Metodologia para Avaliar o Grau de Maturidade da Gerência de Riscos

Fernando Henrique Gaffo, Rodolfo Miranda de Barros

Departamento de Computação – Universidade Estadual de Londrina (UEL) – Caixa Postal 6001 – CEP 86.051-990 – Londrina – PR – Brasil

fernandogaffo@gmail.com, rodolfo@uel.br

Abstract. *The risk management (RM) 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 (SDP), in its turn, should implement a serie of activities to adhere to existing standards and regulamentations. However, there are no references to models that enable the evaluation of the SDP through a questionnaire and enables managers have a clear view of the deficiencies of this process. In this way, this study aims to present the diagnostic assessment questionnaire that is part of the GAIA Risks framework as well as the methodology for calculation and display of results.*

Resumo. *O processo de gerenciamento de riscos (GR) compreende atividades coordenadas para identificar, analisar, avaliar, tratar, comunicar e monitorar os riscos dos projetos. As organizações que desejam implementar estas atividades ao seu processo de desenvolvimento de software (PDS) devem conduzir uma série de ações para aderir aos padrões existentes. No entanto, não foram encontradas referências para modelos que permitam avaliar o PDS por meio de questionamentos e apresentam uma visão clara das deficiências deste processo. Desta forma, este estudo tem como objetivo, apresentar o questionário de avaliação diagnóstica que é parte do framework GAIA Riscos, bem como a metodologia de cálculo e exposição dos resultados encontrados.*

1. 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 *Standish Group,* intitulado *Chaos Manifesto* (2011). 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 [Módulo *Security* 2007]. 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 para as mesmas.

Riscos são vistos como a probabilidade que tal ameaça 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 [Mayer e Fagundes 2009].

Neste contexto, este estudo tem como objetivo principal apresentar o questionário de avaliação diagnóstica que compõe o *framework* GAIA Riscos, criado por Gaffo e Barros (2012). A motivação para elaborá-lo deve-se a carência objetividade, pelos modelos disponíveis no mercado, em determinar o nível de maturidade do gerenciamento de riscos de um Processo de Desenvolvimento de Software (PDS).

Para expor o questionário de avaliação diagnóstica, o presente trabalho organiza-se da seguinte forma: a Seção 2 introduz o GR, a Seção 3 descreve o *framework* GAIA Riscos, a Seção 4 expõe os modelos de maturidade pesquisados, a Seção 5 apresenta os o questionário de avaliação diagnóstica, a Seção 6 expõe a os resultados obtidos por meio da validação do modelo proposto e a Seção 7, por fim, descreve as conclusões obtidas até o presente momento.

2. Gerenciamento de Riscos

As comunidades atribuem diferentes significados à palavra riscos [Kloman 1990]. 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 [PMI 2008, ISO 2009, Turley 2010].

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 [PMI 2008, ISO 2009, Turley 2010]. Estas ações estão ligadas à diferentes campos do projeto e a literatura acadêmica, geralmente, as associa ao gerenciamento de projetos [Aldenucci 2009]. Dentre as abordagens estudadas destaca-se o processo de GR da ISO 31000, que compreende:

- **Comunicação e consulta:** atividade na qual 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.

3. GAIA Riscos

O GAIA Riscos é um *framework* para gerenciar riscos baseado em serviços desenvolvido por Gaffo e Barros (2012), cujo propósito é ser flexível e permitir a implantação incremental desta gerência nos processos organizacionais. O GAIA Riscos

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 figura 1 expõe os níveis de maturidade e seus serviços.

