APLICAÇÃO DA PROPOSTA DA ISO 31000 EM AMBIENTES DE DESENVOLVIMENTO DE *SOFTWARE*

Fernando Henrique Gaffo[1]
Dr. Rodolfo Miranda de Barros[2]
Dr. Jacques Duílio Brancher [3]

RESUMO

O processo de desenvolvimento de *software* tem sofrido com divergências entre padrões e modelos para a realização da gestão de riscos eficaz em projetos. Objetivando reduzir esta heterogeneidade de metodologias o *InternationalOrganization for Standardization* propôs a criação de uma norma para esta área, a ISO 31000. Para realização de um estudo detalhado da aplicação da proposta da norma, o processo de gerenciamento de riscos do PMBOK foi tomado como base. A aplicação do estudo foi efetuada no processo de desenvolvimento de *software* da fábrica de *software* GAIA, que é mantida pelo Departamento de Computação da Universidade Estadual de Londrina. Como resultado deste trabalho, o processo de desenvolvimento de *software* está pronto para evoluir para o nível E do MPS.Br, oferecendo maior segurança tanto para o projeto quanto para a equipe responsável pela gerência do mesmo.

Palavras-chave: Gerenciamento de Riscos, Qualidade de Software, PMBOK, ISO 31000.

ABSTRACT

The software development process has suffered by disagreements between models and patterns for the realization of effective risk management in projects. Aiming to reduce the heterogeneity of methodologies of the International Organization for Standardization has proposed a standard for this area, the ISO 31000. To carry out a detailed study of the application of the proposal, the risk management process of the PMBOK was taken as the base. The implementation of the study was done in the software development process of software factory GAIA, which is maintained by the

[1] Titulação Acadêmica: Mestrando em Ciência da Computação
Departamento de Ciência da Computação – Universidade Estadual de Londrina Rodovia Celso Garcia Cid PR 445, KM 380, Campus Universitário, Londrina – PR E-mail: fernandogaffo@gmail.com
Fone: (43) 3371-4000, Fax: (43) 3328-4440

[2] Titulação: Doutor Departamento de Computação - Universidade Estadual de Londrina
Rodovia Celso Garcia Cid, PR 445, KM 380, Campus Universitário, Londrina – PR Email:rodolfo@uel.br
Fone: (43) 3371-4000, Fax: (43) 3328-4440

[3] Titulação: Doutor Departamento de Computação - Universidade Estadual de Londrina
Rodovia Celso Garcia Cid, PR 445, KM 380, Campus Universitário, Londrina – PR Email:jacques@uel.br
Fone: (43) 3371-4000, Fax: (43) 3328-4440

Department of Computing of the State University of Londrina. As a result of this work, the process of software development is ready to progress to the level E of the MPS.Br, providing greater security for both the project and the team responsible for managing it.

Keywords: Risks Management, Software Quality, PMBOK, ISO 31000.

1 INTRODUÇÃO

Os sistemas de computação estão difundidos em todos os setores da vida moderna e apesar dos avanços tecnológicos a maior parte dos produtos é complicada de manter, entender e evoluir.

Fato comprovado pelo estudo realizado pelo *StandishGroup*, o *CHAOS Report* (2009). Apenas 32% dos projetos de *software* são entregues dentro do prazo, com custos compatíveis e cumprindo requisitos estipulados. Do restante, 44% sofrem com atrasos, custos elevados ou problemas de especificação, outros 24% são cancelados.

Outro fator que atinge o sucesso dos projetos é volatilidade do escopo que ele pode possuir. Boehm e DeMarco (1997) afirmam que o escopo do produto altera-se constantemente pelos recursos e necessidades do mercado.

A afirmação acima nos leva a considerar a constante mudança do mercado na hora de se planejar um produto, o que torna necessário o desenvolvimento de soluções que busquem atender os anseios do cliente de maneira prática e que não cause falhas ou transtornos indesejados no futuro.

Desta forma, para evitar que a empresa passe por dificuldades devemos levar em consideração a afirmação feita por McManus (2004) de que os riscos devem ser gerenciados, pois em caso contrário, “a organização perde dinheiro, a confiança de seus *stakeholders*, sua reputação e talvez ‘feche as portas’”.

Podemos dizer então, que conforme o tamanho e a complexidade do sistema aumentam a necessidade de se implantar metodologias de gerência de riscos para auxiliarem os gerentes do projeto a garantir o cumprimento das metas de prazo, custo e qualidade do produto gerado se faz necessário.

