Ferramenta para Avaliar o Grau de Maturidade da Gerência de Riscos de um Processo de Desenvolvimento de *Software*

Fernando Henrique Gaffo, Gabriel Ulian Briganó, Flávio Eduardo Aoki Horita, Rodolfo Miranda de Barros
Departamento de Computação
Universidade Estadual de Londrina - UEL
Londrina, Paraná, Brasil
{fernandogaffo, gabrielbrigano, feahorita}@gmail.com, rodolfo@uel.br

Abstract—**The risk management process comprises a set of coordinated activities to identify, analyze, assess, treat, monitor and communicate project risks. Organizations that wish to implement these set of activities on their software development process, in its turn, should adhere a series of activities in compliance to existing standards and regulations. However, there are not found references for models that evaluate this process through a diagnostic assessment tool, allowing managers to have a clear view of its deficiencies. In this way, this study aims to present the diagnostic assessment tool that is based on the GAIA Risks framework as well as the methodology for calculate and display of results.**

Keywords-risk; risk management; project management; diagnostic assessment tool.

I. INTRODUÇÃO

Os sistemas de informação estão difundidos em todos os setores da vida moderna e, com isso, as pessoas tornam-se cada vez mais dependentes destes *softwares* nas atividades do dia-a-dia. As empresas que desenvolvem estes sistemas, por sua vez, enfrentam vários desafios durante o ciclo de vida destes projetos, como por exemplo, custos excessivos, atrasos no cronograma, erros de especificação e baixa qualidade do produto final.

Tais problemas influenciam diretamente no sucesso dos projetos. Fato este, que pode ser comprovado pelo estudo conduzido pelo *Chaos Manifesto* [1]. Os dados apresentados neste relatório indicam que, em média, apenas 37% dos projetos são entregues dentro do prazo e custos estipulados. Do restante, 42% sofrem com atrasos no cronograma, custos elevados ou problemas de especificação, outros 21% são cancelados.

Para combater esta realidade, as organizações devem adotar recursos e processos cada vez mais eficazes para proteger seus projetos [2]. Para tanto, o gerenciamento de riscos (GR) torna-se uma atividade de suma importância para a saúde organizacional, pois, por meio de métodos, ferramentas e processos os gerentes podem identificar, analisar e prever os impactos de uma ameaça ao projeto e planejar ações corretivas.

Riscos são vistos como a probabilidade que um evento tem de interferir diretamente nos resultados do projeto, causando atrasos, custos excessivos e impactos diretos na organização. O GR, por sua vez, compreende um conjunto de atividades, métodos e processos organizados para conduzir uma organização na qual existe a presença de riscos [3].

Neste contexto, este estudo tem como objetivo principal apresentar uma ferramenta, baseada na metodologia proposta por Gaffo e Barros [4, 5], para avaliar o grau de maturidade do GR de um Processo de Desenvolvimento de *Software* (PDS). A motivação para elaborar esta ferramenta deve-se a carência de mecanismos que ajudem os gerentes de projeto a visualizarem as deficiências de um PDS.

Para expor a metodologia de avaliação do grau de maturidade do GR em um PDS, o presente trabalho organiza-se da seguinte forma: a Seção II introduz o GR, a Seção III descreve o framework GAIA Riscos, a Seção IV expõe os modelos de maturidade pesquisados, a Seção V expõe a os resultados obtidos por meio da validação do modelo proposto e a Seção VI, por fim, descreve as conclusões mais significativas que foram obtidas até o presente momento.

II. GERENCIAMENTO DE RISCOS

As comunidades atribuem diferentes significados à palavra riscos [6]. Entretanto, é um senso comum entre as principais abordagens utilizadas no mercado que riscos são eventos ou condições incertas que, se ocorrerem, terão efeitos positivos ou negativos sobre pelo menos um dos objetivos do projeto, tais como tempo, custos, escopo ou qualidade, por exemplo [7,8,9].

O GR, por sua vez, é um conjunto de componentes que provê políticas, objetivos, planos, responsabilidades, recursos, processos e atividades para identificar, avaliar e monitorar tais eventos, melhorando continuamente os processos da organização [7,8,9]. Estas ações estão ligadas à diferentes campos do projeto e a literatura acadêmica, geralmente, as associa ao gerenciamento de projetos [10]. Dentre as abordagens estudadas destaca-se o processo de GR da ISO 31000, que compreende:

- **Comunicação e consulta:** atividade que ocorre paralelamente a todas as atividades do GR para garantir que os interesses de todos sejam atendidos.
- **Estabelecer o contexto:** fase na qual determinam-se os parâmetros e o escopo interno e externo do GR.

