Planejando e Monitorando Riscos em Engenharia de Software - P&M SE Riscos

Carlos Simões [1]

[1]Makalu Consultoria – Rio de Janeiro – RJ – Brasil

casimoes@outlook.com

Abstract: *One of the main challenges in agile software development is ensuring that planning and monitoring risks and opportunities is simple and effective. It's essential to adopt a method integrated with a planning and monitoring tool that's easy to use and learn, flexible, and provides important information without overloading activities. This article reports on experiences with a simple, agile approach, compatible with CMMI, MPS, ISO 12207, ISO 27000, and ISO 31000 models and standards, used by five organizations at different times to meet maturity assessment, certification, and process improvement needs..*

Resumo. *Um dos principais desafios no desenvolvimento ágil de software é assegurar que o planejamento e o monitoramento de riscos e oportunidades ocorram de forma simples e eficaz. É essencial adotar um método integrado a uma ferramenta para planejamento e monitoramento de fácil utilização e aprendizado, flexível e disponibilizando importantes informações sem sobrecarregar as atividades. Este artigo relata experiências de uma abordagem ágil e simples, compatível com os modelos e normas CMMI, MPS, ISO 12207, ISO 27000 e ISO 31000, utilizada por cinco organizações em momentos distintos, com o objetivo de atender a avaliação de maturidade, certificação e melhoria de processos.*

1. Introdução

As organizações enfrentam o desafio de equilibrar agilidade e governança, sendo que um dos principais entraves é garantir que o planejamento e o monitoramento de riscos e oportunidades seja simples e adequado à execução das atividades em um ambiente ágil e dinâmico. É fator de sucesso o uso de um método para a gestão de riscos e oportunidades, além de ferramenta que apoie de forma prática, leve e adaptável à organização e ao ambiente ágil [2].

Este artigo apresenta uma abordagem de planejamento e monitoramento de riscos e oportunidades, em conformidade com MPS BR SW [5], CMMI [4], ISO 31000 [3], ISO 12207 [1] e ISO 27001 [9], implantada em 5 organizações em momentos e contextos diferentes, sendo 3 submetidas a avaliações CMMI [4], uma à certificação ISO 27001 e a última, com o objetivo de melhoria de processo. Não é objetivo discutir fundamentos teóricos da gestão de riscos, que podem ser consultados nas normas e modelos citados. A proposta foi estruturada com foco em baixo custo, adoção rápida e ser auditável, apoiando a gestão, a evolução do time e avaliação externa.

A proposta não tem objetivo fazer comparação com métodos de gestão de riscos e sim, em apresentar uma abordagem para reduzir riscos, aproveitar oportunidades,

incrementar o comprometimento e garantir uma comunicação eficaz com as partes interessadas, crucial para o sucesso organizacional. Análise de adequação com as áreas práticas RSK e DAR do CMMI-DEV ML5 [4], com resultados esperados relacionados a Risco em GPR e GDE do MPS BR SW [5], requisitos da norma ISO 31000 [3] e ISO 27001 [9] demonstrou cobertura de 100%.

2. Motivação

A motivação deste trabalho vem da observação prática de que há uma lacuna entre a gestão de riscos e oportunidades e sua aplicação prática em organizações que almejam a maturidade, agilidade e simplicidade na gestão de suas atividades, especialmente em organizações em que a estratégia organizacional, foca em conformidade com auditorias, benchmarks, normas, modelos de referência e processos de melhoria contínua.

A gestão de riscos é pouco explorada nos métodos ágeis, ao longo das reuniões diárias e durante a realização das atividades do time, deve-se atentar pelo monitoramento dos riscos. Uma abordagem leve e padronizada de um método e ferramenta de apoio, considerando a características da organização, fundamentada em experiências e orientada a resultados facilita a adoção da gestão de riscos pelo time. Ao final de cada Sprint seria aconselhável fazer uma análise dos riscos que ocorreram.

Atualmente é comum que times ágeis sejam compostos por força de trabalho terceirizada e funcionários internos, tornando-se uma escolha estratégica para organizações que buscam maior agilidade e rapidez para atender à crescente demanda por desenvolvimento de software, resultando em benefícios ou oportunidades e riscos que precisam ser identificados e monitorados com eficácia [7]. A distribuição de tarefas entre o time, deve ser analisada e alinhada com uma estratégia organizacional para terceirização da força de trabalho, com o objetivo de reduzir riscos, como por exemplo, evitar conflito de interesse quando a realização da tarefa e a gestão da força de trabalho terceirizada forem realizadas por pessoas de um mesmo fornecedor [6].

