GAIA Risks - A Service-based Framework to Manage Project Risks

Fernando Henrique Gaffo
Departamento de Computação
Universidade Estadual de Londrina
Londrina, Brazil
fernandogaffo@gmail.com

Rodolfo Miranda de Barros
Departamento de Computação
Universidade Estadual de Londrina
Londrina, Brazil
rodolfo@uel.br

***Abstract*—In the last years the software development industry has faced a lot of challenges to create solutions of quality which fit to the market volatility and the constant technology improvements. Thus, the high number of uncertainties leads to high levels of risk, making necessary incorporate, to the software development process, efficient methodologies to manage the risks. In order to make the adoption of these activities simple, this study presents a framework, called GAIA Risks. This framework aims to quantify the risk management within a software development process and, through maturity levels, services and a well-defined deployment process, provide paths for its improvement. To validate the GAIA Risks framework the deployment process was applied into an organization until the risk management activities reach the highest maturity level.**

***Keywords*—Risk, risk management, software engineering, project management.**

I. Introdução

Os sistemas de informação estão difundidos em vários setores da vida moderna, além do que as pessoas estão cada vez mais dependentes dos *softwares* em suas atividades cotidianas [1], os quais estão presentes desde hospitais até atividades de lazer. Por sua vez, as empresas que os desenvolvem, enfrentam uma série de desafios durante o ciclo de vida destes projetos, como por exemplo, a redução de custos, o cumprimento de prazos, erros de especificação e baixa qualidade do produto final.

Tal afirmação pode ser comprovada pelo do estudo realizado pelo *Standish Group*, o *Chaos Manifesto* [2], que indica que, embora a porcentagem de projetos tidos como sucesso tenha aumentado em relação a 2010, apenas 37% deles são entregues dentro do prazo, com custos planejados e atendem aos requisitos estipulados, do restante, 42% sofrem com atrasos, custos elevados ou problemas de especificação e outros 24% são cancelados.

Neste cenário, o objetivo deste estudo é apresentar um *framework*, intitulado GAIA Riscos, cujo propósito é fornecer uma estrutura flexível para gerenciar os riscos dentro de uma empresa de desenvolvimento de *software*. Este *framework*, por sua vez, compreende: (1) cinco níveis de maturidade, (2) sete serviços, (3) um questionário de avaliação, (4) quatro *checklists* de reavaliação e (5) indicadores de desempenho para o gerenciamento de riscos.

A criação deste *framework* para gerenciar os riscos dá-se por meio da fragmentação do processo de gerenciamento de riscos da ISO 31000 em sete serviços, os quais visam entregar valor aos clientes, facilitando com que eles alcancem seus objetivos. Desta maneira, cada serviço organiza: (1) *templates* de documentos, (2) ferramentas e técnicas, (3) *workflows*, (4) indicadores de desempenho e (5) vocabulários.

O trabalho estrutura-se da seguinte forma: na seção II são expostas pesquisas relacionadas a outros processos e *frameworks* para gerenciar riscos, na seção III apresenta-se o *framework* GAIA Riscos, seus serviços e demais componentes, já a seção IV aborda a implementação do objeto deste trabalho em um processo de desenvolvimento de *software*. Por fim, na seção V são expostas as conclusões, contribuições obtidas e trabalhos futuros relevantes ao tema.

II. Revisão Bibliográfica

Vários estudos têm sido feitos na área de identificação, análise e avaliação dos riscos, de uma maneira geral, sobre o processo de gerenciamento dos mesmos [1]. Boehm [3] é um dos pioneiros na área, propondo um modelo em espiral e composto de atividades iterativas para gerenciá-los. Atualmente existem várias metodologias, das quais se destacam as baseadas em modelos de processos e as baseadas em modelos de *frameworks* [4].

Esta seção compreende a revisão de trabalhos relevantes encontrados na literatura, bem como do gerenciamento de riscos segundo as abordagens da norma ISO 31000 [5], do guia PMBOK [6] e alguns modelos de maturidade, os quais subsidiam o desenvolvimento deste trabalho.

A. Trabalhos Relacionados

É possível encontrar na literatura várias metodologias para administrar os riscos envolvidos nos projetos, entre as quais, estão presentes aquelas que se baseiam na criação de uma memória institucional para auxiliar os gerentes do projeto em todas as etapas envolvidas nesta gerência [7], [8], [9]. Nestes estudos é comum a presença de um repositório de informações

978–1–4673–0793–2/12/$31.00 © 2012 IEEE

sobre os riscos, que contém informações triviais sobre os mesmos.

No caso de ambientes distribuídos de desenvolvimento de *software*, vários estudos apresentam modelos de *frameworks* e processos cujas atividades são especialmente desenvolvidas para identificar, analisar, avaliar e tratar os riscos neste cenário [10], [11], [12], [13]. Dentre as principais características deste modelo de *framework* está a capacidade de armazenar e disseminar as informações obtidas em decorrência do processo de gestão dos riscos.

Outro modelo para administrar os riscos do projeto é o processo utilizado pelos métodos ágeis. Nos casos do SCRUM [14] e do *Extreme Programming* (XP) [15], este gerenciamento é realizado de maneira iterativa e incremental, dentro de reuniões que são realizadas em um período de um mês ou menos. Entre os objetivos destes encontros, está o de aperfeiçoar a previsibilidade dos riscos envolvidos bem como controlá-los empiricamente.

Por sua vez, alguns autores apresentam a gerência de riscos utilizando-se de processos de modelagem e simulação [16], [17]. As atividades envolvidas nestes processos realizam-se mediante elaboração de experimentos, cujo objetivo é auxiliar os gerentes a compreenderem o ambiente, testar, analisar e comparar os resultados para entender o comportamento dos riscos, tornando possível determinar a melhor opção de tratamento e antever o surgimento de novos problemas.

Também foram localizados trabalhos que tratam a gerência dos riscos de maneira concorrente e colaborativa entre os vários projetos de uma organização [18], [19], os quais apresentam processos que buscam prever o surgimento de riscos decorrentes do relacionamento entre os projetos mantidos por uma empresa. Contudo, o trabalho apresentado por Wanqing e Yong [19], possibilita, além das demais funcionalidades, moldar o gerenciamento dos riscos de acordo com as necessidades de cada projeto, levando em consideração os custos e investimentos realizados em cada um deles.

Já nos casos de terceirização de desenvolvimento de *software* em *body shop*, Schreiber et al. [20] apresenta uma proposta cujo objetivo é reduzir os riscos por meio de um conjunto de ações preventivas que seguem os padrões especificados pelo *Capability Maturity Model Integration* (CMMI). No estudo, para diminuir os riscos de insucesso, os autores focam seus esforços no planejamento junto ao cliente, na comunicação e na troca de experiências como fatores decisivos para repassar confiança e qualidade.

