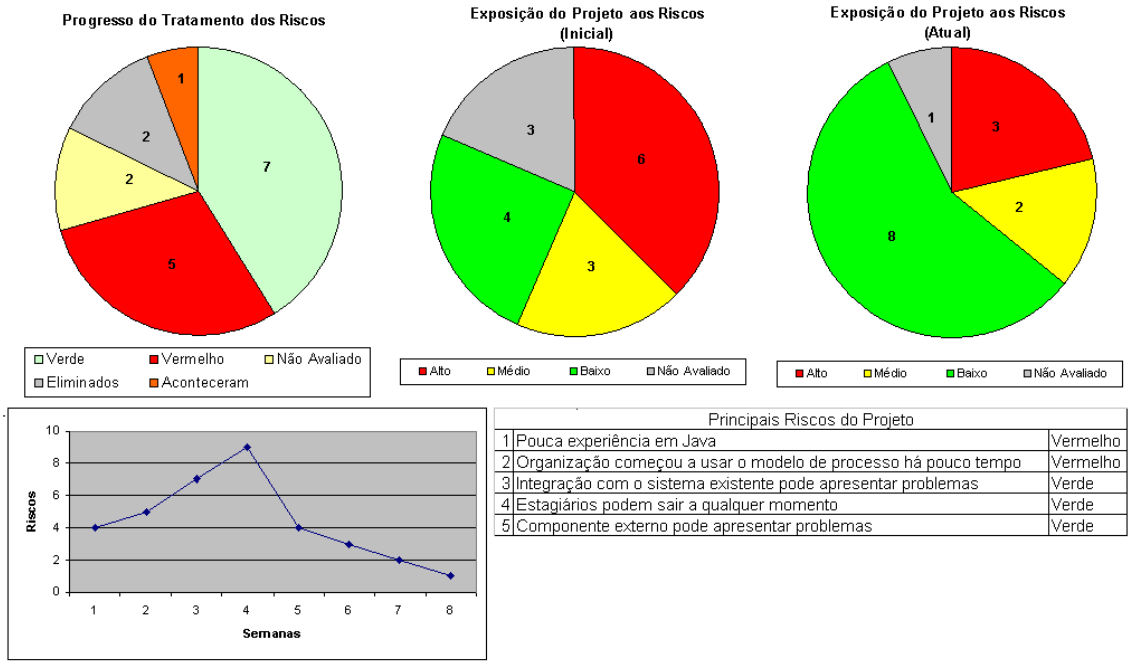

Figura 29 - Painel de Controle de Riscos (Adaptado de [CSO06])

O sucesso é representado por meio do afastamento dos limites estabelecidos para cada um dos riscos ou eliminando o risco. Este afastamento pode ser constatado por meio da monitoração do risco, aplicando um procedimento de medição do risco. A Tabela 15 mostra um exemplo de risco, com o progresso atualizado.

Tabela 15 - Exemplo de Risco (SP3.2)

Id	1
Risco	Falta de Envolvimento do usuário
Descrição do Risco	Se o usuário não se envolver no projeto, então os requisitos podem não atender ao próprio usuário
Categoria	Cliente/Usuário
Fonte de Risco	Envolvimento do usuário
Probabilidade	Baixa
Impacto	Alto
Fator de exposição	Médio
Responsável	Gerente do Projeto
Estratégia	Mitigar
Plano de mitigação	Aumentar o número de reuniões formais entre o usuário e a equipe de desenvolvimento;
Limite	Apenas 1 encontro entre o usuário e a equipe de desenvolvimento por semana
Plano de contingência	Contratação de consultor/especialista na área de domínio do sistema; Levar o problema à gerência sênior.
Progresso	O usuário tem respeitado o horário e datas marcadas para as reuniões formais
Status	Verde

Porém nem sempre o tratamento de riscos é realizado com sucesso, nestes casos novas opções de ação de mitigação de riscos, ou o plano de contingência (caso o risco tenha acontecido) deve ser executado. A nova ação deve ser acompanhada até ser completada, e o status do risco alterado. Os riscos que aconteceram deixam de ser risco, pois já aconteceram. A Tabela 16 apresenta um risco onde foi necessário executar o plano de contingência.

Tabela 16 - Risco onde houve a necessidade de executar o plano de contingência.

Id	1
Risco	Falta de Envolvimento do usuário
Plano de contingência	O problema foi levado a gerência sênior, que procurou o representante da organização cliente, e foi acertado o envolvimento de outro usuário com o sistema, com reuniões semanais com horário pré-definido.
Responsável	José / Gerente do Projeto
Data Início	10/10/2006
Data Final	12/10/2006
Impacto no Projeto	Houve um atraso estimado de duas semanas no projeto por conta da falta de envolvimento com o usuário
Lições aprendidas	Necessidade de acertar formalmente reuniões semanais antes do inicio da execução do projeto, com data e horários pré-estabelecidos. Levar o problema a gerência sênior logo no início (plano de mitigação).

A Figura 30 mostra um exemplo de *template* onde pode ser registrado as ações corretivas, tanto para planos de contingência, como para planos de mitigação de riscos.

Ações Corretivas					
Id Risco	**Responsável**	**Data Inicial**	**Data Final**	**Ação corretiva**	**Impacto**
<< identificador único do risco >>	<< responsável pela ação corretiva >>	<< data da ação corretiva >>	<< data final da ação corretiva >>	<< pro-babi-lidade atual >>	<< impacto do risco >>

Figura 30 - Exemplo de *template* para registrar ações corretivas

No final fechamento do projeto, é importante reunir todos os riscos encontrados, e identificar as lições aprendidas com cada um dos riscos encontrados ao longo do projeto, enumerando os motivos pelos quais foi escolhida uma técnica de mitigação ou um plano de contingência, se as opções selecionadas surtiram o efeito desejado ou não, e os motivos pelo qual o risco aconteceu. Todas estas informações devem ser armazenadas no RCO para serem consultadas e revisadas por todos os *stakeholders* e outros projetos da organização. A apresenta um risco com as lições aprendidas cadastradas.

Tabela 17 – Risco com lições aprendidas cadastradas

Id	1
Risco	Falta de Envolvimento do usuário
Descrição do Risco	Se o usuário não se envolver no projeto, então os requisitos podem não atender ao próprio usuário
Categoria	Cliente/Usuário
Fonte de Risco	Envolvimento do usuário
Probabilidade	Baixa
Impacto	Alto
Fator de exposição	Médio
Responsável	Gerente do Projeto
Estratégia	Mitigar
Plano de mitigação	Aumentar o número de reuniões formais entre o usuário e a equipe de desenvolvimento;
Limite	Apenas 1 encontro entre o usuário e a equipe de desenvolvimento por semana
Plano de contingência	Contratação de consultor/especialista na área de domínio do sistema; Levar o problema à gerência sênior.
Progresso	O usuário tem respeitado o horário e datas marcadas para as reuniões formais
Status	Verde
Lições aprendidas	Necessidade de acertar reuniões semanais antes do inicio da execução do projeto, com data e horários pré-estabelecidos.

A Figura 31mostra um exemplo de *template* onde pode ser registrada as lições aprendidas.

Lições Aprendidas			
Id Risco	**Risco (Se.. Então...)**	**Aconteceu?**	**Lição Aprendida**
<< identificador único do risco >>	<< se determinada condição acontecer, então determinado impacto acontecerá >> >>	<< indica se o risco aconteceu ou não >>	<< lições aprendidas com o risco >>

Figura 31 - Exemplo de *template* onde pode ser registrado as lições aprendidas

5 Análise de Ferramentas

O uso de ferramentas para a gerência de riscos proporciona diversos benefícios às atividades de identificação, análise, monitoração e comunicação de riscos, tais como, a organização das informações de forma mais eficiente e acessível, o auxilio ao monitoramento dos riscos e acompanhamento do histórico, a oportunidade de análises automatizadas de riscos, a integração com outras ferramentas de gerência de projeto, a comunicação dos riscos e o desenvolvimento de relatórios.

Para auxiliar a gerência de riscos, várias ferramentas estão disponíveis no mercado. Esses programas são aplicáveis no auxilio à identificação de riscos, cálculo de probabilidades e impactos com base em dados históricos, registro de riscos, comunicação do progresso dos riscos, armazenamento de informações e comunicação entre os *stakeholders* do projeto. Dentre as opções de software disponíveis, é importante escolher aquelas que atendem melhor à todo o processo de gerência de riscos.

Existem hoje no mercado, tanto ferramentas comerciais quanto ferramentas gratuitas (free), integradas a outras ferramentas, que funcionem em ambiente web ou em formato *standalone.* Dentre as ferramentas disponíveis para a gerência de riscos e que serão analisadas neste trabalho estão:

- MS Project;
- TRIMS;
- RISK RADAR;
- RiskFree;
- RISK+;

5.1 Critérios para a análise de ferramentas

Considerando as práticas especificas para a gerência de riscos alinhada ao CMMI-SE/SW, os *templates* propostos pelo guia, a necessidade de comunicação entre os stakeholders do projeto, as restrições apresentadas em uma MPE e os benefícios do uso de ferramentas de apoio a gerência de riscos, foram definidos critérios para que uma ferramenta possa suportar as atividades requisitadas pelo guia. São estes:

- R01. Permitir o registro de taxonomia de riscos (fontes de riscos e categorias);
- R02. Permitir definir os parâmetros de riscos (probabilidade, impacto, fator de exposição e limites);
- R03. Permitir registrar a estratégia de gerência de riscos;
- R04. Permitir registrar riscos (Descrição, Categoria, Fonte de Risco, Responsável)
- R05. Permitir avaliar, categorizar e priorizar riscos (Probabilidade, Impacto e Fator de exposição);
- R06. Permitir registrar planos de mitigação de riscos (Estratégia adotada, plano de mitigação, limites a ser monitorado, plano de contingência);
- R07. Permitir acompanhar a execução dos planos de mitigação de riscos (Definição do progresso, emissão de relatórios de acompanhamento de mitigação e de planos de contingência);
- R08. Documentação das lições aprendidas para os riscos;

- R09. Ser em português;
- R10. Baixo custo;
- R11. Ser de fácil uso;
- R12. Integração com outras ferramentas de gerência de projetos;
- R13. Interface acessível por múltiplos *stakeholders*;
- R14. Possuir documentação
- R15. Fácil instalação

5.1 TRIMS

A ferramenta TRIMS [TRIMS06] (*Technical Risk Identification and Mitigation System*) [TRIMS06] faz parte do PMWS (Program Manager's WorkStation), que é grupo de ferramentas gratuito, disponível no idioma inglês, *standalone*, que provê informações de desenvolvimento e aquisição de sistemas, desenvolvido pelo programa BMP (*Best Manufacturing Practices*) .

TRIMS é baseada em conhecimento, e mede a gerência de risco tecnicamente, ao invés de medir custo ou prazo. Estouro no custo e prazo são indicadores de problemas técnicos. Segundo o site da ferramenta, projetos normalmente tem problemas no processo antes dos problemas técnicos serem identificados. Para impedir este progresso, TRIMS funciona como uma ferramenta orientada a processo baseada em uma abordagem de engenharia de sistema. A análise e o monitoramento do processo permitem identificar estes problemas o mais cedo possível, e assim ter mais tempo para realizar ações corretivas, mitigar os riscos e evitar problemas. TRIMS identifica áreas de risco, monitora os objetivos e responsabilidades do projeto, e pode gerar uma série de relatórios.

A tela principal de TRIMS indica o risco de cada elemento, que podem ser módulos, fases ou projetos (Figura 32. Para cada um destes elementos, são apresentados questionários agrupados por categorias e subcategorias. Para cada categoria e subcategoria também é indicado o risco. Por exemplo, para a categoria 1.0 Requisitos, são apresentadas as subcategorias estáveis, completos, claros, válidos, implementáveis, precedentes e escaláveis.

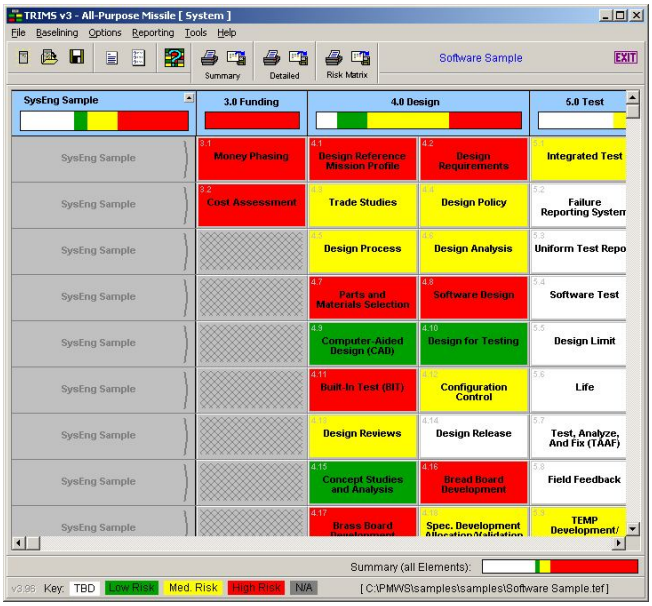

Figura 32 - Tela principal do TRIMS

Para cada categoria (Requisitos, Design, Testes etc.) são feitas diversas perguntas, tais como “Os requisitos são estáveis?”, “As interfaces externas serão finalizadas?” (Figura 33). Estas categorias e perguntas foram desenvolvidas com base no questionário da SEI [CARR93]. E então o usuário responde o grau de confiança que tem nessa afirmação, que pode ser: Sim, Não, Parcialmente, Não sabe ou Não aplicável. Cada uma das perguntas possui um peso na categoria, que pode ser customizável, e então com base nas respostas do usuário, é calculado se o risco é alto, médio, baixo, desconhecido ou não aplicável.

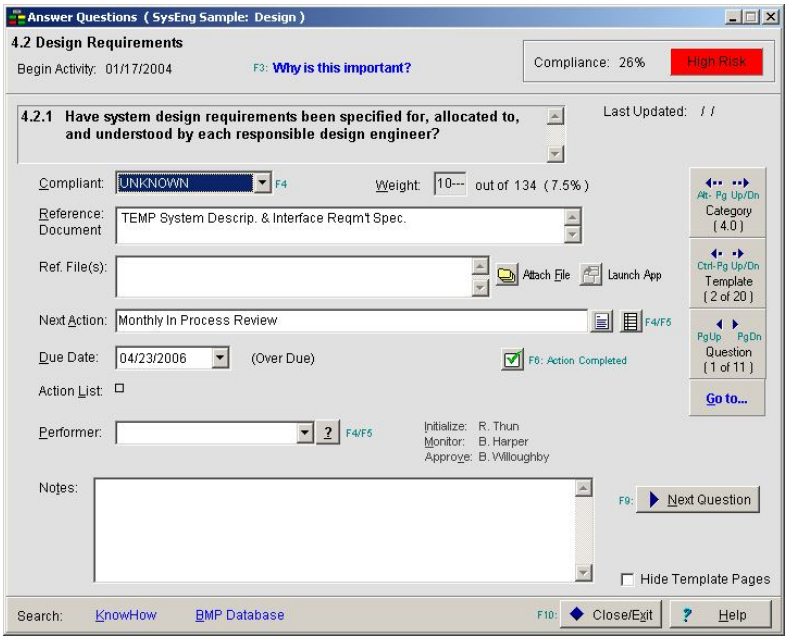

Figura 33 - Formulário do TRIMS

Caso o usuário responda sim, não ou parcial, o TRIM vai pedir que o usuário indique os documentos que serviram como base para responder as questões, planejar ações de mitigação e prazos para execução e resultados destas ações, associarem pessoas responsáveis aos risos e incluir observações. Também é possível customizar as perguntas, categorias e subcategorias, e informar o grau de impacto no custo, desempenho, segurança e prazo para cada subcategoria.

Em relação aos requisitos relacionados à SG1 - Preparar a gerência de riscos -, o TRIMS permite o cadastro de uma taxonomia ou a utilização da taxonomia previamente cadastrada (R01), porém não permite configurar os parâmetros de probabilidade, impacto ou fator de exposição (R02). O usuário apenas indica o grau de confiança que tem em relação a pergunta feita, e com base no peso de cada pergunta é calculado o grau do risco. A estratégia de gerência de risco não pode ser cadastrada no TRIMS (R03), e teria que ser informada em outro documento.

Em relação aos requisitos relacionados à SG2 – Preparar para a gerência de riscos - não é possível registrar riscos específicos (R04), pois as atividades de tratamento de riscos são associadas a cada uma das perguntas respondidas. Com base nas respostas, ações são pedidas e responsáveis são definidos. Não são associados impactos e probabilidades aos riscos, não permitindo a priorização (R05).

Em relação aos requisitos relacionados à SG3 - Nas ações informadas é possível informar os planos de mitigação de riscos e limites a serem monitorados (R06). O status do grau de riscos de cada uma das categorias é acompanhada pela tela principal ou de uma forma mais detalhada por meio de relatórios (R07). As lições aprendidas podem ser documentadas no próprio campo de observações (R08).

Em relação aos demais requisitos, o programa não apresenta versão em português (R09), não possui custo de aquisição (R10), é de fácil uso (R11), não é integrável a outras ferramentas de gerência de projetos (R12), sua interface *standalone* não permite um acesso por múltiplos *stakeholders* (R13), possui documentação e apresentação de como usar (R14) e possui fácil instalação (R15).

5.2 RISK RADAR

A ferramenta RISK RADAR [RADAR06] possui arquitetura Web, disponível no idioma inglês, e não é gratuita (Ver preços na Tabela 18). Foi desenvolvida pela empresa ICE (Integrated Computer Engineering). Por meio da ferramenta RISK RADAR é possível identificar, analisar, acompanhar, mitigar, controlar e reportar os riscos.

Tabela 18 - Preço em Dólares Americanos da ferramenta RISK RADAR [RADAR06]

Quantidade de usuários	Custo Unitário
1	$795,00
5	$2100,00
10	$3200,00
25	$5300,00

A ferramenta RISK RADAR permite gerenciar múltiplos projetos, gerenciar riscos em diversos níveis (categorias, subcategorias etc.), criar novos riscos, atributos para cada projeto e gatilhos que enviam e-mail de notificação quando o risco aconteceu ou está se aproximando de acontecer baseados em datas, valores ou números.

Outras características do RISK RADAR são:

- Customizar o cubo do fator de exposição, por exemplo, escolhendo matrizes 3 x 3, 4 x 4 ou 5 x 5, e identificar qual as faixas de fator de exposição para riscos baixos, médios ou alto (0.1 até 0.2 é baixo, 0.80 é médio, etc.).
- Customizar os tipos de risco, status, fases afetadas, fontes de risco, tipo de controle (interno, externo à organização etc.) e classificação da segurança da informação (confidencial, público, etc.).

A Figura 34 apresenta a tela de entrada de dados para o detalhamento do risco.

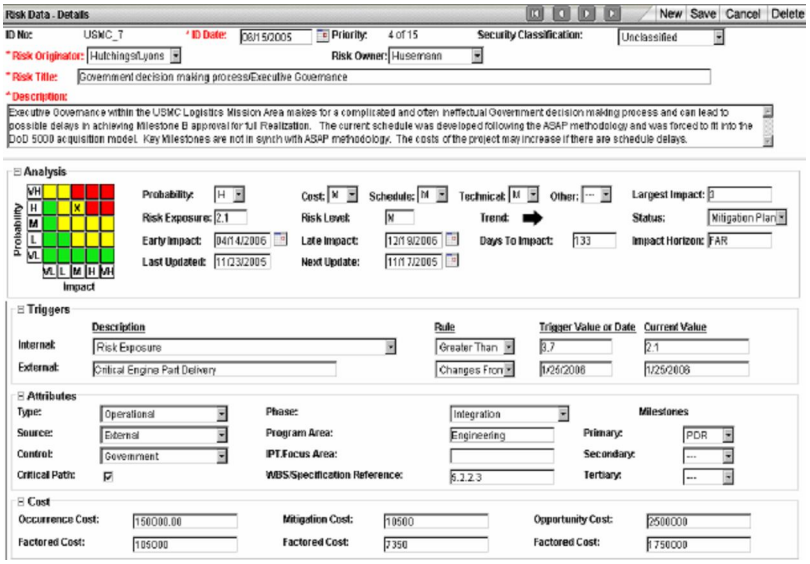

Figura 34 - Tela de detalhe do risco da ferramenta RISK RADAR

Em relação aos requisitos relacionados à SG1 - Preparar a gerência de riscos -, a RISK RADAR permite o cadastro de uma taxonomia – categorias e fontes de riscos (R01), permite configurar os parâmetros de probabilidade, impacto ou fator de exposição (R02). A estratégia de gerência de risco não pode ser cadastrada no RISK RADAR (R03), e teria que ser informada em outro documento.

Em relação aos requisitos relacionados à SG2 – Preparar para a gerência de riscos - é possível registrar riscos específicos (R04), com probabilidade, impacto e cálculo do fato de exposição, e então priorização de riscos (R05).

Em relação aos requisitos relacionados à SG3 – é possível registrar planos de mitigação, e planos de contingência (R06). Cada alteração feita no risco é registrada no histórico, permitindo o acompanhamento progressivo, além de relatórios do próprio sistema (R07). Não há um espaço para lições aprendidas ou um campo de observações onde pudessem ser documentadas lições aprendidas (R08).

Em relação aos demais requisitos, o programa não apresenta versão em português (R09), possui custo de aquisição (R10), é de fácil uso (R11), é parcialmente integrável a outras ferramentas de gerência de projetos (Por exemplo, MS Project) por meio da exportação de dados (R12), sua interface WEB permite acesso por múltiplos *stakeholders* (R13), apresenta documentação de como usar (R14) e possui fácil instalação.

5.3 MS Project 2003

A ferramenta MS Project 2003 [MICROSOFT06] é um software comercial que permite gerenciar projetos (atividades, durações, recursos, calendário, prazos, custos, marcos etc.).

Com o MS Project 2003 é possível trabalhar com a versão Standard ou com a versão Professional. A Standard é a versão para *desktop*, que funciona de forma independente, e não é possível conexão com a versão Server. Esta versão inclui todas as funções básicas para gerência de projetos. A versão Professional tem tudo que a versão Standard têm, e também um ambiente colaborativo com interface Web, onde a equipe pode se comunicar e atualizar as informações do projeto em uma base única, além de permitir a gerência de diversos projetos dentro da uma mesma organização. A versão *standard* não permite gerenciar riscos, desta forma a versão avaliada por este trabalho é a versão Server. O custo de aquisição do MS Project Server 2003 com 5 clientes é de R$3105,77 [DELL06]. Outras diferenças da versão Professional incluem:

- A colaboração entre times usando os módulos Project Server 2003 e Web Access 2003. Com o Project Server 2003 o gerente pode enviar alocar pessoas às tarefas, e por meio do Web Access 2003, que possui uma interface Web, estas pessoas podem atualizar as informações das tarefas.
- Permite personalizar os projetos de forma independente;
- Permite alocar recursos de uma base de recursos de um grupo ou de toda a organização;
- Visões gerais de todos os projetos da organização.

Com os módulos Project Server 2003 e Web Access 2003 instalados é possível gerenciar riscos do projeto com o Project Professional 2003. Por meio do módulo de gerência de riscos, os usuários podem registrar informações sobre riscos e monitorar riscos. Riscos podem ser associados a atividades, recursos, documentos ou a outros riscos. Alertas podem ser enviados por e-mail aos responsáveis pelo risco. O WBS do projeto é totalmente integrado a gerência de riscos, de forma que as atividades relacionadas a mitigação de riscos podem ficar no histórico do projeto para consultas futuras. A Figura 35 mostra a tela de inclusão de novos riscos.

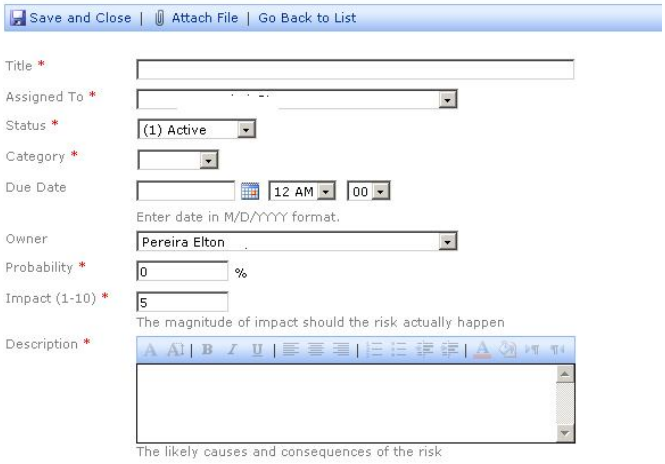

Figura 35 - Tela de cadastro de um novo risco no MS Project.