Na primeira parte deste trabalho são apresentadas as referências utilizadas como base para elaboração deste estudo. Na sequencia é apresentado o processo de desenvolvimento de software utilizado atualmente na fábrica GAIA, que é mantida pelo Departamento de Computação (DC) da Universidade Estadual de Londrina (UEL). Logo após é apresentado o processo de desenvolvimento de software modificado para a utilização da proposta da ISO 31000 em conjunto com as

ferramentas e técnicas do PMBOK. Por fim é exposta a conclusão contendo as contribuições obtidas e os trabalhos futuros que serão realizados.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção é realizada uma revisão da literatura dos tópicos abordados neste estudo. Primeiramente conceitua-se risco, na sequencia são abordados o gerenciamento de riscos (GR) no PMBOK e a ISO 31000.

2.1 RISCO

Risco pode ser definido, basicamente, como qualquer ocorrência que ameasse um projeto e pode ser tratados de duas maneiras distintas em uma organização, ou seja, um risco pode ocasionar perdas ou ganhos (Pfleeger, 2004).

Desta maneira, perdas e ganhos devem ser compreendidos, respectivamente, como qualquer aspecto negativo ou positivo decorrente de um risco.

Outro aspecto importante a se ressaltar é que a palavra risco deve ser interpretada como todas as incertezas que cercam um determinado projeto e não apenas como problemas, pois estes são incertezas já concretizadas (Salles, 2008).

2.2 GERENCIAMENTO DE RISCOS NO PMBOK

O *Project Management BodyofKnowledge*, PMBOK (2008), é um guia das melhores práticas para o gerenciamento de projetos eficaz e é composto por uma série de processos que visam aumentar a eficácia com que o projeto é gerenciado.

Com o objetivo de aumentar a chance de ocorrência de eventos positivos e reduzir a probabilidade dos eventos negativos, o referido guia propõe um processo padrão para gerenciar os riscos em projetos que deve ser utilizado em todos os níveis da organização.

Tal processo envolve uma série de atividades que buscam planejar, identificar, analisar qualitativa e quantitativamente os riscos, além de elaborar um plano de resposta para os mesmos e garantir que eles sejam monitorados e controlados efetivamente.

2.3 ISO 31000

A ISO 31000, criada pelo *InternationalOrganizationStandarization* (ISO), trata dos aspectos positivos e negativos da ocorrência de um risco, com o objetivo de

fornecer princípios, guias e terminologias comuns para o gerenciamento de riscos de forma a se obter uma padronização das metodologias já existentes.

Esta norma pode ser utilizada em qualquer empresa, independentemente de ramo ou atividade. Dentro de uma mesma empresa, por exemplo, esta norma propõe que as diversas áreas tratem a incerteza de acordo com as regras específicas de cada uma, mas utilizando-se de um processo único e integrado.

Segundo tal norma, para a gestão de risco ser eficaz, uma organização deve respeitar uma série de princípios que devem ser tidos com lei dentro das organizações que desejarem implantá-la.

Além dos princípios estabelecidos, o sucesso na implantação do gerenciamento de riscos está diretamente ligado à eficiência que o *framework* irá ser aplicado nos diversos níveis da organização. O *framework* completo para implantação da ISO 31000 pode ser visto na Figura 1:

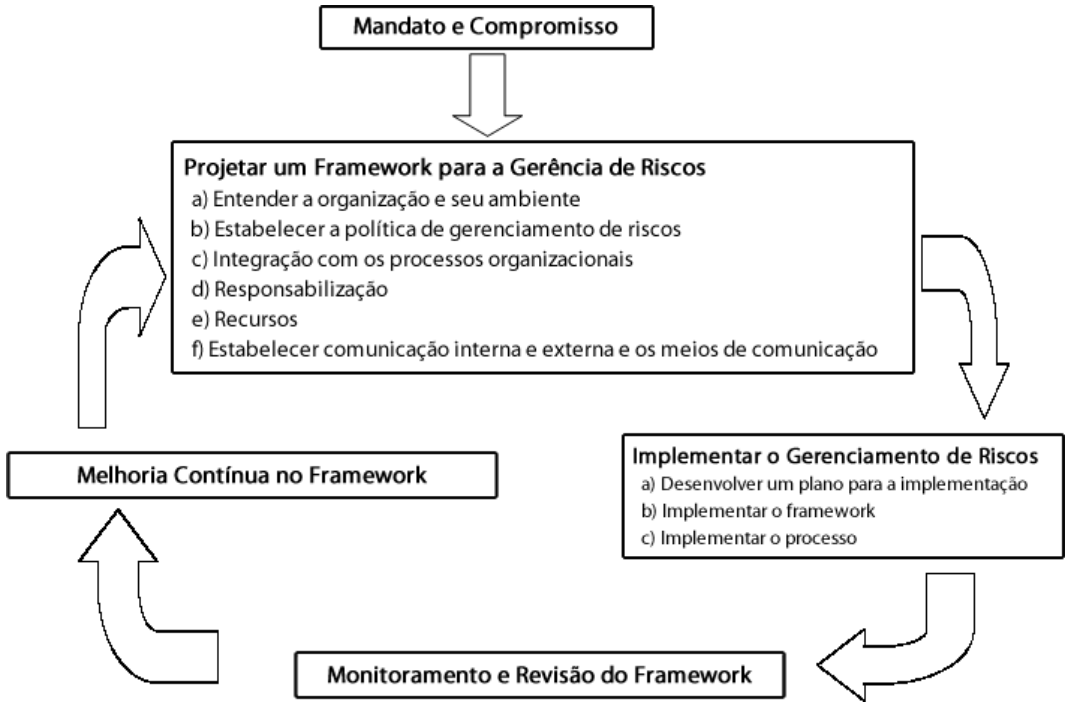

Figura 1. Relacionamento entre os componentes do framework de gerenciamento de riscos da ISO 31000.

Este *framework* não se destina a estabelecer um sistema de gerenciamento de riscos, mas sim ajudar as organizações a integrar a gestão das incertezas ao seu sistema de gestão utilizado atualmente.

Tal integração deve ser feita adaptando os componentes do *framework* às suas necessidades específicas da organização em conjunto com as práticas propostas pelo processo de gerenciamento de riscos da norma.

Por sua vez, o processo proposto pela ISO 31000, exibido na Figura 2, deve ser utilizado para controlar as incertezas de um projeto. Tais atividades devem fazer parte dos procedimentos gerenciais, além de estarem incorporadas na cultura da organização.

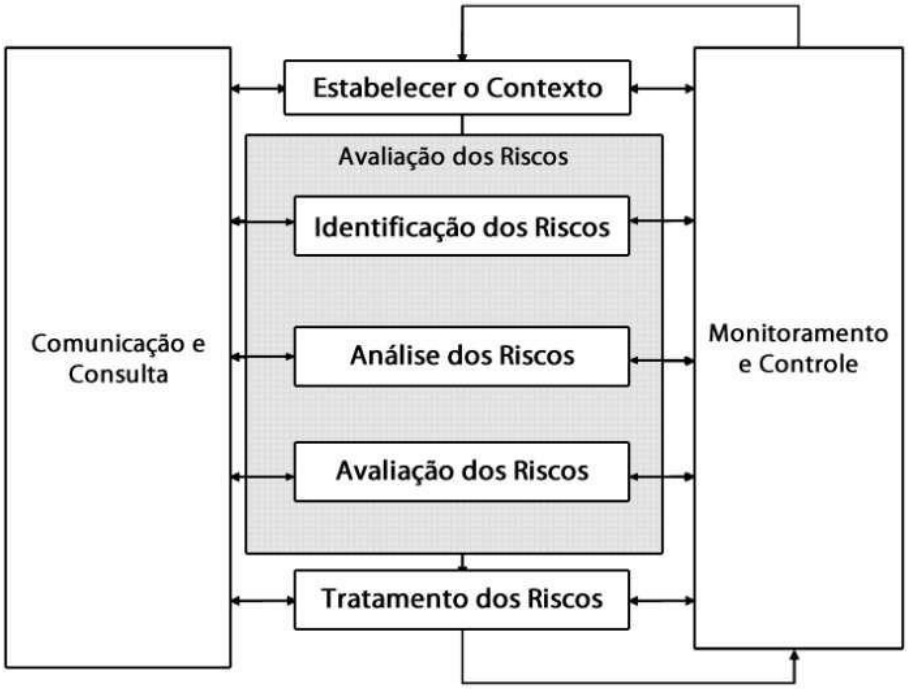

Figura 2. Processo de gerenciamento de riscos da ISO 31000.

O referido processo é composto por cinco atividades principais, são elas: comunicação e consulta, estabelecer o contexto, avaliação dos riscos, tratamento e monitoramento e controle.

3 PROCESSO DE DESENVOLVIMENTO DE *SOFTWARE*

O processo de desenvolvimento de *software* engloba atividades, ferramentas e procedimentos que têm por objetivo gerar produtosque atendam aos requisitos especificados pelos usuários e clientes.

A fábrica de *software* GAIA, que é mantida pelo Departamento de Computação (DC) da Universidade Estadual de Londrina (UEL), é o foco do estudo de caso deste artigo baseia-se no Processo Unificado, iterativo e incremental,

direcionado a casos de uso e centrado na arquitetura, como o proposto por Krunchten (2003).