- **Avaliação dos riscos:** etapa que envolve processos para identificar, avaliar e analisar os riscos com o objetivo de compreendê-los.
- **Tratamento dos riscos:** estágio no qual ocorre o planejamento e a implantação das soluções dos riscos avaliados.
- **Monitoramento e controle:** atividade que visa garantir que os riscos tratados não reapareçam, além de documentar e compreender as novas ameaças.

III. *Framework* GAIA Riscos

O GAIA Riscos é um *framework* para gerenciar riscos baseado em serviços, cujo propósito é ser flexível e permitir a implantação incremental desta gerência nos processos organizacionais. O *framework* compreende: (1) cinco níveis de maturidade, (2) sete serviços, (3) um questionário de avaliação diagnóstica, (4) quatro *checklists* de reavaliação e (5) indicadores de desempenho. A Fig. 1 expõe os níveis de maturidade e seus serviços.

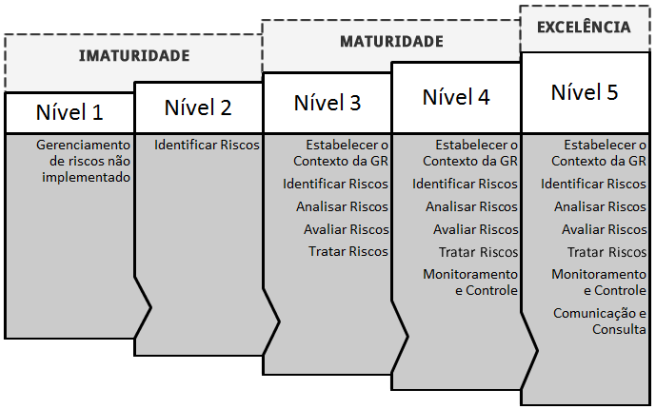

Figura 1. Níveis de maturidade do GAIA Riscos

Cada um dos sete serviços, ilustrados na Fig. 1, tem como objetivo entregar valor ao cliente, permitindo assim que ele alcance seus objetivos [11]. Além disto, cada serviço compreende cinco áreas, as quais mantém as informações organizadas e podem ser customizadas de acordo com as necessidades do projeto, cliente e organização. A Fig. 2 representa a estrutura básica dos serviços.

Figura 2. Estrutura do serviço

Conforme apresentado na Fig. 2, as informações que compõe cada serviço são obtidas por meio da organização das melhores práticas de GR de vários guias e normas. As ferramentas e técnicas provêm da ISO 31010 [12], os vocabulários são retirados do Guia 73 da ISO [13], os workflows procedem das instruções da ISO 31000 [8], os indicadores de desempenho baseiam-se na estrutura do *Balanced Scorecard* (BSC) e os templates de documentos são retirados do PMBOK.

Para enquadrar uma organização em um dos cinco níveis de maturidade e, por conseguinte, apresentar os serviços que devem ser implantados, um processo de implantação do GAIA Riscos deve ser seguido. O ponto de partida de todas as atividades é o preenchimento de um questionário de avaliação diagnóstica que contém, em sua versão atual, 48 questões sobre o GR. As respostas fornecidas serão utilizadas para calcular o nível de maturidade do PDS.

As questões buscam identificar a taxa com que o PDS atende aos serviços do *framework*. Para isso, elas possuem um conjunto de alternativas que traduzem objetivamente as situações do dia-a-dia da organização. Cada alternativa possui fatores multiplicativos, os quais quantificam os impactos com relação à questão que pertencem. Estes fatores são utilizados para calcular a taxa de atendimento.

Além da relação entre as questões e as alternativas, que são os fatores multiplicativos, outro importante componente da avaliação diagnóstica é o relacionamento entre as questões e os serviços do GAIA Riscos, o qual é dado por pesos. Deste modo, uma questão pode exercer diferentes influências em cada serviço do *framework*.

Baseado nas informações coletadas pelas respostas do questionário se obtém o resultado da avaliação, o qual é orientado aos serviços. Para tanto, é necessário calcular o produto entre o peso da questão no serviço e o fator multiplicativo relacionado à alternativa selecionada. A pontuação final, por sua vez, é obtida pela somatória destes produtos para cada serviço.