3. Revisão da Literatura

O propósito da gestão de riscos é a criação e proteção de valor. Ela melhora o desempenho, encoraja a inovação e apoia o alcance de objetivos. Gerenciar riscos é iterativo e auxilia as organizações no estabelecimento de estratégias, no alcance de objetivos e na tomada de decisões fundamentadas.

Riscos e Oportunidades devem ser identificados e impactos, probabilidade de ocorrência, prioridade de tratamento, fontes e consequência devem ser identificadas e documentadas. Em adição, devem ser monitorados em relação às estratégias definidas e seus resultados comunicados às partes interessadas [4] [5].

A gestão de riscos é um processo dinâmico e iterativo, personalizado para as necessidades e cultura da organização. Convém que a gestão de riscos seja uma parte integrada e não separada das atividades significativas e do propósito organizacional.

A gestão de riscos é parte da governança e liderança, fundamental para estratégia de como a organização é gerenciada em todos os níveis [3]. A eficácia da gestão de riscos dependerá da sua integração com a governança, com os processos e em todas as atividades da organização, incluindo a tomada de decisão. Requer apoio das partes interessadas, em particular da Alta Direção e os Órgãos de Supervisão [3].

4. Abordagem Utilizada

O tratamento de riscos e oportunidades deve permitir a disseminação dos conceitos de forma eficaz, simples, clara, fácil de usar, apoiando a identificação, registro, análise e gerência de potenciais riscos ou oportunidades. Com o objetivo de aumentar a probabilidade de atingir os objetivos, reduzir retrabalho, reduzir custos causados por não conformidade, atenuar impactos negativos, alavancar e capitalizar impactos positivos, foi definido um método e ferramenta para contemplar todos os requisitos e informações necessárias para uma eficaz gestão de riscos e oportunidades, facilitando o uso e a aplicação. Tal método e ferramenta foram implantados em 5 organizações.

Na primeira organização, o projeto de melhoria de processo, realizado entre 2010 e 2017 teve como objetivo evoluir o nível de maturidade dos processos [8], que estava no CMMI ML3 para o CMMI ML5 [4]. A primeira versão do método e da ferramenta de gestão de riscos e oportunidades elaborada, não contemplava a possibilidade de monitoramento na ferramenta. Riscos organizacionais foram identificados e associados às causas e estratégia de mitigação. O método e a ferramenta contribuíram significantemente para apoiar e agilizar a gestão de riscos e oportunidades na realização das atividades, onde mais de 900 evolutivos de pequeno tamanho foram desenvolvidos ao longo de 6 anos de projeto, agregando valor à organização.

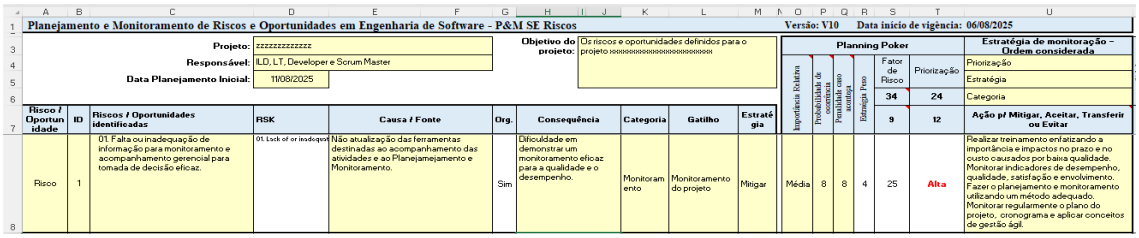
Na segunda organização, o projeto de melhoria de processo realizado em 2021, teve como objetivo alcançar o nível de maturidade 3 do modelo de referência CMMI [4]. Na abordagem anterior foi adicionado o monitoramento dos riscos e oportunidades, fazendo que todas as práticas estabelecidas para a área prática RSK fossem atendidas. Foi adicionado o uso de critérios para o tratamento dos riscos, em conformidade com *Decision Analysis and Resolution* do CMMI [4], contemplando as 6 práticas.