As etapas que envolvem o processo de desenvolvimento de *software* da GAIA podem ser visualizadas na Figura 3:

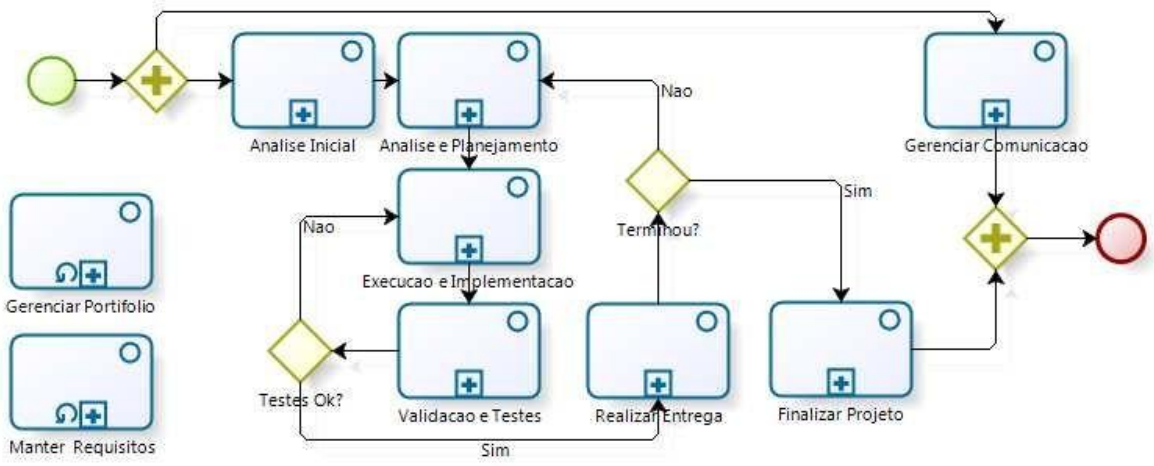

Figura 3. Processo de Desenvolvimento de *Software* utilizado na Fábrica GAIA.

Todas as etapas do processo utilizado pela fábrica GAIA estão em concordância com o MPS.Br (Melhoria do Processo de Software Brasileiro) e tem o objetivo de garantir que o produto gerado atenda todos os requisitos estipulados e consequentemente atinja níveis satisfatórios de qualidade.

3.1 APLICAÇÃO DA ISO 31000, EM CONJUNTO COM AS PRÁTICAS DO PMBOK, AO PROCESSO DE DESENVOLVIMENTO DE SOFTWARE DA GAIA

Para que um programa de gerenciamento de riscos seja eficiente ele deve ser dinâmico e contínuo ao longo de todo o processo de desenvolvimento, além de exigir a participação de todos os envolvidos (Molt, 2000).

Além da participação de todos os *stakeholders*, é necessário que as informações estejam disponíveis durante todo o tempo, a todos os interessados de maneira correta, pois o sucesso de um projeto depende da eficácia das informações (Disnmore, 2004).

Deste modo, para integrar o PDS da fábrica GAIA com a proposta da ISO 31000, a atividade gerenciar comunicação, presente atualmente no PDS, foi mantida para atender tanto o gerenciamento de riscos quanto aos demais processos organizacionais.

Por conseguinte, uma atividade que contém os processos de gerenciamento de riscos foi criada. Tal atividade denominada de gerenciar riscos e deve ser executada em paralelo a todo o PDS. O resultado da integração está disposto na Figura 4.

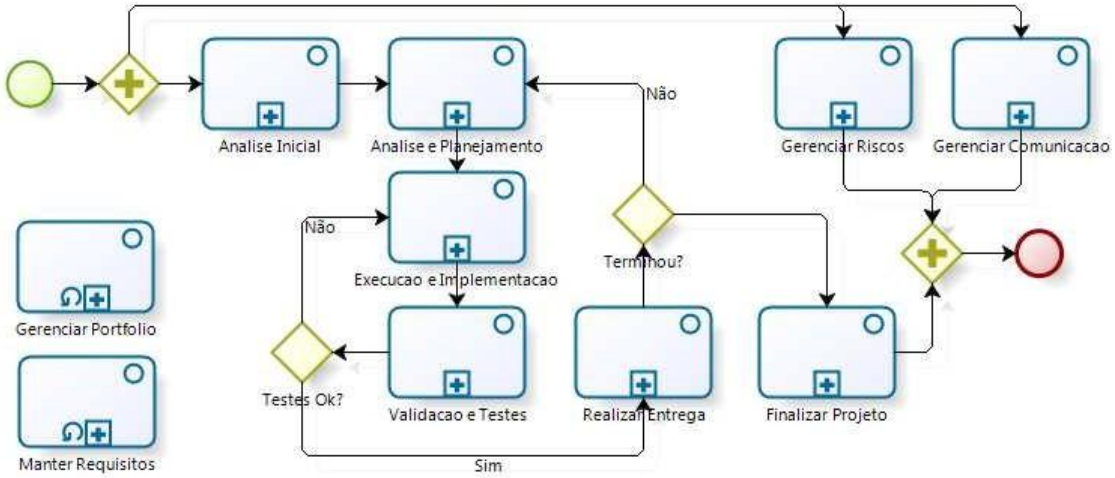

Figura 4. Aplicação da proposta da ISO 31000, em conjunto com as práticas do PMBOK, ao PDS da Fábrica de *Software* GAIA.

