UNIVERSIDADE ESTADUAL DE LONDRINA

FERNANDO HENRIQUE GAFFO

GAIA RISCOS:

FRAMEWORK PARA O GERENCIAMENTO DE RISCOS NO PROCESSO DE DESENVOLVIMENTO DE *SOFTWARE*

Londrina
2013

FERNANDO HENRIQUE GAFFO

GAIA RISCOS

FRAMEWORK PARA O GERENCIAMENTO DE RISCOS NO PROCESSO DE DESENVOLVIMENTO DE *SOFTWARE*

Dissertação apresentada ao Programa de Mestrado em Ciência da Computação do Departamento de Computação da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

Orientador: Dr. Rodolfo Miranda de Barros

Londrina
2013

Catalogação elaborada pela Divisão de Processos Técnicos da Biblioteca Central da Universidade Estadual de Londrina

Dados Internacionais de Catalogação-na-Publicação (CIP)

G131g Gaffo, Fernando Henrique.
GAIA Riscos: f*ramework* para o gerenciamento de riscos no processo de desenvolvimento de *software* / Fernando Henrique Gaffo. – Londrina, 2013.
115 f. : il.

Orientador: Rodolfo Miranda de Barros.
Dissertação (Mestrado em Ciência da Computação) – Universidade Estadual de Londrina, Centro de Ciências Exatas, Programa de Pós-Graduação em Ciência da Computação, 2013.
Inclui bibliografia.

1. Software – Desenvolvimento – Teses. 2. Programação (Computadores) – Gerência – Teses. 3. Engenharia de software – Teses. 4. Framework (Programa de computador) – Teses. 5. Software – Desenvolvimento – Avaliação de riscos – Teses. I. Barros, Rodolfo Miranda de. II. Universidade Estadual de Londrina. Centro de Ciências Exatas. Programa de Pós-Graduação em Ciência da Computação. III. Título.

CDU 519.68.02

FERNANDO HENRIQUE GAFFO

GAIA RISCOS:

FRAMEWORK PARA O GERENCIAMENTO DE RISCOS NO PROCESSO DE DESENVOLVIMENTO DE *SOFTWARE*

Dissertação apresentada ao Programa de Mestrado em Ciência da Computação do Departamento de Computação da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

BANCA EXAMINADORA

_____

Prof. Dr. Rodolfo Miranda de Barros
UEL – Londrina - PR

_____

Prof. Dr. Mario Lemes Proença Jr.
UEL – Londrina - PR

_____

Prof. Dr. Bruno Bogaz Zarpelão
UEL – Londrina - PR

_____

Prof. Dr. Alexandre L'Erario
UTFPR – Londrina - PR

Londrina, 16 de Setembro de 2013.

À Deus por permitir minha existência e conquistas.

Aos meus pais, José Moacyr Gaffo e Fátima Aparecida Cavalaro Gaffo pelo incentivo e suporte incondicional em todas as horas.

À minha noiva e futura esposa, Tatiana Figueiredo Correa, pelo companheirismo, compreensão, carinho e amor.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus por me dar forças para concluir mais esta etapa da minha vida.

Ao meu orientador, Prof. Dr. Rodolfo Miranda de Barros, que durante todos estes anos procurou me auxiliar com conselhos, dicas e conversas que contribuíram para elaboração deste trabalho.

À minha amada família pelo incentivo e por entender a importância deste projeto para minha vida.

À minha noiva e futura esposa, Tatiana Figueiredo Correa, pelo carinho, apoio, compreensão, amor e ajuda despendidos.

Aos amigos de trabalho (professores e colaboradores), especialmente ao professor e amigo Jaime Geraldo da Silva, pelo apoio, compreensão, conselhos e auxílios.

Aos amigos do programa de mestrado que contribuíram direta ou indiretamente, nomeadamente: Anderson, Gabriel, Gomede, Hisatomi e Horita.

Por fim, mas em posição não menos importante que os demais, agradeço à Faculdade Paranaense – FACCAR, representada pela professora Clarisse Neide Rodrigues Brun e pelos professores Nelson Henrique Zanete e Nelson Luis Vidotto, empresa que tanto me orgulho como empregado, pelo aprendizado e oportunidade de me desenvolver como pessoa, profissional e academicamente.

“A Capacidade de administrar o risco, e com ele a vontade de correr riscos e de fazer opções ousadas, são elementos-chave da energia que impulsiona o mundo”

(Peter L. Bernstein, 1996)

GAFFO, Fernando H. **GAIA riscos:** *framework* para o gerenciamento de riscos no processo de desenvolvimento de *software*. 2013. 115 f.. Dissertação (Mestrado em Ciência da Computação) – Universidade Estadual de Londrina, Londrina, 2013.