Na terceira organização, o projeto de melhoria teve como objetivo apoiar o planejamento e monitoramento de riscos para a certificação na norma ISO 27001 [9], contemplando a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização. Os requisitos para a gestão de riscos são os mesmos, estabelecidos na Norma ISO 31000 [3], o que difere são os tipos de riscos que foram identificados. A organização aplicou um processo de tratamento dos riscos de segurança da informação, preparou um plano para tratamento dos riscos e obteve a aprovação dos responsáveis pelos riscos identificados. Ao analisar fontes e identificar riscos, deve-se considerar: Contexto da organização; Atendimento aos requisitos das Partes Interessadas pertinentes; Aspectos de Segurança da Informação; Dia a dia da realização dos processos; Registrar na ferramenta os riscos identificados, o respectivo tratamento, a priorização e realizar os monitoramentos.

Na quarta organização, o projeto de melhoria de processo, realizado em 2024 e 2025, teve como objetivo alcançar o nível de maturidade 3 do modelo de referência CMMI [4]. A versão da ferramenta de gerenciamento de risco e oportunidade utilizada na segunda e terceira organização evoluiu e incorporou várias melhorias inclusive a possibilidade de monitoramento e apresentação de gráficos, além da possibilidade de elaboração de plano de ação para tratar as ocorrências de riscos, contemplando ação a ser realizada, monitoramento, data e responsável pela solução.

Na quinta organização, analisando os cenários de uso e comentário do líder do projeto da quarta organização: “Melhorar a alocação das telas e layout, pois em alguns

momentos gera uma confusão para o usuário, devido a grande quantidade de elementos, em linhas e colunas. No geral, em quesito de elementos para ajudar na gestão dos riscos ela atende super bem e achei bem completa, o que necessita de melhoria é justamente a interface com o usuário, em que os elementos estejam dispostos de uma forma mais limpa e fácil visualização". Foi proposta uma nova estruturação das informações e telas para facilitar o preenchimento e visualização, inclusive a separação das informações de planejamento (Figura 1) e de monitoração, criando uma aba específica para registrar o monitoramento dos riscos e oportunidades (Figura 2). Inclusive com geração de gráficos e importantes informações para o monitoramento (Figura 3).



Planejamento e Monitoramento de Riscos e Oportunidades em Engenharia de Software - P&M SE Riscos — Versão: V10 — Data início de vigência: 06/08/2025

Projeto: zzzzzzzzzzzzz
Responsável: ILD, LT, Developer e Scrum Master
Data Planejamento Inicial: 11/08/2025
Objetivo do projeto: Os riscos e oportunidades definidos para o projeto xxxxxxxxxxxxxxxxxxxxxxxxxx

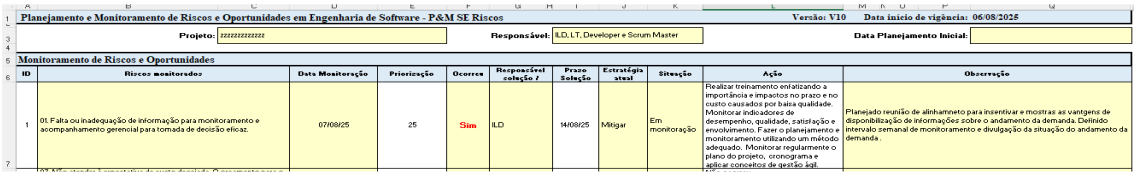
Planning Poker: Importância Relativa | Probabilidade de ocorrência | Prioridade caso ocorra | Estratégia Peso | Fator de Risco | Priorização
Estratégia de monitoração – Ordem considerada: Priorização; Estratégia; Categoria; Ação p/ Mitigar, Aceitar, Transferir ou Evitar

Risco / Oportunidade	ID	Riscos / Oportunidades identificadas	RSK	Causa / Fonte	Org.	Consequência	Categoria	Gatilho	Estratégia	Importância Relativa	Probabilidade de ocorrência	Prioridade caso ocorra	Estratégia Peso	Fator de Risco	Priorização
														9	12
Risco	1	01. Falta ou inadequação de informação para monitoramento e acompanhamento gerencial para tomada de decisão eficaz.	01. Lack of or inadequate	Não atualização das ferramentas destinadas ao acompanhamento das atividades e ao Planejamejamento e Monitoramento.	Sim	Dificuldade em demonstrar um monitoramento eficaz para a qualidade e o desempenho.	Monitoramento	Monitoramento do projeto	Mitigar	Média	8	8	4	25	Alta

Estratégia de monitoração – Ordem considerada: 34 | 24 | Categoria

Ação p/ Mitigar, Aceitar, Transferir ou Evitar: Realizar treinamento enfatizando a importância e impactos no prazo e no custo causados por baixa qualidade. Monitorar indicadores de desempenho, qualidade, satisfação e envolvimento. Fazer o planejamento e monitoramento utilizando um método adequado. Monitorar regularmente o plano do projeto, cronograma e aplicar conceitos de gestão ágil.