Em relação aos requisitos relacionados à SG1 - Preparar a gerência de riscos -, o MS PROJECT 2003 permite o cadastro de uma taxonomia – apenas categorias de riscos (R01), porém não permite configurar os parâmetros de probabilidade, impacto ou fator de exposição (R02). A estratégia de gerência de risco não pode ser cadastrada no MS PROJCT 2003 (R03), e teria que ser informada em outro documento.

Em relação aos requisitos relacionados à SG2 – Preparar para a gerência de riscos - é possível registrar riscos específicos (R04), com probabilidade, impacto e cálculo do fato de exposição, e então priorização de riscos (R05).

Em relação aos requisitos relacionados à SG3 – é possível registrar planos de mitigação, e planos de contingência (R06). Também é possível emitir diversos relatórios do próprio sistema (R07). Não há um espaço para lições aprendidas ou um campo de observações onde pudessem ser documentadas lições aprendidas diretamente associadas ao risco (R08).

Em relação aos demais requisitos, o programa apresenta versão em português (R09), possui um alto custo de aquisição para MPEs (R10), é de fácil uso (R11), já faz parte de uma ferramenta de gerência de projetos (R12), sua interface WEB permite acesso por múltiplos *stakeholders* (R13) e, por ser uma ferramenta muito usada no mercado, possui muita documentação do próprio fabricante, além de livros escritos por outros autores (R14), e possui fácil instalação, característica dos produtos da Microsoft (R15).

5.4 RiskFree

A ferramenta RiskFree [SILVEIRA06], desenvolvida por alunos da PUCRS, possui arquitetura Web, disponível no idioma português, e é gratuita. Por meio da ferramenta RiskFree é possível auxiliar as equipes de projetos nas atividades de gerência de riscos. A ferramenta tem como base as práticas descritas no PMBOK [PMI04]. A ferramenta RiskFree também contempla as práticas de gerência de riscos do CMMI-SE/SW [SILVEIRA06]. A Figura 36 apresenta a tela de registro de riscos da ferramenta RiskFree.

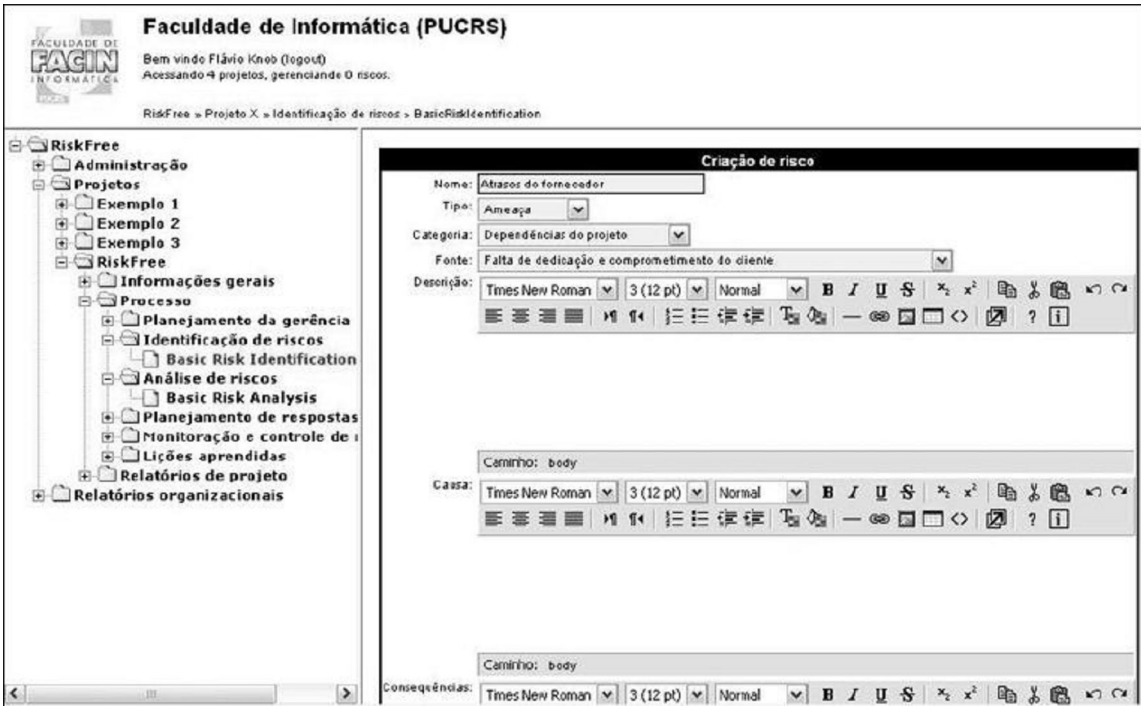

Figura 36 - Tela de registro de riscos da ferramenta RiskFree

Em relação aos requisitos relacionados à SG1 - Preparar a gerência de riscos -, a RiskFree permite o cadastro de uma taxonomia – categorias e fontes (R01), porém não permite configurar os parâmetros de probabilidade, impacto ou fator de exposição (R02). A estratégia de gerência de risco pode ser cadastrada na própria ferramenta (R03).

Em relação aos requisitos relacionados à SG2 – Preparar para a gerência de riscos - é possível registrar riscos específicos (R04), e são associados impactos e probabilidades aos riscos, permitindo a priorização (R05).

Em relação aos requisitos relacionados à SG3 - É possível informar os planos de mitigação de riscos e limites a serem monitorados (R06). É possível emitir diversos relatórios (R07). As lições aprendidas podem ser documentadas durante a etapa de monitoramento e controle (R08).

Em relação aos demais requisitos, o programa apresenta versão em português (R09), não possui custo de aquisição (R10), é de fácil uso (R11), não é integrável a outras ferramentas de gerência de projetos (R12), sua interface WEB permite um acesso por múltiplos *stakeholders* (R13), apresenta pouca documentação sobre a ferramenta (R14) e apresenta dificuldades na instalação (R15) devido aos softwares externos necessários.

5.5 RISK+

A ferramenta RISK+ [CS06] é um *plug-in* do MS Project de análise de riscos que tem como função quantificar incertezas de custo e prazo associadas aos planos de projeto. A ferramenta RISK+ busca responder questões como “Quais são as chances de o projeto completa antes de 2 de fevereiro?” ou “qual o grau de certeza que o custo será abaixo de $9 milhões?”. A ferramenta é baseada nas técnicas de estimativa de três pontos e de Monte Carlo (Ver SP2.2 – Avaliar, categorizar e priorizar riscos - neste guia), e por meio destas

técnicas consegue calcular a probabilidade de custo ou prazo acontecer. Para cada atividade é informado o custo mais provável, o custo para um caso otimista, e um custo para um caso pessimista (a mesma coisa para prazo), e com base nessa distribuição é aplicada a técnica de Monte Carlo para encontrar as probabilidades do projeto atingirem o custo para cada atividade, para um conjunto de atividades, ou para o projeto inteiro. Desta forma, para ser usada, é necessária a consulta à especialistas ou ao histórico da organização para saber estimar os valores e prazos para os casos mais pessimistas, e para os casos mais otimistas.

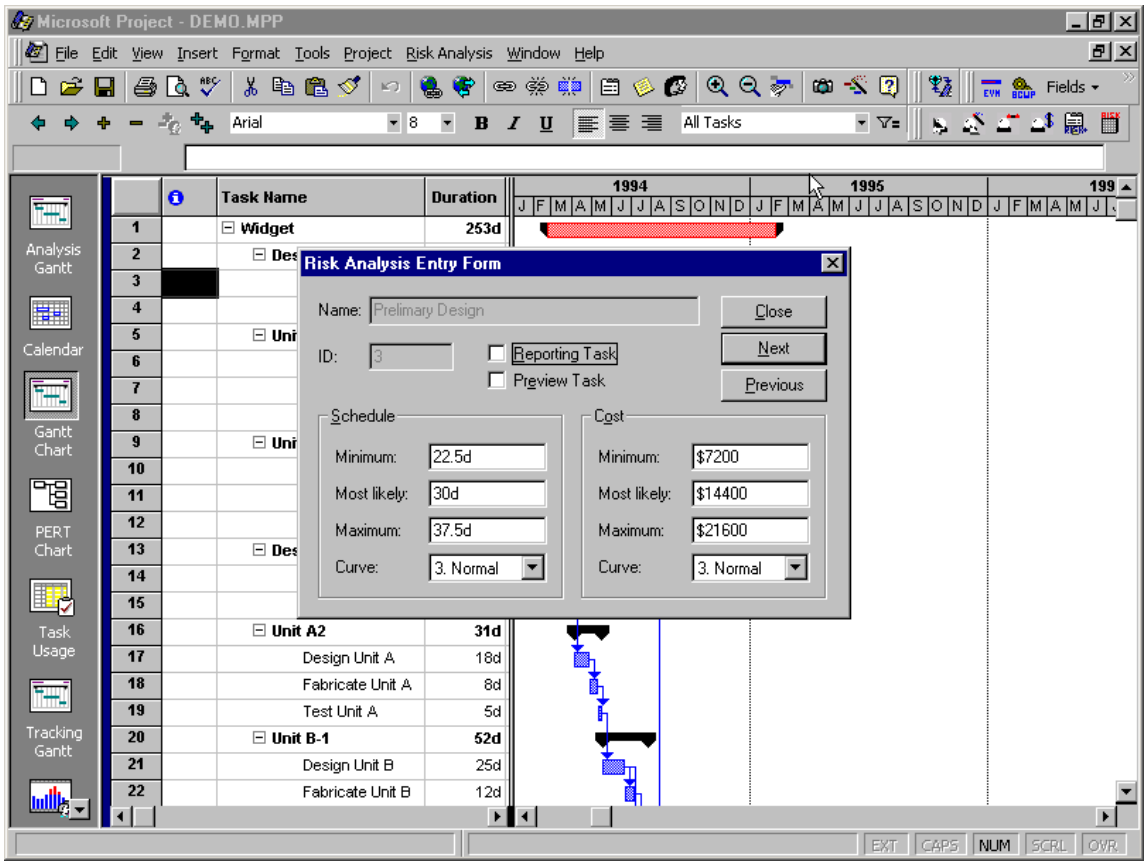

Figura 37 - Tela do MS Project com o *plug-in* Risk+ instalado

A ferramenta RISK+ é diferente das demais atualizadas, pois para funcionar depende de outra ferramenta, o MS Project. Desta forma, é um complemento para as demais ferramentas, não atendendo aos requisitos relacionados aos SG1, SG2 e SG3.

Em relação aos demais requisitos, o programa não apresenta versão em português (R09), possui custo de aquisição (R10) (Cerca de $695 dólares norte americanos) [CS06], é de fácil uso (R11), é integrável ao MS Project (R12), é aplicável somente à versão *standalone* (R13), apresenta documentação sobre a ferramenta (R14) e possui fácil instalação.

5.6 Comparação entre as ferramentas

Com o objetivo de avaliar ferramentas de apoio à gerência de risco, foram definidos requisitos apropriados considerando as atividades de gerência de risco propostas por este guia, e o contexto de MPEs. A Tabela 19 mostra a comparação entre as 5 ferramentas avaliadas.

Tabela 19 - Comparação entre as ferramentas de apoio à gerência de risco

Requisito	TRIMS	RADAR	MS PROJECT 2003	RiskFree	RISK+
R01. Permitir o registro de taxonomia de riscos (fontes de riscos e categorias)	+	+	O	+	-
R02. Permitir definir os parâmetros de riscos (probabilidade, impacto, fator de exposição e limites)	-	+	-	-	-
R03. Permitir registrar a estratégia de gerência de riscos	-	-	-	+	-
R04. Permitir registrar riscos (Descrição, Categoria, Fonte de Risco, Responsável)	O	+	+	+	-
R05. Permitir avaliar, categorizar e priorizar riscos (Probabilidade, Impacto e Fator de exposição)	-	+	+	+	-
R06. Permitir registrar planos de mitigação de riscos (Estratégia adotada, plano de mitigação, limites a ser monitorado, plano de contingência)	+	+	+	+	-
R07. Permitir acompanhar a execução dos planos de mitigação de riscos (Definição do progresso, emissão de relatórios de acompanhamento de mitigação e de planos de contingência)	+	+	+	+	-
R08. Documentação das lições aprendidas para os riscos	O	-	-	+	-
R09. Ser em português	-	-	+	+	-
R10. Baixo custo	+	-	-	+	-
R11. Ser de fácil uso	+	+	+	+	+
R12. Integração com outras ferramentas de gerência de projetos	-	O	+	-	+
R13. Interface acessível por múltiplos *stakeholders*	-	+	+	+	-
R14. Possuir documentação	+	+	+	O	+
R15. Fácil instalação	+	+	+	-	+

Legenda: (+)atende requisito (o) atende parcialmente (-)não atende

Entre as ferramentas analisadas, nenhuma delas apresentou suporte a todos os objetivos específicos do CMMI (SG1, SG2 e SG3) – R01 ao R08. Porém, a que melhor se adequou aos requisitos apresentados, apesar do alto custo, foi o módulo de riscos do MS Project, principalmente pela simplicidade, arquitetura Web, por ser integrado ao MS Project, já amplamente usado pelo mercado, e por ser em português.

As ferramentas TRIMS e o RISK+ são ferramentas de apoio à gerência de riscos e possuem funcionalidades que as demais ferramentas não têm: questionário eletrônico para identificação de riscos e cálculo da probabilidade de riscos de custo e prazo respectivamente.

A ferramenta RISK RADAR, tal como o MS Project, é paga e também permite o apoio à gerência de riscos, arquitetura Web, porém não é tão integrada quanto ao MS Project, e não tem versão em português. Apesar disso, é a única em que é possível definir a escala de probabilidade, impacto e fator de exposição a ser utilizada pela gerência de risco.

A ferramenta RiskFree foi desenvolvida com base nas práticas do PMBOK, desta forma ela consegue apoiar a gerência de riscos, além de ser gratuita e em português. Porém, a ferramenta ainda esta em fase inicial de desenvolvimento, possui complexidade de instalação devido aos diversos componentes externos necessários para a sua utilização. Vale ressaltar que é a única ferramenta que permite registrar a estratégia da gerência de riscos, entre as analisadas.

6 Exemplo

Este capítulo apresenta um exemplo da aplicação do guia de gerência de risco. O exemplo mostra a aplicação da gerência de riscos em uma empresa fictícia, com características típicas de uma MPE usando as técnicas apresentadas neste guia, adequando-as à realidade de uma MPE.

A EMPRESA

A empresa é a VENDESOFT, uma pequena empresa de Software criada há 5 anos na grande Florianópolis, estado de Santa Catarina.

A empresa conta com 2 sócios (Jane e Jones), 6 funcionários (Barney, Fred, Vilma, Betty, Pedrita, Bambam, Dino) e 4 estagiários (Tom e Tim, Tina e Taís). O horário de funcionamento é o comercial (das 8 horas até 18 horas), com jornada de 5 dias por semana. A disponibilidade e competências dos funcionários são detalhadas na Tabela 20.

Tabela 20 - Quadro de funcionários da VENDESOFT

Pessoa	Papéis	Salário liquido (R$ por hora)	Disponibilidade						
			S	T	Q	Q	S	S	D
Jane	Diretor comercial	75,00	8	8	8	8	8	-	-
Jonas	Diretor técnico/Gerente de Projeto	75,00	8	8	8	8	8	-	-
Barney	Analista/projetista	45,00	8	8	8	8	8	-	-
Fred	Programador sênior	30,00	8	8	8	8	8	-	-
Vilma	Analista/projetista	45,00	8	8	8	8	8	-	-
Betty	Testadora	30,00	8	8	8	8	8	-	-
Pedrita	DBA/projetista	45,00	8	8	8	8	8	-	-
Dino	Programador sênior	30,00	8	8	8	8	8	-	-
Bambam	Secretário/assistente	20,00	8	8	8	8	8	-	-
Tom	Programador junior	20,00	4	4	4	4	4	-	-
Tim	Programador junior	20,00	4	4	4	4	4	-	-
Tina	Testadora	20,00	4	4	4	4	4	-	-
Taís	Documentadora	20,00	4	4	4	4	4	-	-

Atualmente a empresa está prestando suporte e fazendo manutenção dos sistemas em operação nos clientes. Para isto os funcionários dedicam o esforço apresentado na Tabela 21 da disponibilidade total (incluindo também outras atividades internas).

Tabela 21 - Esforço dedicado pelos funcionários da VENDESOFT ao projeto

Pessoa	Papéis	Disponibilidade						
		S	T	Q	Q	S	S	D
Jane	Diretor comercial	2	2	2	2	2	-	-
Jonas	Diretor técnico	2	2	2	2	2	-	-
Barney	Analista/projetista	2	2	2	2	2	-	-
Fred	Programador senior	2	2	2	2	2	-	-
Vilma	Analista/projetista	2	2	2	2	2	-	-
Betty	Testadora	2	2	2	2	2	-	-
Pedrita	DBA/projetista	2	2	2	2	2	-	-
Dino	Programador senior	2	2	2	2	2	-	-
Bambam	Secretário/assistente	2	2	2	2	2	-	-
Tom	Programador junior	1	1	1	1	1	-	-
Tim	Programador junior	1	1	1	1	1	-	-
Tina	Testadora	1	1	1	1	1	-	-
Taís	Documentadora	1	1	1	1	1	-	-

A VENDESOFT apresenta a seguinte infra-estrutura:

- 10 computadores pessoais, onde 2 são *notebooks* Pentium-M 512mb, 4 são *desktops* Pentium IV 3.2*Ghz*, 512mb Ram, em perfeitas condições, e 4 são *desktops* Pentium IV 256Mb Ram 1.8Ghz, precisando de atualização de processador e memória;
- 2 servidores Pentium IV 3.2Ghz 2Gb Ram.

O PRODUTO

O produto produzido pela VENDESOFT é o VideoABC, que surgiu partir da análise necessidade que os donos de vídeolocadoras tem para conseguir um bom sistema, que pudesse lhes ajudar nas tarefas diárias da locadora, gerenciando as locações, devoluções, promoções, clientes, etc. de uma maneira fácil e confiável. Desta forma, a VENDESOFT decidiu desenvolver um sistema para atender locadoras de todos os estilos ou tamanhos, que seja de simples utilização e que permita o total controle do estabelecimento, eliminado qualquer possibilidade de erro ou perda de informação.

A empresa vende um sistema de software customizável para controle de empréstimos em videolocadoras. A versão atual do sistema é uma versão Cliente/ Servidor, desenvolvida na linguagem Object-Pascal (ambiente DELPHI), com banco de dados PostgreSQL. As principais funcionalidades da versão atual são:

- Cadastro de clientes
- Cadastro de acervo de filmes em diferentes mídias (Fitas, CDs, DVDs, etc)
- Controle de empréstimo e devolução

Tipicamente, a empresa customiza o sistema padrão para um cliente específico, instala o sistema e oferece treinamento. A empresa também presta manutenção/suporte para os sistemas em operação. Em alguns casos, novas funcionalidades são desenvolvidas em novos projetos a pedido de clientes.

A equipe tem experiência com DELPHI. Atualmente, um dos funcionários (Barney) tem boa experiência em JAVA, sendo que os demais tiveram contato com JAVA apenas em suas universidades.

Para o desenvolvimento de sistemas, a empresa adota, há 6 meses, um modelo de ciclo de vida cascata, composto pelas seguintes fases:

1. No início do projeto a empresa realiza a análise de requisitos, começando com uma ou mais reuniões com o cliente para o levantamento de requisitos. Os requisitos funcionais e não funcionais são documentados.
2. Com base nisto, casos de uso são identificados e documentados, incluindo também protótipos das telas do sistema a ser desenvolvido. No final, os requisitos são revisados em conjunto com o cliente e aprovados pelo gerente e pelo cliente.
3. Com base na análise de requisitos, é feito um projeto informal do sistema, incluindo basicamente a arquitetura do sistema, diagrama(s) de classe e o modelo Entidade-Relacionamento do banco de dados.
4. Depois o sistema é codificado, incluindo a codificação das interfaces, à parte da aplicação e o banco de dados. São realizados testes de unidades de forma ad hoc.

5. O sistema é integrado e é gerado um sistema executável.
6. Com base nos casos de uso documentados na análise de requisitos, são desenvolvidos casos de teste. Seguindo os casos de teste, o sistema executável é testado.
7. Assim que os testes do sistema sejam considerados satisfatórios, o sistema é instalado e liberado para o cliente. São realizados testes de aceitação de forma informal pelo cliente e o cliente confirma que o sistema está pronto para ser utilizado.

Apesar do processo estar definido, ele ainda não é totalmente seguido pelos funcionários menos experientes (Tom, Tim, Tina e Taís).

Após a confirmação e aceitação dos clientes, o sistema é considerado finalizado. Quaisquer alterações futuras, sejam motivadas por erros ou por novas necessidades dos clientes devem ser tratadas pela gerência de mudanças.

A VENDESOFT conta com os seguintes processos de apoio:

- Controle de configuração/versões do sistema utilizando o CVS e adota uma estratégia de acesso/segurança. O CVS é usado para artefatos e para o código fonte do sistema. A empresa também formaliza a detecção e correção de defeitos detectados durante o processo de desenvolvimento utilizando Bug Reports;
- É adotada a ferramenta CASE Enterprise Architect (EA) para a modelagem dos sistemas, Microsoft WORD como editor de texto, e CVS para gerência de configuração e Microsoft Project para gerência de projetos, OTRS para gerencia de mudanças e relatar defeitos;
- É adotada a seguinte política de backup: realizar uma cópia diária do servidor em outra máquina e, uma vez por semana, baixar em alguma mídia externa, com as cópias sendo armazenadas na residência dos diretores da empresa;
- É adotada a seguinte política de treinamento: Sempre que são adotadas novas tecnologias ou procedimentos, é feito um treinamento “in-house” para os funcionários sem experiência, com a contratação de profissionais especializados ou com a participação de funcionários experientes e capacitados a transmitir a tecnologia aos demais.

O PROJETO

A VENDESOFT fechou um novo contrato com Bart Simpson, dono da vídeo-locadora BestFilmes. Neste projeto, o cliente quer além do sistema videoABC (e as funcionalidades já incluídas), mais algumas funcionalidades:

- Consulta de filmes por título e/ou categoria (ação, infantil, etc.) via web para qualquer interessado;
- Reserva de filmes via web para os clientes já cadastrados na vídeo-locadora. O cliente já cadastrado (o cadastro continua somente possível pelo modulo cliente/servidor instalado na vídeo-locadora) pode reservar filmes via web. A reserva é mantida por 24 horas;

De acordo com estas funcionalidades, a empresa criou um novo projeto de desenvolvimento de um módulo a ser integrado ao sistema videoABC que tem estas funcionalidades. A empresa pretende desenvolver o novo módulo Web em JAVA.

A decisão pelo JAVA foi tomada devido a VENDESOFT ter planos futuros de migração de todo a sua aplicação (incluindo o cliente/servidor). Desta forma, a curva de aprendizado futura seria reduzida. Como o escopo é pequeno, seria uma oportunidade para minimizar o impacto em relação ao atendimento das funcionalidades/prazo de entrega.

Além disso, conforme acordado com o cliente, as novas funcionalidades têm que estar disponíveis para o cliente 1 mês após o fechamento do contrato, data de aniversário da vídeo-locadora BestFilms.

EXECUÇÃO DA GERÊNCIA DE RISCO

1ª Reunião de Riscos

Durante o planejamento inicial do projeto após o contrato assinado, foi também realizada a gerência de riscos. Neste momento, deu-se início a 1ª reunião de riscos. Em uma reunião entre os dois diretores da empresa (Jane e Jones), o analista/projetista (Barney) e o programador sênior (Fred), foi elaborada a taxonomia de riscos adequada à organização. Esta taxonomia foi elaborada por meio da revisão de outras taxonomias apresentadas na literatura, e então, usando a técnica Delphi, foram identificadas algumas fontes de riscos apropriadas à organização de consenso de todos os participantes. Para este projeto, não será criada uma taxonomia de riscos própria do projeto.