Entre os trabalhos pesquisados, o modelo proposto por Aldenucci [21] apresenta um modelo de maturidade para o processo de gerenciamento de risco, cuja estrutura é capaz de avaliar, classificar e analisar as áreas desta gestão de acordo com os padrões do CMMI. Todavia, a proposta do estudo não se baseia em serviços, não possui processo de implantação, questionário para avaliação diagnóstica, *checklists* de reavaliação e nem permite a customização da gerência dos riscos.

Por fim, a gerência dos riscos proposta por padrões amplamente utilizados pelo mercado foi pesquisada. É comum aos modelos consultados a presença de atividades para identificar, analisar, avaliar, tratar, comunicar e monitorar os riscos [6], [5], [22]. Este conjunto de atividades, por sua vez, visa fazer com que a gerência dos riscos anteveja o acontecimento de problemas e, consequentemente, reduza a chance de insucesso do projeto e aumente sua probabilidade de sucesso, reduzindo gastos com retrabalhos.

B. ISO 31000

A ISO 31000 [5], criada pelo *International Organization for Standardization* (ISO), trata aspectos positivos e negativos da ocorrência dos riscos, com o objetivo de fornecer princípios, guias e terminologias comuns para o gerenciamento dos mesmos, buscando estabelecer padrões para as metodologias já existentes.

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

O *framework* para implantação desta norma consiste em cinco atividades, que são: (1) Mandato e Compromisso, (2) Projetar um *Framework* para a Gerência de Riscos, (3) Implementar o Gerenciamento de Riscos, (4) Monitoramento e Revisão do *Framework* e (6) Melhoria Contínua do *Framework*. Por sua vez, o processo de gerenciamento de riscos é composto de cinco atividades principais, que seguem:

- **Comunicação e consulta:** ocorre paralelamente a todas as etapas da gerência de riscos para garantir que os interesses das partes envolvidas sejam atendidos. Esta atividade deve ser conduzida pelo plano de gerenciamento de comunicações, que é elaborado nas etapas iniciais do planejamento.
- **Estabelecer o contexto:** atividade realizada para determinar os parâmetros e o escopo da gerência de riscos. Para ser completa, esta fase deve possuir contexto interno, externo e do gerenciamento de riscos, além dos critérios utilizados para identificá-los.
- **Avaliação dos riscos:** envolve processos para identificar, analisar e avaliar os riscos, com o objetivo principal de desenvolver uma compreensão sobre os mesmos, além de determinar quais as maiores ameaças para impedir/dificultar o sucesso do projeto.
- **Tratamento dos riscos:** etapa de planejamento e implementação das soluções para os riscos compreendidos e priorizados na etapa anterior, com o objetivo de mitigá-los até que desapareçam ou atinjam níveis satisfatórios, de acordo com os parâmetros do plano de gerenciamento de riscos.
- **Monitoramento e controle:** atividade que deve ser executada de maneira iterativa ou *ad-hoc* ao longo do ciclo de vida do projeto, com o intuito de manter a lista de riscos atualizada, reavaliar a eficácia do gerenciamento, garantir que as ameaças tratadas não reapareçam, além de armazenar as lições aprendidas no banco de dados histórico da organização.

Por fim, como complemento à norma abordada nesta seção, o *International Organization for Standardization* disponibiliza o Guia 73 [23], que contém os vocabulários comuns para a área e a ISO 31010 [24], que descreve um conjunto de ferramentas e técnicas para auxiliar no processo de gerenciamento de riscos.

C. PMBOK

O *Project Management Body of Knowledge* (PMBOK) [6] é um guia, amplamente utilizado por vários setores da indústria, criado e mantido pelo *Project Management Institute* (PMI), que consiste na junção das melhores práticas de gerenciamento de projetos disponíveis no mercado.

Este guia divide-se em nove áreas de conhecimento e cinco grupos de processo: os gerenciamentos de integração, escopo, tempo, custos, qualidade, recursos humanos, comunicações, riscos e aquisições são áreas de conhecimento, já a iniciação, planejamento, execução, monitoramento e controle e encerramento são os grupos de processo.

Entre o conjunto de áreas apresentadas, o gerenciamento de riscos é a que está alinhada com o foco deste estudo. Seu objetivo é aumentar a chance de ocorrência de eventos positivos e reduzir a probabilidade de eventos negativos. As etapas envolvidas nesta gerência estão descritas abaixo:

- **Planejar o gerenciamento de riscos:** consiste em estabelecer as regras que irão nortear as atividades da gerência de riscos durante todo o ciclo de vida do projeto, com o objetivo de criar elementos para indicar como a gerência será conduzida, critérios, *stakeholders* envolvidos e suas responsabilidades, orçamento, prazo e métricas de probabilidade de ocorrência do risco.
- **Identificar os riscos:** etapa de levantamento dos riscos. Ocorre durante todo o ciclo de vida do projeto, com o objetivo de criar e manter atualizada uma lista descritiva com os riscos com potencial para afetá-lo, além de conter os possíveis impactos que eles podem causar ao projeto no caso de sua concretização.
- **Realizar a análise qualitativa dos riscos:** atividade para priorizar os riscos de acordo com os impactos que podem causar ao projeto, além de sua probabilidade de ocorrência. O objetivo desta fase é categorizar os riscos em grupos de alto, moderado ou baixo impacto.
- **Realizar a análise quantitativa dos riscos:** complemento à análise qualitativa, entretanto o intuito desta atividade é mensurar os efeitos que os riscos exercem sobre os objetivos do projeto, além de determinar as prioridades presentes na lista de riscos.
- **Planejar as respostas aos riscos:** fase de planejamento das medidas que serão tomadas para controlar os riscos, com o objetivo de definir qual abordagem será utilizada, quais os responsáveis, custos envolvidos, planos de contingência e prazo para realizar o tratamento.
- **Monitorar e controlar os riscos:** etapa de acompanhamento do risco e implementação dos planos de resposta, com o objetivo de monitorar riscos residuais, identificar novos e analisar a eficácia do processo de gerenciamento de riscos, além de armazenar as lições aprendidas no banco de dados histórico da organização.

Além do processo de gerenciamento de riscos, o guia do PMBOK também apresenta um conjunto de documentos de entrada, saída e várias ferramentas e técnicas que tem por objetivo auxiliar os gerentes nas atividades realizadas no dia-a-dia da organização.