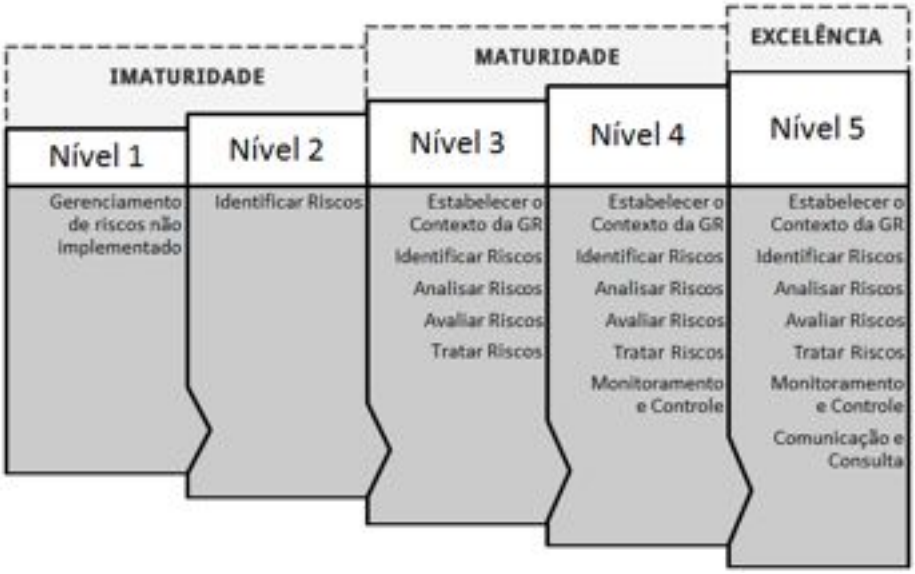

Figura 1. *Framework* GAIA Riscos

Cada um dos sete serviços, ilustrados na figura 1, tem como objetivo entregar valor ao cliente, permitindo assim que ele alcance seus objetivos [ITSMF 2007]. 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 figura 2 representa a estrutura básica dos serviços.

Figura 2. Estrutura do Serviço

Conforme apresentado na figura 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 (2009), os vocabulários são retirados do Guia 73 da ISO (2009), os *workflows* procedem das instruções da ISO 31000 (2009), 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. As respostas fornecidas serão utilizadas para calcular o nível de maturidade do PDS.

Determinado o grau de maturidade do PDS da organização, consultas são realizadas ao GAIA Riscos para aderir aos serviços do nível alcançado. 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 alcançado.

4. 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 (SOFTEX 2011). Os 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 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 [PMI 2008] sob as 9 áreas de conhecimento do PMBOK.
- ***Standard CMMI Appraisal Method For Process Improvement* (SCAMPI)**: é um método de avaliação de maturidade criado e mantido pelo *Software Engineering Institute* (SEI). O método utilizado para identificar o grau de maturidade limita-se em definir o grau de maturidade baseando-se em evidências diretas, indiretas e afirmnações [Ehsan et al. 2010].
- ***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 [ITGI 2007].
- **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 [SOFTEX 2011].
- ***Maturity Model in Information Security* (MMGRSeg)**: modelo criado com base no CMMI e na norma ISO/IEC 27005 (2008) por Mayer e Fagundes (2009). 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.

5. Questionário de Avaliação Diagnóstica

Conforme exposto na Seção 1, o questionário de avaliação diagnóstica faz parte do GAIA Riscos. Sua função é identificar, por meio das respostas fornecidas pelo usuário, o grau de maturidade com que o PDS de uma organização atende ao *framework*. Desta forma, o questionário organiza-se em sete Grupos de Questões (GQ) que compreendem

questões objetivas sobre cada um dos serviços do processo de GR. Para estar alinhado as diretrizes da ISO 31000, as questões de cada grupo respondem aos propósitos da norma.

As questões são de múltipla escolha e possuem um conjunto de alternativas que traduzem objetivamente as situações ocorridas no dia-a-dia da organização, com o intuito de simplificar o preenchimento do questionário pelos gerentes de projeto. Ainda, cada alternativa, possui fatores multiplicativos (FM) que quantificam seu impacto com relação à questão que pertencem. Estes fatores são utilizados para calcular a taxa de atendimento, conforme exemplificado na tabela 1.

Tabela 1. Modelo de questão

Questão 01: A organização possui critérios e parâmetros bem definidos para identificar os riscos presentes em seus projetos?		
Alternativa	**Texto**	**Fator Multiplicativo**
A	Sim, a organização possui critérios e parâmetros bem definidos e eles são conhecidos por todos.	3
B	Sim, a organização possui critérios e parâmetros bem definidos, entretanto eles não são divulgados.	2
C	Desconheço esta informação.	0
D	A organização possui alguns critérios e parâmetros, os quais não são conhecidos por todos.	-2
E	Não, a organização não possui critérios e parâmetros para gerenciar os riscos.	-3

Além da relação entre as questões e as alternativas, que são os FM, exemplificados na tabela 1, outro importante componente do Questionário de Avaliação Diagnóstica é o relacionamento entre as questões e os serviços do *framework*, que é dado por pesos. Desta forma, uma mesma questão pode influenciar um ou vários serviços ao mesmo tempo. A tabela 2 apresenta a matriz de relacionamento entre uma questão e os pesos que ela exerce sobre cada serviço.