Para calcular o percentual (P) de atendimento sobre cada serviço, a pontuação final deve ser ajustada com base nos valores extremos do questionário, que determinam um intervalo entre os maiores e os menores valores possíveis para cada serviço. Desta 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 estabelecido de acordo com o serviço com menor taxa e classificado de acordo com a tabela I.

TABELA I. Conversão de percentual em nível de maturidade

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

Determinado o grau de maturidade do PDS da organização, consultas são realizadas ao GAIA Riscos para aderir aos serviços do nível almejado. Ao término do processo, preenche-

se o *checklist* de reavaliação. Caso existam pendências, armazenam-se os indicadores de desempenho no banco de dados histórico e executam-se atividades para aderir aos serviços restantes. Caso contrário, registram-se os indicadores de desempenho e finaliza-se o processo de implantação para o nível.

IV. 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 [14]. Estes, 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 se podem destacar:

- ***Organizational Project Management Maturity Model* (OPM3):** criado pelo *Project Management Institute* (PMI) e com atividades baseadas no PMBOK. A metodologia para identificar o nível de maturidade consiste em executar um sistema de auto avaliação [15] sob as 9 áreas da gerência de projetos propostas pelo PMBOK.
- ***Capability Maturity Model Integration* (CMMI):** é um modelo de avaliação de maturidade criado e mantido pelo *Software Engineering Institute* (SEI). O método utilizado para identificar o grau de maturidade limita-se em comparar subjetivamente o processo em questão com as diretrizes do nível de maturidade desejado [16].
- **Control Objectives for Information and Related Technology (COBIT):** criado pelo *IT Governance Institute* e, atualmente, mantido pelo *Information Systems Audit and Control Association* (ISACA). A forma de estabelecer o grau de maturidade consiste em comparar subjetivamente o processo em questão com as diretrizes do nível de maturidade desejado [17].
- **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). O método de avaliação de um nível de maturidade consiste em verificar se a organização atende aos resultados de atributos de processo no nível almejado [14].
- ***Maturity Model in Information Security* (MMGRSeg):** modelo criado com base no CMMI e na norma ISO/IEC 27005 [18] por Mayer e Fagundes [3]. A metodologia de avaliação de um nível de maturidade consiste em analisar o processo em questão para verificar se ele atende os objetivos de controle estabelecidos pelo modelo.

V. FERRAMENTA DE AVALIAÇÃO DIAGNÓSTICA

Conforme exposto na Seção I, a ferramenta para avaliação diagnóstica baseia-se na metodologia proposta por Gaffo e Barros [4, 5]. Desta forma a ferramenta possibilita automatizar a coleta das respostas do usuário para o questionário de avaliação diagnóstica, automatizando o processo de cálculo e de apresentação do resultado, o qual será melhor apresentado na Seção V-B.

No âmbito das funcionalidades, a área administrativa do sistema permite controlar usuários, questionários, eixos – que representam os serviços do GAIA Riscos, questões e alternativas, além de imprimir relatórios sobre as organizações avaliadas. Na área de acesso comum é possível que o visitante se cadastre. Uma vez registrado, o usuário pode responder aos questionários e administrar suas respostas por meio de relatórios, os quais irão guiar a implantação do *framework*. A Fig. 3 apresenta o diagrama de casos de uso da ferramenta de avaliação diagnóstica.

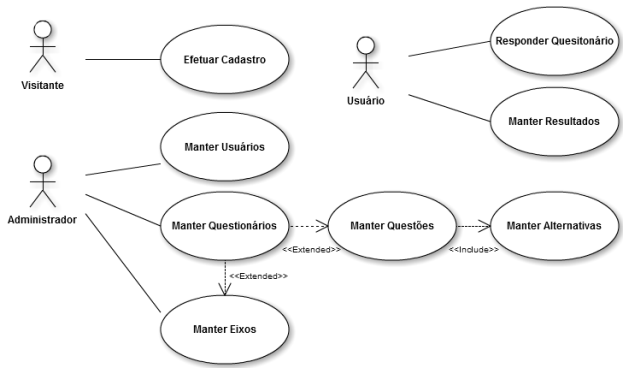

Figura 3. Diagrama de casos de uso da ferramenta de avaliação diagnóstica

Para implementar a ferramenta a linguagem de programação utilizada foi o PHP com o *framework* Yii e a IDE de desenvolvimento NetBeans. Como sistema de gerenciamento de banco de dados foi utilizado o MySQL. Tais tecnologias foram escolhidas devido a três principais variáveis: (1) gratuidade, (2) versatilidade da linguagem e do ambiente de desenvolvimento e (3) familiaridade com as tecnologias.

