PUC Minas
A B A K Ó S
Instituto de Ciências Exatas e Informática

Uma Análise Comparativa das Práticas do Processo de Gerência de Riscos usando Modelos de Qualidade para o Processo de *Software*[*]

A Comparative Analysis of Practices in the Risk Management Process using Quality Models for the Software Process

Heresson João Pampolha de Siqueira Mendes[1]
Sandro Ronaldo Bezerra Oliveira[2]

Resumo

A Gerência de Riscos é uma área de conhecimento estudada nos principais modelos de qualidade de *software*, e trata-se de um fator importante para o sucesso de um projeto, pois gerencia a probabilidade de um evento inesperado ocorrer e suas consequências, denominado risco. Um modo de atingir o sucesso no gerenciamento de riscos de um projeto de *software* dá-se a partir da adoção de recomendações presentes nos modelos de qualidades de *software*. Este trabalho tem como objetivo propor boas práticas no tratamento de riscos por meio do mapeamento dos principais modelos de qualidade estudados em trabalhos semelhantes (MR-MPS-SW, CMMI-Dev, PMBoK, ISO/IEC 12207 e ISO/IEC 16085), definindo, assim, um modelo de processo que agregue as melhores recomendações presentes nos padrões internacionais.

Palavras-chave: Qualidade de *Software*. Gerenciamento de Riscos. Modelos de Qualidade de *Software*. Processo de *Software*.

[*]Submetido em 02/02/2014 – Aceito em 22/04/2014

[1]Mestre em Ciência da Computação pelo Programa de Pós-graduação em Ciência da Computação da Universidade Federal do Pará, Brasil – heresson@gmail.com

[2]Doutor em Ciência da Computação. Professor da Faculdade de Computação e do Programa de Pós-Graduação em Ciência da Computação da Universidade Federal do Pará, Brasil – srbo@ufpa.br

Abstract

Risk Management is an important knowledge area studied among the main software quality models, and it is a significant success factor of a project, because it manages the occurrence of an unexpected event probability and its consequences. A way to achieve success in the software project risk management is by following the recommendations in the software quality models. This paper aims to propose the best practices in risks treatment by mapping the main quality models studied in related works (MR-MPS-SW, CMMI-DEV, PMBOK, ISO/IEC 12207 and ISO/IEC 16085), defining a process model that combines the best recommendations among international standards.

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

1 INTRODUÇÃO

O mercado de *software* exige, com frequência, a entrega de produtos melhores, mais baratos e de um modo mais rápido do que no passado. Consequentemente, esses fatores exigem um maior gerenciamento das atividades em uma organização, a fim de atingir seus objetivos de negócio (SEI – Software Engineering Institute, 2010). Para desenvolver produtos de *software* alinhados aos atuais requisitos de qualidade, é necessário garantir a qualidade do processo de desenvolvimento por meio do planejamento, medição e monitoramento de cada etapa do ciclo de vida do *software*.

Visando um melhor acompanhamento da evolução do processo de *software*, surgiram modelos de qualidade, que sugerem melhorias de forma gradual e categorizada, envolvendo as mais diversas áreas constantes na engenharia de *software*. Entre os modelos mais utilizados na atualidade, destacam-se a norma ISO/IEC 12207 (ABNT – Associação Brasileira de Normas e Técnicas, 2009), o *Capability Maturity Model Integration for Development* - CMMI-DEV(SEI – Software Engineering Institute, 2010), e, no âmbito nacional, o Modelo de Referência para Melhoria de Processo de *Software* para *Software* (MR-MPS-SW)(SOFTEX – Associação para Promoção da Excelência do Software Brasileiro, 2012a).

A gerência de riscos é uma área de conhecimento estudada nos principais modelos de qualidade, e trata-se de um fator importante para o sucesso de um projeto, pois gerencia a probabilidade de um evento inesperado ocorrer e suas consequências, denominado risco (IEEE – Institute of Electrical and Electronics Engineers, 2006). Um meio de atingir o sucesso no gerenciamento de riscos de um projeto, dá-se por recomendações presentes nos modelos de qualidades citados anteriormente, além de outros, como o guia de gerenciamento de projetos PMBOK – *Project Management Body of Knowledge* (PMI – Project Management Institute, 2013) e o padrão internacional para gerência de riscos definido em conjunto pelo IEEE e ISO/IEC, denominado ISO/IEC 16085:2006 (IEEE – Institute of Electrical and Electronics Engineers, 2006).

A diversidade de normas e padrões internacionais relativos ao gerenciamento de riscos faz com que haja uma grande quantidade de boas práticas dispersas, que eventualmente podem não ser aproveitadas, caso seja utilizado um dos modelos de qualidade para a implantação de melhoria no processo de *software*.

Este trabalho objetiva propor boas práticas no tratamento de riscos, por meio do mapeamento dos resultados esperados do processo de Gerência de Riscos do MR-MPS-SW, presentes no guia de implementação conjunta com CMMI-DEV 1.3 (SOFTEX – Associação para Promoção da Excelência do Software Brasileiro, 2012b), com as tarefas presentes no processo de gestão de risco da norma ISO/IEC 12207:2009 e as orientações de implementação contidas no padrão ISO/IEC 16085:2006 e no guia PMBOK, em sua 5ª edição, por meio das entradas, ferramentas e técnicas, e saídas da área de gerenciamento de riscos do projeto.

As boas práticas serão apresentadas de modo conjunto em um modelo de processo de *software*, que agrega as exigências e as recomendações dos modelos de qualidade selecionados, visando orientar futuras implantações do processo de gerência de riscos de maneira que seja

aderente aos padrões internacionais.

Este artigo apresenta, na Seção 2, alguns trabalhos relacionados ao mapeamento de modelos de qualidade de *software* e gerenciamento de riscos em projetos de *software*. Na Seção 3, é apresentada a metodologia utilizada para realizar o mapeamento e definir o processo de *software*, além de especificar como serão apresentados os resultados. Em seguida, na Seção 4, é apresentado o estudo comparativo dos resultados esperados do MR- MPS-SW com outros modelos. A Seção 5 apresenta as boas práticas coletadas a partir do mapeamento dos modelos de qualidade. Na Seção 6, é apresentado um estudo de caso, que trata de um modelo de processo de *software* agregando as melhores práticas identificadas no mapeamento. Por fim, a Seção 7 apresenta as considerações finais e trabalhos f

2 TRABALHOS RELACIONADOS

Após revisão na literatura especializada, foram analisados diversos trabalhos relacionados ao gerenciamento de riscos. Algumas propostas assemelham-se, porém, não englobam práticas constantes em diversos modelos de qualidade associadas à implementação do programa de melhoria da qualidade do processo de *software*. Os trabalhos com propostas semelhantes serão destacados a seguir.

As pesquisas de Raz e Hillson (2005) e de Gusmão e Moura (2004) apresentam uma comparação entre os principais padrões internacionais para o gerenciamento de riscos, com o objetivo de identificar quais etapas são similares em cada padrão. Por ser um estudo um pouco mais antigo, pode ser considerado desatualizado, pois atualmente existem novas versões para alguns dos padrões abordados.

Outros trabalhos mais recentes apresentaram mapeamentos entre modelos de qualidade de *software*. Wangenheim et al. (2010) realizam um mapeamento entre o modelo CMMI-DEV v1.2 e o Guia de gerência de Projetos PMBOK 5ª edição, porém contemplam apenas atividades relacionadas diretamente ao gerenciamento de projetos do guia CMMI-DEV (PP - *Project Planning*, PMC - *Project Monitoring and Control*, SAM - *Supplier Agreement Management*). Rout e Tuffley (2007) realizam um mapeamento da norma ISO/IEC 15504 e o modelo CMMI-DEV, abordando, também, superficialmente, a norma ISO/IEC 12207, não especificando de modo claro em quais atividades da norma há a aderência entre os modelos. Mutafelija e Stromberg (2009) realizam um mapeamento entre o modelo CMMI e as diversas normas ISO (9001:2000; 20000:2005; 15288:2008; 12207:2008) por meio de uma relação binária entre o modelo CMMI e as normas ISO.

O trabalho de McCaffery et al. (2009) também está relacionado à proposta deste artigo, pois propõe um modelo de capacidade de *software* voltado para o gerenciamento de riscos, abrangendo algumas práticas do CMMI integrada a práticas mandatórias presentes em normas relacionadas às organizações fabricantes de dispositivos médicos. Porém, possui um escopo restrito a essas organizações.

Os resultados encontrados nos trabalhos relacionados evidenciam a importância do mapeamento de modelos de qualidade, assim como a necessidade de realizar estudos a respeito das novas versões desses modelos. Outra observação destacada é o fato de haver muitas pesquisas relacionadas ao modelo de maturidade CMMI-DEV, porém, há uma deficiência em estudos de mapeamentos relacionados ao modelo de maturidade nacional MR- MPS-SW.

3 METODOLOGIA DE PESQUISA

Para mapear todas as boas práticas, foi tomado como base o modelo MR-MPS-SW, visto que esse é mais utilizado no âmbito nacional. Inicialmente, foi realizada uma análise comparativa entre os resultados esperados do processo de gerência de riscos do guia de implementação do MR-MPS-SW parte 11 e as tarefas do processo de Gestão de Risco da norma ISO/IEC 12207, resultando em uma tabela que agregou itens dos dois modelos.

Posteriormente, o guia de implementação parte 11 foi analisado em conjunto com a área de processos de gerenciamento de riscos do guia PMBOK - 5ª edição, por meio do mapeamento de resultados esperados com as entradas, ferramentas e técnicas, e saídas de cada processo dessa área. Além disso, foi realizado um mapeamento semelhante com o padrão internacional IEEE ISO/IEC 16085:2006, que trata da implementação de gerência de riscos. Esses estudos resultaram em uma tabela comparativa entre os resultados esperados e as orientações de implementação contidas nestes modelos de qualidade.

Logo, há dois tipos de mapeamentos: (1) o mapeamento do MR-MPS-SW e da norma ISO/IEC 12207, que visa identificar a possibilidade de um processo aderente a ambos, por meio de resultados esperados e tarefas em comum; e (2) o mapeamento do MR-MPS-SW e das recomendações presentes nos padrões PMBOK e 16085, que visa agrupar um conjunto de sugestões de implementação do processo de gerência de riscos.