Tabela 22 - Taxonomia de Riscos da VendeSoft

Taxonomia de riscos da organização					
Categoria	**Fonte de Risco**	**Justificativa**	**Técnicas de tratamento de riscos**	**Limites para monitoração**	**Procedimento de medição**
Equipe	Problemas em utilizar novas tecnologias em projetos [OLIVEIRA06]	Falta de profissionais na equipe treinados com habilidades para utilização de novas tecnologias	Transferência de conhecimento; treinamento; consultoria; contratação de profissionais com experiência.	Caso após a 1 semana, a habilidade de 50% dos membros da equipe são avaliadas insuficientes.	Avaliação subjetiva da habilidade dos funcionários baseado no acompanhamento feito por outro trabalhador com experiência por 2 horas/dia [suficiente, insuficiente].
Cronograma	Falta ou insuficiência de tempo para assegurar a implementação das mudanças [OLIVEIRA06]	Os projetos podem possuir um curto prazo para entrega; a equipe pode não se sentir confiante em atingir a meta de prazo.	Estimativa de cronograma detallhada, desenvolvimento incremental, re-utilização de software e limpeza dos requisitos	Caso o cronograma geral esteja atrasado em 2 dias;	Resultado da diferença de dias entre o cronograma planejado em relação ao cronograma realizado para o dia da avaliação.
Integração entre Sistemas	Necessidade de integração com outros sistemas pode afetar desempenho do sistema original [THOMSETT03]	Os produtos desenvolvidos podem necessitar de integração com outros sistemas.	Revisão da documentação do sistema atual; Contratação de especialista; *Benchmark* do sistema atual após integração.	Caso o *Benchmark* do sistema atual mostra principais queries com perda de 15% de desempenho.	Resultados dos testes de *benchmark* com as principais queries do sistema definidas pelo analista sênior [Passou, não passou].
Equipe	Falta de Disponibilidade dos membros da equipe [THOMSETT03] [JONES94]	Possibilidade de saída dos estagiários e funcionários no meio dos	Horas extras; contratação de trabalhadores temporários; contratação de	Mais de um funcionário de um projeto em férias; Média de ausência dos funcionários superior a 2 horas por semana;	Quantidade de horas de atraso (sem justificativa) do funcionário.

Taxonomia de riscos da organização					
Categoria	**Fonte de Risco**	**Justificativa**	**Técnicas de tratamento de riscos**	**Limites para monitoração**	**Procedimento de medição**
		projetos. Dispensas por férias ou atrasos.	estagiários; aumento salarial; oferecer incentivos extras; reuniões para obtenção de *feedback*.		
Fornecedores	Componentes externos adquiridos podem estar abaixo da expectativa [BOEHM91] [JONES94]	Possibilidade de aquisição de componentes de terceiros	Desenvolvimento de um contrato por um advogado; Análise de desempenho; Checar as referências do fornecedor.	Componente entregue não atender ao requisito com base em testes de desempenho abaixo de 10% do desejado (requisito) e menos de 100% dos testes de funcionalidade não atendidos após 10 testes realizados ao integrar o componente ao sistema;	Resultado dos testes de *benchmark* [passou, não passou]; Resultado dos testes de integração realizado pelo testador [Passou, não passou].
Equipe	Falta de Experiência com o modelo de processo da organização [DIR06]	Possibilidade dos funcionários não estarem preparado para o modelo de processo da empresa	Acompanhamento das atividades; Exigência dos produtos de saída; Treinamento; Reuniões diárias de status;	Caso a quantidade diária de artefatos produzidos fora dos padrões do processo seja superior a 10;	Quantidade de artefatos produzidos fora do padrão (defeito).
Integração entre Sistemas	Documentação inexistente [OLIVEIRA06]	Possibilidade de integração com outros sistemas que não possuem documentação	Contratação de consultoria dos desenvolvedores originais;	Caso não existir documentação para menos de 70% das funções	Avaliação da documentação por função do sistema [Tem = 100%, parcial = 50%, não tem = 0%]
Equipe	Ambiente Físico / de Suporte para o time [THOMSETT04]	Computadores ou ambiente podem não ser adequados para as atividades do time	Investimento em computadores, cadeiras, mesas, luz etc.	Reclamação de mais de 50% da equipe sobre os aspectos físicos da organização	Avaliação realizada por cada um dos membros da equipe [Ruim – 0%, bom = 50%, ótimo = 100%]

Inicialmente nem todas as fontes de riscos da organização foram identificadas no projeto, porém são válidas dentro do contexto da organização, e podem acontecer em outros projetos. Componentes externos adquiridos abaixo da expectativa, documentação inexistente, e ambiente físico / de suporte para o time não adequado são três exemplos de fontes não identificadas para o projeto.

Ainda na 1ª reunião foi realizada a identificação de parâmetros de riscos como parte da definição da estratégia da gerência de riscos. Todos os participantes da reunião optaram por utilizar uma escala ordinal de valores bastante simples, com apenas três valores possíveis (baixo, médio e alto) facilitando a identificação do nível de probabilidade, impacto e grau de exposição de riscos. Foi decidido também que a identificação de limites seria realizada junto com a identificação de riscos.

Para a elaboração da estratégia de riscos, foram feitas as seguintes definições:

- A **Erro! Fonte de referência não encontrada.** mostra a alocação de recursos de pessoal para a gerência de riscos;

- Tabela 23 mostra os métodos e ferramentas que serão utilizados para a gerência de risco;
- As fontes de riscos e categorias do projeto serão apresentadas no próprio registro de riscos do projeto;
- A organização dos riscos é feita por meio de categorias e fontes, são comparados a partir do cálculo de fator de exposição (probabilidade x impacto), usando a escala ordinal de valores definida (baixo, médio e alto). E os limites são identificados para cada um dos riscos pertinentes ao projeto;
- Possíveis técnicas de prevenção de riscos e limites de monitoramento estão informadas na própria taxonomia de riscos da organização;
- Por ser um projeto com um prazo muito curto, de forma a garantir o prazo estabelecido, os riscos deverão monitorados diariamente pelos responsáveis, e as reuniões de risco deverão ser realizadas uma vez por semana.

Tabela 23 – Métodos e Ferramentas que serão utilizados para a gerência de risco

Atividade	Métodos e Ferramentas
SP1.1 – Determinar fontes de riscos e categorias	Guia de Implantação da Gerência de Riscos em Micro e Pequenas Empresas alinhado ao CMMI-SE/SW *Template* da taxonomia de riscos Taxonomia da organizacão Consulta ao plano de projeto e ao RCO da empresa
SP1.2 – Definir parâmetros	Escala ordinal de valores simples, com apenas 3 valores: Baixo, Médio e Alto Priorização de riscos a partir do cálculo do fator de exposição com base nos níveis de impacto e probabilidade Consulta ao RCO da empresa
SP1.3 – Estabelecer uma estratégia de gerência de riscos	*Template* da estratégia de gerência de riscosI. Consulta ao RCO da empresa
SP2.1 – Identificar Riscos	Revisão da documentação Estratégia da gerência de risco Consulta ao RCO da empresa Brainstorming Taxonomia de riscos da organização *Template* de Registro de Riscos
SP2.2 – Avaliar, categorizar e priorizar riscos	Brainstorming Estratégia da gerência de risco Avaliação de probabilidade e impacto Cálculo do fator de exposição Taxonomia de riscos da organização Consulta ao RCO da empresa Registro de Riscos
SP3.1 – Desenvolver planos de mitigação de riscos	Registro de Riscos Estratégia da gerência de risco Evitar, mitigar, aceitar ou transferir Taxonomia da organização Consulta ao RCO da empresa *Template* de planos de mitigação de riscos
SP3.2 – Implementar plano de mitigação de riscos	Registro de riscos Estratégia da gerência de risco Coleta de dados Gráficos de monitoramento de riscos *Template* de relatório de progresso de riscos *Template* de relatório de acompanhamento de ações corretivas *Template* de relatório de lições aprendidas

Tabela 24 – Alocação de recursos de pessoal da VENDESOFT para a gerência de riscos

Recursos	Atividade
Jane/Diretora, Jonas/Gerente do Projeto, Barney/Analista e Fred/Programador	SG1 - Preparação para a gerência de riscos SG2 – Identificar e Analisar Riscos
Jonas/Gerente do Projeto, Barney/Programador	SG3 – Mitigar Riscos

Tabela 25 - Estratégia da Gerência de Riscos do projeto VídeoABC

ESTRATÉGIA DA GERÊNCIA DE RISCOS

1 Escopo da Gerência da Risco

SG1 - Preparação para a gerência de riscos: Jane, Jonas, Barney e Fred
SG2 – Identificar e Analisar Riscos: Jonas, Barney e Fred
SG3 – Mitigar Riscos: Jonas / Softwares: Microsoft Word e Excel / Hardware: Laptop Jonas

2 Tempo de reavaliação e monitoração de riscos

Os riscos deverão monitorados e reavaliados semanalmente

3 Métodos e ferramentas

A VendeSoft segue o seguinte processo de gerência de risco:

- **Determinar as fontes de riscos e categorias –** Nesta etapa, é elaborada e/ou revisada a taxonomia de riscos da organização com base em outras taxonomias disponíveis para consulta, e na consulta ao RCO da própria organização.
- **Definir parâmetros –** Nesta etapa é definido os parâmetros a serem usados para classificar probabilidade, impacto e fator de exposição. Com base no fator de exposição será definida a priorização dos riscos da empresa. Para esta definição é realizada uma consulta ao RCO da própria organização.
- **Estabelecer uma estratégia –** Com base no *template* apresentado no anexo I é identificada todas as informações que compõe a estratégia de gerência de risco a ser usada na organização.
- **Identificar os riscos –** Toda a documentação do projeto é revisada pela equipe identificada para a gerência de riscos, em busca de novos riscos ou riscos que não são mais aplicáveis ao projeto, especialmente os documentos que foram atualizados desde a última reunião de gerência de riscos. Esta revisão é realizada por meio da técnica de *brainstorming* entre os integrantes da equipe. Além da documentação, é usada a taxonomia de riscos da organização e a consulta ao RCO da organização, para a identificação de riscos.
- **Avaliar, categorizar e priorizar riscos –** Com o registro de riscos em mãos, a equipe responsável pela avaliação de riscos, irá identificar por meio de brainstorming e delphi, a probabiliade e o impacto prováveis para os riscos identificados. Com base nestas duas informações, será identificado o fator de exposição, e então priorizados. Neste momento o registro de risco é atualizado.
- **Desenvolver planos de mitigação de riscos –** Com os riscos priorizados, é definida a estratégia de tratamento do risco, entre as opções de evitar, mitigar, aceitar ou transferir o risco. Com base na opção escolhida, são selecionadas técnicas de mitigação do risco, um plano de contingência, limites para monitoramento e definição de procedimentos de medição para identificar se os limites do risco foram ultrapassados. Neste momento a equipe de riscos deve atualizar a taxonomia de riscos com estas opções, para que estas informações estejam disponíveis para outros projetos da organização, e também atualizar o registro de riscos com estas informações.
- **Implementar planos de mitigação de riscos –** Nesta etapa é feito o monitoramento e acompanhamento dos riscos identificados. É avaliado o progresso nas ações de mitigação dos riscos. Caso houver progresso, e os riscos estejam afastados do limite, é indicado um alerta verde para o risco, caso não houver progresso nas ações de mitigação de risco, é ligado o alerta vermelho. Caso os limites sejam ultrapassados, o plano de contingência deve ser executado. Nesta etapa são avaliadas se os planos de mitigação de riscos ou de contingência ainda continuam válidos. O registro de riscos deve ser atualizado, e a taxonomia também deve ser atualizada com as novas opções. Gráficos de monitoramento devem ser produzidos para cada risco, com base nos limites e procedimentos de medição.

4 Organização dos riscos

A organização dos riscos é feita por meio de categorias e fontes, são comparados a partir do cálculo de fator de exposição (probabilidade x impacto), usando a escala ordinal de valores definida (baixo, médio e alto). E os limites são identificados para cada um dos riscos pertinentes ao projeto;

5 Parâmetros

Probabilidade: Baixo, Médio e Alto
Impacto: Baixo, Médio e Alto
Limites: Identificados no documento “Taxonomia de Riscos do Projeto”
Fator de exposição: Baixo, Médio e Alto

Com a estratégia de gerência de risco elaborada (

Tabela 25), iniciou-se a identificação de riscos. Foram reunidos os seguintes documentos para revisão e análise, como fontes de informação para identificação de riscos: Taxonomia de riscos da organização, Plano do projeto, WBS e estratégia da gerência de risco. O plano do projeto para este exemplo pode ser visto no guia de planejamento de projeto de software [KUNTZE06].

Como a elaboração da taxonomia foi realizada pela própria equipe, já foi possível identificar, avaliar e categorizar os riscos pertinentes ao projeto. Com a revisão da documentação e posterior *brainstorming* entre os participantes, várias sugestões foram dadas e então foi possível, por meio de consenso usando a técnica Delphi, agrupar os riscos semelhantes, e descrever melhor os riscos e identificar responsáveis pela mitigação.

Além disso, durante a identificação dos riscos, foi realizada também a avaliação e categorização dos riscos, identificando probabilidade, impacto e fator de exposição com base na escala ordinal definida na estratégia de gerência de riscos (baixo, médio e alto) usando a técnica Delphi entre os participantes. Com base nos riscos identificados, foi elaborado o registro de riscos (Tabela 26), documentando as seguintes informações:

- Id – Código do risco;
- Risco – Descrição sucinta do risco;
- Categoria e Fonte do Risco com base na taxonomia;
- Descrição – Descrição do risco no formato Se-Então;
- Probabilidade, impacto e fator de exposição.

Tabela 26 - Registro de Riscos (1ª Reunião)

Riscos identificados							
Id	Categoria	Fonte de Risco	Se...	Então...	Proba-bilidade	Impacto	Fator de Exposição
1	Equipe	Problemas em utilizar novas tecnologias em projetos	Se o time não tiver habilidade com Java	Então é possível que o prazo estimado não seja cumprido, e que o sistema não seja elaborado com qualidade	Médio	Alto	Alto
2	Equipe	Falta de Experiência com o modelo de processo da organização	Se o processo de software não for usado por todos os integrantes da equipe	Então defeitos podem ser encontrados após a implantação do produto no cliente	Médio	Médio	Médio
3	Cronograma	Falta ou insuficiência de tempo para assegurar a implementação das mudanças	Se não for entregue o produto em 1 mês	Então o cliente não poderá inaugurar o sistema na data de aniversário, e a VidieoABC	Alto	Alto	Alto
4	Integração entre sistemas	Necessidade de integração com outros sistemas pode afetar desempenho do sistema original	Se houver problemas de integração com o sistema atual	Então o sistema poderá baixar o desempenho com a integração	Baixo	Médio	Baixo

Riscos identificados							
Id	Categoria	Fonte de Risco	Se...	Então...	Proba-bilidade	Impacto	Fator de Exposição
5	Equipe	Falta de Disponibilidade dos membros da equipe	Se os estagiários saírem da organização no meio do projeto,	Então o projeto poderá sofrer atrasos, uma vez que os estagiários estão assumindo responsabilidades no projeto	Alto	Alto	Alto

Com os riscos identificados, e priorizados com base no fator de exposição, foi definido um plano de tratamento para os riscos. Foi identificado que mitigar o risco será a estratégia para todos os riscos identificados. As opções de transferir ou aceitar foram descartadas. Revisando a taxonomia foram selecionadas, para cada risco, ações de prevenção e limites para identificar quando o risco aconteceu, procedimentos de medição do progresso do risco, e uma ação a ser executada caso o risco aconteça (plano de contingência). O plano de mitigação de riscos pode ser visto na Tabela 27.

Tabela 27 - Plano de mitigação de riscos - 1a Reunião

Plano de mitigação de riscos					
Id	Responsável	Estratégia	Prevenção	Limite	Plano de Contingência
1	Barney	Mitigar	Treinamento da Equipe por Barney; Compra de Livros Java para Consulta	Caso após 1 semana, a habilidade de 50% dos membros da equipe são avaliadas insuficientes.	Contratação de profissionais com experiência em Java.
2	Jonas	Mitigar	Treinamento da equipe no modelo de processo / Acompanhamento do processo de desenvolvimento	Caso a quantidade diária de artefatos produzidos fora dos padrões do processo seja superior a 10;	Contração de consultoria especializada em melhoria de processos de software.
3	Jonas	Mitigar	Pedir que os funcionários e estagiários façam horas extras para cobrir o atraso inferior a 4 dias	Caso o cronograma geral esteja atrasado em 2 dias;	Contratação de profissionais com experiência em Java por período limitado
4	Barney	Mitigar	Testes de *Benchmark* de sistema para avaliar o desempenho.	Caso o Benchmark do sistema atual mostra principais queries com perda de 15% de desempenho.	Contratação de mão de obra temporária para resolver problema
5	Jonas	Mitigar	Obter *feedback* dos estagiários	Média de ausência dos estagiários superior a 2 horas por semana;	Contratação do estagiário ao depender do desempenho; Contratação de trabalhadores temporários com experiência em Java

Até o momento desta 1ª reunião, nenhuma ação de tratamento de risco foi disparada. O projeto ainda está no início, e ainda não foram coletas as medidas necessárias para identificar se o limite foi ou não atingido. Desta forma, todos os riscos estão com o alerta verde. Este alerta pode passar para vermelho caso as ações de tratamento dos riscos não estejam surtindo efeito.

2º Reunião da gerência de riscos

Após 1 semana de início do projeto, a 2ª reunião da gerência de risco foi iniciada. Foram reunidos novamente os recursos alocados para a gerência de riscos, conforme estratégia da gerência de risco definida na 1ª reunião. Foi feita uma revisão da taxonomia de riscos adotada pela organização, e de algumas outras taxonomias, e não foram encontradas nenhuma categoria ou fonte de risco nova, ou nenhuma que devesse ser retirada.

Também foi acordado que nenhuma mudança nos parâmetros ou na estratégia da gerência de risco deveria ser feita. A empresa ainda dispõe dos mesmos recursos para a gerência de risco, tal como planejado na 1ª reunião.

Para a identificação de riscos, foi revisada a taxonomia de riscos da organização, e os documentos do projeto (ex. requisitos, WBS, plano de projeto etc) que sofreram alteração desde a última reunião de riscos, e assim foi realizado um *brainstorming* entre os membros da reunião. Foi levantado que existe um novo requisito do cliente, e será necessário utilizar um componente pronto para visualização dos trailers dos filmes. Desta forma, um novo risco foi detectado para a fonte de risco "dependência de um fornecedor externo para atingir um cumprimento de um requisito". Este risco foi enquadrado na categoria "Fornecedores", e foi incluído no registro de riscos conforme a seguir. "Se o componente adquirido junto ao fornecedor não atender aos requisitos de desempenho e funcionalidade, então os requisitos do cliente não serão atendidos".

Tabela 28 - Registro de riscos (Novo risco identificado) (2a Reunião)

Riscos identificados							
Id	Categoria	Fonte de Risco	Se...	Então...	Proba-bilidade	Impacto	Fator de Exposição
6	Fornecedores	Dependência de um fornecedor externo para atingir um cumprimento de um requisito	Se o componente adquirido junto ao fornecedor não atender aos requisitos de desempenho e funcionalidade,	Então os requisitos do cliente não serão atendidos	Baixo	Alto	Médio

A segunda etapa da atividade de gerência de riscos é a avaliação de todos os riscos levantados. Para realizar esta avaliação, foi feito uma avaliação do progresso dos riscos, com base nos limites identificados, dados coletados por Jonas, e opções de tratamento para cada um dos riscos.

Foi identificado que o alerta vermelho deveria ser ligado para o risco 5, uma vez que as ações de mitigação do risco não estão surtindo o efeito desejado. Os demais riscos apresentam progresso com as ações de mitigação definidas. Para o risco 5, uma nova opção de mitigação de risco deve ser executada, e esta ação foi documentada no documento de ações corretivas (Tabela 29).

Tabela 29 - Ações corretivas

Ações Corretivas					
Id Risco	**Responsável**	**Data Inicial**	**Data Final**	**Ação corretiva**	**Impacto**
1	Jonas	10/Jan	-	Oferecer incentivos extras	Aumentar o estimulo dos estagiários, especialmente Tim

Continuando a reunião de riscos, foi decidido que alguns riscos deveriam manter os mesmos níveis de probabilidade e impacto no projeto, e os riscos a seguir deveriam ter sua probabilidade alterados: “Estagiários podem sair a qualquer momento”, “Pouca Experiência em Java Web” e “Período de Desenvolvimento de apenas 1 mês”.

Tim, programador estagiário, está atrasando mais de 1 hr por semana e aparenta estar com um grau de satisfação ruim em relação ao projeto, apesar do bom desempenho do mesmo em cumprir as tarefas designadas a ele. Com isto, foi consenso de todos elevarem a probabilidade do risco de o estagiário sair para alta.

A equipe está tendo um bom desempenho no aprendizado de Java, apesar de continuar a necessidade de Barney acompanhar o trabalho dos outros membros da equipe. Com isto, foi consenso que a probabilidade do risco 1 deveria ser reduzida para baixa. Como conseqüência desta evolução técnica da equipe, o prazo de apenas 1 mês para conclusão do projeto deve ser cumprido (mas deve continuar sendo acompanhado), e este risco teve sua probabilidade baixa para médio.

Foi também avaliado o novo risco relacionado ao fornecimento de um componente para exibição de trailers. Devido ao grau de confiança no fornecedor, segundo Jonas, a probabilidade foi identificada como baixa, porém o impacto, caso o risco aconteça, seja alto no projeto, podendo impactar no prazo previsto. O responsável pelo novo risco será o próprio Jonas.

Com estas alterações, o principal risco passa a ser o risco de um estagiário sair do projeto. Jonas vai continuar avaliando este grau de insatisfação dos estagiários. Este risco está com o alerta vermelho. A **Erro! Fonte de referência não encontrada.** mostra o relatório de progresso dos riscos.

Tabela 30 - Progresso dos Riscos

Progresso dos Riscos								
Id	Prob. Inicial	Imp. Inicial	F.E. Inicial	Prob. Atual	Imp. Atual	F.E. Atual	Progresso	Observações
1	Médio	Alto	Alto	Baixo	Alto	Médio	Verde	Barney realizou procedimento de medição previsto, e analisou de forma subjetiva a habilidade da equipe em satisfatório e não satisfatório, e mais de 50% da equipe apresentou rendimento satisfatório nesta 1ª semana, porém o risco conitnua, e este acompanhamento deve continuar sendo feito (A Figura 41 mostra o monitoramento do risco ao longo de todas as semanas).
2	Médio	Médio	Médio	Médio	Médio	Médio	Verde	Jonas coletou a quantidade de artefatos produzidos fora do padrão do processo, e menos de 5 artefatos por dia foram produzidos com defeitos. As atividades continuam sendo acompanhadas.

Progresso dos Riscos								
Id	Prob. Inicial	Imp. Inicial	F.E. Inicial	Prob. Atual	Imp. Atual	F.E. Atual	Progresso	Observações
3	Alto	Alto	Alto	Alto	Alto	Alto	Verde	Jonas mostrou que o cronograma do projeto está dentro do prazo estabelecido, sem atrasos, quando comparado ao já realizado. Os requisitos estão claros e o WBS está bem detalhado.
4	Baixo	Médio	Baixo	Baixo	Médio	Baixo	Verde	Ainda não foi possível realizar testes de desempenho no sistema, visto que o módulo não tem nenhuma parte pronta ainda. Estes testes deverão ser realizados apenas a partir da 3ª semana.
5	Médio	Alto	Alto	Alto	Alto	Alto	Vermelho	Tim (estagiário) possui uma média de atraso de 1 hr por semana, além de aparente insatisfação em relação a empresa. Jonas reuniu os estagiários ter um feedback de todos em relação ao projeto e a organização, porém não houve efeito positivo em relação a Tim (A Figura 42 mostra o monitoramento do risco ao longo das 4 semanas).
6	Baixo	Alto	Médio	-	-	-		<< Risco Novo >>

Na terceira parte da reunião de riscos, não foram identificadas novas opções de tratamento para os riscos já existentes. Para o novo risco identificado, relacionado ao fornecedor, foi registrado o limite de 10% acima no desempenho de testes de *benchmarking* em relação a condição atual do sistema, e menos de 100% dos testes de funcionalidade não atendidos. Este risco deverá ser mitigado, desenvolvendo um contrato legal firmando os requisitos de funcionalidades necessários, e buscar outros fornecedores capazes de entregar um componente similar caso o escolhido não atenda. Caso o risco se torne realidade, deverá ser fechado um acordo com um novo fornecedor (Tabela 31). A taxonomia de riscos da organização também foi atualizada com estas opções de tratamento de risco, limites e planos de contingência.