Por sua vez, a etapa de gerenciar riscos, apresentada na Figura 5, foi criada contendo as quatro atividades restantes do processo de GR proposto pela ISO. São elas: estabelecer o contexto do gerenciamento de riscos, avaliação e tratamento dos riscos e monitoramento e controle.

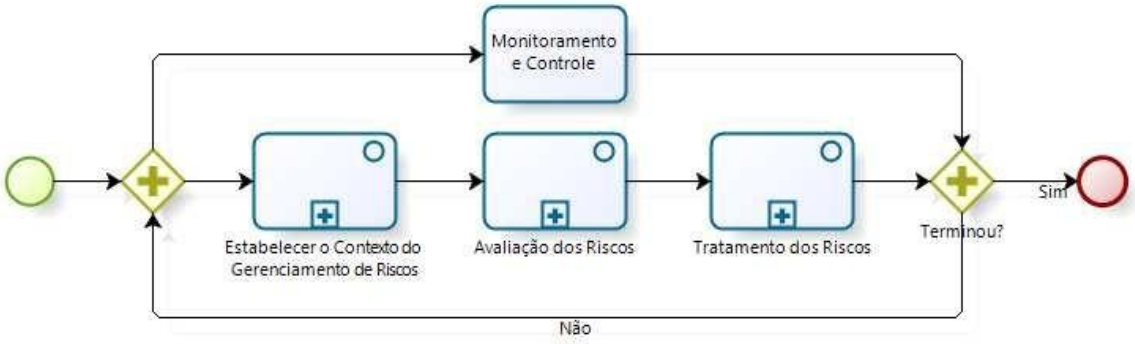

Figura 5. Fluxo do Processo de Gerenciamento de Riscos baseado na ISO 31000, em conjunto com as práticas do PMBOK, aplicado à Fábrica de *Software* GAIA.

A etapa denominada estabelecer contexto do gerenciamento de riscos, cujo fluxo está apresentado na Figura 6, engloba atividades para definir o contexto interno, externo e da própria gerência da incerteza, bem como os critérios que serão utilizados durante toda a atividade relativa ao tratamento das ameaças.

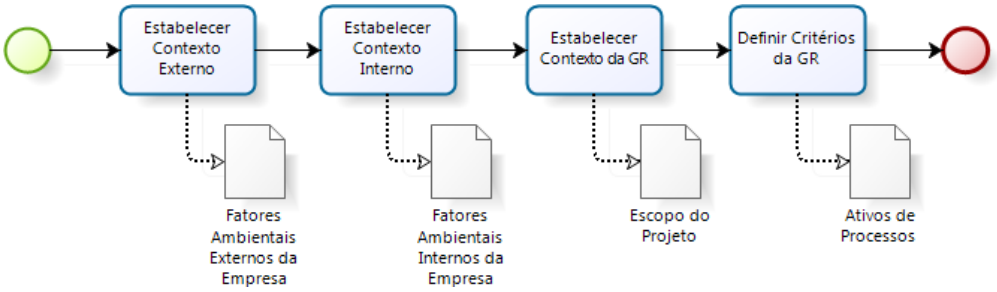

Figura 6. Processo de Estabelecer o Contexto do Gerenciamento de Riscos baseado na ISO 31000, em conjunto com as práticas do PMBOK, aplicado à Fábrica de *Software* GAIA.

Os artefatos que compõe esta fase são: fatores ambientais (internos e externos) da empresa, escopo do projeto e os ativos dos processos organizacionais. Tais documentos fornecem informações detalhadas da abrangência do *software* e também de outras experiências que a empresa possui em seu banco de dados histórico.

A etapa de avaliação das incertezas, disposta na Figura 7, envolve ações para identificar os riscos ligados ao projeto e analisa-los conforme sua probabilidade de ocorrência, além de elaborar os planos de tratamento. Tais informações são úteis para auxiliar os processos de tomada de decisão.

Por sua vez, o processo de avaliação dos riscos é composto de três atividades, são elas: identificação, análise e avaliação dos riscos. Todas com o objetivo principal de fornecer uma base consistente para o de tratamento das incertezas.