A. *Mecanismo de Cálculo do Resultado*

O mecanismo de cálculo do resultado é baseado no relacionamento entre os pesos (ρ) e fatores multiplicativos (fm) aplicados sobre eixos (e), estes por sua vez, são definidos conforme a necessidade.

Do modo como foi concebido, o mecanismo de cálculo do resultado é aplicável para questões objetivas, de forma que cada questão possui um peso (ρ) que determina qual a influência do objeto avaliado pela questão no eixo (e). Também são atribuídos valores sobre as alternativas das questões, que são chamados fatores multiplicativos (f). Estes indicam variações aplicadas aos pesos das questões de acordo com a alternativa selecionada.

Os pesos das questões com relação aos eixos são dados por uma matriz Q × E, onde cada coluna corresponde ao peso da questão em um eixo (e) e o número de linhas e colunas é dado pelo número de questões Q e de eixos E respectivamente. Ainda, cada questão também possui um vetor de fatores multiplicativos (f), que são associados à suas alternativas, e o elemento f_i representa o fator multiplicativo selecionado da i-ésima questão. Então é calculado o valor do questionário VQ no eixo *e*, conforme a equação 1.

$$VQ(e) = \sum_{i=1}^{Q} f_i \times p_{i,e} \quad (1)$$

Para que o resultado possa ser obtido com relação ao percentual de atendimento é necessário obter os valores máximo e mínimo para cada eixo, os quais são dados pelas equações 2 e 3 respectivamente.

$$VMX(e) = \sum_{i=1}^{Q} \max[\mathbf{f}] \times p_{i,e} \quad (2)$$

$$VMN(e) = \sum_{i=1}^{Q} \min[\mathbf{f}] \times p_{i,e} \quad (3)$$

Onde *max* [] é o operador que retorna o elemento de maior valor e *min* [] é o operador que retorna o elemento de menor valor entre os elementos de um vetor.

Finalmente, para cada eixo (*e*) o percentual de atendimento P, resultante da aplicação do questionário, é dado pela equação exposta em 4.

$$P(e) = \frac{VQ(e) + (0 - VMN(e))}{FVMX(e) - VMN(e)} \quad (4)$$

Desta forma, determina-se o valor percentual que representa o nível de maturidade da organização no eixo avaliado, conforme o escopo do questionário, o qual é aplicado ao gráfico de resultado exposto na Seção V-B.

B. Apresentação dos Resultados

Para demonstrar os resultados obtidos com a aplicação do questionário a ferramenta utiliza-se de três gráficos de radar, nos quais cada eixo representa um serviço do GAIA Riscos e sua área define a taxa de atendimento. A Fig. 4 demonstra o primeiro gráfico de resultado, o qual contém a avaliação individual do PDS.

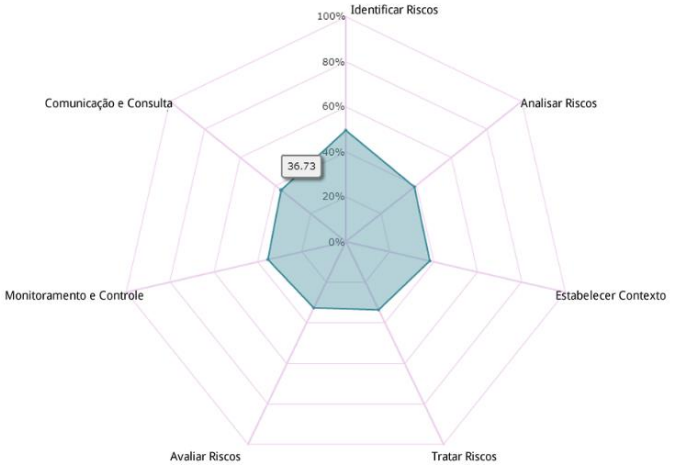

Figura 4. Resultado individual da avaliação do PDS

Diferentemente do ilustrado pela Fig. 4, o segundo gráfico de resultado, exposto na Fig. 5, contém a média aritmética de todas as respostas coletadas pelas empresas que responderam ao questionário.