O resultado dos estudos comparativos, apresentado na Seção 4, dá-se do seguinte modo: por meio de tópicos, cada resultado esperado no MR-MPS-SW será apresentado com uma breve descrição e análise relacionada à implantação em conjunto com o modelo CMMI- DEV e com a norma ISO/IEC 12207; em seguida, serão relacionadas aos resultados esperados do MR-MPS-SW as orientações de implementação presentes no Guia PMBOK e no padrão internacional IEEE ISO/IEC 16085. Os ativos (resultados esperados, práticas específicas, tarefas, entradas, ferramentas e técnicas, e saídas) constantes nos modelos de qualidade que não possuem uma prática equivalente no modelo MR-MPS-SW são apresentados na última subseção (4.10) deste segmento do trabalho.

Para categorizar a análise conjunta de modo mais claro, cada mapeamento realizado entre o guia MR-MPS-SW e os outros modelos recebeu uma classificação relacionada ao grau de mapeamento. Esta classificação, baseada na classificação que o guia de implementação parte 11 realiza entre os modelos MR-MPS-SW e CMMI-DEV, divide-se nas seguintes categorias:

- Equivalente (EQU): As exigências do MR-MPS-SW e da ISO/IEC 12207 são exatamente

as mesmas; e/ou uma sugestão de implementação do PMBOK ou da IEEE ISO/IEC 16085 atende às necessidades do resultado esperado do MR- MPS-SW em sua totalidade;

- Equivalente em conjunto (EQU+): As exigências do MR-MPS-SW e da ISO/IEC 12207 são exatamente as mesmas quando complementadas com mais de um resultado esperado ou tarefa; e/ou duas ou mais sugestões de implementação do PMBOK ou da IEEE ISO/IEC 16085 atendem às necessidades do resultado esperado do MR-MPS-SW;

- Não Equivalente (NEQ): As exigências do MR-MPS-SW e da ISO/IEC 12207 não são exatamente as mesmas; e/ou uma sugestão de implementação do PMBOK ou da IEEE ISO/IEC 16085 não atende totalmente ao resultado esperado do MR-MPS-SW, nem possui complementação para ser atendida em conjunto;

- Inexistente (INE): Não existe resultado esperado do MR-MPS-SW na ISO/IEC 12207 ou vice-versa; e/ou não existe sugestão de implementação no PMBOK ou na IEEE ISO/IEC 16085 que atenda ao resultado esperado, ou vice-versa.

Todos os resultados obtidos incluindo mapeamentos e suas categorizações foram avaliados detalhadamente, por meio de revisão por pares com um implementador e avaliador oficial da SOFTEX – Associação para a Promoção do *Software* Brasileiro (órgão brasileiro mantenedor do MR-MPS-SW) e SEI – *Software Engineering Institute* (órgão norte-americano mantenedor do CMMI-DEV), que possui experiência na implementação e avaliação de modelos de qualidade de *software* em empresas de todo o Brasil.

Em seguida, a partir da análise dos mapeamentos, foi elaborado um conjunto de boas práticas, identificando quais destas são semelhantes em todos os modelos, e/ou quais se destacam em apenas um ou mais modelos. Essas boas práticas também foram avaliadas pela revisão por pares, de modo semelhante à etapa anterior.

Após a consolidação das boas práticas presentes nos modelos, foi elaborado um modelo de processo de *software*, que visa auxiliar a implementação da gerência de riscos em um projeto de desenvolvimento de *software*, de modo que seja aderente às boas práticas identificadas e, consequentemente, aos modelos analisados neste trabalho. Igualmente, esse processo foi avaliado por um revisor com vasta experiência em implementação de modelos de maturidade de *software*, e suas revisões foram consideradas para a definição da versão final do processo aqui apresentado.

4 MAPEAMENTO ENTRE MODELOS DE QUALIDADE

Cada tópico desta seção apresenta um resultado esperado do processo de Gerência de Riscos (GRI) do MR-MPS-SW juntamente com os resultados obtidos no estudo. O primeiro resultado esperado possui o acrônimo de GRI1, o segundo de GRI2 e, assim, sucessivamente. A última subseção apresenta as práticas dos modelos de qualidade estudados que não possuem equivalência com nenhum resultado esperado do MR-MPS-SW.

4.1 GRI1 - O escopo da gerência de riscos é determinado

Esse resultado esperado exige que seja definida claramente a abrangência da aplicação do processo de gerência de riscos na organização e dentro do âmbito de projetos. Segundo o guia de implementação 11 do MR-MPS-SW (SOFTEX – Associação para Promoção da Excelência do Software Brasileiro, 2012b), existe uma relação do tipo NEQ com a prática específica SP1.3 da área de Processo de Gestão de Riscos do CMMI-DEV, pois a prática do CMMI-DEV refere-se apenas ao escopo em projetos.

No mapeamento com a norma ISO/IEC 12207 apresentado no Quadro 1, foi identificada uma relação do tipo EQU+ com duas tarefas da norma, são elas: a tarefa 6.3.4.3.1.1, que está alinhada ao GRI1 por exigir o tratamento da gerência de riscos no contexto da organização por meio de uma política de gestão; e a tarefa 6.3.4.3.2.1, que define que devem ser descritas as perspectivas das partes interessadas, as categorias de riscos e uma descrição de objetivos técnicos e gerenciais, além de suposições e limitações. Esse detalhamento pode estar incluso em uma política organizacional para o tratamento do risco, e em cada Plano de Risco individual de um projeto.

Quadro 1 - Mapeamento do resultado esperado GRI1 e das tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa de Norma ISO/IEC 12207	Grau de Mapeamento
GRI1 – O escopo da gerência de riscos é determinado.	6.3.4.3.1.1 – As politicas de gestão de risco que descrevem as diretrizes sob as quais a gestão de risco será executada devem ser definidas.	EQU +
	6.3.4.3.2.1 – O contexto do Processo de Gestão de Risco deve ser definido e documentado	EQU +

Fonte: Criado pelos autores, com dados extraídos dos mapeamentos

As orientações de implementação deste resultado esperado, segundo o PMBOK, sugerem que sejam utilizadas as entradas, ferramentas e técnicas, e saídas referentes ao processo 11.1 (Planejar o Gerenciamento de Riscos), que determina a realização de reuniões e a análise de planejamento para definir o escopo de um projeto. Como entradas podem ser utilizados a declaração do escopo do projeto, os planos de gerenciamento de custos, cronograma, comunicações e alguns ativos de processos organizacionais, como categorias de riscos, formatos da declaração de riscos, papéis e responsabilidades, entre outros. A saída do processo 11.1, que equivale ao GRI1, é implementada no item metodologia do plano de gerenciamento de riscos, porém, apenas no que diz respeito ao âmbito de um projeto, por isso possui classificação (NEQ).

O padrão internacional IEEE ISO/IEC 16085 recomenda, em seu item 5.1.1.1, que devem ser estabelecidas políticas de gestão de riscos descrevendo: como a gerência de riscos deve

ser implementada, administrada e apoiada pela gerência e funcionários; como deve ser obtido e mantido o compromisso contínuo das partes interessadas; como o processo de gerenciamento de riscos deve ser coordenado; como orientações e treinamentos a respeito de gerenciamento de riscos devem ser conduzidos; como informações sobre riscos são comunicadas e realizadas pelas partes interessadas. Em um plano de projeto, essa política deve ser referenciada, e detalhados apenas os pormenores específicos ao projeto. Possui grau de mapeamento EQU+ atendido em conjunto com o item 5.1.2.1 do padrão.

Outro item equivalente, descrito no tópico 5.1.2.1 do padrão proposto pelo IEEE e ISO/IEC, descreve acerca da definição e documentação do contexto do gerenciamento de riscos, no qual deve conter uma descrição técnica e gerencial dos objetivos, suposições e restrições, entre outras informações relevantes que surgirem.

4.2 GRI2 - As origens e as categorias de riscos são determinadas e os parâmetros usados para analisar riscos, categorizá-los e controlar o esforço da gerência de riscos são definidos

Esse resultado esperado exige que seja definida uma classificação e critérios para determinação da probabilidade e severidade dos riscos no âmbito organizacional. O guia de implementação parte 11 (SOFTEX – Associação para Promoção da Excelência do Software Brasileiro, 2012b) sugere que o GRI2 seja atendido em conjunto pelas práticas específicas 1.1 e 1.2 do CMMI-DEV, que exigem a determinação das fontes e categorias de riscos (SP 1.1) e parâmetros para definição, categorização e controle dos riscos (SP 1.2).

O mapeamento do GRI2 com a norma ISO/IEC 12207 acontece em três tarefas, são elas: 6.3.4.3.2.2 e 6.3.4.3.2.3 na categoria EQU+, pois as tarefas descrevem, respectivamente, sobre um perfil de risco, que seriam as categorias de riscos organizacionais, e os limites destes riscos, que é a realização de cálculos para determinar quando um risco é aceitável. Também foi identificado um mapeamento na categoria NEQ com a tarefa 6.3.4.3.2.4, que determina, após priorizados, estimados e classificados, que os perfis dos riscos devem ser comunicados aos interessados, comunicação essa não mencionada pelo MR-MPS-SW. Essas informações estão resumidas no Quadro 2 abaixo.

As orientações de implementação presentes no Guia PMBOK, recomendam que, para atingir este resultado esperado, é possível utilizar a ferramenta e técnica constante no item 11.3.2: Categorização dos riscos, do processo Realizar a Análise Qualitativa dosa Riscos. Durante a realização da categorização de riscos, é possível utilizar a EAR (Estrutura Analítica de Riscos), contendo as categorias de riscos organizacionais, com severidade e probabilidade de ocorrência.