D. Modelos de Maturidade

Os modelos de maturidade buscam estabelecer patamares de evolução de processos, chamados de níveis de maturidade, que caracterizam estágios de melhoria na implementação de processos na organização [25]. Estes níveis de maturidade, por sua vez, indicam o perfil da empresa e os caminhos para a melhoria do processo em questão. Vários modelos de maturidade foram estudados, dentre os quais podem-se destacar:

- ***Organizational Project Management Maturity Model* (OPM3)**: criado e mantido pelo PMI, cujas atividades são baseadas no guia do PMBOK. É composto por quatro níveis de maturidade e três domínios: (1) Padronizar, (2) Medir, (3) Controlar e (4) Melhoria Contínua, são os níveis de maturidade e (1) Portfólio, (2) Programa e (3) Projeto, são os domínios [26].
- ***Capability Maturity Model Integration* (CMMI)**: é um modelo de avaliação de maturidade criado e mantido pelo *Software Engineering Institute* (SEI), cujo foco são os processos de Tecnologia da Informação (TI). Este modelo possui cinco níveis de maturidade: (1) Inicial (*Ad Hoc*), (2) Gerenciado, (3) Definido, (4) Quantitativamente Gerenciado e (5) Em Otimização [27].
- ***Control Objectives for Information and Related Technology* (COBIT)**: criado pelo *IT Governance Institute* (ITGI) e mantido pelo ISACA é um padrão amplamente utilizado para a área de governança. É composto por seis níveis de maturidade: (0) Não existente, (1) Inicial (*Ad Hoc*), (2) Repetitivo, (3) Definido, (4) Gerenciado e (5) Otimizado [28].
- **Modelo de Referência para a Melhoria do Processo de *Software* (MR-MPS)**: o desenvolvimento deste modelo é coordenado pela Associação para Promoção da Excelência do *Software* Brasileiro (SOFTEX) [25] em conjunto com várias empresas nacionais. Contém sete níveis de maturidade: (1) Em Otimização, (2) Gerenciado Quantitativamente, (3) Definido, (4) Largamente Definido, (5) Parcialmente Definido, (6) Gerenciado e (7) Parcialmente Gerenciado.
- ***Maturity Model in Information Security* (MMGRSeg)**: modelo criado com base no CMMI e na norma ISO/IEC 27005 [28] por Mayer e Fagundes [29]. Tem seu foco voltado para o gerenciamento de riscos em segurança da informação. Divide-se em cinco níveis de maturidade: (1) Inicial, (2) Intuitivo, (3) Padronizado, (4) Gerenciado e (5) Otimizado e três estágios: (1) Imaturidade, (2) Maturidade e (3) Excelência.

III. Framework para gerenciar riscos por meio de serviços

Conforme exposto anteriormente, este estudo tem como objetivo apresentar o *framework* GAIA Riscos. Esta estrutura baseia-se em serviços, que tem como foco auxiliar os gerentes de projeto a incluírem, de maneira incremental e flexível, as atividades referentes à gerência dos riscos no Processo de Desenvolvimento de *Software* (PDS) das organizações. Isto, para permitir que tais práticas sejam executadas sem a necessidade de grandes modificações no PDS.

A obtenção destes serviços, por sua vez, dá-se pela fragmentação do processo de gerenciamento de riscos da ISO 31000 em sete serviços, que são: (1) Identificar Riscos, (2) Estabelecer o Contexto, (3) Analisar Riscos, (4) Avaliar Riscos, (5) Tratar Riscos, (6) Monitoramento e Controle e (7) Comunicação e Consulta. A organização dos mesmos nos níveis de maturidade respeitam os critérios estabelecidos pelo MMGRSeg (seção II-D). A figura 1 ilustra os níveis de maturidade e seus componentes.

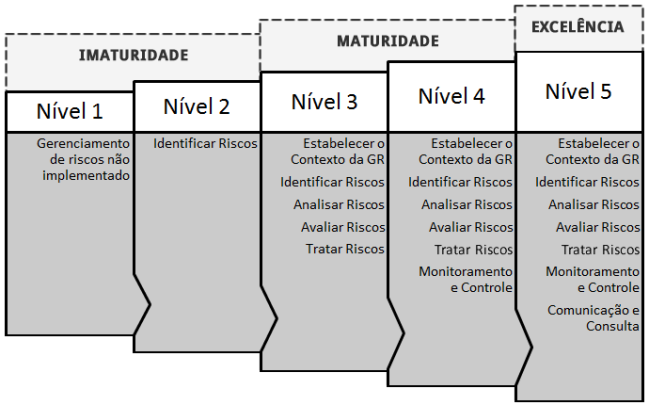

Figura 1. *Framework* GAIA Riscos.

Conforme ilustrado pela figura 1, o modelo consiste em cinco níveis de maturidade, que são norteados por três estágios: (1) Imaturidade, (2) Maturidade, (3) Excelência. Embora a proposta do MMGRSeg seja voltada para a segurança da informação seus critérios são aplicáveis ao desenvolvimento de *software*, uma vez que os autores baseiam-se no CMMI. As características de cada nível de maturidade são descritas abaixo:

- **Nível 1 - Inicial:** a organização tem conhecimento da existência do gerenciamento de riscos porem não o aplica. A empresa também pode não conhecer esta gerência.
- **Nível 2 - Conhecido:** adoção de práticas propostas pelo Serviço de Identificar os Riscos, porém elas são executadas de maneira intuitiva.
- **Nível 3 - Padronizado:** definição formal dos parâmetros e processos de gerência dos riscos, por meio da adoção das práticas determinadas pelos Serviços de Estabelecer o Contexto, Analisar, Avaliar e Tratar os riscos.
- **Nível 4 - Gerenciado:** adoção das práticas propostas pelo Serviço de Monitoramento e Controle, buscando identificar novos riscos e comparar as informações obtidas com os padrões estabelecidos.
- **Nível 5 - Otimizado:** adoção das práticas estabelecidas no Serviço da Comunicação e Consulta para garantir que os interesses de todos os envolvidos sejam comunicados.

Cada serviço do *framework* GAIA Riscos tem como objetivo entregar valor aos clientes, permitindo assim que eles alcancem seus objetivos. Além disso, cada um deles é composto de cinco áreas, as quais mantem as informações organizadas e podem ser customizados de acordo com a necessidade do projeto, cliente e organização. A figura 2 apresenta a estrutura básica dos serviços do *framework*.

Figura 2. Estrutura do serviço.

Conforme ilustrado pela figura 2 as informações básicas que compõem cada serviço são obtidas por meio da organização das boas práticas de vários guias e normas. As Ferramentas e Técnicas são propostas pela norma ISO 31010, os Vocabulários retirados do Guia 73 da ISO, os *Workflows* baseados na norma ISO 31000, os Indicadores de Desempenho baseados no *Balanced Scorecard* (BSC) e *Templates* de Documentos de entrada e saída propostos pelo PMBOK. A descrição de cada serviço segue abaixo:

- **Identificar Riscos:** realização de análises no plano de gerenciamento do projeto para obtenção de uma lista que contém todos os riscos identificados. A catalogação dos riscos é elaborada por meio de reuniões de *brainstorming*, entrevistas com os *stakeholders* ou, ainda, pela utilização da técnica de Wideband Delphi [24].
- **Estabelecer o Contexto:** definição dos parâmetros que irão nortear as atividades de análise, avaliação e tratamento dos riscos, os quais são obtidos por meio da análise dos documentos do projeto. Para isso, são realizadas reuniões, entrevistas com os interessados, consultas no banco de dados histórico da organização ou, ainda, a técnica de Wideband Delphi.
- **Análisar Riscos:** compreensão dos riscos identificados para gerar uma lista de riscos analisados, o que é realizado por meio de simulações, análises de árvore de decisão, criação de matrizes de probabilidade/impacto,

ou, ainda, pela aplicação da técnica do "e se" (*what if*) [24].

