

2 Análise de Risco

A definição de risco mais comumente encontrada nos dicionários (pesquisa realizada em www.dictionary.com) é “exposição à chance de perdas ou danos”. O conceito de risco é um produto da incerteza dos eventos futuros e é parte de todas as atividades. Toda oportunidade de sucesso sempre carrega consigo uma possibilidade de falha, cabendo a cada um avaliar a relação risco *versus* retorno e determinar se estar sujeito a esta perda vale a pena, se este evento é muito grave, ou ainda se o procedimento para a mitigação não oferece um retorno satisfatório.

Um exemplo que ilustra este conceito é a oportunidade de sairmos de casa para trabalhar. Embora estejamos sujeitos a vários riscos, como assaltos, acidentes e outros problemas, a possibilidade da ocorrência de algum destes eventos, quando comparada ao retorno oferecido pela oportunidade (receber um salário e ter recursos para o próprio sustento e diversão) e aos riscos associados ao seu não aproveitamento, geram uma relação risco x retorno favorável para que as pessoas, na maioria dos casos, optem por ir trabalhar.

Por mais controlada e precisa que seja a execução de uma atividade, sempre existe o risco, mesmo que muito remoto, de algo dar errado. Este fato decorre do grande número de variáveis que podem influenciar no resultado final e da sua natureza muitas vezes imprevisível. A partir desse cenário, torna-se necessário aprender a conviver com riscos, balanceando as possíveis conseqüências negativas ou estratégias para a mitigação das perdas.

2.1. Gerência de Risco

A disciplina de gerência de riscos foi criada com o objetivo de manter esta convivência com riscos (DeMarco, Lister, 2003) e fornece meios para a identificação e acompanhamento e controle de riscos ao longo da execução de projetos, sendo as suas principais atividades:

- **Identificação:** Nesta atividade os riscos inerentes a uma etapa do desenvolvimento (fase, processo, iteração) são identificados, através

do levantamento das ameaças presentes e do impacto que podem provocar caso se realizem.

- **Análise:** Nesta atividade os riscos identificados são analisados no projeto, identificando o nível de exposição de cada um. Em seguida, é realizado um estudo de classificação dos riscos no qual, baseando-se no relacionamento entre a exposição e consequência negativa do risco e o benefício da oportunidade, determina-se quais serão eliminados, quais serão mitigados, quais serão aceitáveis e quais serão acompanhados.
- **Planejamento:** Nesta atividade é realizado um planejamento de como os riscos serão abordados ao longo do projeto. Comumente são elaborados planos de mitigação, eliminação e acompanhamento de riscos que serão utilizados como base para a gerência de riscos.
- **Controle:** Nesta atividade os planos elaborados são executados e o projeto é acompanhado no que se refere aos riscos. Os riscos identificados são analisados constantemente para a identificação do seu estado atual e atualização dos planos elaborados. Novos riscos podem ser identificados também.

A gerência de riscos utiliza como base o conceito de exposição de risco (Boehm, 1991 e Boehm, DeMarco, 1997). Para cada ameaça ou possível fonte de problema que possa causar perdas ao projeto, a exposição (*Exp*) é definida como o produto da probabilidade da perda ocorrer (*P*) e do tamanho da perda (impacto *I* no projeto, artefato, ativo ou qualquer elemento que seja o foco da análise de risco):

$$Exp = P * I$$

A estratégia de diminuição de riscos utilizada nos planos elaborados durante a atividade de planejamento pode tentar reduzir a probabilidade do risco, fazendo com que a concretização da perda seja algo muito difícil de ocorrer, pode tentar reduzir o impacto do risco, fazendo com que a consequência da materialização do risco seja tão pequena que a sua ocorrência não afetará o resultado final do projeto, ou ambas, resultando em um balanceamento razoável entre as perdas e a probabilidade de sua ocorrência no projeto.

A eliminação total dos riscos associados a um projeto ou iniciativa é um conceito utópico (DeMarco, Lister, 2003). Cada ação de identificação,

acompanhamento e controle (redução, mitigação ou contenção de riscos) possui um custo associado, cabendo a cada indivíduo ou organização identificar o ponto de equilíbrio entre o nível de exposição aos riscos e o custo de redução. Para cada projeto ou iniciativa deve-se determinar um índice de exposição aos riscos aceitável, que seja suficiente para as características do projeto e tenha um custo que não comprometa o retorno do investimento.

2.2. Análise de Risco em Processos

Embora a análise e o gerenciamento de riscos sejam amplamente utilizados em diversos setores da economia, como no mercado financeiro e no setor de seguros, onde a sua utilização é a base de todas as decisões tomadas, na área de desenvolvimento de software esta abordagem é raramente encontrada nos projetos, principalmente no que se refere aos processos utilizados (Boehm, 1991 e Boehm, DeMarco, 1997).

Com a crescente demanda por qualidade dos produtos de software, a adoção de modelos de maturidade, normas de qualidade e guias de boas práticas tem se tornado cada vez mais frequentes, o que contribui para a utilização de algum controle sobre riscos ao longo dos projetos realizados (modelos como CMMI e MPS.BR, normas como a ISO/IEC 15504 (ISO/IEC, 2004) e 12207 e guias de boas práticas como o PMBOK (PMI, 2004) pregam a realização de uma gerência de riscos. Entretanto, este controle se restringe ao escopo do projeto e em muitos casos possui uma visão limitada e isolada dos riscos, ameaças e suas conseqüências.

Muitas vezes, departamentos, projetos e equipes de uma mesma organização não compartilham informações (Brache, Rummler, 1995). Isto implica que neles, o mesmo risco pode ser identificado e tratado de forma diferente em projetos com características semelhantes ou até mesmo por equipes diferentes de um mesmo projeto, gerando re-trabalho, consumo desnecessário de recursos e, conseqüentemente, comprometendo a qualidade do produto final. É necessário, portanto a utilização de meios que forneçam uma visão geral dos riscos da organização, permitindo o direcionamento eficiente de recursos e a reutilização de soluções.

Partindo do princípio de que a qualidade do produto está intimamente relacionada à qualidade dos processos utilizados na sua produção e que o objetivo do negócio de mais alto nível (objetivo do negócio que deriva todos os demais) de uma organização é o de entregar o produto solicitado com a qualidade esperada, pode-se concluir que qualquer risco à qualidade do produto e, conseqüentemente, qualquer risco associado aos processos utilizados, representam uma possibilidade de perda para a organização. Sendo assim, um dos principais pontos de controle para que se tenha uma visão geral dos riscos é o processo produtivo.

Embora algumas abordagens já utilizem este conceito, como (Poulin, 2005) e (ISO/IEC, 2004), a grande maioria dos métodos de controle de processos se limita a verificação de conformidade, o que pode levar a um processo com uma conformidade de 90%, mas com 90% dos riscos presentes.

Neste trabalho é proposta uma abordagem na qual é identificado de forma customizada tanto o nível de conformidade como o nível de risco em cada área de processo. Dessa forma uma análise dos processos da organização fornece duas classes de dados para a tomada de decisão e direcionamento de recursos.