RESUMO

O processo de gerenciamento de riscos (GR) compreende um conjunto de atividades para identificar, analisar, avaliar, tratar, comunicar e monitorar os riscos dos projetos de uma empresa. As organizações que desejam implementar estas atividades em seu processo de desenvolvimento de *software* (PDS) devem conduzir uma série de ações para aderir aos padrões já existentes. No entanto, não foram encontradas referências para modelos que permitam avaliar o PDS por meio de questionamentos e apresentem uma visão objetiva e clara de seus pontos positivos e suas deficiências. Para suprir esta necessidade, este estudo tem como objetivo apresentar o *framework* GAIA Riscos, cujo propósito é permitir a implantação gradativa e incremental desta gerência em um PDS e aumentar a qualidade do *software* gerado. Para tanto, o *framework* compreende cinco níveis de maturidade, sete serviços, um questionário de avaliação diagnóstica, *checklists* de reavaliação, um processo de implantação e indicadores de desempenho. Neste contexto, este trabalho inova ao propor aos gerentes de projeto uma metodologia organizada em patamares para evolução do GR, além de possibilitar que os mesmos quantifiquem esta gerência por meio do questionário de avaliação diagnóstica, cujas questões e alternativas buscam traduzir as situações ocorridas no dia-a-dia da empresa.

Palavras-chave: Gerenciamento de riscos. Gerenciamento de Projetos. Níveis de Maturidade. Serviços. Qualidade do *software*.

GAFFO, Fernando H. **GAIA risks**: framework for risk management in software development process. 2013. 115 p. Dissertation (Master's degree in Science Computer) – Universidade Estadual de Londrina, Londrina, 2013.

ABSTRACT

The risk management (RM) process comprises a set of activities to identify, analyze, evaluate, treat, monitor and communicate project risks. Organizations wishing to implement these activities on its software development process (SDP) must conduct a series of actions to adhere to existing standards. However, there were not found references to models that assess the SDP through questions and present a clear and objective view of their strengths and their weaknesses. To meet this need, this study aims to present the framework GAIA Risks, whose purpose is to allow gradual and incremental deployment of these activities on a SDP and increase the quality of software generated. Therefore, the framework comprises five maturity levels, seven services, a diagnostic assessment questionnaire, revaluation checklists, an implementation process and performance indicators. This paper innovates by proposing to project managers a methodology based on maturity levels, and enable them quantify this their processes through the diagnostic assessment questionnaire, whose questions and alternatives seek translate the situations that occurred on the day -to-day business.

Keywords: Risk management. Project management. Maturity levels. Services. Software quality.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABENO	Associação Brasileira de Ensino Odontológico
BDH	Banco de Dados Histórico
CMMI	*Capability Maturity Model Integration*
COBIT	*Control Objectives for Information Technology and Related Technology*
DC	Departamento de Computação
FA	Fator de Ajuste
FM	Fator Multiplicativo
FP	Faixa de Pontuação
GP	Gerenciamento de Projetos
GQ	Grupo de Questões
GR	Gerenciamento de Riscos
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infrastructure Library*
ITGI	*IT Governance Institute*
MMGRSeg	*Maturity Model in Information Security*
MPS.BR	Programa para Melhoria de Processo de *Software* e Serviços
MR-MPS-SW	Modelo de Referência MPS para *Software*
OGC	*Office of Government Commerce*
OPM3	*Organizational Project Management Maturity Model*
PDS	Processo de Desenvolvimento de *Software*
PDSG	Processo de Desenvolvimento de *Software* da Fábrica GAIA
PI	Processo de Implantação
PMI	*Project Management Institute*
PMBOK	*A Guide to Project Management Body of Knowledge*
PRINCE2	*Projects in Controlled Environments*
QAD	Questionário de Avaliação Diagnóstica
RF	Resultado Final
SAD	Sistema de Avaliação Diagnóstica
SEI	*Software Engineering Institute*
SI	Sistemas de Informação
SOFTEX	Associação para Promoção da Excelência do *Software* Brasileiro

TIC	Tecnologia da Informação e Comunicação
UEL	Universidade Estadual de Londrina
XP	*Extreme Programming*

SUMÁRIO

1 INTRODUÇÃO

Os sistemas de informação (SI) estão difundidos em vários setores da vida moderna, além do que as pessoas estão cada vez mais dependentes dos *softwares* em suas atividades cotidianas [25], os quais estão presentes em diferentes setores que vão de atividades de lazer até hospitais. Por sua vez, as empresas que desenvolvem estes sistemas enfrentam uma série de desafios durante seus ciclos de vida, como por exemplo, custos excessivos, atrasos no cronograma, erros de especificação e baixa qualidade do produto final.

Somado a isto, no mundo globalizado, os *softwares* estão sujeito a várias alterações ao longo do seu ciclo de vida [8] [49]. Com isso, prever os caminhos de sua evolução torna-se uma tarefa árdua de se realizar. Mudanças nas regras de negócio ou regulamentações, falhas não previstas ou o surgimento de novos requisitos são exemplos de fatores que podem influenciar no sucesso ou insucesso de um determinado projeto de desenvolvimento de *software*.