- **Avaliar Riscos:** comparação dos riscos analisados com os parâmetros estipulados no Serviço de Estabelecer o Contexto, com o intuito de determinar quais os riscos com maior potencial. Para tanto são realizadas simulações, análises de causa/consequência, análises estatísticas e informações presentes no banco de dados histórico da organização.
- **Tratar Riscos:** ações para desenvolver as opções de tratamento e os planos de contingência para as prioridades estipuladas no Serviço de Avaliar Riscos. As correções resultam em relatórios de desempenho e lições aprendidas, que devem ser armazenadas no banco de dados histórico da organização.
- **Monitoramento e Controle:** atividades para determinar a eficiência do processo de gestão dos riscos. As informações obtidas decorrem da execução dos outros serviços e devem ser armazenadas no banco de dados histórico da organização. Tais dados representam a evolução das atividades do gerenciamento dos riscos dentro de uma organização.
- **Comunicação e Consulta:** realização de análises nos planos do projeto para estabelecer a comunicação e os meios de comunicação entre os *stakeholders*. Como resultado deste serviço obtêm-se a disseminação da informação entre os interessados e indicadores de desempenho de comunicação.

Deste modo, baseando-se na estrutura apresentada na figura 2 e nas informações expostas anteriormente, a figura 3 ilustra a composição das áreas do Serviço de Monitoramento e Controle.

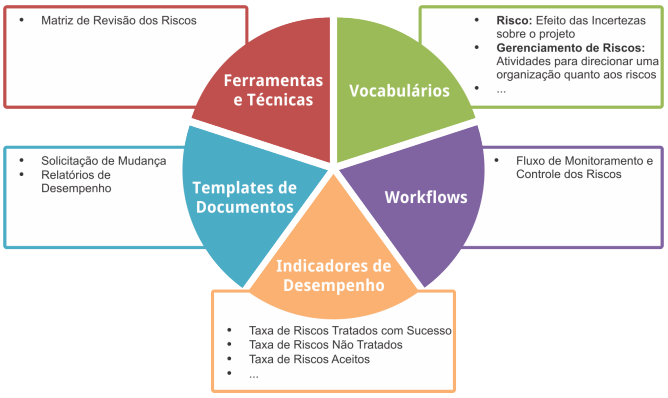

Figura 3. Serviço de Monitoramento e Controle.

Os demais serviços do GAIA Riscos estão disponíveis a todos os membros da equipe através da *internet* (acessível no endereço http://www.gaia.uel.br/gaia_riscos). Isso favorece a disseminação das informações e garante que todos os membros da equipe tenham acesso, em tempo real, as informações sobre a estrutura e as áreas que compõem cada serviço do GAIA Riscos.

Por fim, para aplicar o GAIA Riscos em seu PDS uma organização deve, obrigatoriamente, respeitar um Processo de Implantação, além de realizar verificações a cada evolução de nível de maturidade, com o intuito de garantir que as alterações estejam de acordo com a proposta do *framework*, as possibilidades da organização e atendam completamente suas expectativas.

A. *Processo de Implantação do GAIA Riscos*

Para aplicar o *framework* GAIA Riscos a um PDS algumas atividades devem ser seguidas. Estes procedimentos buscam determinar o nível de maturidade do PDS e reavaliar sua aderência a um determinado nível, além de permitir mensurar a capacidade de evolução do PDS para níveis superiores. As atividades que compõem o Processo de Implantação do GAIA Riscos estão ilustradas na figura 4.

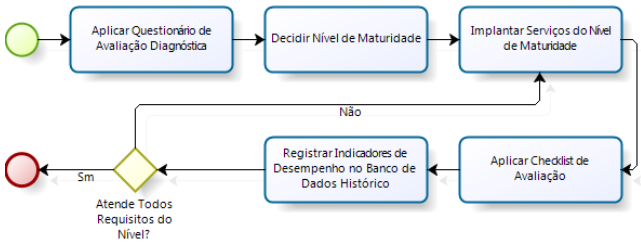

Figura 4. Processo de Implantação do GAIA Riscos.

Conforme apresentado na figura 4, a entrada do Processo de Implantação do GAIA Riscos é o preenchimento de um Questionário de Avaliação Diagnóstica, o qual deve ser respondido eletronicamente pelos gerentes de projeto através do Sistema de Avaliação Diagnóstica. As questões são de múltipla escolha e o resultado de seu preenchimento corresponde ao o posicionamento do PDS da organização em um dos cinco níveis de maturidade do *framework*.

As questões que compõem o Questionário de Avaliação Diagnóstica buscam identificar a taxa com que o PDS analisado atende a cada serviço do *framework*. Para isso, elas possuem um conjunto de alternativas que traduzem objetivamente as situações ocorridas no dia-a-dia da organização, com o objetivo de simplificar o preenchimento do questionário pelos gerentes de projeto. Ainda, cada alternativa possui fatores multiplicativos que quantificam seu impacto com relação a questão que pertencem. Estes fatores são utilizado para calcular a taxa de atendimento, os quais estão dispostos na tabela I.

Além da relação entre as questões e as alternativas, que são os fatores multiplicativos, outro importante componente do Sistema de Avaliação Diagnóstica é o relacionamento entre as questões e os os serviços do GAIA Riscos, que é dado por pesos. Deste modo, uma questão pode exercer diferentes pesos em cada serviço do *framework*. A tabela II representa a relação entre uma questão e os pesos que ela pode exercer sobre cada serviço.

Baseado nas informações coletadas pelas respostas do questionário e seguindo o modelo de questão exposto nas tabelas I e II, se obtém o resultado da avaliação do PDS, o qual é orientado aos serviços. Para tanto, é necessário calcular o produto

Tabela I
QUESTÃO DO SISTEMA DE AVALIAÇÃO DIAGNÓSTICA

Questão: A organização possui parâmetros bem definidos para identificar os riscos dos projetos?		
Alternativa	**Texto**	**Fator Multiplicativo**
A	Sim, a organização possui parâmetros bem definidos e eles são conhecidos por todos.	3
B	Sim, a organização possui parâmetros bem definidos mas eles não são conhecidos por todos.	2
C	A organização possui alguns parâmetros, os quais não são conhecidos por todos.	-2
D	Não, a organização não possui parâmetros para gerenciar riscos.	-3

Tabela II
PESO DA QUESTÃO NOS SERVIÇOS DO GAIA RISCOS

Questão: A organização possui parâmetros bem definidos para identificar os riscos dos projetos?		
Serviço	**Justificativa**	**Peso**
Identificar Riscos	Os parâmetros fixam a abrangência do gerenciamento de riscos.	3
Estabelecer Contexto	Os parâmetros são decisivo para o gerenciamento dos riscos.	4
Analisar Riscos	Os parâmetros definem as metodologias que serão utilizadas para analisar.	1
Avaliar Riscos	Os parâmetros definem as métricas e objetivos para determinar as prioridades.	2
Tratar Riscos	Os parâmetros estabelecem como o tratamento deve ocorrer.	1
Monitoramento e Controle	Os parâmetros indicam como a eficácia deve ser avaliada.	2
Comunicação e Consulta	Os parâmetros determina, quais informações comunicar ao cliente.	1

entre o peso da questão no serviço e o fator multiplicativo relacionada à alternativa selecionada. A pontuação final, por sua vez, é obtida pela somatória destes produtos para cada serviço.