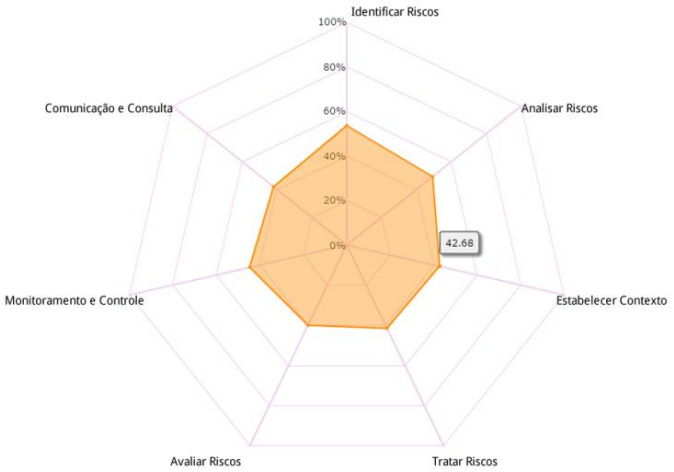

Figura 5. Média de todas as respostas de um questionário

O último gráfico de resultado, ilustrado pela Fig. 6, apresenta a comparação entre o primeiro (Fig. 4) e o segundo (Fig. 5) gráficos.

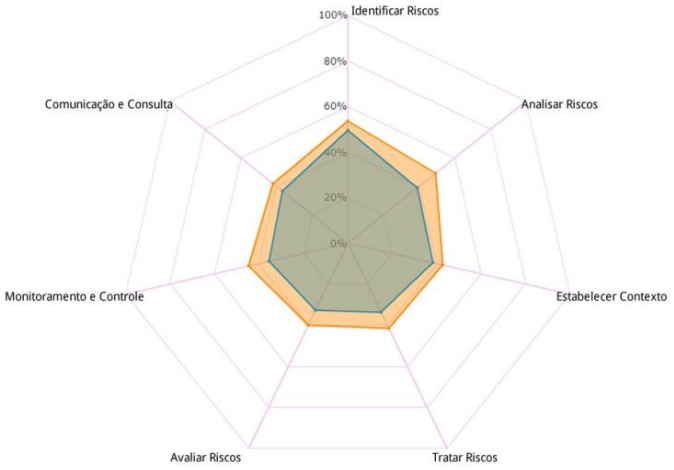

Figura 6. Comparação entre o resultado individual e a média do questionário

VI. VALIDAÇÃO DO MODELO

Para validar a ferramenta de avaliação diagnóstica, o sistema foi disponibilizado via e-mail para gerentes de projeto de cerca e 50 empresas de desenvolvimento de software da região metropolitana de Londrina/PR. Até o presente momento 13 já preencheram um total de 27 respostas. Do total de empresas que utilizaram o sistema, 8 encontram-se no segundo nível de maturidade do GAIA Riscos ($\cong 61{,}53\%$), 4 encontram-se no primeiro ($\cong 30{,}77\%$) e 1 no terceiro ($\cong 7{,}7\%$).

Além desta validação, a ferramenta de avaliação diagnóstica recebeu questionários provenientes outros domínios, como por exemplo a governança de tecnologia da informação e comunicação (TIC) [19] e o gerenciamento de recursos humanos em empresas de desenvolvimento e software [20]. Em ambos os casos foi possível verificar que a ferramenta atendeu as expectativas de usabilidade, confiabilidade e desempenho.

VII. CONCLUSÃO

O GR cada vez mais assume um papel importante dentro das organizações de desenvolvimento de software, devido as demandas do mercado e, principalmente, exigências regulatórias dos clientes. Neste contexto, a possibilidade automatizar a avaliação do PDS de uma organização e apresentar os caminhos para sua melhoria, por meio de níveis de maturidade, implementa mais alternativas ao gerenciamento de projetos, além de incrementar confiabilidade ao produto.

A ferramenta para avaliação diagnóstica está alinhada aos serviços GAIA Riscos, bem como a seu questionário, os quais atendem as diretrizes da norma ISO 31000, um padrão internacional para GR em projetos. Desta forma, pode-se afirmar que dentre as principais contribuições observadas a ferramenta proposta possibilita:

- Automatizar a coleta de informações de GR sobre o PDS avaliado, bem como facilitar o cálculo do resultado e elaboração do gráfico.
- Coletar informações de questionários de outras áreas de conhecimento, conforme exposto na Seção VI.
- Disponibilizar os resultados da avaliação diagnóstica para qualquer computador conectado à *internet*.