Figura 1 - Planejamento de Riscos e Oportunidades



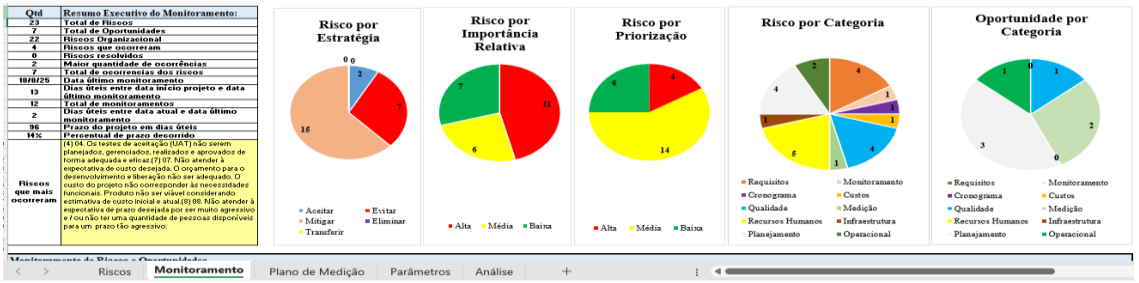
Planejamento e Monitoramento de Riscos e Oportunidades em Engenharia de Software - P&M SE Riscos — Versão: V10 — Data início de vigência: 06/08/2025

Projeto: zzzzzzzzzzzzz — Responsável: ILD, LT, Developer e Scrum Master — Data Planejamento Inicial:

Monitoramento de Riscos e Oportunidades

ID	Riscos monitorados	Data Monitoração	Priorização	Ocorre	Responsável coleção /	Prazo Seleção	Estratégia atual	Situação	Ação	Observação
1	01. Falta ou inadequação de informação para monitoramento e acompanhamento gerencial para tomada de decisão eficaz.	07/08/25	25	Sim	ILD	14/08/25	Mitigar	Em monitoração	Realizar treinamento enfatizando a importância e impactos no prazo e no custo causados por baixa qualidade. Monitorar indicadores de desempenho, qualidade, satisfação e envolvimento. Fazer o planejamento e monitoramento utilizando um método adequado. Monitorar regularmente o plano do projeto, cronograma e aplicar conceitos de gestão ágil.	Planejado reunião de alinhamento para incentivar e mostras as vantgens de disponibilização de informações sobre o andamento da demanda. Definido intervalo semanal de monitoramento e divulgação da situação do andamento da demanda.

Figura 2 - Monitoramento de Riscos e Oportunidades



Qtd	Resumo Executivo do Monitoramento:
23	Total de Riscos
7	Total de Oportunidades
22	Riscos Organizacional
4	Riscos que ocorreram
0	Riscos resolvidos
2	Maior quantidade de ocorrências
7	Total de ocorrencias dos riscos
18/8/25	Data último monitoramento
13	Dias úteis entre data início projeto e data último monitoramento
12	Total de monitoramentos
2	Dias úteis entre data atual e data último monitoramento
96	Prazo do projeto em dias úteis
14%	Percentual de prazo decorrido
Riscos que mais ocorreram	(4) 04. Os testes de aceitação (UAT) não serem planejados, gerenciados, realizados e aprovados de forma adequada e eficaz.(7) 07. Não atender à espectativa de custo desejada. O orçamento para o desenvolvimento e liberação não ser adequado. O custo do projeto não corresponder às necessidades funcionais. Produto não ser viável considerando estimativa de custo inicial e atual.(8) 08. Não atender à espectativa de prazo desejada por ser muito agressivo e / ou não ter uma quantidade de pessoas disponíveis para um prazo tão agressivo.