Para calcular o percentual de atendimento (M) sobre cada serviço, esta pontuação final deve ser ajustada com base nos valores extremos do questionário, que determinam um intervalo entre seu maior e menor valor possível. Dessa forma, a pontuação final é posicionada no intervalo descrito, determinando assim, a taxa de atendimento de cada serviço. Por conseguinte, o nível de maturidade da organização é determinado com base no serviço que obteve a menor taxa e classificado conforme exposto na tabela III.

Tabela III
CONVERSÃO DE PERCENTUAL EM NÍVEL DE MATURIDADE.

Percentual	**Nível de Maturidade**
$0 \leq M \leq 20$	GAIA Riscos Nível 1
$21 \leq M \leq 40$	GAIA Riscos Nível 2
$41 \leq M \leq 60$	GAIA Riscos Nível 3
$61 \leq M \leq 80$	GAIA Riscos Nível 4
$81 \leq M \leq 100$	GAIA Riscos Nível 5

Para demonstrar os resultados obtidos com a aplicação do questionário utiliza-se um gráfico de radar, no qual cada eixo representa um serviço e sua área é definida pelos seus percentuais de atendimento. Desta maneira tem-se uma visão global sobre os mesmos, o que facilita a visualização por parte dos gerentes de projeto.

No âmbito das funcionalidades do Sistema de Avaliação Diagnóstica, a área administrativa permite controlar os usuários, questionários, eixos, questões e alternativas, além de imprimir relatórios. Na área de acesso comum é possível que o visitante se cadastre. Uma vez cadastrado o usuário pode responder aos questionários e administrar suas respostas, obtendo relatórios que irão guiar a implantação do *framework*. A figura 5 representa uma das interfaces do sistema.

Figura 5. Interface do Sistema de Avaliação Diagnóstica.

Por sua vez, o diagrama de casos de uso, exposto na figura 6, representa as principais estas funcionalidades do Sistema de Avaliação Diagnostica.

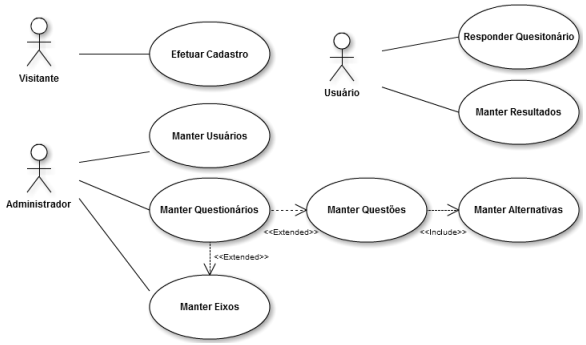

Figura 6. Diagrama de Casos de Uso do Sistema de Avaliação Diagnóstica.

Como, além de implantar o GAIA Riscos em um PDS, este Processo de Implantação também busca garantir a melhoria contínua do gerenciamento de riscos, uma reavaliação deve ser realizada a cada iteração, por meio de *checklists*. As informações obtidas são utilizadas para verificar se o PDS contempla as áreas do nível de maturidade.

Após validar a aderência do PDS com o nível alcançado, os Indicadores de Desempenho devem ser registrados no banco de dados histórico da organização. O objetivo destas informações é indicar é criar uma memória organizacional sobre os riscos. A tabela IV representa um dos indicadores do Processo de Implantação.

Por fim, enquanto todas as entradas do *checklist* de avaliação não forem atendidas, torna-se necessário adotar medidas para

Tabela IV
INDICADOR DE TOTAL DE RISCOS IDENTIFICADOS POR PONTOS DE CASOS DE USO

Identificador	TRI.
Nome	Total de Riscos Identificados por Ponto de Casos de Uso.
Objetivo da Medição	Acompanhar número de riscos em cada nível de maturidade.
Objetivo de Negócio Associado	Detectar o maior número de riscos.
Fórmula	TRI = Total de Riscos Identificados.
Interpretação da Medição	Quanto mais riscos identificados menor a chance de surpresas.
Responsável pela Medição	Gerente do Projeto.
Frequência da Medição	Será realizada após a aplicação do *checklist* de reavaliação.
Fonte de Dados	Lista de riscos identificados.
Unidade de Medida	Número inteiro.
Meta	Detectar o maior número de riscos.
Público Alvo	As medições devem ser apresentadas a toda equipe.
Frequência da Análise	Sempre que houver medição do numero total de riscos identificados.
Responsável pela Análise	Gerente do Projeto
Método de Análise	Analisar logo após a medição.

contemplar os serviços, ou áreas especificas dos mesmos, que ainda não satisfazem as exigências desta lista. Ao término deste Processo de Implantação, com o alcance de todos os objetivos do *checklist* de reavaliação, torna-se possível executar este processo novamente para aderir a um novo nível de maturidade do GAIA Riscos.

IV. APLICAÇÃO DO FRAMEWORK EM UM PROCESSO DE DESENVOLVIMENTO DE SOFTWARE

Com o objetivo de verificar e validar o GAIA Riscos (seção III), o Processo de Implantação (seção III-A) foi executado, iterativamente, até que o Processo de Desenvolvimento de *Software* da Fábrica GAIA (PDSG) alcançasse ao nível 5 de maturidade. Para isso, seis meses e dois projetos da fábrica GAIA[1] foram necessários para evoluir o PDSG até a excelência na gestão dos riscos. A figura 7 ilustra o *workflow* do PDSG.

Conforme a representação gráfica do PDSG (figura 7) é possível verificar que ele é composto por nove atividades. Estas atividades envolvem ações para identificar as premissas do projeto, expandir a *Work Breakdown Structure* (WBS) do projeto, estimar prazos e custos, elaborar os planos de gerenciamento, gerenciar a comunicação entre os interessados, identificar novos requisitos, implementar as entregas, testar e validar o *software*, entregar as partes desenvolvidas e gerenciar o portfólio de produtos da organização.