Tabela 2. Peso da questão nos serviços

Questão 01: A organização possui critérios e parâmetros bem definidos para identificar os riscos presentes em seus projetos?		
Serviço	**Justificativa**	**Peso**
Estabelecer Contexto	Os parâmetros estão presentes em todas as fases do GR.	4
Identificar Riscos	Os parâmetros determinam o escopo do GR.	3
Analisar Riscos	Os parâmetros definem as metodologias que serão utilizadas para analisar os riscos.	1
Avaliar Riscos	Os parâmetros definem métricas para classificar os riscos.	2
Tratar Riscos	Os parâmetros estabelecem como proceder no tratamento.	1
Monitoramento e Controle	Os parâmetros indicam como avaliar a eficácia.	2
Comunicação e Consulta	Os parâmetros determinam o que deve ser comunicado.	1

A primeira versão do questionário de avaliação diagnóstica contém 48 questões alocadas nos GQ no qual possuem maior influência. Caso uma questão possua o mesmo peso para dois GQ o critério utilizado para alocação é aleatório. Para elaborar as respostas do questionário, as diretrizes da ISO 31000 foram fundamentais, pois fornecem os casos ideais esperados para o GR. Os GQ são melhor detalhados a seguir.

5.1. GQ1 - Estabelecer Contexto

O propósito deste GQ é medir o grau com que as atividades do processo de estabelecimento do contexto estão presentes no PDS avaliado. O contexto inclui elementos como políticas, critérios, métodos, premissas e restrições do GR. Para avaliar o grau com que o PDS atende as finalidades desta atividade as seguintes questões são propostas:

- GQ1.1: A organização possui critérios e parâmetros bem definidos para identificar os riscos presentes em seus projetos?
- GQ1.2: A organização define claramente os objetivos do GR?
- GQ1.3: A organização define claramente o escopo do GR?
- GQ1.4: A organização define claramente as responsabilidades do GR?
- GQ1.5: A organização define claramente as políticas, normas, regulamentações e guias para o GR?
- GQ1.6: A organização define claramente metodologias para avaliar os riscos?
- GQ1.7 A organização define claramente níveis de aceitação ou tolerância para os riscos?
- GQ1.8: A organização define claramente a metodologia para determinar probabilidade de ocorrência de um risco?
- GQ1.9: A organização define claramente as decisões necessárias no caso de um risco se concretizar?
- GQ1.10: A organização define as premissas e as restrições do processo de GR?

5.2. GQ2 – Identificar Riscos

O propósito deste GQ é medir o grau com que as atividades do processo de identificação dos riscos estão presentes no PDS avaliado. Este processo inclui atividades para identificar as fontes de riscos, suas causas, probabilidade de ocorrência e áreas de impacto para gerar uma lista de riscos. Para avaliar o grau com que o PDS atende as finalidades desta atividade as seguintes questões são propostas:

- GQ2.1: A organização busca identificar as fontes causadoras de riscos?
- GQ2.2: A organização documenta de maneira clara e completa uma lista com os riscos identificados e suas descrições?
- GQ2.3: Se necessário, a organização busca auxílio em outras pessoas com conhecimentos apropriados sobre o projeto?
- GQ2.4: A organização documenta de maneira clara outras ameaças atreladas a um determinado risco?
- GQ2.5: As informações utilizadas para identificar os riscos sempre estão atualizadas?
- GQ2.6: Se necessário, a organização utiliza ferramentas e técnicas específicas para identificar os riscos do projeto?
- GQ2.7: Quando um risco é documentado, as áreas de impacto, suas causas e as consequências possíveis complementam a identificação dos riscos?