Tabela 31 - Plano de mitigação de riscos parcial (2ª Reunião)

Id	Responsável	Estratégia	Prevenção	Limite	Plano de Contingência
6	Jonas	Mitigar	Desenvolver um contrato legal com a empresa; buscar referências da empresa; buscar novas opções de fornecedores;	Componente entregue não atender ao requisito com base em testes de desempenho abaixo de 10% do desejado (requisito) e menos de 100% dos testes de funcionalidade não atendidos após 10 testes, no mínimo, realizados ao integrar o componentes ao sistema;	Contratação de outro fornecedor com componentes de pronta entrega.

3º Reunião de Riscos

Na semana seguinte, a 3ª reunião de riscos foi iniciada. Foi reunida novamente a equipe designada para a gerência de riscos. Foram reunidos novamente os recursos alocados para a gerência de riscos, conforme estratégia da gerência de risco definida. Antes de iniciar a reunião foi divulgado um quadro com a visão geral dos riscos com base no fator de exposição das duas últimas reuniões (38). Por meio desta figura é possível que o número de riscos aumentou, e que aumentou o fator de exposição de mais um risco.

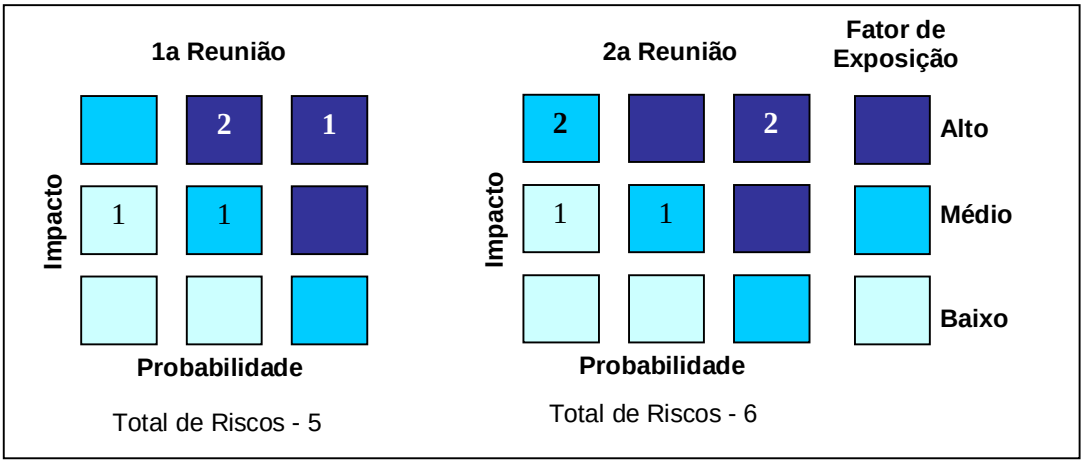

Figura 38 - Visão geral da gerência de riscos

Foi feita uma revisão da taxonomia de riscos adotada pela organização, e de algumas outras taxonomias, e não foram encontradas nenhuma categoria ou fonte de risco nova, ou nenhuma que devesse ser retirada.

Também foi acordado que nenhuma mudança nos parâmetros ou na estratégia da gerência de risco deveria ser feita. A empresa ainda dispõe dos mesmos recursos para a gerência de risco, tal como planejado na 1ª iteração.

Para a identificação de riscos, foi revisada a taxonomia de riscos da organização, e os documentos do projeto (ex. requisitos, WBS, plano de projeto etc.) que sofreram alteração desde a última reunião de riscos, e assim foi realizado um *brainstorming* entre os membros da reunião. Não foram levantados novos riscos.

A segunda etapa da atividade de gerência de riscos é a avaliação de todos os riscos levantados. Para realizar esta avaliação, foi feito uma avaliação do progresso dos riscos, com base nos limites identificados, dados coletados por Jonas, e opções de tratamento para cada um dos riscos.

Tabela 32 - Progresso dos Riscos (3ª Reunião)

Progresso dos Riscos								
Id	Prob. Inicial	Imp. Inicial	F.E. Inicial	Prob. Atual	Imp. Atual	F.E. Atual	Progresso	Observações
1	Médio	Alto	Alto	-	-	-		O risco foi eliminado, pois depois de uma semana mais de 50% da equipe apresentou capacidade em aprender Java.

Progresso dos Riscos								
Id	Prob. Inicial	Imp. Inicial	F.E. Inicial	Prob. Atual	Imp. Atual	F.E. Atual	Progresso	Observações
2	Médio	Médio	Médio	-	-	-	Eliminado	Jonas coletou a quantidade de artefatos produzidos fora do padrão do processo, e não houve erros de artefatos essa semana.
3	Alto	Alto	Alto	Médio	Alto	Alto	Verde	Jonas mostrou que o cronograma do projeto está dentro do prazo estabelecido, sem atrasos, quando comparado ao já realizado. Os requisitos estão claros e o WBS está bem detalhado.
4	Baixo	Médio	Baixo	Baixo	Médio	Baixo	Verde	Ainda não foi possível realizar testes de desempenho no sistema, visto que o módulo não tem nenhuma parte pronta ainda. Estes testes deverão ser realizados apenas a partir da 3ª semana.
5	Médio	Alto	Alto	-	-	-	Aconteceu	Tim, o estagiário, pediu demissão, e se desligou do projeto.
6	Baixo	Alto	Médio	-	-	-	Eliminado	O fornecedor entregou o componente conforme previsto, foram realizado os testes previstos com o componente, e atende aos requisitos.

Um dos riscos se manifestou: Tim, o estagiário pediu para ir embora da empresa. Com isto, houve a necessidade de executar o plano de contingência. Tim não aceitou a proposta de permanecer na equipe, foi então contratado um profissional Java, que já havia atuando na empresa em outros projetos, para esta última semana. O custo com a equipe aumentou em 10% com esta contração. O risco 1, 2 e 6 foram eliminados. A equipe apresentou habilidade suficiente para trabalhar com Java e com o modelo de processo, e o fornecedor entregou o componente conforme previsto. Os outros dois riscos riscos apresentaram progresso nas atividades de mitigação, mas mesmo assim foi consenso que deveriam manter os mesmos status da semana anterior.

Tabela 33 - Ações Corretivas (3a Reunião)

Ações Corretivas					
Id Risco	**Responsável**	**Data Inicial**	**Data Final**	**Ação corretiva**	**Impacto**
1	Jonas	17/Jan	18/Jan	Contratação de um profissional com conhecimento em Java.	Aumento do custo da equipe em 10%

Na terceira parte da reunião de riscos, não foram identificadas novas opções de tratamento para os riscos já existentes.

4º Reunião de Riscos

Na semana seguinte, a 4ª e última iteração de gerência de risco foi iniciada. O projeto está concluído com sucesso. Foi reunida novamente a equipe designada para a gerência de riscos. Foram reunidos novamente os recursos alocados para a gerência de riscos, conforme estratégia da gerência de risco definida.

Todos os riscos foram mapeados, planos de mitigação de riscos foram realizados, apenas um plano de contingência foi executado, três riscos foram eliminado e os demais não se manifestaram. A Figura 39 apresenta a quantidade de riscos ao longo do projeto.

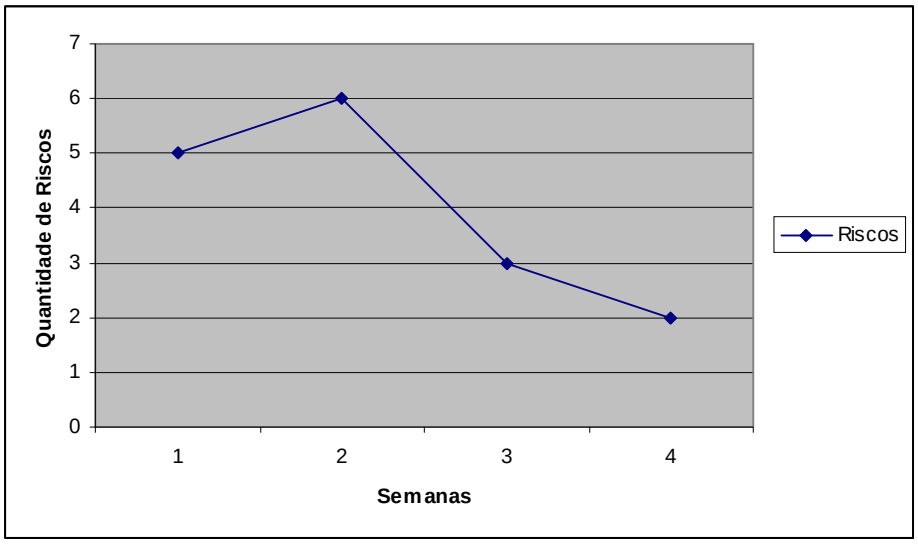

Figura 39 - Quantidade de riscos ao longo do projeto

A Figura 40 mostra a visão geral do resultado das ações de gerência de risco. Na 2ª reunião haviam 6 riscos, onde 4 apresentaram progresso com as ações de mitigação, 1 ainda estava em fase de avaliação, e 1 não apresentava progresso com as ações de mitigação. Na quarta e última reunião de riscos, 1 risco aconteceu, 3 riscos foram eliminados, e 2 riscos continuaram existindo até o fim do projeto, porém não se manifestaram.

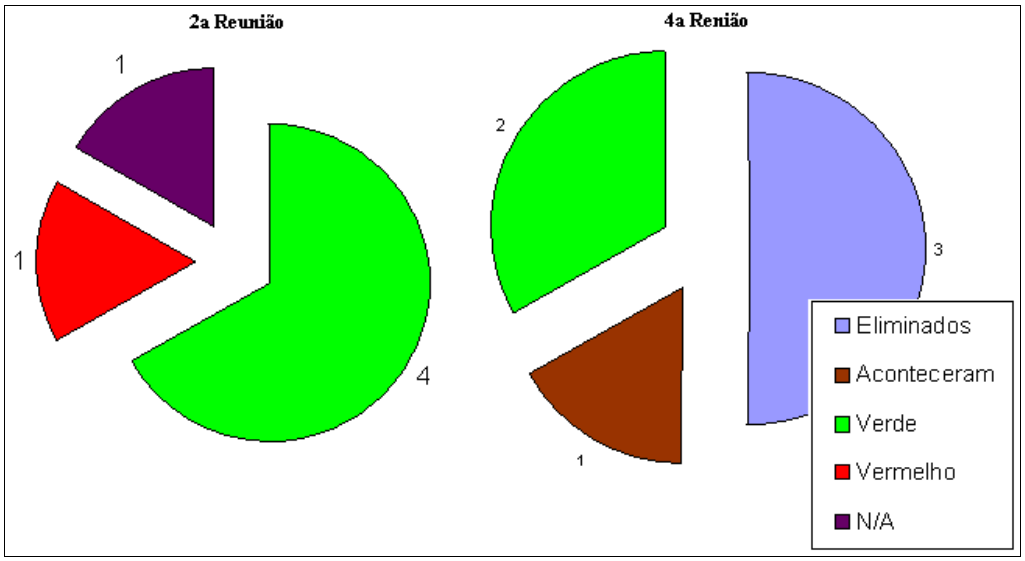

Figura 40 - Resultado das ações da gerência de riscos

Foi feita uma revisão da taxonomia de riscos adotada pela organização, e foi consenso que todas as categorias e fontes de riscos deveriam ser mantidas na taxonomia da organização. A Tabela 34 apresenta a taxonomia atualizada.

Tabela 34 - Taxonomia de Riscos da VendeSoft

Taxonomia de riscos da organização					
Categoria	**Fonte de Risco**	**Justificativa**	**Técnicas de tratamento de riscos**	**Limites para monitoração**	**Procedimento de medição**
Equipe	Problemas em utilizar novas tecnologias em projetos [OLIVEIRA06]	Falta de profissionais na equipe treinados com habilidades para utilização de novas tecnologias	Transferência de conhecimento; treinamento; consultoria; contratação de profissionais com experiência.	Caso após a 1 semana, a habilidade de 50% dos membros da equipe são avaliadas insuficientes.	Avaliação subjetiva da habilidade dos funcionários baseado no acompanhamento feito por outro trabalhador com experiência por 2 horas/dia [suficiente, insuficiente].
Cronograma	Falta ou insuficiência de tempo para assegurar a implementação das mudanças [OLIVEIRA06]	Os projetos podem possuir um curto prazo para entrega; a equipe pode não se sentir confiante em atingir a meta de prazo.	Estimativa de cronograma detallhada, desenvolvimento incremental, re-utilização de software e limpeza dos requisitos	Caso o cronograma geral esteja atrasado em 2 dias;	Resultado da diferença de dias entre o cronograma planejado em relação ao cronograma realizado para o dia da avaliação.
Integração entre Sistemas	Necessidade de integração com outros sistemas pode afetar desempenho do sistema original [THOMSETT03]	Os produtos desenvolvidos podem necessitar de integração com outros sistemas.	Revisão da documentação do sistema atual; Contratação de especialista; *Benchmark* do sistema atual após integração.	Caso o *Benchmark* do sistema atual mostra principais queries com perda de 15% de desempenho.	Resultados dos testes de *benchmark* com as principais queries do sistema definidas pelo analista sênior [Passou, não passou].
Equipe	Falta de Disponibilidade dos membros da equipe [THOMSETT03] [JONES94]	Possibilidade de saída dos estagiários e funcionários no meio dos projetos. Dispensas por férias ou atrasos.	Horas extras; contratação de trabalhadores temporários; contratação de estagiários; aumento salarial; oferecer incentivos extras; reuniões para obtenção de *feedback*.	Mais de um funcionário de um projeto em férias; Média de ausência dos funcionários superior a 2 horas por semana;	Quantidade de horas de atraso (sem justificativa) do funcionário.
Fornecedores	Componentes externos adquiridos podem estar abaixo da expectativa [BOEHM91] [JONES94]	Possibilidade de aquisição de componentes de terceiros	Desenvolvimento de um contrato por um advogado; Análise de desempenho; Checar as referências do fornecedor.	Componente entregue não atender ao requisito com base em testes de desempenho abaixo de 10% do desejado (requisito) e menos de 100% dos testes de funcionalidade não atendidos após 10 testes realizados ao integrar o componente ao sistema;	Resultado dos testes de *benchmark* [passou, não passou]; Resultado dos testes de integração realizado pelo testador [Passou, não passou].
Equipe	Falta de Experiência com o modelo de processo da organização [DIR06]	Possibilidade dos funcionários não estarem preparado para o modelo de	Acompanhamento das atividades; Exigência dos produtos de saída;	Caso a quantidade diária de artefatos produzidos fora dos padrões do processo seja superior a 10;	Quantidade de artefatos produzidos fora do padrão (defeito).

Taxonomia de riscos da organização					
Categoria	**Fonte de Risco**	**Justificativa**	**Técnicas de tratamento de riscos**	**Limites para monitoração**	**Procedimento de medição**
		processo da empresa	Treinamento; Reuniões diárias de status;		
Integração entre Sistemas	Documentação inexistente [OLIVEIRA06]	Possibilidade de integração com outros sistemas que não possuem documentação	Contratação de consultoria dos desenvolvedores originais;	Caso não existir documentação para menos de 70% das funções	Avaliação da documentação por função do sistema [Tem = 100%, parcial = 50%, não tem = 0%]
Equipe	Ambiente Físico / de Suporte para o time [THOMSETT04]	Computadores ou ambiente podem não ser adequados para as atividades do time	Investimento em computadores, cadeiras, mesas, luz etc.	Reclamação de mais de 50% da equipe sobre os aspectos físicos da organização	Avaliação realizada por cada um dos membros da equipe [Ruim – 0%, bom = 50%, ótimo = 100%]

Também foi acordado que nenhuma mudança nos parâmetros ou na estratégia da gerência de risco deveria ser feita. A empresa ainda dispõe dos mesmos recursos para a gerência de risco, tal como planejado na 1ª iteração.

A segunda etapa da atividade de gerência de riscos é a avaliação de todos os riscos levantados. Como o projeto foi concluído, o registro de riscos foi armazenado no RCO da organização. As lições aprendidas deste projeto serão bastante úteis para outros projetos da organização.

Tabela 35 - Lições aprendidas no projeto

Lições Aprendidas			
Id Risco	**Risco (Se.. Então...)**	**Aconteceu?**	**Lição Aprendida**
5	Se os estagiários saírem da organização no meio do projeto, Então o projeto poderá sofrer atrasos, uma vez que os estagiários estão assumindo responsabilidades no projeto	Sim	Apenas obter o feedback não eficiente. É necessário que os estagiários assumam menos responsabilidades no projeto. Ter contatos com profissionais com experiência, antes do início do projeto, foi fundamental para resolver o problema, apesar do custo ter crescido.
6	Se o time não tiver habilidade com Java, Então é possível que o prazo estimado não seja cumprido, e que o sistema não seja elaborado com qualidade	Não	Barney se mostrou um excelente instrutor, e esta característica poderá ser usada quando for necessário trabalhar com outros projetos novamente.

Na terceira etapa da atividade de gerência de riscos, foi avaliado o progresso das atividades de tratamento de riscos. Apesar de não ter conseguido evitar o risco de o estagiário Tim sair do projeto, foi possível executar o plano de contingência conforme definido no plano de tratamento do risco. Foi consenso da equipe de riscos manter o tratamento de risco na taxonomia de riscos.

A Figura 41 e a Figura 42 apresentam o monitoramento de dois riscos apresentados neste exemplo, ao longo das 4 semanas de projeto.

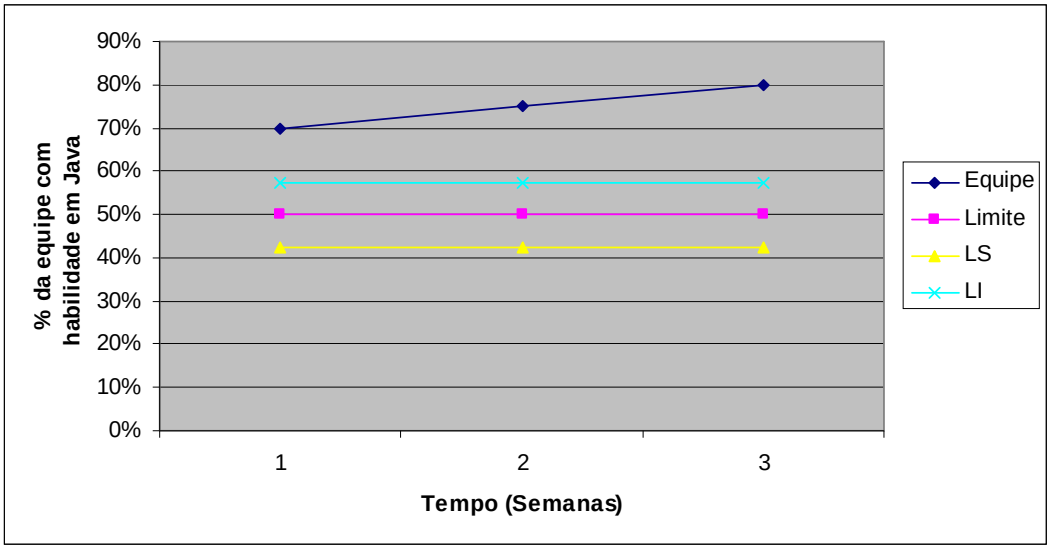

Figura 41 - Monitoramento do risco da equipe não ter habilidade com Java

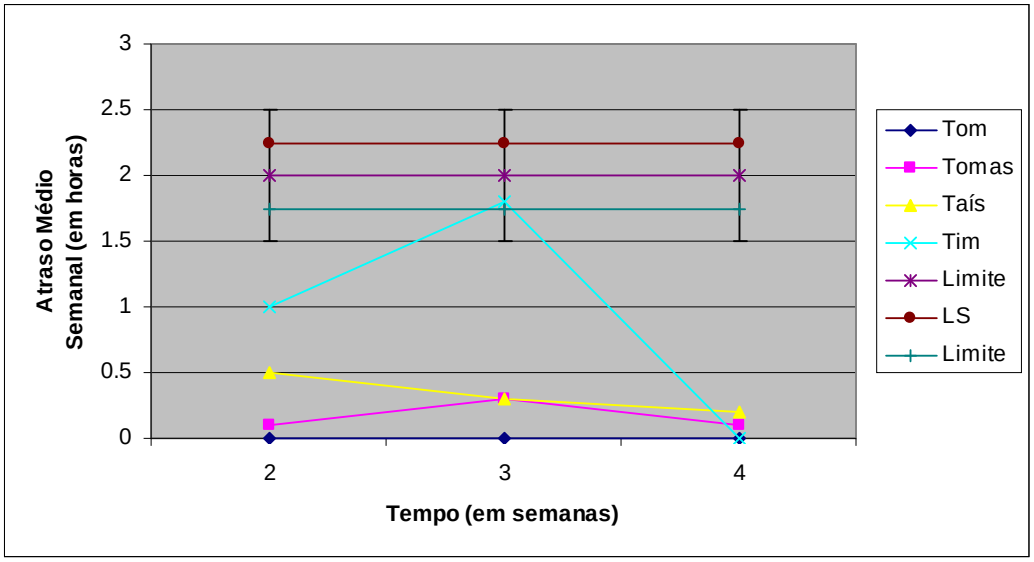

Figura 42 - Atraso médio (em horas) por semana dos estagiários

7 Conclusão

Com a implantação da gerência de riscos, a organização pode se capacitar a lidar com as incertezas que rondam o projeto, atuando de forma pró-ativa. Desta forma, evitando que os riscos se tornem realidade, e ações com um custo maior do que as ações de gerência de riscos tenham que ser disparadas.

Como foi visto no exemplo do capítulo 6, ao monitorar os limites, foram identificadas ações que poderiam ser disparadas para tratar os riscos: Treinamentos foram realizados pela própria organização, horas extras foram autorizadas para corrigir o atraso, testes de *benchmark* foram realizados identificando problemas previamente. Todas estas ações impediram que os riscos se tornassem realidade. Porém, mesmo com a gerência de risco, riscos podem se tornar realidade, tal como aconteceu na saída do estagiário. Neste caso, a gerência do projeto estava preparada, e uma solução alternativa foi encontrada, mesmo que tenha tido um custo maior do que o previsto no início do projeto. O importante é que o projeto foi entregue dentro do prazo estabelecido.

Também foi identificado que, apesar do CMMI-SE/SW identificar as boas práticas da gerência de riscos em seqüência, à medida que a gerência de riscos é realizada, não há necessidade de seguir a ordem exata destas atividades. Pode-se, por exemplo, fazer uma avaliação do progresso dos riscos, antes de decidir pela mudança de status da probabilidade e do impacto dos riscos.

As técnicas e métodos apresentados por este guia foram selecionados com base na simplicidade de execução destes métodos. Técnicas de *brainstorming*, *delphi* e taxonomias se mostraram mais adequadas à realidade das MPEs, por usarem um conhecimento já validado pelo mercado, e a medida que a gerência de riscos é realizada em diversos projetos, uma base de conhecimento da própria organização é gerada (taxonomias de risco, opções de tratamento de riscos etc.) e a experiência dos integrantes da equipe do projeto aumenta a cada projeto realizado, facilitando o consenso de opiniões em reuniões e a identificação e análise de novos riscos,.

Para avaliar a aplicabilidade deste guia na pratica estão previstos estudos de casos aplicando o guia na pratica e com base nisto o guia será continuamente melhorado.

Além disto, espera-se que este guia possa servir também como uma guia para desenvolvimento de uma ferramenta de gerência de riscos, que atenda a todos os requisitos levantados na análise de ferramentas (Capítulo 5).

Referências Bibliográficas

[AHERN03] AHERN, Dennis M.; CLOUSE, Aaron; TURNER, Richard. **CMMI Distilled: A practical Introduction to Integrated Process Improvement**. Second Edition. Person, 2003.

[BASILI94] BASILI, Victor R. CALDIERA, Gianluigi. ROMBACH, H. Dieter. **The Goal Question Metric Approach**. Encyclopedia of Software Engineering, Two Volume Set, New York City: John Wiley & Sons, 1994. Disponível em: <http://wwwagse.informatik.uni-kl.de/pubs/repository/basili94b/encyclo.gqm.pdf>. Acesso em: 19 Julho 2006.

[BOEHM91] BOEHM, Barry W. **Software Risk Management: Principles and Practices**. IEEE Software 8 (1):32-41, 1991.

[CARR93] CARR, Marvin. KONDA, Suresh; MONARCH, Ira. **Taxonomy-Based Risk Identification.** Technical Report CMU/SEI-93-TR-6 ESC-TR-93-183**,** SEI – Software Engineering Institute, Carnegie Mellon University, 1993.