Neste contexto, para iniciar a aplicação do GAIA Riscos, o PDSG foi submetido ao Sistema de Avaliação Diagnóstica, conforme o proposto pelo Processo de Implantação do GAIA

[1]A fábrica de *software* GAIA é composta por equipes de alunos dos cursos de graduação e mestrado do Departamento de Computação (DC) da Universidade Estadual de Londrina (UEL) e utiliza um processo de desenvolvimento prescritivo concebido de forma gradual para atender ao nível F do modelo de referência MR-MPS [25], com o intuito de padronizar seus processos, aumentar a qualidade do *software* produzido, satisfação do cliente e a produtividade da equipe.

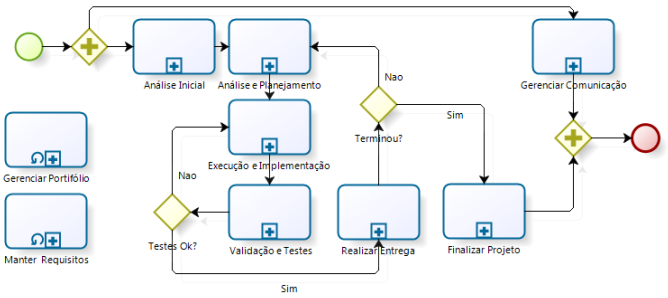

Figura 7. Componentes do Processo de desenvolvimento de *software* da fábrica GAIA (PDSG).

Riscos. As informações coletadas indicaram a ausência de metodologias para administrar os riscos do projeto, ou seja, de acordo com o GAIA Riscos, o processo da fábrica GAIA encontra-se no primeiro nível de maturidade. A figura 8 ilustra o resultado obtido do após a aplicação do sistema.

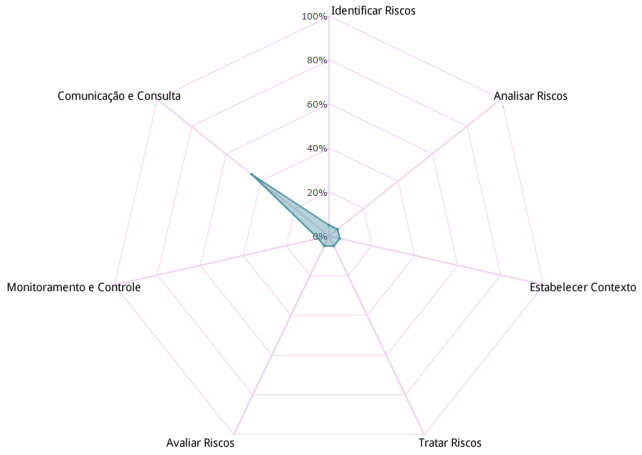

Figura 8. Resposta obtida na primeira execução do Sistema de Avaliação Diagnóstica.

Conforme pode ser observado na figura 8, o nível alcançado para o Serviço de Comunicação e Consulta foi elevado em relação aos demais serviços. Após a análise deste gráfico foi possível determinar que o PDSG já possui atividades para comunicar os interessados sobre o andamento do projeto, deste modo, estas atividades também atendem parcialmente ao gerenciamento de riscos.

Primeiramente o PDSG sofreu alterações para evoluí-lo do primeiro para o segundo nível de maturidade. Para isso, um projeto de pequeno porte. Após seguir o Processo de Implantação, verificou-se que as ações limitaram-se a criação de referências para o Serviço de Identificar Riscos nas instruções de trabalho da atividade de análise e planejamento. Por fim, os indicadores de desempenho foram armazenados no banco de dados histórico da organização.

No entanto, estas modificações não forneciam métricas comparativas. Deste modo, à medida que a equipe se acostumou a identificar os riscos, surgiu a necessidade de documentá-los e avaliá-los. Como consequência, a progressão para o

próximo nível de maturidade tornou-se necessária. Para isso, um projeto de maior porte, realizado para a Associação Brasileira de Ensino Odontológico (ABENO) (disponível em http://www.abeno.org.br).

Para tanto, o PDSG foi submetido a uma nova execução do Processo de Implantação do GAIA Riscos. Como resultado, o Sistema de Avaliação Diagnóstica sugeriu três alterações para que o processo evoluísse para o terceiro nível de maturidade. Em um primeiro momento, referências foram adicionadas, nas instruções de trabalhos da atividade de análise inicial, para o Serviço Estabelecer o Contexto.

Na sequencia, seguindo as orientações do Sistema de Avaliação Diagnóstica, a atividade de Análise e Planejamento foi alterada. Para isso, a referência para o Serviço de Identificar Riscos foi substituída por uma nova atividade, a qual possui indicações para os Serviços de Identificar, Analisar e Avaliar os Riscos. A execução desta nova atividade deve ocorrer paralelamente a criação/manutenção dos planos do projeto.

Para concluir as alterações, uma atividade representando o Serviço de Tratamento dos Riscos foi adicionada à atividade de Execução e Implementação, cuja execução deve ocorrer em paralelo ao desenvolvimento da fase em questão. Ao término desta etapa os indicadores de desempenho foram registrados.

Por meio das mudanças realizadas, as etapas fundamentais para administrar os riscos do projeto estavam presentes no PDSG. Contudo, após algumas entregas observou-se a necessidade de métricas que demonstrassem a eficácia da gerência de riscos. Deste modo, foi necessária a evolução para o quarto nível de maturidade.

O resultado do Sistema de Avaliação Diagnóstica propôs a inclusão de uma nova atividade indicando ao Serviço de Monitoramento e Controle, o que foi executado na atividade de Realizar Entrega. A figura 9 ilustra a alteração realizada na atividade de Realizar Entrega do PDSG. Ao término desta etapa os indicadores de desempenho foram registrados no banco de dados histórico da organização.

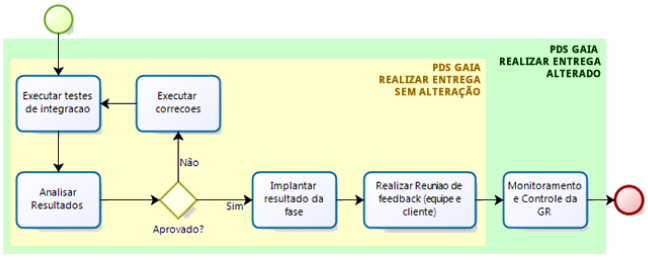

Figura 9. Alteração realizada na atividade Realizar Entrega do PDSG.

Entretanto, no decorrer do desenvolvimento do *software* notou-se a necessidade de melhorar a integração entre o cliente e a equipe do projeto, tanto para informar os riscos quanto o andamento das ações. Deste modo, a ações para evoluir o PDSG para o quinto nível de maturidade do GAIA Riscos foram realizadas. Como resultado das alterações, foi incluída referência para o Serviço de Comunicação e Consulta na atividade de Gerenciar Comunicação.

Na tabela V pode-se verificar a síntese das alterações realizadas no Processo de Desenvolvimento de *Software* da Fábria GAIA.