A etapa de identificação dos riscos consiste em análises realizadas no plano de gerenciamento das incertezas e demais documentos, isso para garantir uma melhor visualização das ameaças. Técnicas com *brainstorming*, entrevistas e *checklists* podem aumentar a quantidade e a qualidade das informações geradas por esta fase. O produto desta etapa é uma lista de riscos identificados.

Já na análise dos riscos, medidas são tomadas para compreender as ameaças identificadas. Técnicas como a "*WhatIf...*" ("E Se..."), simulações e análise de árvore de decisão podem ser utilizadas para categorizar esta lista de ameaças. O resultado desta etapa é uma lista categorizada de riscos que serve como base para a avaliação dos riscos.

No processo de avaliação os riscos as ameaças são estudadas com a finalidade de auxiliar a tomada de decisão. Podem-se utilizar técnicas de simulações, análises de causa e efeito ou análises estatísticas para compreender melhor os riscos. Os produtos desta fase são a lista de riscos identificada e categorizada, os planos de contingência e os planos de tratamento das ameaças.

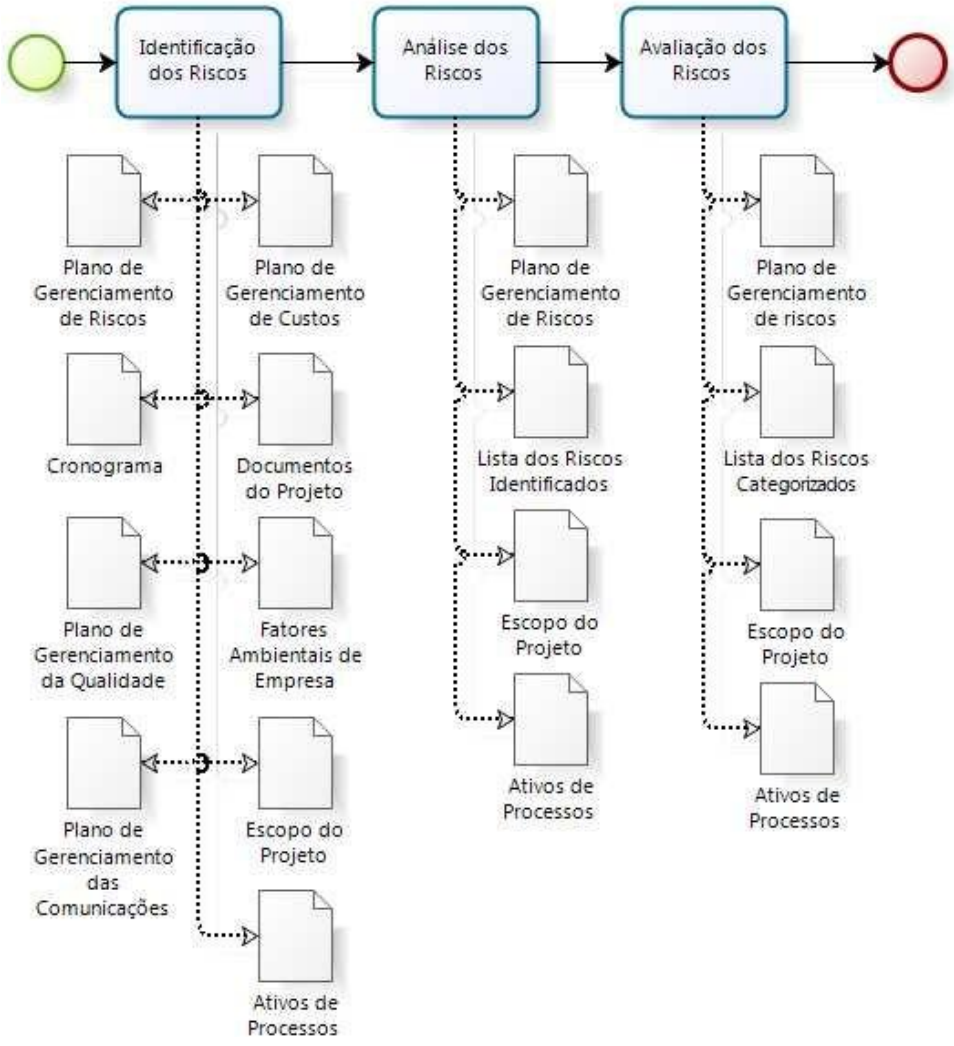

Figura 7. Processo de Avaliação dos Riscos baseado na ISO 31000, em conjunto com as práticas do PMBOK, aplicado à Fábrica de *Software* GAIA.