Quadro 2 - Mapeamento do resultado esperado GRI2 e das tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa de Norma ISO/IEC 12207	Grau de Mapeamento
GRI2 – As origens e as categorias de riscos são determinadas e os parâmetros usados para analisar riscos, categorizá-los e controlar o esforço da gerência de riscos são definidos	6.3.4.3.2.2 – Os limites de risco que definem as condições sob as quais um nível de risco pode ser aceitável, deve ser documentado.	EQU +
	6.3.4.3.2.3 – Um perfil de risco deve ser estabelecido e mantido	EQU +
	6.3.4.3.2.4 – O perfil de risco relevante deve ser comunicado periodicamente para as partes interessadas com base em suas necessidades.	NEQ

Fonte: Criado pelos autores, com dados extraídos dos mapeamentos

O resultado do mapeamento com o padrão IEEE ISO/IEC 16085, identificou as sugestões de implementação contidas no item 5.1.2.2, definindo que os limites de riscos identificados podem ser medidos para custo, cronograma, fatores técnicos ou outros fatores relevantes. O item 5.1.2.3 sugere que um perfil de risco deve ser estabelecido e mantido, esse perfil de risco pode conter, pelo menos: o contexto da gerência de risco, um registro de cada categoria de risco, incluindo probabilidade, consequência e limite de risco, a prioridade de cada categoria de risco, e as ações recomendadas para tratamento de cada risco. Também podem ser utilizadas as orientações de implementação que constam no item 5.1.2.4, que sugere que os riscos acima do limite determinado devem ser comunicados periodicamente às partes interessadas baseado em suas necessidades, direcionando apenas as informações de riscos necessárias a cada.

4.3 GRI3 - As estratégias apropriadas para a gerência de riscos são definidas e implementadas

O resultado esperado GRI3 determina que, em um projeto, devem ser relacionados aspectos como: escopo, ferramentas, métodos, a serem utilizados na identificação, análise, mitigação, monitoração dos riscos, entre outros. Essas informações podem ser agregadas em um plano de gerência de riscos. O mapeamento com o CMMI-DEV identificou que existe uma prática específica totalmente equivalente a esse resultado esperado: SP1.3 - Estabelecer e manter a estratégia a ser utilizada para a gestão de riscos.

O mapeamento com a norma ISO/IEC 12207, demonstrado no Quadro 3, identificou relação entre este resultado esperado e quatro tarefas da norma, de modo que sejam equivalentes ao GRI3 ao serem agregadas. As tarefas 6.3.4.3.1.2, 6.3.4.3.1.3, 6.3.4.3.1.4 e 6.3.4.3.1.5

determinam etapas da estratégia da gerência de risco, analogamente, cada tarefa representa um tópico no plano de gerenciamento de riscos resultante do GRI3, como o detalhamento de todo processo de gestão de riscos, a definição das partes interessadas com seus papéis e responsabilidades, e o meio de acesso aos recursos, além do modo como a gestão de riscos será avaliada e monitorada.

Quadro 3 - Mapeamento do resultado esperado GRI3 e das tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa de Norma ISO/IEC 12207	Grau de Mapeamento
GRI3 – As estratégias apropriadas para a gerência de riscos são definidas e implementadas	6.3.4.3.1.2 – A descrição do Processo de Gestão de Risco a ser implementado deve ser documentada.	EQU +
	6.3.4.3.1.3 – As partes responsáveis em realizar a Gestão de Risco, seus papéis e responsabilidades devem ser identificados.	EQU +
	6.3.4.3.1.4 – As partes responsáveis devem ter acesso aos recursos adequados para a realização do processo de Gestão de Risco.	EQU +
	6.3.4.3.1.5 – Uma descrição do processo para avaliar e melhorar o Processo de Gestão de Risco deve ser fornecida.	EQU +

Fonte: Criado pelos autores, com dados extraídos dos mapeamentos

Segundo o PMBOK, esse resultado esperado, sendo totalmente equivalente (EQU) ao processo 11.1 - Planejar o Gerenciamento de Riscos, todas as entradas, ferramentas e técnicas, e saídas sugeridas são aplicáveis para atingir o resultado. O principal artefato desse processo do PMBOK é o plano de gerenciamento de riscos, que pode conter: a metodologia de trabalho relacionado a riscos durante o ciclo de vida do projeto; os papéis e responsabilidades; orçamento atribuído ao tratamento e mitigação de riscos; prazos; categoria de riscos do projeto; definições de probabilidade e impacto; matriz de probabilidade e impacto; tolerâncias revisadas das partes interessadas; formatos dos relatórios; acompanhamento de riscos.

As orientações de implementação deste resultado esperado, segundo o padrão IEEE ISO/IEC 16085, determinam que deve ser estabelecido um processo de gerenciamento de riscos (item 5.1.1.2), no qual devem-se descrever: a frequência com que cada risco será analisado novamente e monitorado; o tipo de análise de risco necessário (quantitativo ou qualitativo); as

escalas de probabilidade e consequências dos riscos; os tipos de limites de riscos; os tipos de medidas utilizadas para monitorar os riscos; como os riscos são priorizados para tratamento; as fontes de riscos e categorias de riscos. Outros itens relacionados à implementação desse resultado esperado são 5.1.1.3 e 5.1.1.4, que determinam que as partes responsáveis pelo gerenciamento de riscos devem ser explicitamente identificadas, e os recursos necessários para aplicar o gerenciamento de riscos devem ser devidamente fornecidos. Além disto, o item 5.1.1.4 determina que deve ser estabelecido um processo de avaliação do gerenciamento de riscos, identificando como as métricas serão capturadas para futuras lições aprendidas.

4.4 GRI4 - Os riscos do projeto são identificados e documentados, incluindo seu contexto, condições e possíveis consequências para o projeto e as partes interessadas

O resultado esperado GRI4 determina que os riscos potenciais para um projeto devem ser identificados, assim como o contexto e as prováveis causas do risco, além de suas decorrentes consequências. Esse resultado esperado é categorizado como NEQ com a prática específica SP 2.1 do CMMI-DEV, pois ambos exigem a identificação de riscos, porém o guia MR-MPS-SW é mais exigente, obrigando a menção do contexto, condições e consequências.

Esse resultado esperado é mapeado de modo totalmente equivalente com a tarefa 6.3.4.3.3.1 da norma ISO/IEC 12207, que exige que os riscos devem ser identificados nas categorias descritas no contexto de gestão de riscos. O Quadro 4 apresenta o resumo das informações do mapeamento desse resultado esperado.

Quadro 4 - Mapeamento do resultado esperado GRI4 e das tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa de Norma ISO/IEC 12207	Grau de Mapeamento
GRI4 – Os riscos do projeto são identificados e documentados, incluindo seu contexto, condições e possíveis consequências para o projeto e as partes interessadas	6.3.4.3.3.1 – Os riscos devem ser identificados nas categorias descritas no contexto de gestão de riscos	EQU

Fonte: Criado pelos autores, com dados extraídos dos mapeamentos

O GRI4 é totalmente equivalente (EQU) ao processo 11.2 do guia PMBOK, logo todas suas entradas, saídas, ferramentas e técnicas podem ser aplicadas para atender esse resultado esperado. Como sugestão de implementação, para coletar a lista de riscos, identifica-se: a revisão de documentação de projetos anteriores; as técnicas de coletas de informações, como *brainstormings*, técnica Delphi, entrevistas e análise de causa raiz; a análise de *checklists* de riscos; a análise de premissas; as técnicas de diagramas (de causa e efeito, fluxograma, de influência); a análise de matriz SWOT. As sugestões de artefato que atendem a esse resultado esperado é uma

lista de riscos contendo a identificação, o impacto, a causa, o efeito e os responsáveis, além da lista de potenciais respostas para cada risco identificado.

O padrão IEEE ISO/IEC 16085 sugere várias abordagens para a implementação deste resultado esperado no item 5.1.3.1. Essas abordagens podem incluir o uso de questionários, *brainstormings*, análise de cenários, lições aprendidas, prototipação, entre outras. É importante ressaltar que riscos não identificados são automaticamente considerados implicitamente como aceitos. Esse item também sugere que os riscos precisam ser categorizados de modo a relacioná-los combinadamente, facilitando análise, monitoramento, tratamento e comunicação com as partes interessadas.

4.5 GRI5 - Os riscos são priorizados, estimados e classificados de acordo com as categorias e os parâmetros definidos

O resultado esperado GRI5 determina que cada risco identificado deve ser priorizado, estimado e classificado, para que sejam direcionados recursos de tratamento de riscos aos mais prioritários. O guia de implementação 11 (SOFTEX – Associação para Promoção da Excelência do Software Brasileiro, 2012b) sugere que esse resultado esperado seja totalmente equivalente (EQU) à prática SP 2.2: Avaliar e categorizar cada risco identificado, utilizando as categorias e os parâmetros definidos para riscos, e determinar suas prioridades relativas, pois possuem as mesmas exigências.

O GRI5 está alinhado com a norma ISO/IEC 12207 por meio de duas tarefas (6.3.4.3.3.2 e 6.3.4.3.3.3), que, em conjunto, atingem as necessidades exigidas pelo MR- MPS-SW. Estas tarefas determinam, respectivamente, que a probabilidade de cada risco deve ser estimada, e que cada risco deve ser avaliado se está acima do limite, ou seja, acima dos parâmetros definidos. Esse mapeamento está resumido no Quadro 5.

Quadro 5 - Mapeamento do resultado esperado GRI5 e das tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa de Norma ISO/IEC 12207	Grau de Mapeamento
GRI5 – Os riscos são priorizados, estimados e classificados de acordo com as categorias e os parâmetros definidos	6.3.4.3.3.2 – A probabilidade de ocorrência e as consequências de cada risco identificado devem ser estimadas.	EQU +
	6.3.4.3.3.3 – Cada risco deve ser avaliado em comparação com seu limite.	EQU +

Fonte: Criado pelos autores, com dados extraídos dos mapeamentos

Esse resultado esperado possui o grau de mapeamento EQU com o processo 11.3 do guia PMBOK, portanto, suas recomendações são totalmente aplicáveis para atingir os objetivos exigidos pelo MR-MPS-SW. Logo, como orientação de implementação desse resultado esperado,

sugere-se a realização de: avaliação de probabilidade e impacto de riscos; utilização de matriz de probabilidade e impacto; avaliação da qualidade dos dados sobre os riscos; categorização de riscos; avaliação da urgência de riscos; e sugestão de opinião especializada. A sugestão de artefato alinhado ao GRI5 é a atualização da lista de riscos priorizada e categorizada, mencionando a causa dos riscos, uma lista de riscos que requerem respostas a curto prazo, uma lista de observação de riscos de baixa prioridade e a tendência nos resultados da análise qualitativa dos riscos.