[CS06] CS Solutions, Inc. **Risk+**. Disponível em: <http://www.cs-solutions.com/products/?Product=Risk%20Plus>. Acesso em: 25 Julho 2006.

[CSO06] Chief Security Officers. Enterprise Risk Assessment. Disponível em: <http://www.chiefsecurityofficers.com/era.htm>. Acesso em: 25 julho 2006.

[COLEMAN98] COLEMAN, Gerry; VERBRUGGEN, Renaat. **A quality software process for rapid application development.** Software Quality Journal 7: 107-122, 1998.

[COOPER04] COOPER, Dale; GREY, Stephen; RAYMOND, Geoffrey; WALKER, Phil. **Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements**. John Willey & Sons, 2004.

[DELL06] DELL Small Business. **Office Project 2003 Server CD w/ 5 CALs.** Disponível em: <http://accessories.us.dell.com/sna/productdetail.aspx?sku=A0157392&cs=04&c=us&l=en>. Acesso em: 24 Julho 2006.

[DIR06] DIR – Departament of Information Resources. **Generic Software Project Risk Factors**. Disponível em: <http://www.dir.state.tx.us/eod/qa/risk/swrisk.htm>. Acesso em: 21 Abril 2006.

[DORNER97]. DORNER, William W. **Using Excel for Data Analysis.** Quality Digest Outubro 1997. Disponível em: <http://www.qualitydigest.com/oct97/html/excel.html>. Acesso em: 19 Julho 2006.

[ENGERT99] ENGERT, Pamela A.; LANSDOWNE, Zachary F.; **Risk Matrix Users's Guide Version 2.2.** Bedford, Massachusetts, 1999.

[FREIRE02] FREIRE, Emerson. **Inovação e competitividade: O desafio a ser enfrentado pela indústria de software.** Campinas, 2002. Disponível em: <http://libdigi.unicamp.br/document/?code=vtls000242713>. Acesso em: 20 Julho 2006.

[GOLDPRACTICES06] DACS Gold Practices Website. **Software Acquisition Gold Practice Formal Risk Management.** Disponível em: <http://www.goldpractices.com/practices/frm/index.php>. Acesso em: 25 Julho 2006.

[HIGUEIRA96] HIGUERA, Ronald P.;HAIMES, Yacov Y. **Software Risk Management (CMU/SEI-96-TR-012)**. Pittsburgh, PA.: Software Engineering Institute, Carnegie Mellon University, 1996

[IRM02] IRM – UK Institute of Risk Management; AIRMIC – Association of Insurance and Risk Managers; ALARM – Association of Local Authority Risk Managers. **A Risk Management Standard**. 2002. Disponível em: <http://airmic.com/stats/track.asp?r=../Downloads/Pubs/AIRMIC_Risk-Management-Standard.pdf>. Acesso em: 25 Julho 2006.

[JONES04] JONES, Capers. **Assesment & Control of Software Risks**. Englewood Cliffs: Prentice-Hall, 1994.

[KASSE04] KASSE, T. **Practical Insight into the CMMI.** Ed. Artech House. Massachussets, 2004.

[KULPA03] KULPA, Margaret K.; JOHNSON, Kent A. **Interpreting the CMMI: A process Improvement Approach.** Auerbach Publications, 2003.

[KUNTZE06] KUNTZE, Guiton César. **Guia de Planejamento de Projeto de Software.** Trabalho de Conclusão de Graduação, São José, 2006.

[LEOPOLDINO04] LEOPOLDINO, Cláudio Bezerra. **Avaliação de Riscos em Desenvolvimento de Software.** Dissertação de Mestrado, Porto Alegre, 2004. Disponível em: <http://volpi.ea.ufrgs.br/teses_e_dissertacoes/td/002941.pdf>. Acesso em: 25 Julho 2006.

[LQPS06] LQPS. Laboratório de Qualidade e Produtividade de Software. 2006. Disponível em: <http://ssooweb04.univali.br>. Acesso em: 13/05/2006.

[MACHADO02] MACHADO, Cristina. A-RISK: Um método para identificar e quantificar risco de prazo em projetos de desenvolvimento de software. Dissertação de Mestrado, Curitiba, 2002.

[MARTENS01] MARTENS, Cristina. **A Tecnologia da Informação (TI) em Pequenas Empresas Industriais do Vale do Taquari/RS**. Porto Alegre, 2001. Disponível em: <http://professores.ea.ufrgs.br/hfreitas/projetos/gianti/arquivos/pequenas_empresas.pdf>. Acesso em: 21 Novembro 2005.

[MCT05] MCT. Ministério da Ciência e Tecnologia. **Qualidade e Produtividade no Setor de Software Brasileiro:** Resultados da pesquisa 2005. Disponível em: <http://www.mct.gov.br/sepin/Dsi/Quali2005/Public2005.htm>. Acesso em 26/08/2005.

[MICHAELIS02] MICHAELIS. **Moderno Dicionário da Língua Portuguesa.** São Paulo, Melhoramento, 1998.

[NATWICK03] NATWICK, Gary. **Integrated Metrics for CMMI and SW-CMM.** CrossTalk – The Journal of Defense Software Engineering, Maio 2003. Disponível em: <http://www.stsc.hill.af.mil/crosstalk/2003/05/natwick.html>. Acesso em: 04 Julho 2006.

[OLIVEIRA06] OLIVEIRA, Kathia M.; WEBSTER, Kênia P. B.; ANQUETIL, Nicolas. **Riscos para Manutenção de Software.** Artigo 2.22. Disponível em: <http://www.mct.gov.br/index.php/content/view/14515.html>. Acesso em: 25 Julho 2006.

[PMI04] PMI. Project Management Institute. **Guia PMBOK: Um guia do conjunto de conhecimentos em gerenciamento de projetos.** 2004. Disponível em: <http://www.pmi.org/info/default.asp>. Acesso em: 15/08/2005.

[MICROSOFT06] Microsoft Office Online. **MS Project 2003.** Disponível em: <http://office.microsoft.com/pt-br/FX010857951046.aspx>. Acesso em: 10 Julho 2006.

[PSM06] Practical Software and System Meaurement. **Practical Software Measurement: A foundation objective project management, v. 4.0b1.** Disponível em: <http://www.psmsc.com/PSMGuide.asp>. Acesso em: 19 Julho 2006.

[RADAR06] ICE - Integrated Computer Engineering. **Risk Radar.** Disponível em: <http://www.ascriskradar.com/Products.aspx?p=Products_RiskRadar>. Acesso em: 25 Julho 2006.

[RAMP03] Office of Information Technology Services. **RAMP – Risk Assessment Management Process**. North Carolina, USA, 2003.

[ROVERE01] ROVERE, R. L. **Perspectivas das micro, pequenas e médias empresas no Brasil. Revista Econômica Contemporânea.** UFRJ, 2001. Disponível em: <http://www.ie.ufrj.br/revista/pdfs/perspectivas_das_micro_pequenas_e_medias_empresas_no_brasil.pdf>. Acesso em: 21 Novembro 2005.

[ROUILLER01] ROUILLER, A. C. **Gerenciamento de Projetos de Software para Empresas de Pequeno Porte.** Tese de Doutorado, UFPE. 2001. Disponível em: <http://www.qualidadesoftware.org.br>. Acesso em: 11 Novembro 2005.

[RUBIK06] RUBIK, Rafael. **Guia para Medição e Análise de Projetos de Software em Micro e Pequenas Empresas Alinhado ao CMMI-SE/SW**. Trabalho de Conclusão de Graduação, São José, 2006.

[SILVEIRA06] SILVEIRA, Filipe P.; KNOB, Flávio F. **RiskFree – Uma ferramenta de apoio à gerência de riscos em projetos de software.** Trabalho de Conclusão de Graduação, Porto Alegre, 2005.

[SANTOS04] SANTOS, Cássio. **Gerência de Risco na Modernização de Sistemas Legados.** Dissertação de Mestrado, São Paulo, 2004. Disponível em: <http://www.pcs.usp.br/~lucia/teses/CassioSantos.pdf>. Acesso em: 25 julho 2006.

[SEI01] SEI. Software Engineering Institute. **CMMI for Systems Engineering/Software Engineering, Version 1.1 (CMMI-SE/SW, V1.1). Continuous Representation.** Dezembro, 2001.Disponível em: <http://www.sei.cmu.edu/cmmi>. Acesso em: 15 Agosto 2006.

[SEBRAE05] SEBRAE. Serviço Brasileiro de Apoio às Micro e Pequenas Empresas. **Boletim Estatístico de Micro e Pequenas Empresas**, 2005. Disponível em: <http://www.sebrae.com.br/br/mpe_numeros/empresas.asp>. Acesso em: 25 Julho 2006.

[SEBRAE06] SEBRAE. Serviço Brasileiro de Apoio às Micro e Pequenas Empresas. **Legislação Básica da Micro e Pequena Empresa**. Disponível em: <http://www.sebrae.com.br/br/aprendasebrae/estudosepesquisas_legislacao.asp>. Acesso em: 25 Julho 2006.

[SOMMERVILLE03] SOMMERVILLE, I. **Engenharia de Sotware.** São Paulo: Addison-Wesley, 2003.

[THOMSETT02] THOMSETT, Rob. **Radical Project Management.** Prentice Hall PTR, 2002.

[TRIMS06] BMP – Best Manufactoring Practices. **TRIMS - Technical Risk Identification and Mitigation System**. Disponível em: <http://www.bmpcoe.org/pmws/download/trims.html>. Acesso em: 09 Julho 2006.

Anexo A – Taxonomia de Riscos genérica para projetos de Software [DIR06]

Este taxonomia de riscos está disponível on-line no site do DIR – *Departament of Information Resources* [DIR06], e foi traduzida livremente pelo autor. Além desta taxonomia, o DIR disponibiliza outras taxonomias para projetos genéricos (inclusive não relacionados a software), projetos de aquisição de software e projetos de software desenvolvidos por terceiros.

O time do projeto deve usar essa tabela para facilitar pensar em riscos do projeto. O time pode decidir que fontes de riscos são relevantes ao projeto. E então identifica qual o nível do risco baseado nos indícios do risco.

Quando o projeto terminar, a organização deve revisar se há novas fontes de riscos a serem adicionadas, ou se há novos indícios que poderiam ser modificados para ajudar a outros projetos a identificar riscos.

		Indícios			Classificação				
#	Fontes de Risco	Baixo	Médio	Alto	Baixo	Médio	Alto	Não Aplicável	Notas
Missão e Objetivo									
1	Projeto é adequado a organização cliente	Diretamente suporta as missões e objetivos da organização cliente	Indiretamente impacta nos objetivos ou missão da organização cliente	Não suporta ou não está relacionado a organização cliente					
2	Projeto é adequado a organização patrocinadora	Diretamente suporta missões e objetivos da organização patrocinadora	Indiretamente impacta nos objetivos ou missão da organização patrocinadora	Não suporta ou não está relacionado a organização patrocinadora					
3	Percepção do cliente	Cliente espera que esta organização prove este	Organização que está trabalhando no projeto em uma area não esperada pelo	Projeto não está relacionado produtos ou serviços prioritários desta organização					
4	Fluxo de Trabalho	Pequena ou nenhuma mudança no fluxo de trabalho	Será mudado algum aspecto ou existirá um impacto pequeno no fluxo de trabalho	Significativamente muda o fluxo de trabalho ou os métodos da organização					
Gerenciamento do Programa									
5	Conflito de Objetivos	Objetivos dos projetos do programa são complementares e suportados pelo programa	Objetivos dos projetos não são conflitantes, porém oferecem pouco suporte ao programa	Objetivo dos projetos estão em conflito, direta ou indiretamente					

		Indícios			Classificação				
#	Fontes de Risco	Baixo	Médio	Alto	Baixo	Médio	Alto	Não Aplicável	Notas
6	Conflito de recursos	Projetos do programa compartilham recursos sem problema	Projetos do programa compartilham recursos com cuidados para evitar problemas	Projetos do programa frequentemente precisam dos mesmos recursos ao mesmo tempo, ou competem por estes recursos no mesmo orçamento					
7	Conflito com clients	Múltimos clients do programa possuem os mesmos interesses	Múltiplos clientes do programa tem necessidades diferentes, porém não há conflito	Múltiplos clientes do programa tentam direcionar o programa para direções distintas					
8	Liderança	Programa possui um gerente de programa ativo que coordenada o programa	Programa temuma pessoa ou um time responsável pelo programa, mas incapaz de gastar tempo suficiente para liderar efetivamente	Programa não tem líder, ou conceito de gerente de programa em uso					
9	Experiência do gerente do programa	Gerente do programa tem forte experiência no domínio	Gerente do programa tem experiência no domínio, e é capaz de conseguir respostas com especialistas	Gerente do programa é novo no domínio					
10	Definição do programa	Programa é bem definido, com um escopo gerenciável por esta organização	Programa é bem definido, porém incapaz de ser gerenciável por esta organização	Programa não é bem definido ou carrega objetivos conflitantes no próprio escopo					
Direção das decisões									
11	Influências políticas	Nenhuma decisão com influência política da organização foi tomada	Projeto tem muitas decisões motivas por influências políticas, tais como usar um fornecedor selecionado por razões polícas, ao invés de qualificações	Projeto tem uma variedade de influências políticas ou a maior parte das decisões são feitas em salas fechadas					

		Indícios			Classificação				
#	Fontes de Risco	Baixo	Médio	Alto	Baixo	Médio	Alto	Não Aplicável	Notas
12	Data conveniente	Data para entrega foi acertada por um processo razoável de comprometimento	Data está baseada na necessidade de estar alinhada a uma demonstração ao mercado, evento ou não está relacionado a uma estimativa técnica	Data está totalmente associada a uma demonstração ao mercado, evento ou outro marco deste tipo; pouca consideração à estimativa do time do projeto.					
13	Tecnologia atrativa	Tecnologia selecionada é usada por algum tempo	Projeto está sendo feito levando em consideração o aprendizado de uma nova tecnologia	Projeto está sendo feito para mostrar uma nova tecnologia ou como uma desculpa para trazer a tecnologia para dentro da organização					
14	Solução de curto prazo	Projeto tem necessidades de curto prazo, sem comprometer perspectivas de longo prazo	Projeto é focado em soluções de curto prazo para um problema, com pouco entendimento do que é necessário a longo prazo	Time do projeto explicitamente foi direcionado a ignorer perspectivas a longo prazo e focar em completar a entrega a curto prazo					
Gerência da Organização									
15	Estabilidade da organização	Pouca ou nenhuma mudança na gerênia ou estrutura é esperada	Alguma mudança de gerência ou reorganização é esperada	Gerência ou estrutura da organização está continuamente ou rapidamente mudando					
16	Papéis e responsabilidades da organização	Indivíduos da organização entendem seus papéis e responsabilidades e dos outros também	Indivíduos entendem seus papéis e responsabilidades, mas não possuem certeza de quem é responsável pelo trabalho de outros grupos	Muitos na organização não estão certos ou não tem conhecimento de quem é responsável pelas atividades na organização					
17	Políticas e padrões	Padrões e políticas de desenvolvimento são definidos e cuidadosamente seguidos	Padrões e políticas de desenvolvimento existem, mas são fracos, ou não são seguidos	Padrões e políticas não existem, ou são definidos de forma fraca, e não são usados					

		Indícios			Classificação				
#	Fontes de Risco	Baixo	Médio	Alto	Baixo	Médio	Alto	Não Aplicável	Notas
18	Suporte da gerência	Fortemente comprometida com o sucesso do projeto	Algum comprometimento, não total	Pouco ou nenhum suporte					
19	Envolvimento da direção	Visível e forte suporte	Suporte occasional, prove ajuda em questões quando perguntadas	Não há suporte visível, não há ajuda em questões não resolvidas					
20	Objetivos do projeto	Objetivos de projeto verificados, requisitos razoáveis	Alguns objetivos do projeto, medidas podem ser questionadas	Objetivos do projeto não estão estabelecidos ou objetivos não estão medidos					
Cliente/Usuário									
21	Envolvimento do usuário	Usuários estão altamente envolvidos com o time do projeto, fornecendo valiosas informações	Usuários participam de forma modesta, impacto moderado no sistema	Envolvimento do usuário mínimo ou nenhum envolvimento do usuário; pouca informação do usuário					
22	Experiência do usuário	Usuários com grande experiência em projetos imilares; possuem idéias especificas de como as necessidades podem ser atendidas	Usuários tem experiência em projetos similares e tem as necessidades em mente	Usuários não tem experiência em projetos imilares; não estão certos de como as necessidades podem ser atendidas					
23	Aceitação do usuário	Usuários aceitam conceitos e detalhes do sistema; processo está para ser aprovado pelos usuários	Usuários aceitam a maior parte dos conceitos e detalhes do sistema; processo está para ser aprovado pelos usuários	Usuários não aceitam nenhu conceito ou detalhes de design do sistema					
24	Necessidade de treinamento do usuário	Necessidade de treinamento do usuário considerada; trienamento em progresso ou plano existe user training	Necessidade de treinamento do usuário considerada; nenhum treinamento está sendo considerado ou nenhum plano foi desenvolvimento	Requisitos não identificados ou não endereçados					

		Indícios			Classificação				
#	Fontes de Risco	Baixo	Médio	Alto	Baixo	Médio	Alto	Não Aplicável	Notas
25	Justificativa do usuário	Justificativa do usuário é completa, acurada, clara	Justificativa do usuário foi dada, completa com algumas questões sobre aplicabilidade	Nenhuma justificativa satisfatória para o sistema					
Parâmetros do projeto									
26	Tamanho do projeto	Pequeno, não complexo, ou facilmente decomposto	Médio, complexidade moderada, pode ser decomposto	Grande, altamente complexo, ou não pode ser decomposto					
27	Restrições de Hardware	Poucas ou nenhuma restrição de hardware ou plataforma única imposta	Algumas imposições de restrição de hardware; várias plataformas	Imposições de restrições de hardware significativas; múltiplas plataformas					
28	Componentes reutilizáveis	Componentes disponíveis e compatíveis com a estratégia	Componentes disponíveis, mas precisam de alguma revisão	Componentes identificados, precisão de modificações sérias para serem usados					
29	Componentes fornecidos	Components disponíveis e diretamente usáveis	Componentes trabalham na maior parte das circustâncias	Componentes falham em certos casos, estão atrasados, ou incompatíveis com partes da estratégia					
30	Tamanho do orçamento	Orçamento alocado suficiente	Orçamento alocado questionável	Orçamento duvidável está disponível					
31	Restrições do orçamento	Fundos alocasdos sem restrições	Algumas questão sobre a disponibilidade dos fundos	Alocação em dúvida ou provavelmente irá mudar sem notícia prévia					
32	Controle de custos	Bem estabilizados, Existem	Sistema existe, fraco nas areas	Ausência de sistema ou não existe					
33	Comprometimento de entrega	Datas de comprometimento estáveis	Alguns comprometimentos incertos	Instáveis, comprometimentos flutuantes					
34	Desenvolvimento do cronograma	Time concorda que o cronograma é aceitável e pode ser cumprido	Time acha que uma fase do plano está bastante agressiva	Time concorda que duas ou mais fases do cronograma estão impossíveis de ser atingidas					

		Indícios			Classificação				
#	Fontes de Risco	Baixo	Médio	Alto	Baixo	Médio	Alto	Não Aplicável	Notas
Produto									
35	Estabilidade dos requisitos	Pouca ou nenhuma mudança é esperada ao projeto aprovado (baseline)	Alguma mudança é esperada em relação ao baseline definido	Muitas mudanças ou baseline definida sem acordo					
36	Requisitos completos e claros	São completamente especificados e claramente escritos	Alguns requisitos são incompletos ou não são claros	Alguns requisitos estão apenas na cabeça do cliente					
37	Testabilidade	Requisitos do produto são fáceis de testes, planos de teste estão a caminho	Parte do produto é dificil de teste, ou pouco plano está sendo feito	Maior parte do produto é dificil de teste, ou nenhum plano está sendo feito					
38	Dificuldade de Design	Interfaces bem definidas; design bem entendido	Incerteza de como elaborar o design, ou aspectos do design ainda precisam ser definidos	Interfaces não estão definidas ou controladas; tendem a mudar					
39	Dificuldade de implementação	Algoritimos e design são razoáveis para o time implementer	Algoritimos e/ou design tem elementos que são dificeis para o time implementar	Algoritimos e/ou design tem componentes que este time terá dificuldade de implementar					
40	Dependências do sistema	Dependência de outras partes do sistema e da esforço de software (hardware, mudanças de processo, documentação, ...) estão claramente definidas	Alguns elementos do sistema estão bem entendidos e planejados; outros ainda não são compreendidos	Nenhum plano claro ou prazo para integrar o sistema inteiro					
									Implantação
41	Recursos de hardware para implantação	Maduros, sistema com capacidade de crescimento, flexível	Disponível, alguma capacidade de crescimento	Sem possibilidade crescimento, ou flexibilidade					
42	Resposta a outros fatores de desempenho	Rapidamente se adapta aos limites necessários; análises foram feitas	Opera ocasionalmente nos limites	Opera continuamente nos níveis de limite					

		Indícios			Classificação				
#	Fontes de Risco	Baixo	Médio	Alto	Baixo	Médio	Alto	Não Aplicável	Notas
43	Impacto no service do cliente	Requer pouca mudança ao service do cliente	Requer algumas mudanças ao service do cliente	Requer grandes mudanças à estratégia do serviço do cliente ou aos produtos oferecidos					
44	Migração de dados requerida	Pouco ou nenhum dado precisa ser migrado	Muitos dados para serem migrados, mas descrições da estrutura e do uso estão disponíveis	Muitos dados para serem migrados; muitos tipos de bases de dados ou não há boas descrições de onde está o que					
45	Plano piloto	Lugar ou time para plano piloto está disponível e interessado em participar	Plano piloto precisa ser feito com vários lugares (interessados em participar) ou com um que precisa de muita ajuda	Os lugares disponíveis não são cooperativos ou já estão em crise					
46	Interfaces externas de hardware e software	Pouca ou nenhuma integração ou interface necessária	Alguma integração ou interface necessária	Interface extensivas requeridas					
Processo de Desenvolvimento									
47	Análise de alternative	Análise de alternativas completa, todas consideradas, suposições verificadas	Análise de alternativas completa, algumas suposições questionáveis ou alternativas não foram completamente consideradas	Análise não está completa, nem todas as alternativas foram consideradas, ou suposições com defeitos					
48	Processo de comprometimento	Mudanças de comprometimentos em escopo, conteúdo, prazo são revisadas e aprovadas pelos envolvidos	Mudanças aos comprometimentos são comunicadas a todos os envolvidos	Mudanças aos comprometimentos são feitas sem revisão ou envolvimento do time					
49	Abordagem de Garantia de Qualidade	Sistema de Garantia de Qualidade estabilizado, seguido, efetivo	Procedimentos estabelecidos, mas não são seguidos ou efetivados	Não há processo de garantia de qualidade ou procedimentos estabelecidos					
50	Documentação de desenvolvimento	Correta e disponível	Algumas deficiencias, mas disponível	Não existe					

		Indícios			Classificação				
#	Fontes de Risco	Baixo	Médio	Alto	Baixo	Médio	Alto	Não Aplicável	Notas
51	Uso de um processo de engenharia definido	Processo de Desenvolvimento existe, estabiilizado, efetivo, seguido por um time	Processo estabelecidos, mas não é seguido ou não é efetivo	Nenhum processo formal é usado					
52	Identificação prévia de defeitos	peer reviews são feitas	peer reviews são usadas esporadicamente	Time espera que os defeios sejam encontrados durante a fase de testes					
53	Rastreamento de defeitos	Rastreamento de defeitos definido, consistente e efetivo	Processo de Rastreamento de defeitos definido, porém usado de forma inconsistente	Nenhum processo existe para rastrear defeitos					
54	Controle de mudanças para produtos de trabalho	Processo de controle de mudanças formal existe, seguido, efetivo	Proceso de controle de mudanças existe, mas não é seguido ou não é efetivo	Nenhum processo de controle de mudanças é usado					
Ambiente de desenvolvimento									
55	Facilidades físicas	Pouca ou nenhuma modificação necessária	Alguma modificação necessárial; algumas existents	Várias modificações necessárias, ou facilidades não existentes					
56	Plataforma de hardware	Estável, nenhuma mudança esperada, capacidade é suficiente	Algumas mudanças estão evoluindo, mas controladas	Plataforma sendo desenvolvida junto com o software					
57	Disponibilidade de ferramentas	Existem, documentadas, validadas	Disponível, validada, algum desenvolvimento necessário (ou pouca documentação)	Não estão validadas, proprietárias ou muito desenvolvimento necessário; não há documentação					
58	Suporte do fornecedor	Suporte complete por um preço razoável, e no tempo necessário	Suporte adequado ao preço contratado, tempo de resposta adequado	Pouco ou nenhum suporte, alto custom, e/ou tempo de resposta não adequado					
59	Adequabilidade do contrato	Contrato com o cliente tem bons termos, comunicação com o time é boa	Contrato tem algumas questões em aberto que poderiam interromper esforços de trabalho do time	Contrato tem requisitos incômodos ou que causam trabalho extra para estar em conformidade					
60	Recuperação de desastre	Todas as áreas seguem diretrizes de segurança; backup de dados	Algumas medidas de segurança existe; backups são feitos;	Nenhuma medida de segurança existe; não há backup;					