5.3. GQ3 - Analisar Riscos

O propósito deste GQ é medir o grau com que as atividade do processo de análise dos riscos estão presentes no PDS avaliado. Este processo inclui atividades para filtrar os riscos identificados, mantendo apenas os mais relevantes com os critérios e parâmetros. Para avaliar o grau com que o PDS atende as finalidades desta atividade as seguintes questões são propostas:

- GQ3.1: A organização busca compreender o risco após a identificação do mesmo?
- GQ3.2: Quando um risco é compreendido, suas causas, impactos, consequências e probabilidade de ocorrência são levadas em consideração?
- GQ3.3: Riscos com maior probabilidade de ocorrer ou que com maiores impactos ao projeto são analisados de maneira especial?
- GQ3.4: A organização documenta de maneira clara e completa a lista dos riscos analisados?
- GQ3.5: Se novos riscos surgirem durante a análise de uma ameaça eles são inclusos na lista de riscos identificados?
- GQ3.6: A organização realiza análises quantitativas, qualitativas ou uma combinação das duas para determinar o impacto de uma ameaça?
- GQ3.7: A análise dos riscos leva em consideração a documentação do projeto?

5.4. GQ4 - Avaliar Riscos

O propósito deste GQ é medir o grau com que as atividades do processo de avaliação dos riscos estão presentes no PDS avaliado. Este processo inclui atividades para quantificar os riscos para classifica-los de acordo com sua probabilidade de ocorrência e criticidade. Para avaliar o grau com que o PDS atende as finalidades desta atividade as seguintes questões são propostas:

- GQ4.1: A organização utiliza os dados da análise de riscos para determinar se um risco será aceito ou não?
- GQ4.2: A organização utiliza os dados da análise de riscos para estabelecer os riscos com maior prioridade?
- GQ4.3: A organização compara os dados obtidos durante a análise de riscos com os parâmetros e critérios estabelecidos?

5.5. GQ5 - Tratar Riscos

O propósito deste GQ é medir o grau com que as atividades do processo de tratamento dos riscos estão presentes no PDS avaliado. Este processo inclui atividades para implementar e elaborar os planos de tratamento e determinar a aceitação dos riscos residuais. Para avaliar o grau com que o PDS atende as finalidades desta atividade as seguintes questões são propostas:

- GQ5.1: A organização possui algum processo para avaliar as opções de tratamento de um determinado risco?
- GQ5.2: A organização avalia os riscos residuais para determinar se eles são toleráveis ou não?
- GQ5.3: Caso um risco residual não seja tolerável, a organização possui um processo de tratamento desta ameaça?
- GQ5.4: A organização avalia a efetividade do tratamento realizado?

- GQ5.5: Se houverem dados decorrentes da avaliação de efetividade do tratamento, estes são armazenados em um banco de dados histórico?
- GQ5.6: A organização define um cronograma para tratamento dos riscos?
- GQ5.7: A organização elabora planos de contingência para ser executado caso um risco se concretize?

5.6. GQ6 - Monitoramento e Controle

O propósito deste GQ é medir o grau com que as atividades do processo de monitoramento e controle estão presentes no PDS avaliado. Este processo inclui atividades para garantir que o GR está relevante e efetivo frente aos planos. Para avaliar o grau com que o PDS atende as finalidades desta atividade as seguintes questões são propostas:

- GQ6.1: A organização utiliza os dados do tratamento para avaliar a eficácia e eficiência do GR?
- GQ6.2: A organização se preocupa com mudanças no contexto interno e externo do projeto?
- GQ6.3: A organização realiza reavaliações constantes em seus planos do projeto para identificar novos riscos?
- GQ6.4: A organização possui métodos para armazenar e recuperar as informações do GR?
- GQ6.5: A organização armazena informações sobre custos e esforços necessários para manter o GR?
- GQ6.6: Existem políticas que determinam por quanto tempo a informação deve ser mantida no banco de dados histórico do GR?
- GQ6.7: A organização utiliza os dados armazenados para incentivar os *stakeholders* para melhorar continuamente o GR?

5.7. GQ7 - Comunicação e Consulta

O propósito deste GQ é medir o grau com que as atividades do processo de comunicação e consulta estão presentes no PDS avaliado. Este processo inclui atividades para garantir que os interesses e conhecimentos de todos os *stakeholders* sejam entendidos e considerados. Para avaliar o grau com que o PDS atende as finalidades desta atividade as seguintes questões são propostas:

- GQ7.1: A organização comunica e consulta as partes interessadas para estabelecer o contexto do GR?
- GQ7.2: A organização considera e entende os interesses dos *stakeholders*?
- GQ7.3: A organização agrega o conhecimento de diferentes áreas para auxiliar no processo de análise dos riscos?
- GQ7.4: A organização elabora um plano que rege a comunicação entre as partes interessadas?
- GQ7.5: A organização considera o conhecimento de diferentes áreas para auxiliar na tomada de decisão?
- GQ7.6: A organização fornece meios para comunicar os assuntos referente aos riscos?
- GQ7.7: A organização distribui as informações relevantes a todos os membros da equipe, respeitando os dados confidenciais e a integridade do conteúdo?