O GRI5 tem como sugestão de implementação, no padrão IEEE ISO/IEC 16085, o item 5.1.3.2, que especifica que a estimativa de riscos pode ser qualitativa ou quantitativa. As partes interessadas devem definir quais riscos já priorizados serão avaliados detalhadamente, e o item 5.1.3.3, que detalha a avaliação de riscos de forma comparada aos seus limites, através de árvores de decisão, planejamento de cenários e análise probabilística.

4.6 GRI6 - Planos para a mitigação de riscos são desenvolvidos

Esse resultado esperado determina a criação de planos de mitigação e contingência, que têm como objetivo diminuir a probabilidade de ocorrência do risco ou atenuar seus possíveis efeitos, antes que o risco ocorra (mitigação), ou depois (contingência). O guia de implementação 11 (SOFTEX – Associação para Promoção da Excelência do Software Brasileiro, 2012b) sugere que este resultado esperado seja totalmente equivalente (EQU) à prática SP 3.1: Elaborar um plano de mitigação de riscos conforme a estratégia para gestão de riscos, pois possuem as mesmas exigências.

O GRI6 está alinhado com a norma ISO/IEC 12207 por meio de duas tarefas (6.3.4.3.3.4 e 6.3.4.3.4.1), que em conjunto atingem as necessidades exigidas pelo MR-MPS-SW. Essas tarefas determinam, respectivamente, que: (1) para riscos acima do limite definido, ou seja, prioritários, devem ser definidas estratégias de tratamento dos riscos por planos de mitigação e contingência; e (2) após a priorização e desenvolvimento dos planos, todas as informações devem ser reportadas às partes interessadas, para serem tomadas decisões relativas ao tratamento ou aceitação dos riscos. O mapeamento desse resultado esperado possui equivalência em conjunto (EQU+) e está resumido no Quadro 6.

O GRI6 é totalmente equivalente (EQU) ao processo 11.5 do guia PMBOK. Logo, todas as suas entradas, saídas, ferramentas e técnicas podem ser aplicadas para atender este resultado esperado. Como sugestão de implementação desse resultado, podem ser adotadas as seguintes estratégias para tratamento de riscos negativos: eliminação, transferência, mitigação ou aceitação. Para riscos positivos, é possível adotar estratégia de explorar, compartilhar, melhorar e aceitar. Os artefatos recomendados pelo guia para a saída desse processo são os próprios planos de tratamento dos riscos e decisões contratuais relacionadas à transferência de riscos.

O GRI6 tem como sugestão de implementação, no padrão IEEE ISO/IEC 16085, o item 5.1.3.3, que sugere um modelo de requisição de ação de risco, agregando informações de es-

copo, assunto, originador da solicitação, perspectiva da parte interessada, categorias do risco, limites do risco, descrição detalhada do risco, com probabilidade e consequência, alternativas para o tratamento de risco com justificativas e disposição das ações a serem tomadas. Outro item do padrão que possui orientações para implementação desse resultado esperado é o item 5.1.4.1, o qual determina que as alternativas de tratamento de riscos devem ser avaliadas pelas partes interessadas, podendo aceitar riscos que excederam o limite estipulado, em situações em que o custo de mitigação seja demasiadamente alto, porém esses riscos devem ser considerados de alta prioridade e devem ser continuamente monitorados. As partes interessadas podem, também, solicitar novas alternativas para os tratamentos apresentados, nesses casos, o risco deve ser reanalisado pela equipe responsável.

Quadro 6 - Mapeamento do resultado esperado GRI6 e das tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa de Norma ISO/IEC 12207	Grau de Mapeamento
GRI6 – Planos para a mitigação de riscos são desenvolvidos	6.3.4.3.3.4 – Para cada risco que esteja acima do limite definido, estratégias recomendadas para tratamento devem ser definidas e documentadas. As medições que indicam a eficácia das opções de tratamento também devem ser definidas e documentadas.	EQU +
	6.3.4.3.4.1 – As partes interessadas devem ter acesso às opções recomendadas para o tratamento de risco e as ações solicitadas	EQU +

Fonte: Criado pelos autores, com dados extraídos dos mapeamentos

4.7 GRI7 - Os riscos são analisados e a prioridade de aplicação dos recursos para o monitoramento desses riscos é determinada

Esse resultado esperado determina a priorização de aplicação de recursos no monitoramento dos riscos. Devido às ações de gerenciamento de riscos serem custosas, faz- se necessária a otimização dos recursos materiais e humanos para otimizar esta tarefa. No modelo CMMI-DEV, não há prática específica equivalente a esse resultado esperado.

O GRI7 possui uma relação do tipo NEQ com a tarefa 6.3.4.3.4, apresentado no Quadro 7, que determina que os riscos que as partes interessadas aceitaram e estavam acima do limite, deverão ser tratados como mais alta prioridade para deslocamento de recursos em seu monito-

ramento. Porém, estes itens não podem ser totalmente equivalentes, pois a norma 12207 não especifica como priorizar recursos em projetos que não há riscos no qual as partes interessadas não aceitaram estar acima do limite estabelecido.

Quadro 7 - Mapeamento do resultado esperado GRI7 e das tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa de Norma ISO/IEC 12207	Grau de Mapeamento
GRI7 – Os riscos são analisados e a prioridade de aplicação dos recursos para o monitoramento desses riscos é determinada	6.3.4.3.4.3 – Se as partes interessadas aceitarem um risco que exceda seu limite, ele deve ser considerado um caso de alta prioridade e monitorado continuamente, a fim de determinar se outras ações de tratamento são necessárias no futuro.	NEQ

Fonte: Criado pelos autores, com dados extraídos dos mapeamentos

O resultado esperado desse tópico possui grau de mapeamento inexistente com o guia PMBOK, portanto, não possui orientações de implementação.

O padrão IEEE ISO/IEC 16085 não possui recomendação de implementação alinhada às exigências de GRI7.

4.8 GRI8 - Os riscos são avaliados e monitorados para determinar mudanças em sua situação e no progresso das atividades para seu tratamento

O resultado esperado GRI8 exige que seja determinada a periodicidade para reavaliar e monitorar riscos, planos de mitigação e contingência, e o processo de gerência de riscos como um todo, podendo, também, serem identificados novos riscos. Esse risco atende parcialmente à prática do CMMI-DEV SP 3.2: monitorar periodicamente o status de cada risco e executar o plano de mitigação quando apropriado, sendo complementado com o GRI9 para obter o grau de mapeamento EQU+ a essa prática.

Esse resultado esperado está alinhado a sete tarefas da norma ISO/IEC 12207, são elas: (1) 6.3.4.3.4.3, que determina que os riscos selecionados previamente devem ser monitorados como alta prioridade, caso as partes interessadas aceitem que o risco exceda seu limite; (2) 6.3.4.3.5.1, que determina que riscos devem ser monitorados, além de estender esse monitoramento para o contexto da gestão de riscos; (3) 6.3.4.3.5.2, o qual determina que durante o monitoramento, as medições devem ser realizadas, de forma a existir dados concretos a respeito desta etapa; (4) 6.3.4.3.5.3, determinando que durante o monitoramento poderá ocorrer a identificação de um novo risco, devendo esse ser classificado e priorizado como os demais;

(5) 6.3.4.3.6.1, o qual exige que durante o monitoramento devem ser coletadas informações que possam gerar lições aprendidas; (6) 6.3.4.3.6.2, que determina que todo o processo de gestão de riscos seja verificado periodicamente; (7) 6.3.4.3.6.3, que exige que cada risco coletado seja revisado periodicamente, afim de identificar possíveis riscos organizacionais. O Quadro 8 apresenta o resumo desse mapeamento, identificando também o grau de equivalente em conjunto (EQU+).

Quadro 8 - Mapeamento do resultado esperado GRI8 e das tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa de Norma ISO/IEC 12207	Grau de Mapeamento
GRI8 – Os riscos são avaliados e monitorados para determinar mudanças em sua situação e no progresso das atividades para seu tratamento	6.3.4.3.4.3 – Se as partes interessadas aceitarem um risco que exceda seu limite, ele deve ser considerado um caso de alta prioridade e monitorado continuamente, a fim de determinar se outras ações de tratamento são necessárias no futuro.	EQU +
	6.3.4.3.5.1 – Todos os riscos e o contexto de gestão de risco devem ser constantemente monitorados para verificação de alterações. Os riscos cujos níveis tenham sido alterados devem passar por uma avaliação de risco	EQU +
	6.3.4.3.5.2 – Medições devem ser implementadas e monitoradas para avaliar a eficácia dos tratamentos de riscos	EQU +
	6.3.4.3.5.3 – O projeto deve monitorar de forma continua os novos riscos e fontes de risco durante todo o ciclo de vida	EQU +

Resultado Esperado do MR-MPS-SW	Tarefa de Norma ISO/IEC 12207	Grau de Mapeamento
GRI8 – Os riscos são avaliados e monitorados para determinar mudanças em sua situação e no progresso das atividades para seu tratamento	6.3.4.3.6.1 – Informações devem ser coletadas durante o ciclo de vida do projeto, a fim de melhorar o Processo de Gestão de Risco e gerar lições aprendidas	EQU +
	6.3.4.3.6.2 – O processo de Gestão de Risco deve ser periodicamente revisado para verificação de eficácia e eficiência	EQU +
	6.3.4.3.6.3 – As informações sobre os riscos identificados, seus tratamentos e o sucesso de seus tratamentos devem ser revisados periodicamente, a fim de identificar sistematicamente os riscos organizacionais do projeto	EQU +

Fonte: Criado pelos autores, com dados extraídos dos mapeamentos

O GRI8 é totalmente equivalente (EQU) ao processo 11.6 do guia PMBOK, logo todas suas entradas, saídas, ferramentas e técnicas podem ser aplicadas para atender esse resultado esperado. Como sugestão de implementação desse resultado, sugere-se realizar: reavaliação de riscos; auditoria de riscos; análise de variação e tendências; medição de desempenho técnico; análise de reservas e reuniões de andamento. Artefatos que estão alinhados às exigências do resultado esperado são: lista de riscos atualizadas, contendo o resultado das reavaliações e solicitações de mudanças na forma de ações corretivas e ações preventivas.