		Indícios			Classificação				
#	Fontes de Risco	Baixo	Médio	Alto	Baixo	Médio	Alto	Não Aplicável	Notas
		são feitos; sistema de recuperação de desastre existe; procedimentos são seguidos; all areas following security guidelines; data backed up; disaster recovery system in place; procedures followed	recuperação de desastre considerada, mas há ausência de procedimentos ou não são seguidos	recuperação de disastre não considerada.					
Gerência de Projeto									
6 1	Abordagem de Gerência de Projeto	Planejamento de produto e processo e monitoração existem	Planejamento e monitoração precisam de melhorias	Planejamento ou monitoração fraca ou não existente					
6 2	Comunicação da gerência de projeto	Claramente comunica objetivos e status entre o time e o resto da organização	Comunica alguma das informações algumas vezes	Raramente comunica claramente com o time ou com os outros que precisam ser informados sobre o status do time					
6 3	Experiência da gerência de projeto	Gerência de projeto muito experiente em projetos similares	Gerência de projeto tem uma experiência moderada ou tem experiência com diferentes tipos de projeto	Gerência de projeto não tem experiência com este tjpo de projeto ou é novo na gerência de projetos					
6 4	Atitude da gerência de projeto	Fortemente comprometida com o sucesso do projeto	Interessada em fazer o que é necessário	Não se preocupa muito com o projeto					
6 5	Autoridade da gerência de projeto	Tem uma linha de gerenciamento ou autoridade official que permite a efetividade da liderança de projeto	Tem a possibilidade de influenciar os indivíduos, baseando-se nas relações pessoais	Tem pouca autoridade na estrutura da organização, e pouco poder pessoal para influenciar decisões e recursos					
6 6	Suporte a gerência de projeto	Suporte completo do time	Suporte da maior parte do time, com algumas reservas	Nenhum suporte visível, gerente apenas no nome					
Time do projeto									

		Indícios			Classificação				
#	Fontes de Risco	Baixo	Médio	Alto	Baixo	Médio	Alto	Não Aplicável	Notas
67	Disponibilidade dos membros do time	Existe, poucas mudanças esperada; poucas interrupções para "apagar fogo"	Disponível, alguma mudança esperada; algum "apagar fogo" esperado;	Alta mudança esperada, não está disponível; time gasta a maior parte do tempo em apagar fogo.					
68	Conjunto de habilidades do time	Bom conjunto de disciplinas	Algumas disciplinas representadas de forma inadequada	Algumas disciplinas não são representadas					
69	Experiência na aplicação	Experiência extensive no time em projetos como este	Alguma experiência em projetos similares	Pouca ou nenhuma experiência em projetos similares					
70	Experiência com hardware e software do projetos	Alta experiência	Média experiência	Baixa experiência					
71	Experiência com o processo	Experiência extensive com o processo	Alguma experiência com o processo ou extensive experiência com outro processo	Pouca ou nenhuma experiência com um processo definido					
72	Treinamento do time	Plano de treinamento existe, treinamento está sendo realizado	Treinamento de algumas áreas não está disponível, ou treinamento planejado para o futuro	Nenhum plano de treinamento ou treinamento está disponível					
73	Espírito e atitude do time	Fortemente comprometido com o sucesso do projeto; cooperativo	Interessado em fazer o que é necessário ser feito para o trabalho ser completado.	Pouco ou nenhum comprometimento no projeto; não é um time coeso					
74	Produtividade do time	Todos os marcos foram atendidos, entregas no tempo certo, produtividade alta	Marcos atendidos, alguns atrasos nas entregas, produtividade aceitável	Produtividade baixa, marcos não atendidos, atrasos nas entregas					
75	Experiência no domínio (área da aplicação)	Time com bom background com o domínio da aplicação	Alguma experiência com o domínio no time, ou habilidade em chamar especialistas quando	Nenhuma experiência no domínio no time, nenhuma disponibilidade de especialistas					

		Indícios			Classificação				
#	Fontes de Risco	Baixo	Médio	Alto	Baixo	Médio	Alto	Não Aplicável	Notas
			necessário						
Tecnologia									
76	Tecnologia aplicada ao projeto	Tecnologia planejada para o projeto foi bem aplicada as necessidades do cliente e ao problema	Alguma da tecnologia aplicada não é adequada ao problema ou cliente	Tecnologia seleciona não é adequada ao cliente ou ao problema					
77	Experiência do time com a tecnologia	Bom nível de experiência do time com a tecnologia	Alguma experiência com a tecnologia	Nenhuma experiência com a tecnologia					
78	Disponibilidade de um especialista na tecnologia	Especialistas na tecnologia estão disponíveis	Especialistas disponíveis em outros locais da organização	Será necessário conseguir ajuda com especialistas fora da organização					
79	Maturidade da tecnologia	Tecnologia vem sendo utilizada na indústria por algum tempo	Tecnologia é bem entendida na indústria	Tecnologia é de ponta					
Manutenção									
80	Complexidade de design	Estruturalmente mantido (baixa complexidade medida ou projetada)	Alguns aspectos são difíceis de manter (complexidade média)	Dificuldade extrema de manter (alta complexidade)					
81	Suporte de pessoal	Existe, com experiência, número suficiente	Falta algumas áreas de conhecimento	Área de conhecimento significante está faltando					
82	Suporte do fornecedor	Suporte completo, em um preço razoável, e em um tempo adequada	Suporte adequada por um preço contratado, e um tempo de resposta aceitável	Pouco ou nenhum suporte, alto custom, e tempo de resposta não aceitável					

Anexo B – Taxonomia de riscos baseada em questionário [CARR93]

Esta taxonomia é apresentada no artigo “Taxonomy-Base Risk Identification” [CARR93] e foi traduzida livremente e adaptada pelo autor deste trabalho. Esta taxonomia foi criada pela SEI e serve como um método para facilitar a identificação sistemática de riscos em um projeto de software, por meio de um questionário. As respostas ajudam o time do projeto a identificar as fontes de risco do projeto.

A. Engenharia do produto

Aspectos técnicos do trabalho a ser realizado

1. Requisitos

a. Estabilidade

[Os requisitos estão mudando à medida que o produto está sendo produzido?]

[1] Os requisitos são estáveis?

(Não) (1.a) Qual é o efeito no sistema?

• Qualidade

• Funcionalidade

• Cronograma

• Integração

• Design

• Teste

[2] Interfaces externas estão mudando?

b. **Completos**

[Existem requisitos ausentes ou especificados de forma incompleta?]

[3] Existe algum requisito a ser definido?

[4] Existem requisitos que deveriam estar na especificação mas não estão?

(Sim) (4.a) Você é capaz de incluir estes requisitos no sistema?

[5] O cliente tem requisitos não escritos ou esperados?

(Sim) (5.a) Existe alguma forma de capturar estes requisitos?

[6] As interfaces externas estão completamente definidas?

c. **Clareza**

[Os requisitos não são claros ou precisam de interpretação?]

[7] Você é capaz de incluir entender estes requisitos da forma que foram escritos?

(Não) (7.a) As ambiguidades estão sendo resolvidas de forma satisfatória?

(Sim) (7.b) Não existe problemas de ambiguidade ou problemas de interpretação?

d. **Validade**

[Os requisitos direcionam para o produto que o cliente tem em mente?]

[8] Existe algum requisito que pode não especificar o que o cliente realmente quer?

(Sim) (8.a) Como você está resolvendo isso?

[9] Você e o cliente entendem a mesma coisa sobre os requisitos?

(Sim) (9.a) Existe um processo para determiner isso?

[10] Como você valida estes requisitos?

• Prototipação

• Análise

• Simulação

e. Implementável
[Requisitos são implementáveis a partir de uma visão analítica?]

[11] Existe algum requisito que é dificil tecnicamente de implementar?

(Sim) (11.a) Quais são eles?

(Sim) (11.b) Porque elas são difíceis de implementar?

(Não) (11.c) Foram feitos estudos de viabilidade para estes requisitos?

(Sim) (11.c.1) O quanto confidente você está a respeito das questões feitas nestes estudos?

f. Histórico

[Os requisitos especificam algo nunca feito anteriormente, ou antes, ou que a sua organização não tenha feito antes?]

[12] Existe algum requisito do tipo “estado da arte” (Tecnologias, métodos, linguagens, hardware)?

(Não) (12.a) Algum destes é novo para você?

(Sim) (12.b) O programa tem conhecimento suficiente nestas áreas?

(Não) (12.b.1) Existe um plano de aquisição destas conhecimentos nestas áreas?

g. Grau de Dificuldade
[Os requisitos especificam um produto maior, mais complexo, ou requerem uma organização maior do que na experiência da companhia?]

[13] O tamanho e a complexidade do sistema é uma preocupação?

(Não) (13.a) Você já fez algo deste tamanho e complexidade antes?

[14] O tamanho requer uma organização maior que o usual para a sua empresa?

2. **Design**

a. Funcionalidade
[Existem problemas em potencial em atingir os requisitos de funcionalidade?]

[15] Existe algum algoritmo que pode não satisfazer os requisitos?

(Não) (15.a) Algum dos algoritmos ou designs que não respeitem os requisitos?

[16] Como você determina a implentabilidade dos algoritmos e designs?

• Prototipação

• Modelagem

• Análise

• Simulação

b. Dificuldade
[O design e a implementação serão difíceis de ser alcançados?]

[17] Algum design depende de suposições realisticas ou otimistas?

[18] Existe algum requisito ou função que são difíceis de realizar o design?

(Não) (18.a) Você tem soluções para estes requisitos?

(Sim) (18.b) Quais são os requisitos?

• Porquê eles são difíceis?

c. Interfaces
[Existe interfaces internas (hardware and software) bem definidas e controladas?]

[19] As interfaces internas são bem definidas?

• Software-para-software

• Software-para-hardware

[20] Existe um processo para definir estas interfaces internas?

(Sim) (20.a) Existe um processo de controle de mudança para interfaces internas?

[21] O hardware está sendo desenvolvido em paralelo com o software?

(Sim) (21.a) Existem especificações de hardware mudando?

(Sim) (21.b) Todas as interfaces com software foram definidas?

(Sim) (21.c) Existirão modelos de design que podem ser usados para testar o software?

d. Desempenho
[Existe uma exigência rigorosa de tempo de resposta ou taxa de transmissão?]

[22] Existem problemas com desempenho?

• Taxa de transmissão

• Programa eventos de tempo real assincronos;

• Resposta em tempo real;

• Tempo de recuperação;

• Tempo de resposta;

• Resposta, contenção ou acesso ao banco de dados

[23] Análise de desempenho foi feita?

(Sim) (23.a) Qual é o seu nível de confiança na análise de desempenho?

(Sim) (23.b) Você tem um modelo para rastrear o desempenho no design e na implementação?

e. Testável
[É possível ou impossível testar o produto?]

[24] O software sera fácil de ser testado?

[25] O design inclue facilidades para ajudar no teste?

[26] Os testadores estão envolvidos na análise de requisitos?

f. Restrições de hardware
[Existem restrições fortes no hardware a ser utilizado?]

[27] O hardware limita sua habilidade de alcançar requisitos?

• Arquitetura

• Capacidade de Memória

• Taxa de transmissão

• Resposta em tempo real

• Tempo de resposta

• Tempo de recuperação

• Desempenho do banco

• Funcionalidade

• Confiança

• Disponibilidade

g. Softwares de terceiros
[Existe problemas com softwares usados pelo programa, mas não foram desenvolvidos pelo programa?]

Se software reutilizado ou refeito existe...

[28] Você está usando software reutilizável ou refeito não desenvolvido pelo programa?

(Sim) (28.a) Você prevê algum problema?

• Documentação

• Desempenho

• Funcionalidade

• Entrega a tempo

• Customização

Se software COTS está sendo usado...

[29] Existe algum problema em usar software COTS (commercial off-the-shelf)?

• Documentação insuficiente para determinar interfaces, tamanho ou desempenho

• Pouca documentação

• Requer uma grande quantidade de memória para armazenamento

• Dificuldade de realizar interfaces com a aplicação

• Não foi totalmente testado

• Possui problemas (bugs)

• Não é mantido de forma adequada
• *Resposta do vendedor lenta*

[30] Você prevê algum problema em integrar atualizações ou revisões do software COTS?

3. **Codificação e teste de unidade**

a. Implemenável
[A implementação do design é difícil ou impossível?]

[31] Existe alguma parte da implementação do produto não completamente definida pelo design?

[32] Os algoritimos selecionados e o design são fáceis de implementar?

b. Testes
[O nível e o tempo para os testes de unidade está adequado?]

[33] Você começa os testes de unidade antes de verificar o código em relação ao design?

[34] Testes de unidades suficientes foram especificados?

[35] Existe tempo suficiente para executar todos os testes de unidade que você esta pensando em realizar?

[36] Caso exista problems de prazo, compromissos futuros serão feitos em relação aos testes de unidade?

c. Codificação/Implementação
[Existe algum problema com codificação ou implementação?]

[37] As especificações de design possuem detalhes suficiente para escrever o código?

[38] O design está sendo alterado enquanto o código está sendo feito?

[39] Existem limitações que fazem com que o código seja difícil de escrever?

• Tempo de resposta

• Memória

• Armazenamento externo

[40] A linguagem é adequada para produzir o software neste programa?

[41] Existem múltiplas linguagens usadas neste programa?

(Sim) (41.a) Existe compatibilidade de interface entre os códigos produzidos pelos diferentes compiladores?

[42] O computador de desenvolvimento o mesmo que o computador que será usado em produção?

(Não) (42.a) Existem diferenças de compiladores entre os dois?
Se hardware produzido pelo programa está sendo usado...

[43] As especificações de hardware adequadas para codificar o software?

[44] As especificações de hardware estão mudando enquanto o código está sendo escrito?

4. Integração e teste

a. Ambiente
[O ambiente de teste e integração adequado?]

[45] Existirá hardware suficiente para realizar a integração e o teste de forma adequada?

[46] Existe algum problema em crier cenários realisticos e testar os dados para demonstrar algum

requisito?

• Tráfego de dados especificado

• Resposta de tempo real

• Tratamento de eventos assíncronos

• Interação multi-usuário

[47] Você é capaz de verificar o desempenho com facilidade?

[48] Hardware ou software facilita o teste?

(Sim) (48.a) É o suficiente para todos os testes?

b. Produto
[A definição da interface é inadequada, facilidades inadequadas ou tempo insuficiente?]

[49] O hardware especificado para produção estará disponível quando necessário?

[50] Critérios de aceitação foram acordados para todos os requisitos?

(Sim) (50.a) Existe um acordo formal?

[51] As interfaces externas estão definidas, documentadas e indicadas na baseline?

[52] Existem algum requisito que sera difícil de testar?

[53] Suficientes integrações do produto foram especificadas?

[54] Tempo adequado foi alocado para integração do produto ou teste?
Se COTS...

[55] Os dados do fornecedor serão aceitos na verificação de requisitos alocados para produtos COTS?

(Sim) (55.a) O contrato está claro em relação a isto?

c. Sistema
[A integração de sistema está não coordenada, com pouca definição de interfaces, ou facilidades inadequadas?]

[56] Integrações de sistema suficiente foram especificadas?

[57] Tempo necessário foi alocado para integração e teste de sistema?

[58] Todos os contratados fazem parte do time de integração?

[59] O produto será integrado a um sistema existente?

(Sim) (59.a) Existe um período paralelo de paralização deste sistema?

(Não) (59.a.1) Como você irá garantir que o produto irá funcionar de forma correta quando integrado?

[60] A integração do sistema acontecerá na organização do cliente?

5. **Especialidades da Engenharia**

a. Manutenibilidade
[A implementação sera dificil de entender ou manter?]

[61] A arquitetura, design ou código criam alguma dificuldade de manutenção?

[62] Existem pessoas de manutenção envolvidas logo no início do design?

[63] A documentação do produto é adequada para manutenção por uma organização externa?

b. Confiança
[Os requisitos de confiança e disponibilidade são difíceis de ser alcançada?]

[64] Requisitos de confiança foram incorporados ao software?

[65] Requisitos de disponibilidade foram incorporados ao software?

(Sim) (65.a) Há problemas de tempo de recuperação?

c. Proteção contra falha
[Os requisitos de proteção contra falha não são implementáveis ou não são demonstrados?]

[66] Os requisitos de proteção contra falha foram incorporados ao software?

(Sim) (66.a) Você vê alguma dificuldade em alcançar os requisitos de proteção contra falha?

[67] Será difícil verificar a satisfação dos requisitos de proteção contra falha?

d. Segurança de acesso
[Os requisitos de segurança de acesso são mais rigorosos do que a prática ou experiência do programa?]

[68] Existe requisitos de segurança de acesso sem precedência?

[69] Este é um sistema “Orange Book”?

[70] Você já implementou este nível de segurança antes?

e. Fatores humanos
[Este sistema sera difícil de ser usado por causa de uma interface homem-máquina mal definida?]

[71] Você vê dificuldade em alcançar os requisitos de fatores humanos?

(Não) (71.a) Como você está garantindo que você irá alcançar os requisitos de fatores humanos?

Se estiver sendo feita uma Prototipação...

(Sim) (71.a.1) É um protótipo “throw-away”?

(Não) (71.a.1a) Está sendo feito desenvolvimento evolucionário?

(Sim) (71.a.1a.1) Você tem experiência com este tipo de desenvolvimento?

(Sim) (71.a.1a.2) Existem versões intermediárias *disponíveis* para entrega?

(Sim) (71.a.1a.3) Isto complica o controle de mudança?

f. Especificações
[A documentação é adequada para elabora o design, implementer, e testar o sistema?]

[72] As especificações dos requisitos de software adequadas para o design do sistema?

[73] As especificações de hardware são adequadas para o design e implementação do software?

[74] Os requisitos de interfaces externas estão bem especificados?

[75] As especificações de teste são adequadas para testar totalmente o sistema?
Se está ou passou da fase de implementação...

[76] As especificações de design são adequadas para implementar o sistema?

• interfaces internas

B. **Ambiente de desenvolvimento**

1. **Processo de desenvolvimento**

a. Formalidade
[A implementação será difícil de entender ou manter?]

[77] Está sendo usado mais de um modelo de desenvolvimento?

• Espiral

• Cascata

• Incremental
(Sim) (77.a) Coordena-los é um problemas?

[78] Existem planos formais e controlados para todas as atividasdes de desenvolvimento?

• Análises de requisitos

• Design

• Codificação

• Integração e teste

• Instalação

• Garantia de qualidade

• Gerência de configuração

(Sim) (78.a) Os planos especificam bem o processo?

(Sim) (78.b) Os desenvolvedores são familiar com o plano?

b. Adequabilidade
[O processo é adequado para o modelo de desenvolvimento escolhido, ex., espiral, prototipação?]

[79] O processo de desenvolvimento é adequado para este produto?

[80] O processo de desenvolvimento é suportado por um conjunto de procedimentos, métodos, e ferramentas compatíveis?

c. Controle do Processo
[O processo de desenvolvimento e software é cumprido, monitorado, e controlado usando métricas? Locais distribuídos de desenvolvimento são coordenados?]

[81] Todos seguem o processo?

(Sim) (81.a) Como isto é garantido?

[82] Você pode medir quando o processo de desenvolvimento está alcançado seus objetivos de qualidade e produtividade?

Se existe locais distribuídos de desenvolvimento...

[83] Existe coordenação adequada entre os locais distribuídos de desenvolvimento?

d. Experiência
[Os membros do projeto possuem experiência de uso do processo? O processo é entendido por todos os membros?]

[84] As pessoas estão confortáveis com o processo de desenvolvimento?

e. Controle de produto
[Existem mecanismos para controlar as mudanças no produto?]

[85] Existem mecanismos de rastramento de requisitos que rastreiam requisitos da especificação da fonte até os casos de testes?

[86] Este mecanisco de rastreabilidade é usado para avaliar a análise de impacto nas mudanças de requisitos?

[87] Existe um processo de controle formal?

(Sim) (87.a) Este processo cobre todas as mudanças os requisitos, design, código e documentação do baseline?

[88] As mudanças, em qualquer nível, são mapeadas para o nível de sistema e para o nível de testes?

[89] Existe análise adequada quando novos requisitos são adicionados ao sistema?

[90] Você tem uma forma de rastrear interfaces?

[91] Os planos de teste e procedimentos alterados como parte do processo de alteração?

2. Ferramenta de desenvolvimento

a. Capacidade
[Existe estações de trabalho suficientes, com poder de processamento, memória e armazenamento?]

[92] Existe estações de trabalho suficientes, e com poder de processamento para todos os membros do projeto?

[93] Existe capacidade suficiente de executar várias etapas ao mesmo tempo, tal como codificação, integração e testes?

b. Adequabilidade
[As ferramentas de desenvolvimento suportam todas as fases, atividades e funções?]

[94] As ferramentas de desenvolvimento suportam todos os aspectos do programa?

• Análise de requisitos

• Análise de desempenho

• Design

• Codificação

• Testes

• Documentação

• Gerência de configuração

• Acompanhamento de gerência

• Rastreamento de requisitos

c. Usabilidade
[O quanto é fácil de usar as ferramentas de desenvolvimento?]

[95] As pessoas acham as ferramentas de desenvolvimento fáceis de serem usadas?

[96] Existe boa documentação das ferramentas de desenvolvimento?

d. Experiência
[Existe experiência da empresa ou de membros do projeto com as ferramentas de desenvolvimento?]

[97] As pessoas usaram estes ferramentas e métodos antes?

e. Disponibilidade
[O sistema possui bugs, down-time, ou backup interno não suficiente?]

[98] O sistema é considerado disponível?

• Compilador

• Ferramentas de desenvolvimento

• Hardware

f. Suporte do sistema
[Existe algum suporte de especialista ou fornecedor ao sistema?]

[99] As pessoas estão treinadas para usar as ferramentas de desenvolvimento?

[100] Você possui acesso a experts quanto ao uso do sistema?

[101] Os fornecedores respondem de rapidamente aos problemas?

g. Entrega
[A definição e os requisitos de aceitação estão definidos para a entrega das ferramentas de desenvolvimento para o cliente no orçamento do cliente?]

[102] Você está entregando as ferramentas de desenvolvimento ao cliente?

(Sim) (102.a) Há um orçamento adequado, prazo, e recursos alocados para esta entrega?

3. Processo de gerência

a. Planejamento
[Os planejamento é feito a tempo, lideres técnicos são incluídos, planos de contingência feitos?]

[103] O programa é gerenciado de acordo com o plano?

(Sim) (103.a) As pessoas normalmente são pegas de surpresa com situações “apaga fogo”?

[104] Re-planejamento é feito quando distorções acontecem?

[105] Pessoas de todos os níveis são incluídas no planejamento do próprio trabalho?

[106] Existem planos de contingência para riscos conhecidos?

(Sim) (106.a) Como você determina quando executar um plano de contingência?

[107] Questões que necessitam de mais tempo para serem resolvidas são endereçadas de forma adequada?

b. Organização do projeto
[Os papéis e as relações de trabalho são claras?]

[108] A organização do programa é efeitva?

[109] As pessoas entendem seu próprio papel e o papel dos outros no programa?

[110] As pessoas sabem quem tem autoridade para o que?

c. Experiência de gerência
[Os gerentes são experientes em desenvolvimento de software, gerenciamento de software ou em programas maiores?]

[111] O programa possui gerentes experientes?

• Gerenciamento de software

• Participação ativa em Desenvolvimento de software

• Com este processo de desenvolvimento

• No domínio da aplicação

• Em um programa com tamanho e complexidade similar

d. Interfaces do programa
[Existe pouca interface com o cliente, outros contratados, outros gerentes ou alta gerência?]

[112] A gerência comunica os problemas tanto para cima ou para baixo hierarquicamente?

[113] Os conflitos com o cliente são documentados e resolvidos em tempo hábil?