A partir dos dados coletados nas etapas anteriores e de toda documentação gerada, a etapa de tratamento dos riscos, presente na Figura 8, é executada. Nesta fase ocorre a real execução dos planos de tratamento das incertezas e, caso necessário, dos planos de contingência.

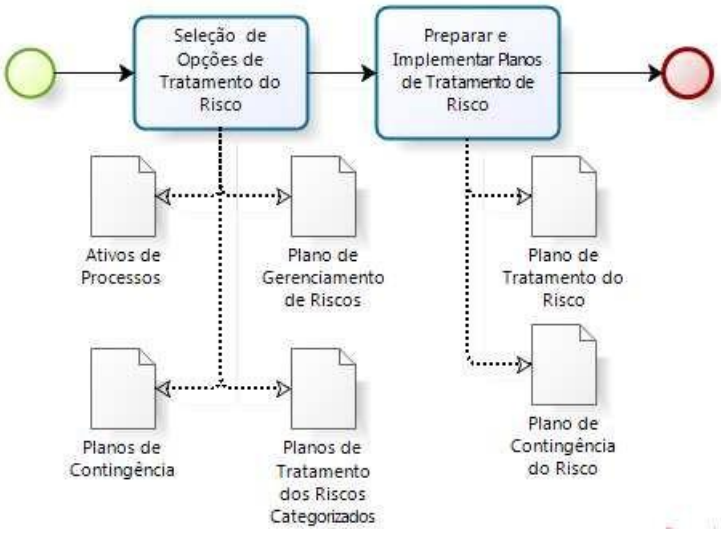

Figura 8. Processo de Tratamento dos Riscos baseado na ISO 31000, em conjunto com as práticas do PMBOK, aplicado à Fábrica de Software GAIA.

Esta fase consiste em mitigar as ameaças até que atinjam níveis aceitáveis para os padrões institucionais. As atividades que a compõe são: seleção de opções de tratamento e preparar e implementar os planos de tratamento dos riscos.

A seleção do plano de tratamento de riscos que será executado é feita mediante ao levantamento das prioridades presentes no plano de tratamento das ameaças gerado na etapa anterior, além de se basear no plano de gerenciamento de riscos e nos ativos de processos organizacionais.

Após selecionar qual plano será mitigado, providências relativas para preprar o ambiente e implementar do respectivo plano devem ser tomadas. No caso de alguma eventualidade o plano de contingência deve ser seguido.

Após executar esta etapa, indicadores são gerados para averiguar a eficiência do processo de GR na etapa de monitoramento e controle. Estas informações possibilitam averiguar o surgimento de novos riscos, desaparecimento de outras ameaças e outras ocorrências.

Por sua vez, o monitoramento e controle podem ser feito através de atividades de reavaliação periódica dos riscos, processos de realização de auditorias, através de reuniões ou à medida que a organização achar interessante.

Além disso, a constante utilização das ferramentas e técnicas de GR, em conjunto com os documentos de entrada e saída propostos pelo PMBOK, merece destaque. A correlação entre os processos da ISO 31000 e os documentos do PMBOK pode ser averiguada na Tabela 1.

Tabela 1. Correlação entre os processos da ISO 31000 e os documentos de entrada e saída do PMBOK.

Processo de GR	PMBOK	ISO 31000
Estabelecer o Contexto	- Documentos: Fatores ambientais da empresa (internos e externos), Escopo do projeto e Ativos de processos. - Técnica: Reuniões.	- Processos: Estabelecer o Contexto Interno e Externo da Organização, Estabelecer o Contexto da GR e Definir os Critérios da GR.

Avaliação dos Riscos	- Documentos: Plano de Gerenciamento de Riscos, Plano de Gerenciamento de Custos, Cronograma, Documentos do Projeto, Plano de Gerenciamento de Qualidade, Fatores ambientais da empresa (internos e externos), Plano de Gerenciamento das Comunicações, Escopo do Projeto, Ativos de Processos, Lista de Riscos Identificados e Lista de Riscos Categorizados. - Ferramentas e Técnicas: Revisões de Documentos, Análise SWOT, Opiniões Especializadas e Brainstorming, Avaliação de Probabilidade x Impacto.	- Processos: Identificação dos Riscos, Análise dos Riscos e Avaliação dos Riscos.

Tratamento dos Riscos	- Documentos: Ativos de Processos, Plano de Gerenciamento de Riscos, Planos de Contingência, Planos de Tratamento dos Riscos Categorizados, Lista de Riscos Identificados e Categorizados. - Ferramentas e Técnicas: Reuniões, Estratégias para riscos (respostas e contingências).	- Processos: Seleção de Opções de Tratamento do Risco e Preparar e Implementar Planos de Tratamento de Risco.
Monitoramento e Controle	- Documentos: Registros dos Riscos, Plano de Gerenciamento de Projeto, Relatórios de Desempenho. - Ferramentas e Técnicas: Medição dos Desempenhos, Reavaliação de Riscos, Reuniões de Andamento, Análise das Variações e Tendências.	- Processo: Monitoramento e Controle.