Tabela V
SÍNTESE DAS ALTERAÇÕES REALIZADAS NO PDSG

Atividade Modificada	**Tipo de Alteração**	**Serviços Referenciados**
Análise Inicial	Instrução de Trabalho	Estabelecer o Contexto
Análise e Planejamento	Inclusão de Atividade	Identificar, Analisar e Avaliar Riscos
Execução e Implementação	Inclusão de Atividade	Tratar Riscos
Realizar Entrega	Inclusão de Atividade	Monitoramento e Controle
Gerenciar Comunicação	Instrução de Trabalho	Comunicação e Consulta

Após realizar as alterações apresentadas na tabela V e com o intuito de apurar se os esforços realizados alcançaram o objetivo de integrar o PDSG com o GAIA Riscos, o processo em questão foi novamente submetido a uma rodada de validações no Sistema de Avaliação Diagnóstica. Conforme ilustrado pela figura 10, é possível verificar que o resultado obtido demonstra a aderência do PDSG ao quinto nível de maturidade do *framework* GAIA Riscos.

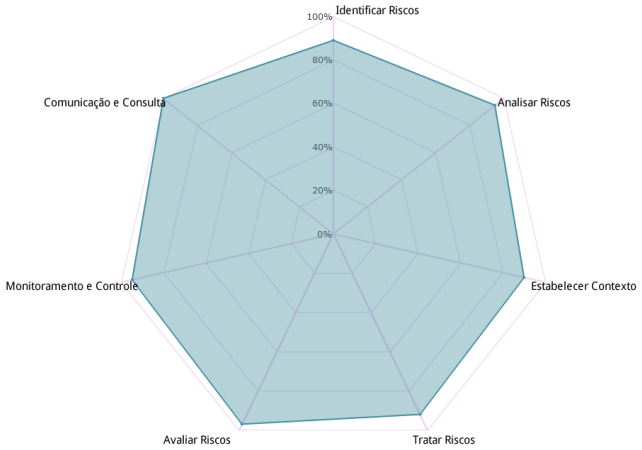

Figura 10. Resposta obtida do Sistema de Avaliação Diagnóstica após as alterações realizadas no PDSG.

Após processar os resultados obtidos e as lições aprendidas no decorrer do Processo de Implantação do GAIA Riscos, tornou-se possível compreender que, reunir as informações do gerenciamento de riscos trouxe segurança para a equipe do projeto. Isso, pois, a execução das ações propostas deram-se de maneira sequencial e natural, respeitando os níveis de maturidade e o Processo de Implantação do GAIA Riscos. Além disso, o agrupamento das melhores práticas propostas pelo PMBOK e pelas normas ISO, bem como sua disponibilização na *internet*, facilitaram a disseminação das mesmas entre os *stakeholders*.

Além das alterações realizadas no PDSG, pode-se destacar também que o *framework* GAIA Riscos possibilita a implan-

tação total ou parcial de seus serviços. Entretanto, como o objetivo deste estudo de caso é verificar e validar a integração da estrutura apresentada com um Processo de Desenvolvimento de *Software*, todas as modificações realizadas foram planejadas almejando-se aderir ao quinto nível de maturidade do *framework*, ou seja, a excelência no gerenciamento dos riscos do projeto.

Deste modo, para demonstrar as contribuições que a adoção do gerenciamento de riscos por meio de serviços trouxe ao PDSG, os resultados coletados pelos indicadores de riscos tratados/mitigados e aceitos/transferidos foram confrontados com os dados presentes no banco de dados histórico da fábrica GAIA. Ressalta-se que, para elaborar esta comparação apenas os dados de projetos semelhantes foram utilizados. Assim, a figura 11 ilustra a comparação entre projetos com e sem o GAIA Riscos.

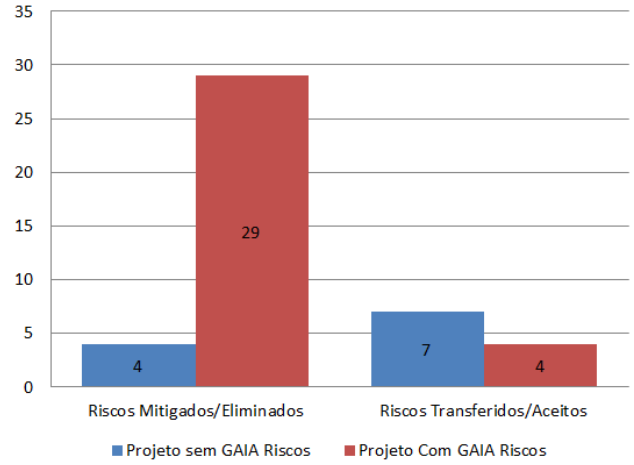

Figura 11. Comparativo entre projetos com e sem o GAIA Riscos.

De acordo com a análise da figura 11 é possível verificar que antes da adoção do GAIA Riscos, em média 11 riscos eram identificados. Destes, apenas 4 ($\approx$ 36%) eram mitigados/tratados. Após a adoção do GAIA Riscos e com o estabelecimento dos parâmetros e mecanismos para identificar, avaliar, tratar, monitorar e comunicar os riscos, este número aumentou para 33 riscos, dos quais, 29 ($\approx$ 88%) passaram a ser mitigados/tratados.

Por fim, pode-se destacar que as mudanças aplicadas no PDSG ao longo da realização deste estudo de caso, prepararam-no para uma futura evolução para o nível C (Definido) do modelo de referência MR-MPS, o qual, é composto por todas as atividades dos níveis anteriores (G ao D), acrescidos dos processos de desenvolvimento para reutilização, gerência de decisões e a gerência dos riscos do projeto.

V. Conclusão e Trabalhos Futuros

A gestão dos riscos do projeto é um fator cada vez mais decisivo para o sucesso do mesmo, uma vez que, a atual volatilidade do mercado e as constantes mudanças de requisitos e escopo podem criar empecilhos para alcançá-lo ou então reduzir a qualidade do produto final. Com isso, o artigo em questão apresenta um *framework*, baseado em serviços e níveis de maturidade para gerenciar os riscos inerentes aos projetos com flexibilidade.

De acordo com o apresentado é possível concluir que a estrutura criada (seção III) organiza, por intermédio dos serviços, os melhores conhecimentos das normas e metodologias mais utilizadas para gerenciar os riscos dos projetos, permitindo assim, a customização dos mesmos, a flexibilidade para adequação da estrutura às necessidades da equipe, projeto e cliente simultaneamente.

Além disso, a possibilidade de integrar o gerenciamento de riscos ao PDS de uma organização, por meio da execução do ciclo PDCA, em conjunto com os níveis de maturidade, conforme apresentado a seção IV, torna possível implementá-lo, de maneira total ou parcial, permitindo que ele evolua ao longo do tempo, até atingir o nível de excelência. Com isso, a estrutura torna-se genérica e pode ser aplicada em projetos que demandem de uma maior ou menor rigorosidade no tratamento dos riscos.