Risco por Estratégia — Aceitar, Evitar, Mitigar, Eliminar, Transferir
Risco por Importância Relativa — Alta, Média, Baixa
Risco por Priorização — Alta, Média, Baixa
Risco por Categoria — Requisitos, Monitoramento, Cronograma, Custos, Qualidade, Medição, Recursos Humanos, Infraestrutura, Planejamento, Operacional
Oportunidade por Categoria — Requisitos, Monitoramento, Cronograma, Custos, Qualidade, Medição, Recursos Humanos, Infraestrutura, Planejamento, Operacional

Riscos | Monitoramento | Plano de Medição | Parâmetros | Análise

Figura 3 - Resumo Executivo, Gráficos e Indicadores

Foi elaborada uma lista com 22 de riscos organizacionais, como: i) Falta ou inadequação de informação para monitoramento e acompanhamento gerencial para tomada de decisão eficaz; ii) Os testes de aceitação não serem planejados, realizados, aprovados e gerenciados de forma adequada e eficaz; iii) Não atender à expectativa de custo desejada. Análise realizada sobre os 22 riscos, possibilitou registrar informações em uma aba específica (Análise), usada como referência e preenchimento automático das informações de planejamento dos riscos, sendo possível trocar ou complementar as informações conforme característica de um projeto. Foi adicionada aba com Plano de Medição e definição de medidas relacionadas aos riscos e oportunidades, atendendo aos resultados esperados do Processo Medição MPS BR SW [5]

5. Consideração Final

A aplicação prática da abordagem em cinco organizações com diferentes objetivos e níveis de maturidade, possibilitou aprendizado e evolução do método e ferramenta, que

foram bem recebidos pelos times, devido à simplicidade, adaptabilidade e baixo custo de adoção. A solução centrada na realidade operacional dos times, e não como soluções genéricas ou impositivas, foi fator-chave para o engajamento. A solução é 100% compatível com normas e modelos nos itens relacionados à Riscos e Oportunidades.

Em avaliações internas, gestores relataram melhora na comunicação entre áreas técnicas e gerenciais devido à maior clareza sobre a gestão de riscos e oportunidades. Em ambientes com terceirização, a separação entre planejamento, execução e monitoramento evitou riscos e aumentou a transparência nas entregas. A experiência em cinco organizações distintas demonstra que é viável integrar métodos ágeis com práticas formais de gestão de riscos e oportunidades. Ao analisar os riscos identificados, deve-se monitorar conforme a estratégia organizacional definida. Especial atenção aos riscos com maior prioridade e os que mais ocorreram.

Este trabalho contribui para o campo da engenharia de software ao apresentar uma solução prática, replicável e adaptável, que equilibra agilidade, rigor técnico, que disponibiliza um conjunto muito importante de informações, fundamentais para a gestão eficaz dos riscos e oportunidades.

6. Referências

[1] ISO/IEC (2017). ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes, Geneve: ISO, 2017.

[2] [Simões and Silva 2024] Simões, C., & Silva, T. S. da C. (2024). Agile Planning and Monitoring with Kanban and Measurement. IFPUG Metric Views, June 2024. Available at: https://ifpug.org/learning-and-events/knowledge-cafe-webinar-series.

[3] ABNT NBR ISO 31000:2018 Gestão de riscos — Diretrizes. Risk management — Guidelines. ICS ISBN 978-85-07-07470-0. Segunda edição 28.03.2018

[4] CMMI Institute. CMMI Model V3.0. Available at: https://cmmiinstitute.com/resource-files/public/cmmi-model-materials/cmmi-model-release-notes. Accessed on: March 3, 2025.

[5] Software Process Improvement Group (Softex). Guia Geral MPS de Software: 2024. Available at: https://softex.br/download/guia-geral-mps-de-software2024/. Accessed on: March 3, 2025.

[6] Simões, C. (2024). A Difícil Arte de Planejar e Monitorar Custo, Desempenho e Qualidade Quando da Adoção de Métodos Ágeis. Workshop Anual do MPS – WAMPS 2024.

[7] Simões, C. (2023). Modelo de Referência de Processo para Terceirização de Força de Trabalho de TI. Tese de Doutorado, Universidade Federal do Estado do Rio de Janeiro, Programa de Pós-Graduação em Informática.

[8] Simões, C., & Montoni, M. (2014). Applying Statistical Process Control in Small-Sized Evolutionary Projects: Results and Lessons Learned in the Implementation of CMMI-DEV Maturity Level 5 in Synapsis Brazil. Journal of Software Engineering Research and Development, 2:2. Available at: 2195-1721-2-2.pdf (springer.com).

[9] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Third edition 2022-1