Frente aos resultados alcançados é possível afirmar que a ferramenta de avaliação diagnóstica atende o propósito deste estudo que é automatizar a definição do grau de maturidade do GR em um PDS, preenchendo a lacuna encontrada nos modelos pesquisados. Além disso, o modelo também colabora significativamente com a implantação do GR, uma vez que identifica áreas em que as organizações devem focar esforços e investimentos para aderir às atividades desta gerência.

No entanto, algumas melhorias necessitam ser feitas no sistema, como por exemplo: (1) permitir a inclusão dos níveis de maturidade para automatizar a conversão de porcentagem em nível de maturidade, (2) ligar o resultado aos serviços do GAIA Riscos e (3) melhorar a experiência com o usuário para tornar o preenchimento do questionário mais intuitivo.

REFERÊNCIAS

[1] Standish Group, Chaos Manifesto, 2011

[2] Módulo Security, "10º Pesquisa Nacional Sobre Segurança da Informação". São Paulo: Módulo Security, 2007. Disponível em: http://www.modulo.com.br/. Acesso em: 19/12/2012

[3] J. Mayer e L.L. Fagundes, "A Model to Assess the Maturiry Level of the Risk Management Process in Information Security". In Symposium on Integrated Network Management – Workshops. p. 61-70. IEEE Computer Society Press. 2009.

[4] F. H. Gaffo e R. M. Barros, "GAIA Risks: A Service-based Framework to Manage Project Risks", In: CLEI 2012, Anais da XXXVIII Conferencia Latinoamericana en Informática. 2012.

[5] F. H. Gaffo e R. M. Barros, "GAIA Risks: A risk management framework", In: Proceedings of the 25th International Conference on Computer Applications in Industry and Engineering, v. 1, p. 57-62. 2012.

[6] H. F. Kloman, "Risk Management Agonists", In: Risk Analysis, v. 10, n. 2, p. 201-205. 1990.

[7] PMI – Project Management Institute, "A guide to project management body of knowledge", 4. Ed., Newton Square, Pennsylvania: Project Management Institute Inc. 2008.

[8] ISO – International Organization for Standardization, "ISO 31000: principles and guidelines". 2009.

[9] F. Turley, "The PRINCE2 training manual: a common sense approach to learning and understanding PRINCE2". 2010.

[10] M. G. Aldenucci, "Um modelo de maturidade para processos de gerenciamento de riscos em projetos", Dissertação de Mestrado, Pontifícia Universidade Católica do Paraná, Brasil. 2009.

[11] ITSMF, "ITIL V3 – Service Strategy". 2007.

[12] ISO – International Organization for Standardization, "ISO 31010: risk assessment techniques". 2009.

[13] ISO – International Organization for Standardization, "ISO Guide 73: risk management vocabulary". 2009.

[14] SOFTEX – Associação para Promoção da Excelência do Software Brasileiro, "MPS.BR – Guia Geral". Brasília: SOFTEX. 2012.

[15] PMI – Project Management Institute, "Organizational Project Management Maturity Model (OPM3)", 3. Ed, Newton Square, Pennsylvania: Project Management Institute Inc. 2003.

[16] N. Ehsan, A. Perwaiz e J. Arif, "CMMI / SPICE based Process Improvement", In: International Conference in Management of Innovation and Technology, p. 859-862. 2010.

[17] ITGI – IT Governance Institute, "CobiT 4.1", Rolling Meadows, Illinois: IT Governance Institute. 2007.

[18] ISO – International Organization for Standardization, "ISO/IEC 27005: Information Technology – Security Techniques – Information Security Risk Management". 2008.

[19] G. U. Briganó e R. M. Barros, "Um framework para desenvolvimento de governança de TIC". Dissertação de Mestrado, Universidade Estadual de Londrina, Brasil. 2012.

[20] F. E. A. Horita, J. D. Brancher e R. M. Barros, "A Process Model for Human Resources Management focused on increasing the Quality of Software Development". In: Proceedings of the 24th International Conference on Software Engineering and Knowledge Engineering, Redwood City. 2012.