O resultado do mapeamento com o padrão IEEE ISO/IEC 16085 identificou seis sugestões de implementação: (1) item 5.1.5.1, que especifica que os riscos devem ser monitorados, inclusive o contexto da gestão de risco e da ordem de prioridade de monitoramento; (2) item 5.1.5.2, que determina que medidas devem ser implementadas e monitoradas para avaliar a eficácia do tratamento dos riscos, podendo identificar e reparar tratamentos ineficazes; (3) item 5.1.5.3, o qual especifica que novos riscos e fontes de riscos devem ser buscados, e caso encontrados, deve ser realizada análise e comunicada às partes interessadas; (4) item 5.1.6.1, que determina que informações acerca de riscos identificados, suas fontes, causas e tratamentos devem ser coletados e comunicados durante o ciclo de vida do projeto, para melhorar procedimentos, processos e políticas da gestão de riscos; (5) item 5.1.6.2, o qual sugere que o processo de gerenciamento de riscos, como um todo, deve ser avaliado, a fim de identificar oportunidades

de melhoria, onde a periodicidade dessa avaliação deve ser determinada pelas partes interessadas; (6) item 5.1.6.3, que determina que os dados coletados, durante a revisão do processo de gerenciamento de riscos, devem ser gerados na forma de lições aprendida.

4.9 GRI9 - Ações apropriadas são executadas para corrigir ou evitar o impacto do risco, baseadas na sua prioridade, probabilidade, consequência ou outros parâmetros definidos

Esse resultado esperado exige que sejam realizadas ações de mitigação e/ou contingência para os riscos, de acordo com as necessidades e com o planejado, essas ações devem ser executadas até sua conclusão. Assim como o GRI8 mencionado anteriormente, o GRI9 é agregado para atender de forma conjunta a prática específica SP 3.2 do guia CMMI- DEV.

O GRI9 está alinhado com a norma ISO/IEC 12207 por meio de duas tarefas, apresentadas no Quadro 9, sendo (1) a tarefa 6.3.4.3.4.2 totalmente equivalente (EQU), pois determina que as ações para minimizar ou corrigir riscos, planejadas anteriormente, devem ser executadas, quando necessário, e a (2), tarefa 6.3.4.3.4.4, categorizada com o grau NEQ, pois detalha ações de gestão de problemas sem correspondentes no processo de gestão de riscos do MR-MPS-SW.

As orientações de implementação, presentes no Guia PMBOK, recomendam que, para atingir esse resultado esperado, é possível utilizar como artefato as solicitações de mudanças, que são uma das saídas do processo 11.6.3 - controlar riscos, comprovando que ações corretivas e/ou preventivas recomendadas foram executadas corretamente.

Quadro 9 - Mapeamento do resultado esperado GRI9 e das tarefas da ISO 12207

Resultado Esperado do MR-MPS-SW	Tarefa de Norma ISO/IEC 12207	Grau de Mapeamento
GRI9 – Ações apropriadas são executadas para corrigir ou evitar o impacto do risco, baseadas na sua prioridade, probabilidade, consequência ou outros parâmetros definidos	6.3.4.3.4.2 – Se as partes interessadas determinarem que ações deveriam ser tomadas para tornar um risco aceitável, então uma opção de tratamento deve ser implementada	EQU
	6.3.4.3.4.4 – Assim que o tratamento for selecionado, ele deve receber as mesmas ações de gestão que os problemas recebem, de acordo com as atividades de avaliação e controle de subseção 6.3.2 desta norma, ou da norma ISO/IEC 15288:2008	NEQ

Fonte: Criado pelos autores, com dados extraídos dos mapeamentos

O padrão IEEE ISO/IEC 16085 possui o item 5.1.4.2, como recomendação de implementação alinhada a esse resultado esperado, possuindo duas alternativas: (1) o tratamento de riscos utilizando auxílio da norma ISO/IEC 15288:2002, o qual uma vez que um tratamento de risco é selecionado, o mesmo deve receber as mesmas ações de correção de problemas da norma 15288; e (2), quando uma alternativa de tratamento de risco é aceita, as partes interessadas devem definir um plano de tratamento detalhado, especificando responsáveis pelo plano, tarefas a serem realizadas, cronograma de tratamento, alocação de recursos para o tratamento, medidas de controle de tratamento, custos, métodos de comunicação entre os envolvidos e ambiente e infraestrutura necessária.

4.10 Práticas dos modelos de qualidade não relacionadas com nenhum resultado esperado do modelo MR-MP-SW

Cada prática identificada no guia PMBOK e no CMMI-DEV possui um mapeamento com práticas abordadas no modelo MR-MPS-SW, porém a norma ISO/IEC 12207 possui algumas recomendações com equivalência parcial em relação às práticas do MR-MPS-SW. As exigências do MR-MPS-SW são menos abrangentes que as exigências na norma, logo existem mapeamentos de tarefas que são totalmente equivalentes a resultados esperados, porém, possuem mais diretrizes alinhadas à exigência internacional.

Essas tarefas geraram boas práticas e, consequentemente, atividades no modelo de processo, por isso, também possuem importância no mapeamento realizado neste estudo.

As tarefas 6.3.4.3.1.2 e 6.3.4.3.1.5 da norma ISO/IEC 12207 determinam, respectivamente, que deve haver uma descrição do processo implementado, e devem haver diretrizes para posterior avaliação e melhoria do processo descrito. Essas atividades dão origem à boa prática "Planejar a Gestão de Riscos", sem vínculo direto com algum resultado esperado do processo de gerência de riscos do MR-MPS-SW.

Também as tarefas 6.3.4.3.6.2 e 6.3.4.3.6.3 da norma ISO/IEC 12207, relacionadas à avaliação da execução do processo, deram origem à boa prática "Avaliar a execução da Gestão de Riscos". Isso se deve ao fato de que, além do monitoramento exigido em resultados esperados do MR-MPS-SW, a norma exige a periodicidade de revisão das atividades planejadas e executadas, assim como a revisão de riscos identificados ao final de um projeto, para orientar outros futuros.

5 BOAS PRÁTICAS IDENTIFICADAS

A partir do mapeamento identificado entre os modelos de qualidade, foram catalogados as boas práticas com suas respectivas recomendações. Práticas semelhantes foram agrupadas a fim de evitar repetições.

O Quadro 10, apresentado abaixo, reúne informações coletadas a respeito do mapeamento dos modelos de qualidade. Cada boa prática possui: identificador, nome, descrição, a identificação em qual modelo de qualidade (MPS.BR, CMMI ou ISO/IEC 12207) é apresentada e o modo de implementar essa prática de acordo com os modelos de qualidade que sugerem implementação (IEEE ISO/IEC 16085 e PMBOK). Essas boas práticas foram insumo para a elaboração do modelo de processo de *software* sugerido neste trabalho. Ao todo foram coletadas quatorze boas práticas distintas dos modelos de qualidade.

Quadro 10 – Boas práticas identificadas a partir do mapeamento de modelos de qualidade

ID	Nome	Descrição	Identificada no(s) modelo(s)	Formas de Implementar esta prática
BP01	Definir o Escopo da Gerência de Riscos em uma organização	definição da abrangência da aplicação da gerência de riscos na organização em relação à sua estrutura organizacional e de processos	MSP.BR (GRI1), CMMI (SP 1.3), ISO/IEX 12207 (6.3.4.3.1.1 e 6.3.4.3.2.1)	Política Organizacional: Descrição técnica e gerencial dos objetivos, suposições e restrições, entre outras informações
BP02	Identificar papeis e responsáveis pelo gerenciamento de risco	Identificar e documentar os envolvidos no gerenciamento de riscos, para ser realizada a comunicação durante o ciclo de vida do projeto	ISO/IEC 12207 (6.3.4.3.1.3 e 6.3.4.3.1.4)	Política organizacional contemplando papeis e responsabilidades; Plano de projeto contemplando alocação de recursos humanos para cada um dos papeis definidos.
BP03	Definir Categorias de Riscos	Definir categorias de riscos, parâmetros para esta categorização e as possíveis origens de riscos de cada categoria	MPS.BR (GRI2), CMMI (SP 1.1), ISO/IEC 12207 (6.3.4.3.2.2, 6.3.4.3.2.3 e 6.3.4.3.2.4)	Estrutura Analítica de Riscos: riscos organizacionais, contendo severidade e probabilidade de ocorrência de cada categoria
BP04	Definir parâmetros para análise de riscos	É importante padronizar o modo como a organização determina parâmetros utilizados na análise de riscos identificados (como a probabilidade e a severidade)	MPS.BR (GRI2), CMMI (SP 1.2), ISO/IEX 12207 (6.3.4.3.2.3)	Estimativas qualitativas, definindo valores numéricos para variáveis subjetivas: muito alto (9-10); alto (8-9); médio (4-7); e baixo (0-3) para cada parâmetro que será utilizado. No caso de probabilidade e severidade, pode ser obtido o grau de exposição através da multiplicação dos valores numéricos para os dois parâmetros.