4 CONCLUSÃO

Avaliando os resultados obtidos é possível concluir que o processo ganhou rigorosidade e está cada vez mais atrelado aos níveis G (Parcialmente Gerenciado) e F (Gerenciado) do MPS.Br. As melhorias do PDS deixaram-no preparado para o nível E (Parcialmente Definido), onde necessariamente, ocorre a evolução do gerenciamento do projeto.

Testes realizados na fábrica de *software* GAIA, apontaram um ganho significativo de segurança, tanto para o cliente quanto para a própria equipe responsável pelo projeto. O principal ganho observado foi a redução de erros durante fase de especificação, que podem causar retrabalhos em fases posteriores atrasando o cronograma ou até mesmo inviabilizando o projeto final.

Com uma maior interação dos *stakeholders*, como proposto pela ISO 31000, houve uma maior comunicação entre as diversas partes da equipe, as trocas de experiências e conhecimentos entre os membros do projeto foram decisivas para a evolução do PDS.

A análise dos primeiros resultados dos testes indicou que o *workflow* de riscos está consistente. Perseguindo sempre a melhoria da qualidade por meio da utilização do ciclo PDCA (*Plan* – Planejar, *Do* – Fazer, *Check* – Checar e *Act* - Agir), buscou-se adaptar o *workflow* ao PDS da GAIA.

Foi realizada a criação de um *framework* padrão e genérico que pode ser utilizado tanto por outras equipes de desenvolvimento quanto pela própria equipe da GAIA em projetos que demandem uma maior ou menor necessidade de análise e gerenciamento de riscos, um *framework* completo adequado tanto às necessidades da equipe de desenvolvimento quanto as do projeto.

Além do desenvolvimento deste *framework* para o gerenciamento de riscos e dos ganhos de segurança, acima citados, outras contribuições importantes foram obtidas através da aplicação da proposta da norma ISO 31000 no PDS da GAIA.

O encorajamento a gestão proativa de riscos em todos os níveis da organização, a consciência da necessidade de se identificar os riscos em todas as áreas da empresa, a busca constante pelo aprimoramento das técnicas de detecção de possíveis problemas, o desenvolvimento de artefatos que apoiem o gerenciamento de riscos e a minimização de perdas surgiram após a aplicação da ISO 31000.

Outro fato a se destacar é o aumento do comprometimento dos *stakeholders* com o projeto, pois um senso comum de que o sucesso de projeto é de suma importância, fez com que todos se dedicassem mais para alcançar o objetivo.

Como ações futuras para este trabalho, estudos estão sendo realizados para o desenvolvimento de uma aplicação de suporte ao gerenciamento de riscos automatizado. Tal ferramenta irá gerar condições para armazenar as lições

aprendidas com os riscos e, consequentemente, criar uma memória organizacional de riscos.

REFERÊNCIAS

Associação para Promoção da Excelência do Software Brasileiro. MPS.Br - Guia Geral. Brasília, 2009.

BOEHM, B.W; DEMARCO, T. *Software risk management*.IEEE Software 14, p. 17-19, 1997.

DISNMORE, P. C. Silveira Neto, F. H. Gerenciamento de Projetos, Como Gerenciar seu projeto com qualidade, dentro do prazo e custos previstos. Rio de Janeiro: Qualitymark. 2004.

ISO 31000.*Risk Management – Principles and Guidelines,* 2010.

ISO 31010.*Risk Management – Risk Assessment Techniques,* 2010.

KRUNCHTEN, P. Introdução ao RUP – *RationalUnifiedProcess*. Rio de Janeiro: Ciência Moderna, 2003.

MOLT, George. *Risk Management Fundamentals in Software Development. Crosstalk: The Journal of Defense Software Engineering*, Agosto de 2000.

McMANUS, J. *Risk Management in Software Development Projects*. Burlington: ElsevierButterworth-Heinemann, 2004.

PFLEEGER, Shari L. Engenharia de Software: Teoria e Prática. 2ª Edição. São Paulo: Prentice Hall, 2004.

PMBOK, *Project Management Institute*. Um Guia do Conhecimento em Gerenciamento de Projeto (Guia PMBOK). Pennsylvania: EUA, 2008.

SALLES, C. *etall.* Gerenciamento de Riscos em Projetos. Editora FGV, 2006.

STANDISH GROUP. *Chaos Summary* 2009: *The 10 Laws of CHAOS*. EstadosUnidos, 2009.