Devido ao agrupamento das melhores práticas de cada norma e metodologia, incentiva-se a gestão proativa dos riscos, o que influencia diretamente no grau de comprometimento da equipe com o sucesso do projeto, criando um senso comum de que o sucesso do projeto é de vital importância para o crescimento da organização.

Após a conclusão do estudo apresentado, futuros trabalhos estão relacionados ao tema: (a) ampliar o número de estudos de caso com o objetivo de aperfeiçoar o *framework* de serviços, aplicando-o, inclusive, a outros domínios, como, por exemplo, a Governança de Tecnologia da Informação e Comunicação (TIC) e outros ramos da indústria, (b) desenvolver uma ferramenta automatizada de apoio ao gerenciamento de riscos que, por meio das lições aprendidas, auxilie os gerentes de projeto a determinar os serviços que melhor atendam as suas necessidades, (c) analisar a aplicação da ferramenta *RiskFree* [30] para auxiliar nas atividades do gerenciamento de riscos.

Por fim, após a realização deste estudo, as principais contribuições obtidas foram: (a) a criação de um *framework* para gerenciar riscos por meio de serviços, cuja estrutura baseia-se em cinco níveis de maturidade (seção III), (b) serviços que são compostos pelas melhores práticas de várias normas amplamente utilizadas (seção III), (c) um Processo de Implantação para o gerenciamento de riscos (seção III-A), (d) um Sistema de Avaliação Diagnóstica que posiciona o respondente em um dos níveis de maturidade (seção III-A), (e) indicadores para medir o desempenho da gerência dos riscos (seção III-A) e (f) *checklists* de reavaliação para nortear a implantação dos serviços (seção III-A).

Referências

[1] S. Islam and W. Dong, "Human Factors in Software Security Risk Management," *Risk Analysis*, pp. 13–16, 2008.

[2] Standish Group, *Chaos Manifesto*, 2011.

[3] B. Boehm, "Software risk management: principles and practices," *Software, IEEE*, no. January, 1991.

[4] P. L. Bannerman, "Risk and risk management in software projects: A reassessment," *Journal of Systems and Software*, vol. 81, no. 12, pp. 2118–2133, Dec. 2008.

[5] ISO, *ISO 31000: Principles and Guidelines*, 2009.

[6] PMI, *A guide to the project management body of knowledge*, 4th ed. Newton Square, Pennsylvania: Project Management Institute, Inc., 2008.

[7] R. Riehle, "Institutional memory and risk management," *ACM SIGSOFT Software Engineering Notes*, vol. 32, no. 6, p. 5, Nov. 2007.

[8] S. Alhawari, L. Karadsheh, and A. N. Talet, "Knowledge-Based Risk Management framework for Information Technology project," *Information Management*, p. 16, 2011.

[9] U. Rosselet and M. Wentland, "Knowledge management framework for IT project portfolio risk management," *Fifth International Conference on Knowledge*, pp. 203–204, 2009.

[10] L. H. R. Leme, "Uma estratégia para apoiar o gerenciamento de riscos em um ambiente distribuído de desenvolvimento de software," Master's thesis, Universidade Estadual de Maringá, 2007.

[11] S. H. Han, D. Y. Kim, and H. Kim, "A web-based integrated system for international project risk management," *Automation in construction*, pp. 342 – 356, 2008.

[12] A. A. Keshlaf and S. Riddle, "Risk Management for Web and Distributed Software Development Projects," *Fifth International Conference on Internet Monitoring and Protection*, pp. 22–28, 2010.

[13] A. Lamersdorf, J. Munch, A. F.-d. V. Torre, and C. R. S´nchez, "A Risk-Driven Model for Work Allocation in Global Software Development Projects," *IEEE Sixth International Conference on Global Software Engineering*, pp. 15–24, Aug. 2011.

[14] K. Schwaber and J. Sutherland, *The Definitive Guide to Scrum: The Rules of the Game*, 2011.

[15] H. Mathkour, G. Assassa, and A. Baihan, "A Risk Management Tool for Extreme Programming," *International Journal of Computer Science and Network Security*, vol. 8, no. 8, pp. 326–333, 2008.

[16] U. Chinbat and S. Takakuwa, "Using Simulation Analysis for Mining Project Risk Management," in *Proceedings of the 2009 Winter Simulation Conference*, 2009, pp. 2612–2623.

[17] D. Liu, Q. Wang, and J. Xiao, "The role of software process simulation modeling in software risk management: A systematic review," *2009 3rd International Symposium on Empirical Software Engineering and Measurement*, pp. 302–311, Oct. 2009.

[18] C. Gusmão, "Um Modelo de Processo de Gestão de Riscos para Ambientes de Múltiplos Projetos de Desenvolvimento de Software," Master's Thesis, Universidade Federal de Pernambuco, 2007.

[19] L. Wanqing and Z. Yong, "Study on Risk Management System for Construction Enterprises Based on Projects," *4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–5, Oct. 2008.

[20] D. Schreiber, C. d. S. Garcia, and D. Domingos, "Terceirização de Desenvolvimento de Software em Body Shop: Uma Proposta para Diminuir os Riscos," *X Simpósio Brasileiro de Qualidade de Software*, p. 8, 2010.

[21] M. Aldenucci, "Um modelo de maturidade para processos de gerenciamento de riscos em projetos," Master's Thesis, Pontifícia Universidade Católica, 2009.

[22] F. Turley, *The PRINCE2 Training Manual: A common sense approach to learning and understanding PRINCE2*, 2010.

[23] ISO, *ISO Guide 73: Risk Management Vocabulary*, 2009.

[24] ——, *ISO 31010: Risk Assessment Techniques*, 2009.

[25] SOFTEX, *MPS . BR - Melhoria de Processo do Software Brasileiro Guia Geral*. Brasília: Associação para Promoção da Excelência do Software Brasileiro, 2011.

[26] J. ao Carlos Araújo da Silva Neto, "Avaliação de maturidade no gerenciamento de projetos em uma empresa de mineração em minas gerais," Master's thesis, Universidade FUMEC, 2011.

[27] N. Ehsan, A. Perwaiz, J. Arif, E. Mirza, and A. Ishaque, "Cmmi / spice based process improvement," in *Management of Innovation and Technology (ICMIT), 2010 IEEE International Conference on*, june 2010, pp. 859 –862.

[28] ISO, *ISO/IEC 27005: Information Technology - Security Techniques - Information Security Risk Management*, 2008.

[29] J. Mayer and L. L. Fagundes, "A model to assess the maturity level of the Risk Management process in information security," *2009 IFIP/IEEE International Symposium on Integrated Network Management-Workshops*, no. 5, pp. 61–70, Jun. 2009.

[30] F. Knob, F. Silveira, and A. Orth, "RiskFree - Uma Ferramenta de Gerenciamento de Riscos Baseada no PMBOK e Aderente ao CMMI," *V Simpósio Brasileiro de Qualidade de Software*, pp. 203 – 217, 2006.