ID	Nome	Descrição	Identificada no(s) modelo(s)	Formas de Implementar esta prática
BP05	Definir Estratégias para a gerência de riscos	devem ser relacionados aspectos da gerência de riscos em um projeto, como escopo, métodos e ferramentas a serem utilizados, técnicas de mitigação, periodicidade, responsáveis.	MPS.BR (GRI3), CMMI (SP 1.3)	Plano de Gerenciamento de Riscos: metodologia de trabalho durante o ciclo de vida do projeto, orçamento atribuído ao tratamento e mitigação de riscos, prazos, categorias de riscos, definições de probabilidade e impacto, entre outros.
BP06	Identificar e Documentar Riscos	Todos os riscos identificados devem ser registrados, juntamente com informações adicionais, como contexto, condições associadas e consequências	MPS.BR (GRI4), CMMI (SP 2.1), ISO/IEC 12207 (6.3.4.3.3.1)	Revisão de documentação de projetos anteriores; Técnicas de coletas de informações: *brainstorming*, *checklists*, análise de matriz SWOT, entre outros.
BP07	Classificar Riscos	Riscos identificados devem ser detalhados de forma que possam ser melhor organizados para monitoramento e reutilização da melhor maneira em projetos futuros. (grau de exposição e categorização)	MPS.BR (GRI5), CMMI (SP 2.2), ISO/IEC 12207 (6.3.4.3.3.2)	Estimativa quantitativa ou qualitativa; matriz de probabilidade e impacto; sugestão de opinião especializada
BP08	Priorizar Riscos	É importante prioriza-los para definir quais riscos merecem maior atenção durante o monitoramento.	MPS.BR (GRI5), CMMI (SP 2.2)	Comparação de grau de exposição (probabilidade x impacto) dos riscos identificados
BP09	Escolher estratégia de ação e definir repostas aos riscos	Estabelecer planos de ação para os riscos (mitigação e/ou contingência para tratar riscos) prioritários afim de reduzir alguma característica, como impacto ou probabilidade de ocorrência	MPS.BR (GRI6), CMII (SP 3.1), ISO/IEC 12207 (6.3.4.3.*)	Adotar uma das seguintes estratégias: eliminação, transferência, mitigação, aceitação; Plano de mitigação do risco: consequências, alternativas para tratamento, justificativa e ações a serem tomadas
BP10	Definir prioridade para aplicação de recursos em riscos	É importante definir quais riscos serão prioritários no recebimento de recursos para mitigação e monitoramento, devido à necessidade de otimização de recursos materiais e humanos.	MPS.BR (GRI7)	Atividades de gerenciamento de riscos especificadas no cronograma
BP11	Monitorar (e reavaliar) riscos	Realizar o monitoramentos e avaliação de riscos em um determinada frequência. Também durante o monitoramento, podem ser identificados novos riscos	MPS.BR (GRI8), CMMI (SP 3.2), ISO/IEC 12207 (6.3.4.3.5.*)	Auditoria de riscos, análise de variação e tendências, reuniões de andamento, *checklists*.
BP12	Realizar ações para reduzir impacto do risco	Realizar ações de contigência e mitigação durante o monitoramento de riscos, com o objetivo de minimizar ou anular o impacto dos riscos	MPS.BR (GRI9), CMMI (SP 3.2)	Execução do plano de ação do risco

ID	Nome	Descrição	Identificada no(s) modelo(s)	Formas de Implementar esta prática
BP13	Planejar a Gestão de Riscos	A Gestão de riscos deve possuir um processo implementado e documentado. Assim como deve haver uma descrição do processo para avaliar e melhorar a execução das atividades planejadas	ISO/IEC 122007 (6.3.4.3.1.5)	Definir previamente um processo sequenciando as atividades de gerência de risco em um projeto de *software*, e garantir que todos possuam conhecimento e executem o que foi planejado.
BP14	Avaliar a execução da Gestão de Riscos	O processo de Gestão de riscos deve ser periodicamente revisado, assim como as informações sobre riscos identificados, seu tratamento e o sucesso desses tratamentos.	ISO/IEC 12207 (6.3.4.3.6.2 e 6.3.4.3.6.3)	Ao término de um projeto, avaliar execução e comparar com o planejamento, para alinhar novas diretrizes em futuros projetos.

Fonte: Criado pelos autores, com dados extraídos dos mapeamentos

As boas práticas identificadas nortearam o desenvolvimento do processo apresentado no estudo de caso, podendo gerar uma ou mais tarefas na sugestão definida.

6 ESTUDO DE CASO

Com o intuito de avaliar o mapeamento resultante do gerenciamento de riscos nos modelos de qualidade estudados, foi definido um processo aderente às recomendações e às exigências encontradas em cada padrão e norma estudados neste trabalho. O objetivo deste estudo de caso é auxiliar futuras implementações da gerência de riscos em uma organização que deseja desenvolver *software* de maneira aderente ao MR-MPS-SW, CMMI, PMBOK, ISO/IEC 12207 e/ou ISO/IEC 16085 de modo conjunto.

O modelo de processo que é apresentado possui algumas limitações com relação ao seu detalhamento, pois tem como principal foco nortear implementações nas mais diversas organizações, sem a necessidade de delimitar papéis, ferramentas e procedimentos de maneira extremamente detalhada, tornando mais simples sua adaptação ao processo padrão da organização.

Para realizar o detalhamento do modelo de processo, foi utilizada a ferramenta Spider-PM (BARROS; OLIVEIRA, 2010), que permite a especificação do modelo em fases e para cada fase um conjunto de tarefas. O processo foi analisado por um implementador e avaliador experiente em modelos de qualidade de *software*, que pontuou sugestões e ajustes na descrição do processo, que integram a versão resultante aqui apresentada.

A Figura 1 apresenta uma visão macro do processo, que possui três fases: planejamento, responsável pela definição inicial de como será trabalhada a gerência de riscos na organização; execução, responsável pelas tarefas de gerenciamento dos riscos durante o ciclo de vida de um projeto; e avaliação, realizada após o fim de um projeto, responsável por tarefas relacionadas a

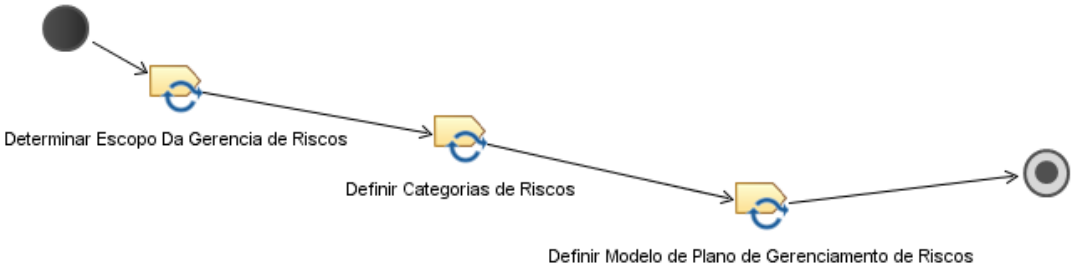
mudanças no processo para futuros projetos. Em seguida, cada fase é apresentada em detalhes, juntamente com a descrição de cada tarefa do processo.

Figura 1 – Fases de um processo de gerenciamento de riscos

Fonte: Criada pelos autores, com dados extraídos dos mapeamentos

A fase de planejamento, apresentada na Figura 2, possui três tarefas. A primeira tarefa, denominada "Determinar Escopo da Gerência de Riscos", deve ser responsável por gerar um artefato que especifique a abrangência da gerência de riscos, tanto no âmbito de cada projeto individualmente, quanto na organização como um todo. Essa tarefa pode ser atendida por meio da elaboração de uma política organizacional, por exemplo, que deve conter informações acerca das possíveis partes interessadas em riscos, as categorias de riscos, uma breve descrição de quais objetivos técnicos e gerenciais devem ser alcançados, assim como suposições e limitações desse gerência. Esta tarefa foi desenvolvida para atender a boa prática BP01: "Definir o Escopo da Gerência de Riscos em uma organização"

Figura 2 – Tarefas da fase de Planejamento



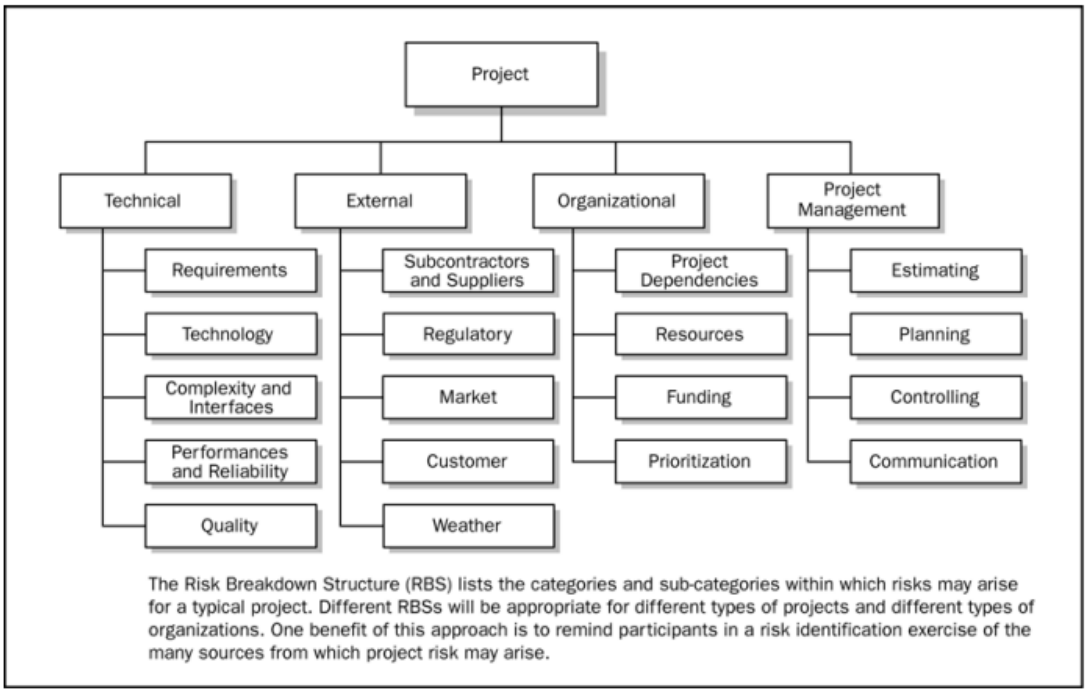
Fonte: Criada pelos autores, com dados extraídos dos mapeamentos

A segunda tarefa da fase de planejamento "Definir Categorias de Riscos", é responsável por gerar uma lista com as categorias de riscos que podem ser encontrados durante a execução de um projeto de *software*. Devem ser disponibilizadas informações a respeito das possíveis origens do risco, além de um conjunto de critérios para a determinação da probabilidade de ocorrência e sua severidade. Outro modo eficiente de organizar as categorias de riscos é por meio de uma estrutura analítica de riscos (EAR), que de forma hierárquica, permite o arranjo de riscos em categorias e subcategorias, como pode ser observado na Figura 3. Essa tarefa está relacionada à boa prática BP03, "Definir Categorias de Riscos".