5.8. Metodologia de Cálculo do Resultado

Baseado nas informações coletadas no preenchimento do questionário e seguindo o modelo de questão exposto nas tabelas 1 e 2, se obtém o resultado da avaliação do PDS, o qual é orientado aos serviços. Para tanto é necessário calcular o produto 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 a taxa 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. Desta forma, a pontuação final é posicionada no intervalo descrito, determinando assim o percentual de atendimento de cada serviço. Por conseguinte, o nível de maturidade da organização é definido com base no serviço com menor taxa de atendimento e classificado conforme a tabela 3.

Tabela 3. Conversão de taxa de atendimento em nível de maturidade.

Taxa de Atendimento (%)	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

5.9. Apresentação dos Resultados

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 pela taxa de atendimento. Desta maneira tem-se uma visão global sobre os mesmos, facilitando a compreensão do resultado pelo gerente do projeto, bem como as áreas que necessitam de atenção. A figura 3 demonstra um gráfico obtido ao término do preenchimento do questionário.

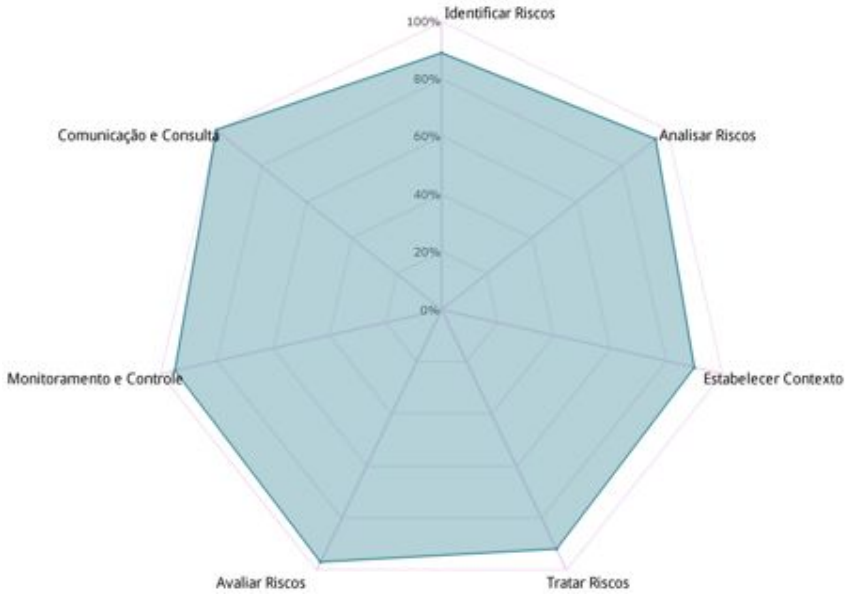

Figura 3. Exemplo de gráfico de resultado

6. Validação do Modelo

Para validar o modelo proposto por este estudo, o questionário de avaliação diagnóstica foi disponibilizado para diversas empresas de desenvolvimento de *software* da região metropolitana de Londrina/PR. Até o presente momento 10 empresas distintas o preencheram. Os resultados mostram que a maioria das companhias ainda não evoluíram além do nível 2 do GR, conforme ilustra a figura 4.