[114] A gerência envolve membros do programa apropriados em reuniões com o cliente?

• Lideres Técnicos

• Desenvolvedores

• Analistas

[115] A gerência trabalha para garantir que todas as facções de consumidores estão representadas quanto a funcioinalidade e operação?

[116] Existem boas políticas para apresentar uma posição otimista para o cliente ou a alta gerência?

4. Métodos de gerenciamento

a. Monitoração
[As métricas de gerenciamento estão definidas e o progresso do desenvolvimento acompanhado?]

[117] Existe relatórios de status periódicos estruturados?

(Sim) (117.a) As pessoas conseguem uma resposta dos seus relatórios de status?

[118] Informações apropriadas são reportadas para os níveis corretos da organização?

[119] Você acompanha o progresso em relação ao plano?

(Sim) (119.a) A gerência tem uma visão clara do que está acontecendo?

b. Gerenciamento de Pessoal
[As pessoas do projeto estão treinadas e sendo usadas adequadamente?]

[120] As pessoas estão sendo treinadas em habilidades necessitadas pelo programa?

(Sim) (120.a) Isto faz parte do plano do programa?

[121] As pessoas recebem trabalho foram da sua area de experiência?

[122] É fácil para os membros do programa tomar attitudes de gerenciamento?

[123] Os membros do programa, em todos os níveis, estão sabendo do status do programa em relação ao plano?

[124] As pessoas sentem que é imortante seguir o plano?

[125] A gerência consulta as pessoas antes de tomar decisões que afetem o trabalho destas pessoas?

[126] A gerência do programa envolve membros do programa adequados em reuniões com o cliente?

• Líderes Tecnicos

• Desenvolvedores

• Analistas

c. Garantia de qualidade
[Existem procedimentos adequados e recursos para assegurar a qualidade do produto?]

[127] Is the software quality assurance function adequately staffed on this program?

[128] Você tem mecanismos definidos para assegurar a qualidade?

(Sim) (128.a) Todas as areas e fases tem procedimentos de qualidade?

(Sim) (128.b) As pessoas estão acostumadas a trabalhar com estes procedimentos?

d. Gerência de configuração
[Os procedimentos de mudança ou controle de versão, incluindo locais de instalação, são adequadas?]

[129] Você tem um sistema de gerenciamento de configuração adequado?

[130] A função de gerenciamento de configuração possui membros adequados?

[131] Uma coordenação é requerida com um sistema instalado?

(Sim) (131.a) Existe gerenciamento de configuração adequada para o sistema instalado?

(Sim) (131.b) O sistema de gerenciamento de configuração sincroniza seu trabalho com as mudanças no local?

[132] Você está instalando em multiplos locais?

(Sim) (132.a) A gerência de configuração está disponível para multiplos locais?

5. Ambiente de Trabalho

a. Atitude de Qualidade
[Existe uma ausência de orientação quanto a qualidade do trabalho?]

[133] Todos os níveis de pessoal são orientados a procedimentos de qualidade?

[134] O cronograma está considerando a qualidade?

b. Cooperação
[Existe ausência de espirito de time? Resolução de conflitos exisgem intervenção da gerência?]

[135] As pessoas trabalham de forma cooperativa entre os limites funcionais?

[136] As pessoas trabalham com objetivos comuns?

[137] É necessária intervenção da gerência para que as pessoas trabalhem juntas?

c. Comunicação
[Existe pouco conhecimento da missão ou objetivos, pouca comunicação de informações técnicas entre os gerentes?]

[138] Existe boa comuicação entre os membros do programa?

• Gerentes

• Líderes técnicos

• Desenvolvedores

• Testadores

• Gerência de configuração

• Garantia de qualidade

[139] Os gerentes são receptivos para comunicados dos membros do programa?

(Sim) (139.a) Você se sente a vontade de pedir ajuda a seus gerentes ?

(Sim) (139.b) Os membros do programa podem levanter riscos sem ter uma solução em mãos?

[140] Os membros do programa recebem notificações de eventos, em tempo hábil, que podem afetar o trabalho deles?

(Sim) (140.a) Isto é forma ou informal?

d. Moral
[Existe uma atmosfera não criativa ou não produtiva? As pessoas sente que não tem reconhecimento ou não tem recompensa por um bom trabalho realizado?]

[141] Como está a moral do programaHow is morale on the program?

(Não) (141.a) Qual é a principal contribuição para o baixo fator de moral?

[142] Existe algum problema em manter as pessoas que você precisa?

C. Definições do programa

1. Recursos

a. Cronograma
[O cronograma é inadequado ou instável?]

[143] O cronograma tem sido estável?

[144] O crongorama é realista?

(Sim) (144.a) Existe um método de estimação baseado em dados históricos?

(Sim) (144.b) O método funcionou bem no passado?

[145] Existe algo no cronograma que não foi adequadamente planejado?

• Análise e estudos

• Garantia de qualidade

• Treinamento

• Cursos e treinamento de manutenção

• Equipamentos

• Ferramentas de desenvolvimento disponíveis

[146] Existem dependencia externas que podem afetar o cronograma?

b. Equipe

[A equipe não tem experiência, não tem conhecimento no domínio, não tem habilidades, ou está sobrecarregada?]

[147] Existe alguma area em que habilidades técnicas estão ausente?

• Engenharia de software e métodos de análise de requisitos

• Experiência em algoritmos

• Design e métodos de design

• Linguagens de programação

• Métodos de teste e integração

• Confiabilidade

• Manutenabilidade

• Disponibilidade

• Fatores humanos

• Gerência de configuração

• Garantia de qualidade

• Ambiente de produção

• Níveis de segurança

• COTS

• Software reutilizável

• Sistema operacional

• Banco de dados

• Domínio da aplicação

• Análise de Desempenho

• Aplicações de tempo crítico

[148] Você tem pessoal adequado para a equipe do programa?

[149] A equipe é estável?

[150] Você tem acesso às pessoas certas quando você precisa delas?

[151] Os membros do programa implementaram sistemas desse tipo?

[152] O programa é dependente de um pequeno numero de pessoas chaves?

[153] Existe algum problema em conseguir pessoas livres?

c. Orçamento

[O fundo é insufficiente ou instável?]

[154] O orçamento é estável?

[155] O orçamento é baseado em uma estimativa realista?

(Sim) (155.a) Is O método de estimativa é baseado em dados históricos?

(Sim) (155.b) O método funcionou bem no passado?

[156] Algumas funcionalidades ou funções foram apagadas como parte de uma política de design baseado em custos?

[157] Existe algo para qual o orçamento não foi alocado?

• Análise e estudos

• Garantia de qualidade

• Treinamento

• Curos de manutenção

• Equipamento

• Ferramentas de desenvolvimento

[158] As mudanças nos requisitos são acompanhadas de mudanças no orçamento?

(Sim) (158.a) Esta é uma parte no processo padrão de controle de mudanças?

d. Facilidades
[As facilidades são adequadas para construir e entregar o produto?]

[159] As facilidades de desenvolvimento são adequadas?

[160] O ambiente de integração é adequado?

2. Contrato

a. Tipo do contrato
[O tipo de contrato é uma fonte de risco para o programa?]

[161] Que tipo de contrato você tem? (Custo mais taxas, preço fixo, etc.)

(161a) Isto representa um problema?

[162] O contrato é rigoroso em algum aspecto do programa?

• Declaracão de trabalho

• Especificações

• Descrições de itens

• Partes do contrato

• Envolvimento excessivo do cliente

[163] A documentação requerida é rigorosa?

• Excesso de documentação

• Cliente detalhista

• Longo ciclo de aprovação

b. Restrições
[O contrato causa alguma restrição?]

[164] Existe algum problema com direitos autorais?

• Software COTS

• Software desenvolvido pela organização

• Itens não desenvolvidos

c. Dependências
[O programa tem alguma dependência em outros produtos ou serviços externos?]

[165] Existe alguma dependencia em produtos ou serviços externos que podem afetar o produto, orçamento ou cronograma?

• Contratados associados

• Contratado principal

• Subcontratados

• Fornecedores

• Equipamento ou software do cliente

3. Interfaces do programa

a. Cliente
[Existe algum problema com o cliente, tais como: longo ciclo de aprovação, pouca comunicação, e experiência no dominio da aplicação?]

[166] O ciclo de aprovação do cliente funciona em tempo hábil?

• Documentação

• Revisão do programa

• Revisões formais

[167] Você continua antes de receber uma aprovação do cliente?

[168] O cliente entende os aspectos técnicos do sistema?

[169] O cliente entende o software?

[170] O cliente interfere no processo ou nas pessoas?

[171] A gerência trabalha com o cliente para alcançar decisões acordadas em tempo hábil?

• Entendimento dos requisitos

• Critério de testes

• Ajustes no calendário

• Interface

[172] O quanto efetivo são seus mecanismos em conseguir acordos com o cliente?

• Grupos de trabalho (Previsto em contrato?)

• Reuniões de intercâmbio técnico (Previsto em contrato?)

[173] As facções de cliente estão envolvidas em alcançar acordos?

(Sim) (173.a) Este é um processo definido formalmente?

[174] A gerência apresenta uma visão realista ou otimista para o cliente?

b. Contratados associados
[Existe algum problema com contratados associados, tais como: definições inadequadas ou interfaces instáveis, pouca comunicação, ou ausência de cooperação?]

[175] As interfaces externas estão mudando sem notificação adequada, coordenação, ou procedimentos formais de mudança?

[176] Existe um plano adequado de transição?

(Sim) (176.a) É suportado por todos os contratados e pessoal do local?

[177] Existe algum problema em conseguir prazos ou dados de interface com o contratados associados?

(Não) (177.a) São precisos?

c. Subcontratados
[O programa é dependente de subcontratados em areas críticas?]

[178] Existe alguma ambiguidade em definições de tarefa para subcontratados?

[179] O procedimento de relatório e monitoração dos subcontratados é diferente dos procedimentos requeridos pelo programa?

[180] A administração do subcontratado e a gerência técnica são feitas por organizações distintas?

[181] Você é fortemente dependente do conhecimento de um subcontratado em alguma área?

[182] O conhecimento do subcontratado está sendo transferido para a companhia?

[183] Existe algum problema em conseguir prazos ou dados de interface com os subcontratados?

d. Contratante Principal (Se o programa é um subcontratado)
[O programa está tendo dificuldades com o seu contratante principal?]

[184] As definições de tarefas do contratante principal estão ambiguas?

[185] Você tem interfaces com duas organizações principais separadas para administração e gerência técnica?

[186] Você é fortemente dependente do contratante principal para alguma area de conhecimento?

[187] Existe algum problema em conseguir prazos ou dados de interface com o contratante principal?

e. Gerência da Organização
[Está faltando um suporte ou micro gerenciamento da alta gerência?]

[188] A gerência do programa tem problemas de comunicação com a alta gerência?

(Sim) (188.a) Isto parece ser efetivo?

[189] A alta gerência dá a você suporte em tempo hábil para resolver seus problemas?

[190] A alta gerência tem tendência a fazer micro gerenciamento?

[191] A gerência apresenta uma visão realista ou otimista do programa?

f. Fornecedores
[Os fornecedores são responsáveis por necessidades do programa?]

[192] Você está dependendo de fornecedores para entrega de components críticos do programa?

• Compiladores

• Hardware

• COTS

g. Política
[Política está causando problemas no programa?]

[193] Políticas estão afetando o programa?

• Compania

• Cliente

• Contratados associados

• Subcontratados

[194] Decisões políticas estão afetando decisões técnicas?

Anexo C – Os 10 principais riscos em projetos de software [BOEHM91]

Esta taxonomia apresentada por Boehm [BOEHM91] no artigo “Software Risk Management: Principles and Practices”, apresenta os 10 principais riscos em projetos de software, baseada em uma pesquisa entre vários gerentes de projetos. Além das fontes de risco, são apresentadas técnicas de gerências de risco usadas com sucesso, em cada fonte de risco, para mitigar ou evitar os riscos.

Item de risco	Técnica de Gerência de Risco
Mão de obra abaixo do esperado	Equipe com talento e qualificado para o trabalho, desenvolvimento do time, treinamento e acordos pessoais
Cronograma e orçamento irreais	Estimativa de orçamento e cronograma detallhadas, projetos com base no custo, desenvolvimento incremental, re-utilização de software e limpeza dos requisitos
Desenvolvimento de funções ou propriedades erradas;	Análise da organização, análise da missão, formulação do conceito de operação, pesquisa com o usuário, participação do usuário, prototipação, manual para os usuários, análise de desempenho, analise do fator de qualidade
Desenvolvimento de uma interface com o usuário errada	Protótipos, cenários, análise de tarefas, participação do usuário
Projetar funcionalidades sem requisitos incluídos por analistas, ou por preciosismo (Gold-Plating);	Limpeza dos requisitos, prototipação, análise de custo benefício, projetar com base no custo
Criação de requisitos contínua	Definição de marcos para mudanças, esconder informações, desenvolvimento incremental (postergando mudanças para próximas iterações)
Componentes externos – por exemplo, equipamentos adquiridos - abaixo da expectativa	Análise de desempenho, inspeções, checar a referência, análise de compatibilidade
Atividades externas – por exemplo, fornecedores - abaixo da expectativa	Checar a referência, contratos com multa, prototipações ou projetos competitivos, desenvolvimento de time
Desempenho em tempo real abaixo da expectativa	Simulação, análise de desempenho, modelagem, prototipação, instrumentação, melhoria fina de desempenho
Requisitos que vão além da capacidade computacional	Análise técnica, análise de custo benefício, prototipação, checar referência

Anexo D – Taxonomia de Riscos [JONES94]

A taxonomia de riscos a seguir foi apresentada por Caper Jones no livro “Assessment and Control of Software Risks” [JONES94]. Este livro apresenta 60 fatores de risco. Para cada risco são apresentados as seguintes informações:

- Definição do risco;
- Grau de severidade;
- Freqüência em que o risco aparece;
- Ocorrência;
- Susceptibilidade e resistência ao risco;
- Causas-Raiz do risco;
- Riscos associados;
- Impacto no custo;
- Métodos de prevenção;
- Métodos de controle;
- Suporte de ferramentas;
- Suporte de consultores;
- Suporte educacional;
- Suporte de publicações;
- Suporte de periódicos;
- Suporte de padrões;
- Associações de profissionais;
- Efetividade de terapias conhecidas;
- Custo de terapias conhecidas;
- Prognóstico a longo prazo do risco.

A tabela a seguir apresenta todos os riscos apresentados por [JONES94]. A primeira coluna apresenta o risco, a segunda coluna indica quais são os riscos mais comuns encontrados em projetos e o tipo de projeto de software onde são encontrados (conforme lista de códigos a seguir) e a terceira coluna indica quais são os riscos mais sérios em projetos de software. Após a tabela é apresentado, de uma forma mais completa, um dos riscos citados por [JONES94].

Tipos de projetos de software

M = Sistemas de Gerencia de Informação

S = Software de Sistema (Sistemas Operacionais, aplicações que controlam dispositivos)

C = Softwares Comerciais

D = Softwares Militares

O = Softwares desenvolvidos por terceiros (contratados)

E = Softwares desenvolvidos pelo próprio usuário

Risco	Mais Comum	Mais Sério
Objetivos de melhoria de qualidade ou produtividade não são claros		
Níveis de maturidade artificiais		
Projetos Cancelados	S	X
Disputas políticas dentro da organização		
Estouro no custo	M	
Requisitos intermináveis dos usuários	D,M,O	X
Escritório com muitas pessoas		
Módulos ou componentes de sistema com um número elevado de erros	E,S	
Excesso de Documentação	D,S	
Excesso de Pressão no Prazo	M	X
Demora do software chegar ao mercado	C,D,S	
Falsos indicadores de produtividade		
Problemas entre clientes e fornecedores de software	O	
Problemas entre gerente de projeto e gerência sênior		
Alto custo de manutenção	O	
Estimativa de custo não acurada	S	X
Métricas não acuradas		X
Estimativa de qualidade não acurada		
Estimativa de tamanho de software não acurada		
Avaliações de software inadequadas		
Planos de compensação inadequados		
Controle de configuração e repositórios de projetos inadequados	M	
Currículo Inadequado do Engenheiro de Software		
Currículo Inadequado do Gerente de Software		
Medição inadequada		X
Métodos de aquisição de pacotes inadequados		
Referências Bibliográficas e Pesquisa inadequada		
Padrões e políticas de software inadequadas		
Análise de Risco do projeto de software inadequada		
Análise de valores do projeto de software inadequada		
Métodos e ferramentas de gerência de projeto inadequadas		
Métodos e ferramentas de garantia de qualidade inadequadas		
Métodos e ferramentas de engenharia de software inadequadas		
Métodos e ferramentas de documentação técnica inadequadas		
Ausência de arquiteturas reutilizáveis		
Ausência de códigos reutilizáveis		
Ausência de dados reutilizáveis		
Ausência de designs reutilizáveis		
Ausência de documentação reutilizável		
Ausência de Templates de estimativas reutilizáveis		

Risco	Mais Comum	Mais Sério
Ausência de intefaces homem-máquina reutilizáveis		
Ausência de Planos de Projetos reutilizáveis		
Ausência de Requisitos reutilizáveis		
Ausência de Planos de Testes, Casos de Testes e Dados de Testes reutilizáveis		
Ausência de Especialização		
Sistemas Obsoletos em uso por um longo tempo	D,E	
Produtividade Baixa	D	
Qualidade Baixa	M	X
Baixo Status hierárquico na organização das pessoas responsáveis pelo projeto		
Baixo grau de satisfação do usuário	C	
Péssimas Práticas na gerência de projeto		X
Péssimas Práticas pela equipe técnica do projeto		
Prazos perdidos		
Definições incompletas de ciclos de vida que omitem atividades importantes		
Organização sem estrutura adequada		
Falta de investimento de tecnologia		
Dispensas e cortes excessivos na equipe do projeto		
Planejamentos de melhorias a curto prazo		
Síndrome de Bala de Prata (Ferramenta ou metodologia que faz milagre)		
Transferência de tecnologia lenta		

Requisitos intermináveis dos usuários

1. Definição: a) Requisitos novos ou modificações significantes aos requisitos existentes que são criados após os requisitos acordados entre clientes e desenvolvedores; b) Falha ao antecipar requisitos que poderiam ser modificados, e falha também ao não fazer planos para lidar com estes requisitos;

2. Severidade: A severidade média deste risco é de 3.5 considerando a escala a seguir:

Severidade 1: Requisitos novos ou modificações excedem 50% dos requisitos originais;

Severidade 2: Requisitos novos ou modificações excedem 40% dos requisitos originais;

Severidade 3: Requisitos novos ou modificações excedem 30% dos requisitos originais;

Severidade 4: Requisitos novos ou modificações excedem 20% dos requisitos originais;

Severidade 5: Requisitos novos ou modificações excedem 10% dos requisitos originais;

3. Frequência: Tipicamente acontece em mais de 70% das aplicações com mais de 1000 pontos de função. A média de requisitos novos ou modificações foi de 35% em uma amostra de 60 projetos.

4. Ocorrência: Todas as classes de softwares possuem experiência com este risco. Softwares militares apresentam mais este risco do que as outras classes, pois os projetos de softwares são mais longos.

5. Susceptibilidade e resistência: Aplicações que são novas ou onde os usuários estão incertos do que é necessário são as mais susceptíveis ao risco. E aplicações que já foram feitas diversas vezes, tais como compiladores, são as mais resistentes.

6. Causas Raiz: 1) Cada vez que novos usuários entram no projeto, haverá alguma incerteza em resolver as necessidades; 2) Para projetos que durem anos, pode acontecer novas mudanças como parte da aplicação

7. Riscos associados: Associados aos riscos de “Problemas entre clientes e fornecedores” e “Problemas entre gerente de projeto e gerência sênior”. Requisitos intermináveis também são tipicamente causas para “Prazos perdidos”, “Tempo excessivo de entrega ao mercado”, e “Estouro no custo”. E também contribuem para problemas como “pressão excessiva no prazo” e “moral baixo da equipe”. Requisitos intermináveis são causados por “Usuários sem experiência”, “Gerência sem experiência”, “Metodologias inadequadas”, “Estimativa de custo inadequado”.

8. Impacto no custo: Pode ser quantificado por métricas de pontos de função. Considerando que o custo por ponto de função é $1000, e o projeto começa com requisitos com o total de 1000 pontos de função, então o projeto tem o custo de $1 milhão. Caso sejam adicionados novos requisitos, 25% além do inicial, o projeto irá custar $1,25 milhões.

9. Métodos de prevenção: um programa de medida baseados em métricas funcionais é a melhor prevenção. Softwares que estimem pontos de função também são ferramentas que apresentam benefícios.

10. Métodos de controle: O uso de protótipos ajuda a controlar este risco. Para projetos muito grandes (> 5000 pontos de função), estabelecer um controle de mudanças formal também ajuda.

11. Suporte de Ferramentas: Ferramentas que estimam pontos de função, por exemplo: ACT/1, Case Dictionary, FirstCASE etc.

12. Suporte de Consultores: Existem diversos consultores para serviços de prototipação e treinamento nesta técnica.

13. Suporte educacional: Diversas universidades estão estudando este risco: Case Western University, George Mason University etc.

14. Suporte de publicações: “Exploring Requirements: Quality Before Design” de Donald Gause e Gerald Weinberg é uma excelente visão geral com dicas importantes..

15. Suporte de periódicos: Algumas revistas como Times, Business Week, e Fortune apresentam este risco apenas quando acontece grandes problemas. Outros jornais e revistas apresentam alguns artigos sobre o problema: Cross Talk, Metrics Views etc.

16. Suporte de padrões: Nenhum dos padrões (E, 1994) cobre este problema: ANSI, IEE, IEEE, DoD ou ISO. Porém DoD especifica técnicas formais para pedidos de mudanças nos requisitos.

17. Associações de profissionais: Existem diversas associações de profissionais que lidam com custos acima do previsto, porém não com requisitos intermináveis. ISPA (*International Society of Parametric Analysis*) está começando a lidar com este problema.

18. Efetividade de terapias conhecidas: A efetividade de terapias conhecidas são excelente para aplicações pequenas e médias, mas não para grandes sistemas com mais de 10.000 pontos de função. Protótipos podem reduzir requisitos intermináveis em 10%.

19. Custo de terapias conhecidas: Aprender a contar pontos de função, custa em média $1000 dólares americanos por estudante. Ferramentas para estimar pontos de função custam entre $1000 e $40000.

20. Prognóstico a longo prazo: Com o tempo os requisitos intermináveis devem reduzir. Técnicas de prototipação devem reduzir o número de novos requisitos, e mais formalidade para lidar com novos requisitos também devem ajudar a reduzir o problema.

Anexo E – Taxonomia de Riscos [LEOPOLDINO04]

Esta taxonomia foi elaborada por Cláudio Bezerra Leopoldino [LEOPOLDINO04] no trabalho "Avaliação de riscos em desenvolvimento de software" por meio de uma pesquisa realizada com empresas nacionais. A lista de riscos e os tipos foram desenvolvidas com base em outras taxonomias existentes.

1. Ambiente Corporativo

a. Mudança na propriedade do produto ou no gerente sênior do projeto: Alteração na chefia do comprador do software ou do próprio projeto, com mudanças de necessidades que influenciam o seu andamento

2. Propriedade do Projeto

a. Falta de comprometimento da alta gerência com o projeto: O compromisso da alta gerência com o projeto não pode ser negligente ou superficial, devendo ser marcante e visível. Envolve também a disponibilidade dos recursos necessários.

b. Falha em obter comprometimento do cliente por parte do gerente do projeto: Neste caso o gerente tem a culpa por não conseguir maior comprometimento do cliente.

c. Conflito de interesses entre departamentos do usuário: Departamentos do cliente apresentam necessidades diferentes de requisitos, prioridades, metas, etc. Torna-se um problema conciliar a propriedade compartilhada de um projeto.

3. Gerência de Relacionamentos

a. Falha em gerenciar as expectativas dos usuários finais: A expectativa sobre um projeto define seu sucesso ou fracasso. Expectativas muito baixas ou muito altas afetam negativamente o projeto.

b. Falta de envolvimento adequado do usuário (pouco tempo disponível e/ou má qualidade na participação): Usuários devem ativamente participar da equipe de desenvolvimento, com responsabilidade e compromissos com suas metas.

c. Falta de Cooperação dos Usuários: Recusa dos usuários em colaborar com a equipe de desenvolvimento.