A terceira tarefa da fase de planejamento baseia-se na boa pratica BP05, "Definir Estratégias para a gerência de riscos"e na boa prática BP04, "Definir parâmetros para análise de

riscos", e é denominada "Definir Modelo de Plano de Gerenciamento de Riscos", sendo responsável por analisar e definir quais informações relacionadas aos riscos serão importantes para serem monitoradas durante a execução do projeto. Ao final dessa tarefa, deve ser gerado um artefato com os tópicos que um plano de gerenciamento de riscos desta organização deve possuir. É importante que um plano de gerenciamento de riscos possua um detalhamento de itens como: metodologia, definindo abordagens e ferramentas utilizadas para identificação e monitoramento dos risos; papéis e responsabilidades, definindo o líder e membros da equipe de gerenciamento de riscos; orçamento; prazos; categorias de riscos, que podem ser exatamente as mesmas categorias definidas no âmbito organizacional na tarefa anterior, ou uma instanciação da mesma, reaproveitando apenas uma parcela; definições de probabilidade e impacto dos riscos, relacionando estas informações às mudanças em custo, tempo escopo e qualidade do projeto; formatos de relatórios que serão utilizados durante a execução do projeto.

Figura 3 – Exemplo de uma EAR



Fonte: PMBOK, 2013

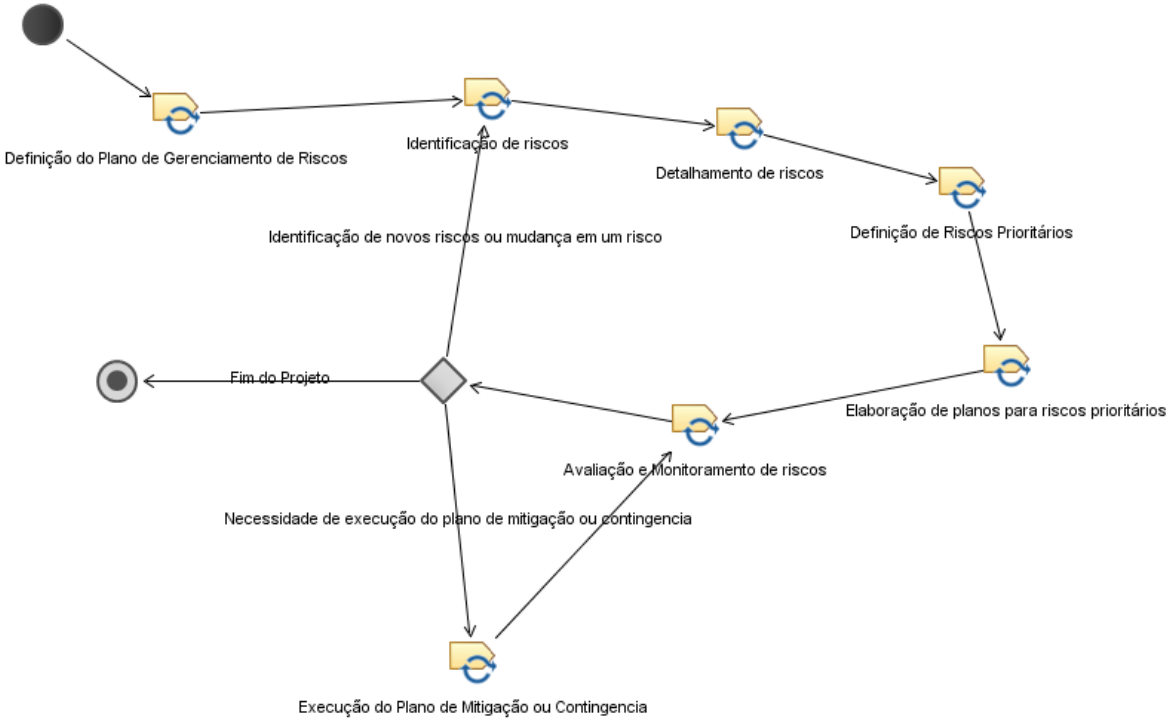
A fase de Execução possui sete tarefas distintas que, como pode ser observado na Figura 4, segue um fluxo linear até a tarefa relacionada à avaliação e monitoramento de riscos, no qual (1) um novo risco pode ser identificado ou um existente alterado, necessitando ajustes no detalhamento e prioridades de riscos, ou (2) pode ocorrer a necessidade de execução de um plano de mitigação ou contingência anteriormente especificado. Ambos os fluxos retornam novamente à tarefa de avaliação e monitoramento de riscos, que deve ser executada até o fim do projeto.

A primeira tarefa dessa fase é a "Definição do Plano de Gerenciamento de Riscos", que deve utilizar o modelo de plano de gerenciamento de riscos, gerado na fase anterior, e preenchê-lo com as informações relevantes para o projeto. É importante que essa tarefa seja executada pelo responsável pela gerência de riscos, porém, em conjunto com a sua equipe e

com outros gerentes, caso haja, uma vez que será necessário especificar informações a respeito do cronograma e orçamento do projeto. Esta tarefa, também, baseia-se na boa prática BP05, "Definir Estratégias para a gerência de riscos", e na boa prática BP02, "Identificar papeis e responsáveis pelo gerenciamento de risco".

Em seguida, deve ser realizada a tarefa "Identificação dos Riscos", que deve documentar os riscos desse projeto, especificando o contexto, as prováveis causas do risco e suas decorrentes consequências. Estas informações podem estar incorporadas no plano de gerenciamento de riscos. A boa prática BP06, "Identificar e Documentar Riscos", originou a criação desta tarefa. Para realizar a identificação de riscos podem ser utilizadas técnicas como a utilização de *checklists* pré-definidos, reuniões e *brainstorming*; análise de cenário de projetos anteriores; técnica Delphi; análise de causa-raiz; ou análise de forças, fraquezas, oportunidades e ameaças, através da matriz SWOT.

Figura 4 – Tarefas da fase de Execução



Fonte: Criada pelos autores, com dados extraídos dos mapeamentos

Cada risco anteriormente identificado deve ser priorizado, estimado e classificado na tarefa "Detalhamento de Riscos". A inclusão destas informações resultam em uma atualização na lista de riscos. De acordo com a categorização de cada risco, podem ser utilizadas informações contidas na EAR para auxiliar no detalhamento, especialmente, na quantificação de probabilidade e impacto. Ao final dessa tarefa, o artefato com a lista de riscos deve estar detalhado e priorizado a partir dos riscos de maior grau de exposição (produto entre probabilidade e impacto), e esta atualização deve ser comunicada aos interessados definidos no plano de gerenciamento de riscos. Essa tarefa também baseia-se na boa prática BP06, "Identificar e Documentar Riscos, e na boa prática BP07, "Classificar Riscos".

A próxima tarefa da fase de execução, denominada "Definição de Riscos Prioritários", originada pelas boas práticas BP08, "Priorizar Riscos, e BP10, "Definir prioridade para aplicação de recursos em riscos", pode ser executada, por exemplo, por uma reunião entre os responsáveis pelo gerenciamento de riscos e pelo projeto como um todo. O artefato contendo a lista de riscos priorizada e detalhada deve ser analisado para definir quais riscos terão maior visibilidade e receberão maior atenção durante a execução do projeto, seja por causar grande impacto, caso ocorra, ou devido à sua grande probabilidade de ocorrência. Essa tarefa é importante, pois devido a limitações de tempo e orçamento, muitas vezes não é possível o monitoramento de todos os riscos identificados.

Após a definição de quais riscos são prioritários, cada um destes riscos selecionados deve possuir um plano de mitigação e um plano de contingência, de acordo com a boa prática BP09, "Escolher estratégia de ação e definir respostas aos riscos".

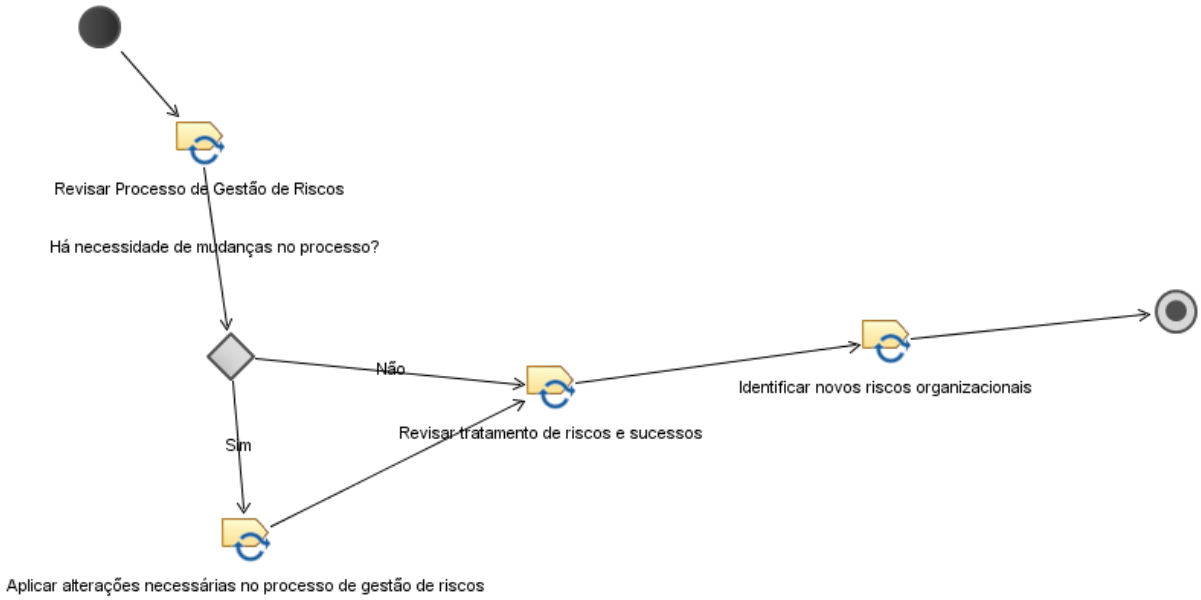
Esses planos são realizados durante a execução da tarefa seguinte, "Elaboração de planos para riscos prioritários". Um plano de mitigação diz respeito à necessidade de reduzir o grau de exposição, ou seja, deve ser reduzida a probabilidade, o impacto ou ambos, antes que um risco ocorra. Enquanto o plano de contingência deve ser executado após a constatação de ocorrência do risco, com o intuito de contornar possíveis prejuízos causados. Para cada risco, é possível adotar estratégias de: eliminação, quando a ameaça é removida por completo; transferência, no qual a responsabilidade sobre um risco é direcionada a um terceiro; mitigação, que é a redução do grau de exposição de um risco; e aceitação, para riscos poucos prováveis, no qual não é detalhada a abordagem para superação da ocorrência.