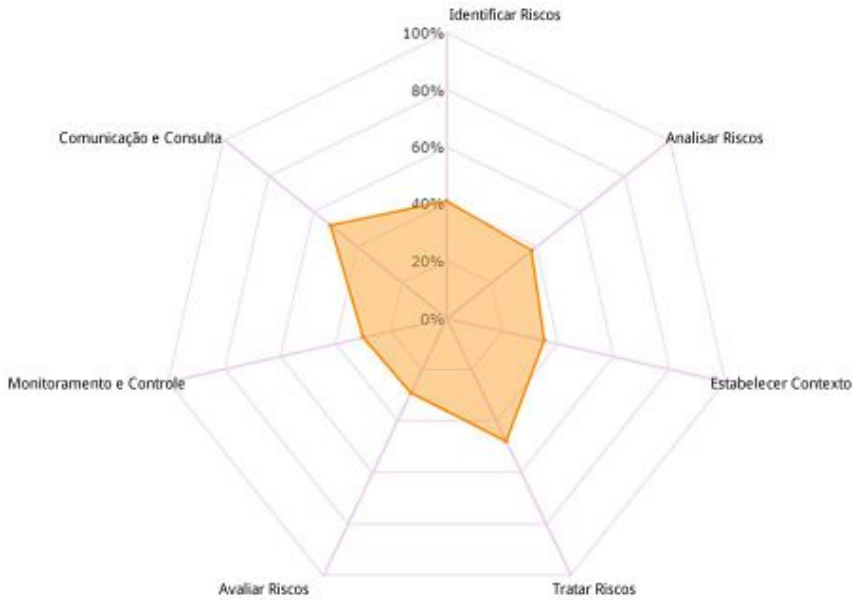

Figura 4. Média da Avaliação das Empresas de Desenvolvimento de Software da Região de Londrina/PR

Além das informações sobre o nível de maturidade, a figura 4 também permite constatar que a maioria das empresas avaliadas tratam os riscos sem antes mesmo de estabelecer parâmetros para o GR, identificar ou compreender os riscos. Neste contexto, o questionário de avaliação diagnóstica é um valioso instrumento, pois indica onde as organizações devem focar seus esforços e investimentos para atingir a maturidade e, posteriormente, a excelência na gestão dos riscos.

7. Conclusão

O GR cada vez mais assume um papel importante dentro das organizações de desenvolvimento de *software*, devido as demandas do mercado e, principalmente, dos clientes. Neste contexto, a possibilidade de avaliar objetivamente o 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 gerado.

O questionário de avaliação diagnóstica está alinhado aos serviços GAIA Riscos, os quais atendem as diretrizes da norma ISO 31000, um padrão internacional para a gerência de riscos nos projetos. Desta forma, pode-se afirmar que o questionário de avaliação proposto permite uma organização:

- Avaliar o desempenho de seu PDS ao longo do processo de implantação do GAIA Riscos, comparando os resultados obtidos durante a evolução dos níveis de maturidade.

- Identificar vulnerabilidades e deficiências em seu PDS, visualizando os pontos do processo que demandam maior atenção.
- Atingir a excelência no GR em seu PDS conforme a proposta do *framework* GAIA Riscos.

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

No entanto, algumas melhorias necessitam ser feitas no questionário, como por exemplo: (1) criação de uma ferramenta que suporte à aplicação do questionário pela *web,* bem como o armazenamento dos resultados em um banco de dados comum, (2) maior validação das questões, pesos e fatores multiplicativos e (3) aplicação do questionário em outros domínios, como por exemplo, a governança de TI.

Referências

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

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

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

Gaffo, F. H., Barros, R. M. (2012) "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.

ISO – International Organization for Standardization (2008) "ISO/IEC 27005: Information Technology – Security Techniques – Information Security Risk Management"

_____ (2009) "ISO 31000: Principles and Guidelines".

_____ (2009) "ISO 31010: Risk Assessment Techniques".

_____ (2009) "ISO Guide 73: Risk Management Vocabulary".

ITGI – IT Governance Institute (2007) "CobiT 4.1", Rolling Meadows, Illinois: IT Governance Institute.

ITSMF (2007) "ITIL V3 – Service Strategy".

Kloman, H. F. (1990) "Risk Management Agonists", In: *Risk Analysis*, v. 10, n. 2, p. 201-205, Junho 1990.

Mayer, J. e Fagundes, L. L. (2009) "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.

Módulo Security (2007) “10º Pesquisa Nacional Sobre Segurança da Informação”. São Paulo:Módulo Security. Disponível em: http://www.modulo.com.br/. Acesso em: 19/12/2012

PMI – Project Management Institute (2008) “A guide to project management body of knowledge”, 4. Ed., Newton Square, Pennsylvania: Project Management Institute Inc.

_____ (2008) “Organizational Project Management Maturity Model (OPM3)”, 4. Ed, Newton Square, Pennsylvania: Project Management Institute Inc.

SOFTEX – Associação para Promoção da Excelência do Software Brasileiro (2011) “MPS.BR – Guia Geral”. Brasília: SOFTEX.

Standish Group (2011) “Chaos Manifesto”.

Turley, F. (2010) “The PRINCE2 training manual: a common sense approach to learning and understanding PRINCE2”.