4. Gerência de Projeto

a. Gerenciamento impróprio de mudanças: Todas as alterações no projeto, por quaisquer razões, devem ser feitas sem que se perca controle sobre escopo e orçamento e de forma harmônica.

b. Falta de habilidades para o gerenciamento de projetos: Gerente não tem habilidades suficientes para ser bem sucedido.

c. Falta de poderes efetivos para o gerenciamento de projetos: Gerente não tem poderes suficientes para ser bem sucedido.

d. Falta de uma metodologia efetiva de gerenciamento de projetos: Equipe não emprega técnicas e/ ou processos necessários ao desenvolvimento.

e. Definição imprópria de papéis e responsabilidades: Falta de clareza de papéis e responsabilidades entre os membros da equipe, consultores e terceirizados.

f. Controle pobre ou inexistente: Causa falta de informação sobre o estado atual do projeto decorrente do acompanhamento indevido/ insuficiente das atividades desempenhadas.

5. Escopo

a. Escopo/ objetivos pouco claros ou equivocados: Antes de se ter clareza, não se consegue estabilizar os requisitos.

b. Mudança de Escopo/ objetivos: Mudanças de regras de negócio no decorrer do projeto.

c. Envolvimento de grande número de unidades organizacionais do cliente: Escopo do software cresce em virtude de muitas unidades organizacionais do cliente estarem envolvidas.

6. Requerimentos

a. Volatilidade nos requisitos: Alterações contínuas no que se espera do software.

b. Requisitos mal entendidos e/ou mal definidos no início do desenvolvimento: Pode levar a estimativas e escolhas equivocadas de tecnologia, tempo recursos e funcionalidade do sistema.

c. Assunto novo ou não familiar tanto para usuários quanto para desenvolvedores: A falta de conhecimento pode levar a uma pobre especificação de requisitos.

7. Financiamento

a. Custos mal estimados: Má definição de custos pode levar a planejamento e decisões errôneas

8. Agenda e Tempo

a. Prazos e tempo de execução de tarefas mal estimados: Tempo adequado deve ser determinado para cada tarefa, inclusive para testes e documentação.

9. Processo de Desenvolvimento

a. Falta de metodologia/ processo efetivo de desenvolvimento: Os métodos empregados não podem retardar a implementação nem tampouco ser leves a ponto de ser frágeis. Também devem ser abrangentes para todo o processo de desenvolvimento.

b. Tentativa de adoção de novo método/ tecnologia durante o projeto. Aumenta a incerteza inerente ao projeto.

10. Pessoal

a. Falta de conhecimentos/ habilidades necessários ao pessoal do projeto: Tais como conhecimento de negócios, tecnologia, experiência, etc.

b. Falta de habilidades interpessoais pelo gestor na liderança da equipe do projeto: Lidar com as pessoas merece cuidado da mesma forma que calendário, orçamento e tecnologia.

11. Pessoal de Apoio

a. Pessoal envolvido insuficiente/ inapropriado: Pessoal insuficiente numericamente ou com habilidades erradas/ inapropriadas.

b. Volatilidade do pessoal da equipe: Troca constante de membros da equipe ou perda de pessoas importantes para a equipe.

12. Tecnologia

a. Introdução de Nova Tecnologia de desenvolvimento: Agregação ao projeto de novas tecnologias, tecnologias “de ponta” ou uso de mudanças radicais de versão de uma tecnologia conhecida.

13. Dependências Externas

a. Dependências complicadas em projetos de múltiplos fornecedores (integração de tecnologias de várias fontes): Nem sempre os fornecedores de várias tecnologias tem compatibilidade adequada entre si.

14. Planejamento

b. Ausência de planejamento ou planejamento inadequado: Visão de que planejamento é pouco prático ou sem importância.

15. Novos Itens

a. Ferramentas inapropriadas para o desenvolvimento: A má definição de linguagem, plataforma de desenvolvimento e ferramentas em geral afeta o ritmo de produção e os requisitos.

b. Falta de motivação da equipe de desenvolvimento: Equipes desmotivadas produzem menos e com menor qualidade.

Anexo F – Questionário de de Riscos [THOMSETT02]

Esta taxonomia de riscos baseada em questionário, foi desenvolvida com base em outras taxonomias existentes e está disponível no livro "Radical Project Management" [THOMSETT02]. Esta taxonomia é aconselhável a ser usada em pequenos projetos (menores que 3 meses). O autor do livro aconselha que para projetos maiores, seja feito uma reunião entre os gerentes de projetos mais experientes, e com a aplicação da técnica de *brainstorming* sejam adicionados considerados novos riscos. Com base na respostas do questionário, o time do projeto consegue identificar quais riscos são aplicáveis ao projeto, e identificar o risco geral do projeto.

Risco de Produto / Sistema				
1.	Visão geral do sistema / serviço / produto	☐ Simples	☐ Médio	☐ Complexo
2.	Dados lógicos (inclui arquivos)	☐ "	☐ "	☐ "
3.	I/O e questões ou impacto organizacional	☐ "	☐ "	☐ "
4.	Interface com outros sistemas / serviços / produtos	☐ "	☐ "	☐ "
5.	Função e processos	☐ "	☐ "	☐ "
6.	Novos procedimentos e alterações no negócio	☐ Nenhum	☐ Algum	☐ Extensivo
7.	Estabilidade dos requisitos	☐ Estável	☐ Médio	☐ Instável
8.	Requisitos de desempenho (incluir qualidade)	☐ Pouco	☐ Médio	☐ Alto
9.	Requisitos de tecnologia	☐ Simples	☐ Médio	☐ Complexo
10.	Nível de inovação	☐ Nenhum	☐ Algum	☐ Extensivo

Risco de Ambiente do Cliente				
11.	Nível de suporte do cliente / usuário	☐ Alto	☐ Médio	☐ Baixo
12.	Experiência do cliente com o produto / sistema	☐ Extensive	☐ Some	☐ Nenhum
13.	Suporte do patrocionador do cliente / projeto	☐ Alto	☐ Médio	☐ Pouco / Nenhum
14.	Impacto nas operações do cliente (tecnologia nova, política)	☐ Pouco	☐ Médio	☐ Alto
15.	Participação de especialistas do cliente / negócio	☐ Tempo integral	☐ Tempo Parcial	☐ Quando requisitado (ad-hoc)
16.	Stakeholders críticos	☐ 1 a 3	☐ 4 a 10	☐ Mais de 10

Risco de Time				
17.	Habilidades gerais	☐ Alto	☐ Médio	☐ Pouco
18.	Nível de habilidade relevante (com aplicação / produto)	☐ Extensivo	☐ Algum	☐ Nenhum
19.	Experiência do gerente do projeto	☐ Extensivo	☐ Algum	☐ Nenhum
20.	Quantidade de pessoas do projeto	☐ 1 a 4	☐ 5 a 10	☐ Mais de 10

21.	Uso de contratados / membros do time em tempo parcial	☐ Nenhum	☐ Algum	☐ Extensivo
22.	Tempo de desenvolvimento do projeto	☐ 1 a 3 meses	☐ 4 a 6 meses	☐ Mais de 6 meses
23.	Cronograma / Prazos	☐ Flexível	☐ Firme	☐ Fixo
24.	Prioridade do projeto para o time	☐ Alto	☐ Médio	☐ Baixo
25.	Experiência do time com hardware / tecnologia	☐ Extensivo	☐ Médio	☐ Algum
26.	Ambiente físico / de suporte para o time	☐ Excelente	☐ Médio	☐ Pobre

RISCO GERAL	☐ LOW	☐ MEDIUM	☐ HIGH

Anexo G – Taxonomia de Riscos para projetos de manutenção [OLIVEIRA06]

Esta taxonomia apresentada por Kathia Oliveira [OLIVEIRA06] é voltada para projetos de manutenção de software. São 42 riscos, não categorizados. É apresentado o fator de risco, e a sua descrição.

	Fatores de Risco	Descrição do Risco
1.	Baixa qualidade do sistema a ser mantido	Quando a qualidade do sistema a ser mantido é pobre e qualquer mudança pode acarretar em problemas imprevisíveis.
2.	Falta de ferramentas de apoio apropriadas	Falta de ferramentas apropriadas e de ambiente para apoiar a manutenção de sistemas, tais como: metodologias, padrões, procedimentos e ferramentas.
3.	Falta de Profissionais treinados	Falta de profissionais na equipe treinados com habilidades para utilização de ferramentas, metodologias e modelos requeridos para manutenção de sistemas.
4.	Dificuldade em reter pessoas	A instabilidade das mudanças, a falta de controle, a falta de informação e a falta de tempo. Faz com que as pessoas não dêem continuidade nas atividades de manutenção de sistemas.
5.	Falta de orçamento	Falta ou insuficiência de orçamento para assegurar a implementação das mudanças
6.	Resistência dos usuários à mudança	A resistência que os usuários tem com relação às mudanças de um produto de software, por mais importante ou lucrativa que tal mudança possa ser.
7.	Estratégia Organizacional	Determinar o orçamento de uma manutenção baseado na concorrência com outras empresas rivais. Muitas vezes o desejo de ganhar faz com que o orçamento seja determinado por estratégias organizacionais e não por uma análise objetiva dos problemas
8.	Prioridades de gerenciamento	A equipe de manutenção compara os desejos dos clientes com as necessidades do sistema. Freqüentemente, as prioridades de gerenciamento se sobrepõem às necessidades técnicas. Algumas vezes os gerentes consideram a manutenção e o aprimoramento mais importantes que a construção de novas aplicações
9.	Dificuldade para realização dos testes	O nível de especificação e o tempo para a realização dos testes são inadequados ou falta de dados precisos para testar as mudanças efetuadas
10.	Escassez de recursos no mercado	Poucos são os recursos experientes com habilidades em atividades de manutenção de software estão disponíveis no mercado
11.	Entendimento limitado	O entendimento do sistema a ser mantido é limitado. Por exemplo, a taxa de limite que uma pessoa pode estudar uma documentação e extrair material relevante ao problema que está sendo resolvido
12.	Moral da equipe	Baixa moral e baixa produtividade da equipe pelo fato das pessoas não sentirem reconhecidas ou recompensadas pelos superiores. A equipe pode sentir desmotivada pela pouca importância dada atualmente para as atividades de manutenção de sistemas
13.	Pouca ou nenhuma documentação	O sistema a ser mantido não possui documentação ou quando a documentação é existente é insuficiente ou confusa
14.	Efeitos colaterais (sistemas)	A execução de mudanças impacta funcionalidades de outros sistemas
15.	Efeitos colaterais (funcionalidade)	execução de mudanças impacta funcionalidades do próprio sistema
16.	Inovação tecnológica	Refere-se as mudanças de hardware e/ou software durante as atividades de manutenção de sistemas
17.	Falta de entendimento do usuário	Os usuários não entendem como o sistema funciona e eles podem fornecer dados incompletos ou errados quando relatarem os efeitos de um problema aos mantenedores
18.	Usuários desinteressados	Falta de comprometimento ou interesse do usuário com relação às atividades de manutenção de sistemas
19.	Mudanças da organização usuária	Mudança da organização usuária durante a execução da manutenção do sistema
20.	Treinamento	Treinamento insuficiente ou inadequado.

	Fatores de Risco	Descrição do Risco
21.	BACKLOG	Grande acúmulo de trabalho a serem executados pelos mantenedores. A equipe de manutenção está sempre tentando equilibrar objetivos distintos
22.	Execução	Grande número de falhas no sistema ou no hardware antes da mudança ser executada
23.	Processamento	Tempo de resposta ou requisitos de processamento restrito do sistema a ser mantido
24.	Confiabilidade do hardware e do software	O hardware ou software ou suporte técnico não são confiáveis e podem dificultar a solução de um problema
25.	Apoio do suporte	Falta de apoio do suporte para ou ocorrem em tempo inoportuno
26.	Orçamento	Pressões orçamentárias
27.	Mudança de prioridade	Dificuldade em gerenciar mudanças emergenciais. Neste caso, os recursos chaves podem não estar disponíveis e na maioria das vezes as soluções emergenciais afetam o custo e o cronograma das atividades de manutenção
28.	Dificuldade de medir desempenho	Dificuldade de medir o desempenho das mudanças realizadas
29.	Sistema e tecnologia antiquados	O sistema e tecnologia a serem mantidos estão obsoletos
30.	Plano estratégico	Plano estratégico inexistente ou inadequado
31.	Adaptações das mudanças empresarias	Adaptar as mudanças referentes ao ambiente empresarial rapidamente
32.	Integração	Integrar ou sobrepor sistemas incompatíveis.
33.	Falta de apoio gerencial	Falta de compreensão e apoio gerencial.
34.	Alta complexibilidade	Alta complexidade do programa a ser mantido.
35.	Métricas inexatas	As métricas são subestimadas, devido a vários fatores: dentre eles: não entendimento da mudança, complexibilidade do sistema a ser mantido, número de linhas de código do sistema a ser mantido
36.	Falta de tempo	Falta ou insuficiência de tempo para assegurar a implementação das mudanças
37.	Requisitos instáveis	Os requisitos de necessários para a manutenção do sistema são instáveis, ou seja, estão sempre mudando

Anexo H – Riscos identificados na modernização de sistemas legados [SANTOS04]

Nesta taxonomia, Cássio Santos [SANTOS04] identificou os riscos inerentes à modernização de sistemas legados, com o objetivo de deixar o processo de modernização previsível e com mais probabilidade de sucesso. São 13 riscos riscos identificados, com as possíveis perdas associadas.

	Riscos	Possível perda
1	Risco e desempenho	Perda de desempenho, lentidão na execução.
2	Risco de manutenção	Esforço envolvido na Manutenção
3	Risco do conhecimento técnico da equipe	Introdução de problemas ou atrasos no projeto em função do conhecimento da tecnologia pela equipe envolvida.
4	Risco da complexidade da tecnologia	Introdução de problemas ou atrasos no projeto em função da complexidade da tecnologia envolvida
5	Risco de inflexibilidade da aplicação	Perda de liberdade de modernizar no sentido de dependência da estrutura do legado (interface, dados ou lógica)
6	Risco de integridade de dados	Possível divergência de dados entre as bases de dados.
7	Risco de indisponibilidade da aplicação	A aplicação pode ficar parada por alguma falha.
8	Risco de implementação	Introdução de problemas ou atrasos no projeto em função do conhecimento inadequado da parte modernizada.
9	Risco de segurança	Perda de segurança da aplicação
10	Risco de qualidade	Introdução de novos defeitos na aplicação, ou não resolver os erros existentes na aplicação antiga.
11	Risco de sincronismo	Perda de sincronismo entre a parte modernizada e a aplicação legada
12	Risco de custo	Alto custo para implementar o projeto de modernização
13	Risco de cronograma	Solução demorada para implementar o projeto de modernização

Anexo I – Taxonomia de Riscos [MACHADO02]

Esta taxonomia é apresenta por Cristina Machado [MACHADO02] foi baseada em diversas outras taxonomias, entre estas a taxonomia apresentada por Caper Jones [JONES94]. São 7 categorias, e 63 fontes de riscos identificados.

1. Cliente
    a. Ausência da participação do cliente
    b. Cliente resistente a mudanças
    c. Conflitos entre clientes
    d. Clientes com atitudes negativas em relação ao projeto
    e. Clientes não comprometidos com o projeto
    f. Ausência de cooperação entre os clientes
2. Equipe de Desenvolvimento
    a. Conflitos entre cliente e organização desenvolvedora
    b. Membros da equipe de desenvolvimento treinados inadequadamente
    c. Ausência de comprometimento da equipe de desenvolvimento em relação ao projeto
    d. Membros da equipe inexperientes
    e. Falta de boas práticas da equipe técnica
    f. Conflitos entre os membros da equipe de desenvolvimento
    g. Freqüente rotação de pessoal na equipe de projeto
    h. Equipe de desenvolvimento não familiarizada com as ferramentas
    i. Membros da equipe de desenvolvimento não familiarizados com o negócio do cliente
    j. Atitudes negativas da equipe de desenvolvimento
    k. Ausência de perfil especializado na equipe de projeto para atender aos requisitos do projeto
3. Política Organizacional
    a. Recursos retirados do projeto por causa de mudanças nas prioridades organizacionais
    b. Mudanças na gerência da organização durante o projeto
    c. Políticas corporativas com efeito negativo no projeto
    d. Influência política no projeto
    e. Ambiente organizacional instável
    f. Reestruturação organizacional durante o projeto
    g. Ausência de suporte gerencial de alto nível para o projeto
    h. Ausência ou perda do compromisso organizacional com o projeto
4. Complexidade do projeto
    a. Dependência de fornecedores externos
    b. Muitos fornecedores externos envolvidos com o projeto
    c. Alto nível de complexidade técnica
    d. Tarefas a serem automatizadas altamente complexas
    e. Projeto afetando um grande número de departamentos ou unidades do usuário
    f. Grande quantidade de interação com outros sistemas
    g. Projeto envolvendo o uso de novas tecnologias
    h. Inadequada transferência de tecnologia para o projeto
    i. Condições de trabalho inadequadas

5. Processo
    a. Padrões, políticas e metodologias de engenharia de software inadequados
    b. Métodos e ferramentas de engenharia de software inadequados
    c. Burocracia excessiva
    d. Falta de suporte para a resolução de problemas técnicos
    e. Falta de estrutura para reuso
    f. Falta de prática de reuso
    g. Repositórios de projeto e controle de configuração inadequados
    h. Ausência de uma metodologia efetiva de gerência de projetos
6. Gerência de Projeto
    a. Planejamento inadequado do prazo
    b. Planejamento inadequado dos recursos necessários
    c. Planejamento inadequado do orçamento
    d. Pressão excessiva de prazo
    e. Baixa produtividade
    f. Baixa qualidade dos produtos intermediários e finais
    g. Ausência de “pessoas com perfil” para liderar o projeto
    h. Acompanhamento do progresso do projeto insuficiente
    i. Fraco planejamento de projeto
    j. Falta de definição dos marcos do projeto
    k. Gerente do projeto ineficiente
    l. Gerente do projeto inexperiente
    m. Comunicação ineficiente
7. Requisitos
    a. Requisitos conflitantes
    b. Mudanças contínuas dos objetivos e escopo do projeto
    c. Mudanças contínuas dos requisitos
    d. Requisitos não definidos de forma adequada
    e. Requisitos não estão claros
    f. Requisitos incorretos
    g. Deficiência no entendimento dos usuários quanto às limitações ou capacidades do sistema

Anexo J – *Templates* usados na gerência de riscos do Guia

1 Estratégia de gerência de riscos

Um documento de estratégia de gerência de riscos é um documento que incorpora os objetivos, estratégias e métodos para executar a gerência de riscos. A estratégia de gerência de riscos descreve todos os aspectos para o processo de identificação, avaliação e controle de riscos.

ESTRATÉGIA DA GERÊNCIA DE RISCOS

1 Escopo da Gerência da Risco

<<Determinar o escopo da gerência de risco que será utilizado pelo projeto, de acordo com as políticas de gerência de risco organizacional. Nesta atividade serão definidos recursos de hardware, software e pessoal necessário à realização da gerência de risco, baseando no escopo do projeto.>>

2 Tempo de reavaliação e monitoração de riscos

<<Intervalo de tempo para monitoramento e reavaliação dos riscos>>

3 Métodos e ferramentas

<<Métodos e ferramentas a serem utilizadas para a identificação, análise, mitigação, monitoramento e comunicação de riscos. Estes métodos são apresentados ao longo deste guia, tais como taxonomia de riscos, cálculo do fator de exposição, entrevistas, brainstorming, delphi, estratégias de tratamento de riscos, emissão de relatórios de risco etc.>>

4 Organização dos riscos

<<Como estes riscos são organizados (por exemplo, por meio de uma taxonomia), categorizados, comparados e consolidados (por exemplo, riscos menores que fazem parte de outros riscos podem ser incluídos nos riscos maiores) >>

5 Parâmetros

<<Parâmetros, incluindo a probabilidade, impacto e limites>>

2 Taxonomia de riscos da organização

A taxonomia de riscos da organização permite que o projeto selecione as categorias e fontes de riscos que são aplicáveis a diversos projetos da organização. Esta taxonomia pode ser baseada em taxonomias já existentes no mercado, e, principalmente, na experiência da própria organização. Com base nesta taxonomia, taxonomias específicas para cada projeto devem ser elaboradas, e taxonomias para cada tipo de projeto (manutenção, desenvolvimento, aquisição etc.) podem ser criadas.

Taxonomia de riscos da organização					
Categoria	**Fonte de Risco**	**Justificativa**	**Técnicas de tratamento de riscos**	**Limites para monitoração**	**Procedimento de medição**
<< categoria do risco>>	<< fonte de risco dentro da categoria>>	<< justificativa para ter incluído o risco dentro desta categoria >>	<< técnicas que podem ser aplicadas para tratar riscos desta fonte de riscos >>	<< limites que podem ser monitorados para verificar se o risco está próximo, ou aconteceu >>	<< procedimentos de coletar dados para as métricas que podem ser usadas para verificar se os limites foram atingidos >>

3 Registro de Riscos

O formulário de registro de riscos deverá conter todas as informações extraídas durante as etapas de identificação e análise dos riscos do projeto (SG2).

Riscos identificados							
Id	**Categoria**	**Fonte de Risco**	**Se...**	**Então...**	**Probabilidade**	**Impacto**	**Fator de Exposição**
<< identificador único do risco >>	<< categoria do risco encontrado >>	<< fonte de risco >>	<< se determinada condição acontecer >>	<< então determinado impacto acontecerá >>	<< probabilidade do risco acontecer com base na escala definida >>	<< impacto caso o risco aconteça com base na escala definida >>	<< cálculo baseado na probabilidade e no impacto definido >>

4 Planos de mitigação dos riscos

O formulário de definição dos planos de mitigação dos riscos deverá conter todas as informações extraídas durante a etapas de desenvolvimento dos planos de mitigação de riscos (SG3 - SP3.1).

Plano de Mitigação de Riscos					
Id	**Responsável**	**Estratégia**	**Prevenção**	**Limite**	**Plano de Contingência**
<< identificador único do risco >>	<< responsável pela prevenção dos riscos >>	<< mitigar, transferir, aceitar, etc. >>	<< técnica de prevença escolhida para tentar mitigar o risco >>	<< limite a ser monitorado para verificar se o risco aconteceu ou está próximo de acontecer >>	<< ação a ser executada caso o risco aconteça >>

5 Relatório de progresso dos riscos

O relatório de progresso dos riscos deve apresentar o status atual do risco (probabilidade, impacto, fator de exposição) e o progresso das ações escolhidas para migiat o risco (SG3 – SP3.2). Além deste formulário, podem ser apresentados gráficos que ajudem no entendimento do progresso das atividades de mitigação e no status dos riscos do projeto. O progresso pode ser indicado por meio de semáforos, onde verde indica progresso nas ações de tratamento, vermelho indica que não está tendo progresso, e os riscos que acontecerem podem ter seu progresso atualizado para “aconteceu” ou caso tenha sido eliminados “eliminado”.

Progresso dos Riscos								
Id	**Prob. Inicial**	**Imp. Inicial**	**F.E. Inicial**	**Prob. Atual**	**Imp. Atual**	**F.E. Atual**	**Progresso**	**Observações**
<< identificador único do risco >>	<< pro-babi-lidade inicial >>	<< im-pacto inicial >>	<< fa-tor de expo-sição inicial >>	<< pro-babi-lidade atual >>	<< im-pacto atual >>	<< fa-tor de expo-sição atual >>	<<verde, vermelho, eliminado ou aconteceu >>	<< observações sobre o prorgresso ou sobre o motivo dos riscos terem acontecido >>

6 Relatório de acompanhamento de ações corretivas

O relatório de acompanhamento de ações corretivas deve conter todos os riscos que aconteceram, e onde foi necessário executar os planos de contingência.

Ações Corretivas					
Id Risco	**Responsável**	**Data Inicial**	**Data Final**	**Ação corretiva**	**Impacto**
<< identificador único do risco >>	<< responsável pela ação corretiva >>	<< data da ação corretiva >>	<< data final da ação corretiva >>	<< pro-babi-lidade atual >>	<< impacto do risco >>

7 Relatório de lições aprendidas

O relatório de lições aprendidas é importante para armazenar todas as lições aprendidas durante a gerência de risco no RCO, para que outros projetos possam consultar estas informações.

Lições Aprendidas			
Id Risco	**Risco (Se.. Então...)**	**Aconteceu?**	**Lição Aprendida**
<< identificador único do risco >>	<< se determinada condição acontecer, então determinado impacto acontecerá >> >>	<< indica se o risco aconteceu ou não >>	<< lições aprendidas com o risco >>