A tarefa seguinte da fase de execução é denominada "Avaliação e Monitoramento de riscos", a qual define que todos os riscos devem ser monitorados e reavaliados em uma periodicidade, que pode ser definida no plano de gerenciamento de riscos. Podem ser adotadas diferentes estratégias de monitoramento para cada categoria ou gravidade de riscos, assim como devem ser revisadas também a prioridade e os planos de mitigação e contingência dos riscos. Essa tarefa originou-se a partir da boa prática BP11, "Monitorar (e reavaliar) riscos".

A tarefa "Execução do Plano de mitigação ou Contingência", originada a partir da boa prática BP12, "Realizar ações para reduzir impacto do risco", é executada apenas quando é detectada esta necessidade durante a avaliação e monitoramento dos riscos. Após a execução do planejado, as mudanças devem ser documentadas no próprio plano, relatando a evolução das medidas tomadas. Também deve haver uma preocupação em reavaliar se essas medidas geraram novos riscos ou afetaram riscos existentes, por isso faz-se necessário uma avaliação detalhada também dos riscos já documentados ao final do plano de mitigação ou contingência.

A fase final, avaliação, apresentada na Figura 5, possui quatro tarefas, que serão executadas ao final de um projeto, com um intuito de avaliar o processo de gerência de riscos como um todo na organização e realizar ajustes necessários para sua otimização na execução em futuros projetos. Todas as tarefas dessa fase baseiam-se na boa prática BP14, "Avaliar a execução da Gestão de Riscos".

Figura 5 – Tarefas da fase de Avaliação



Fonte: Criada pelos autores, com dados extraídos dos mapeamentos

Inicialmente deve ser realizada a tarefa "Revisar Gestão de Riscos", que pode ser atendida por uma reunião entre o responsável pela gerência de riscos e sua equipe. Nessa reunião, devem ser identificados os pontos fracos encontrados durante a execução do processo, para que possam ser ajustados. Outra alternativa eficiente é a elaboração de um *checklist* para avaliação do processo. A forma como será realizada essa avaliação e como serão documentadas as necessidades de ajustes podem estar detalhadas na política organizacional, de modo que seja disponibilizada a todos.

Caso existam alterações, elas devem ser ajustadas na tarefa "Aplicar alterações necessárias no processo de gestão de riscos", que deve ser realizada em conjunto com o responsável pela definição do processo organizacional e, posteriormente, informada aos interessados a respeito das mudanças.

Em seguida, caso haja ou não necessidades de alterações, deve ser realizada a tarefa "Revisar tratamento de riscos e sucessos", responsável por identificar os pontos fortes durante a execução do projeto, armazenando informações para futuros projetos. Essas informações podem ser coletadas em uma reunião, inclusive, podendo ser a mesma reunião realizada na primeira tarefa da fase de avaliação. Para cada ponto forte identificado no tratamento de riscos, deve haver detalhes de como foi realizado o tratamento, qual a categoria, prioridade e impacto do risco trabalhado e, caso haja, quais técnicas para mitigação ou contingência foram utilizadas. Essas informações podem ser armazenadas em uma ferramenta de gerência de conhecimento, como uma *wiki*, por exemplo, de modo que esteja acessível a todos os integrantes da equipe de gerenciamento de riscos.

A tarefa final desse processo, "Identificar novos riscos organizacionais", também pode ser realizada durante uma reunião ao final do projeto, e está relacionada à necessidade de incluir novas categorias de riscos na EAR da organização, que foram identificados nesse projeto e não

estavam documentados anteriormente. Além de estar relacionada ao BP14, como mencionado anteriormente, essa tarefa relaciona-se também com a boa prática BP03, "Definir Categorias de Riscos".

7 CONCLUSÕES

Este artigo apresentou uma proposta de mapeamento dos resultados esperados do processo de Gerência de Riscos do MR-MPS-SW com as práticas específicas do CMMI- DEV e as tarefas da norma ISO/IEC 12207:2009, assim como as orientações de implementação segundo o PMBOK e o padrão internacional IEEE ISO/IEC 16085, em áreas de processos equivalentes. Esse mapeamento orientou a proposta de definição de um modelo de processo de *software* aderente a esses modelos de qualidade, visando auxiliar a implantação da gerência de riscos em organizações desenvolvedoras de *software*.

Este trabalho está restrito, já que as sugestões de implementação estudadas não conseguem atender à gerência de riscos no MR-MPS-SW em sua totalidade, assim como existem outros modelos de qualidade e padrões internacionais que envolvem gerenciamento de riscos de projetos (não necessariamente de *software*), que não estão contemplados no escopo deste estudo. Este trabalho tem maior abrangência no âmbito nacional, pois há um maior foco ao modelo de qualidade desenvolvido no Brasil e voltado, principalmente, para micro, pequenas e médias empresas.

Apesar de não haver um mapeamento total entre os modelos de qualidade, podemos concluir que o MR-MPS-SW possui uma equivalência quase completa em relação aos modelos internacionais, havendo apenas um resultado esperado sem correspondentes. A pesquisa aqui apresentada evidenciou formas de implementar o gerenciamento de riscos quase completamente alinhado às exigências de modelos e padrões internacionais, por meio de sugestões de práticas e de um processo, dando às organizações uma variedade de propostas de implementação que agregam algumas das melhores práticas de gerência de riscos no Brasil e no Mundo.

Como trabalhos futuros a este projeto, pretendemos: (1) relacionar as melhores práticas em gerenciamento de riscos, ou seja, destacar, desses modelos e da literatura acadêmica, quais os passos necessários para implementar uma gerência de riscos eficiente; (2) especificar e desenvolver uma ferramenta de *software* que auxilie o processo aqui definido, sistematizando assim a sua implantação e execução; e, com os resultados das etapas anteriores, (3) prover melhoria no *framework* e ferramenta propostos, e a maior adaptabilidade possível para melhor adequar-se à realidade das diversas organizações interessadas no gerenciamento de riscos.

8 AGRADECIMENTOS

Este trabalho recebeu apoio financeiro da CAPES com a concessão de bolsa institucional de mestrado ao PPGCC-UFPA. Este projeto é parte do Projeto SPIDER-UFPA (OLIVEIRA et al., 2011).

REFERÊNCIAS

ABNT – Associação Brasileira de Normas e Técnicas. **NBR ISO/IEC 12207:2009 – Engenharia de Sistemas de Software – Processos de Ciclo de Vida de Software**. Rio de Janeiro, Brasil, 2009.

BARROS, Renan; OLIVEIRA, Sandro. Spider-PM: Uma Ferramenta de Apoio à Modelagem de Processos de Software. In: VIII ENCONTRO ANUAL DE COMPUTAÇÃO. **Anais...** [S.l.], 2010.

GUSMÃO, Cristine M. G.; MOURA, Hermano P. Gerência de Riscos em Processo de Qualidade de Software: uma análise comparativa. In: III SIMPÓSIO BRASILEIRO DE QUALIDADE DE SOFTWARE. **Anais...** Brasília, 2004.

IEEE – Institute of Electrical and Electronics Engineers. **ISO/IEC 12085 – IEEEStd 16085 – 2006 – Systems and software engineering – Life cycle processes – Risk management**. USA, 2006.

MCCAFFERY, Fergal; BURTON, John; RICHARDSON, Ita. Improving software risk management in a medical device company. In: ICSE. **Proccedings...** Vancouver, Canada, 2009.

MUTAFELIJA, Boris; STROMBERG, Harvey. **Process Improvement with CMMI v1.2 and ISO Standarts**. [S.l.]: CRC Press, 2009.

OLIVEIRA, S. R. B. et al. **SPIDER – Uma Proposta de Solução Sistêmica de um SUITE de Ferramentas de Software Livre de Apoio à Implementação ao Modelo MPS.BR**. [S.l.]: Revista do PBQP-SW. PBQP Software. SEPIN-MCT, 2011.

PMI – Project Management Institute. **A Guide to the Project Management Body of Knowledge (PMBOK Guide)**. 5. ed. USA, 2013.

RAZ, Tzvi; HILLSON, David. A comparative review of risk management standarts. **Risk Management: An International Journal**, v. 7, n. 4, p. 53–66, 2005.

ROUT, Terence P.; TUFFLEY, Angela. Harmonizing ISO/IEC 15504 and CMMI. **Software Process: Improvement and Practice**, v. 12, p. 361–371, mai. 2007.

SEI – Software Engineering Institute. **Capability Maturity Model Integration (CMMI) for Development, Version 1.3**. Carnegie Mellon, USA, 2010.

SOFTEX – Associação para Promoção da Excelência do Software Brasileiro. **Melhoria do Processo de Software Brasileiro (MPS.BR) – Guia Geral MPS de Software**. Brasil, 2012a.

SOFTEX – Associação para Promoção da Excelência do Software Brasileiro. **Melhoria do Processo de Software Brasileiro (MPS.BR) – Guia de Implementação – Parte II: Implementação e Avaliação do MR-MPS-SW:2012 em Conjunto com o CMMI-DEV v1.3**. Brasil, 2012b.

WANGENHEIM, C. G. Von et al. Best practice fusion of CMMI-DEV v1.2 (PP, PMC, SAM) and PMBOK 2008. **Information and Software Technology**, v. 52, p. 749–757, 2010.