Tais afirmações podem ser comprovadas pelo estudo conduzido pelo *Standish Group*, o *Chaos Manifesto* [55], o qual indica que, embora a porcentagem de projetos de *software* tidos como sucesso tenha aumentado em relação ao ano de 2010, apenas 39% deles são entregues dentro do prazo, com custos planejados e atendem plenamente os requisitos estipulados. Do restante, 43% sofrem com atrasos, custos elevados ou problemas de especificação e outros 18% são cancelados.

Com o intuito de combater esta realidade alarmante, na qual mais de 60% dos projetos de *software* são afetados por algum tipo problema, as organizações devem adotar recursos e processos cada vez mais eficazes para protegê-los [40]. Para tanto, o gerenciamento de riscos (GR) torna-se uma atividade de extrema importância para a saúde organizacional, pois, por meio de métodos, ferramentas e processos, os gerentes podem identificar, analisar e avaliar os impactos que uma determinada ameaça pode causar ao projeto e planejar e executar ações corretivas.

Desta forma, para incluir tais atividades ao longo do ciclo de vida de um *software*, o *Project Management Institute* (PMI) em seu livro *A Guide to the Project Management Body of Knowledge* (PMBOK) [44] considera o GR como uma das áreas do gerenciamento de projetos (GP). Este guia de melhores práticas, inclusive, dedica um capítulo exclusivo no qual descreve processos para identificar, analisar, tratar e controlar os riscos dos projetos.

Outro modelo de gestão que incorporou práticas para gerir os riscos é o *PRojects IN Controlled Environments* (PRINCE2) [57], do *Office of Government Commerce* (OGC). Ademais, em 2009, algumas normas da *International Organization for Standardization* (ISO) foram lançadas com intuito de padronizar os processos de GR, são elas: a ISO 31000 [21], a ISO 31010 [22] e o Guia 73 [23].

Neste contexto, este trabalho apresenta um *framework* para gerenciar riscos, o qual, segundo [21], deve fornecer políticas, objetivos, responsabilidades, processos e atividades para permitir que uma organização de desenvolvimento de *software* avalie seu grau de maturidade frente as atividades do GR e encontre caminhos para evoluí-las.

Denominado GAIA Riscos, este *framework* permite a implantação gradativa e incremental das atividades do GR e, por conseguinte, aumenta a qualidade final do *software* gerado. Para tanto, o GAIA Riscos compreende cinco níveis de maturidade, sete serviços, um processo de implantação, um questionário de avaliação diagnóstica, indicadores de desempenho e c*hecklists* de reavaliação, os quais são descritos a partir da Seção 3.

1.1 OBJETIVOS DA PESQUISA

O objetivo principal desta pesquisa é conceber, apresentar e validar o *framework* GAIA Riscos, cujo intuito é permitir que uma organização de desenvolvimento de *software* avalie seu grau de maturidade frente as atividades do GR e encontre caminhos para evoluí-las. Neste sentido, espera-se que o *framework* proporcione uma metodologia para avaliar e classificar o Processo de Desenvolvimento de *Software* (PDS) de uma organização dentro de um nível de maturidade relacionado ao GR.

Analogamente ao objetivo principal supracitado, um conjunto de objetivos específicos foi estabelecido, o que tornou necessário:

- Elaborar um questionário de avaliação diagnóstica;
- Criar os serviços baseados nas melhores práticas de GR existentes;
- Definir níveis de maturidade;
- Definir um processo de implantação para o *framework;*
- Elaborar os *checklists* de reavaliação para cada nível de maturidade;
- Definir indicadores de desempenho para o GR; e
- Codificar uma ferramenta automatizada para coletar os questionários.

1.2 MOTIVAÇÃO

O GP e a Engenharia de *Software* são atividades que se preocupam em criar, produzir e manter de forma sistemática produtos de alta qualidade, entregues no prazo e a um custo mínimo [39]. Uma vez que o sistemas computacionais são fundamentais para o cotidiano das pessoas e empresas, é essencial que eles não causem problemas indesejados aos usuários. Para tanto, as atividades do GR devem possibilitar que as organizações alcancem estes objetivos.

A gerência de riscos propõe abordar de forma proativa as incertezas do projeto, com o intuito de evitar que elas se concretizem e se transformem em problemas [48]. Apesar da grande importância do tema, atualmente muitas organizações não colocam tais atividades em prática pois, na maioria das vezes, são grandes as dificuldades em compreender as etapas envolvidas no GR [43].

Muitas metodologias para GR foram pesquisadas na literatura, no entanto os modelos encontrados não relacionam-se diretamente ao tema desta dissertação, o qual estabelece um conjunto de componentes para avaliar o grau de maturidade do GR de um PDS, propondo os caminhos para implementar esta gerência de maneira gradativa e incremental por meio de níveis de maturidade.

1.3 DELIMITAÇÃO DO TRABALHO

Devido a amplitude do tema escolhido, foi necessário delimitar o campo e a dimensão do estudo, isto para garantir perfeito entendimento dos problemas envolvidos além de cumprir o cronograma e objetivos propostos. Neste sentido, as pesquisas e experimentos realizados para elaborar o GAIA Riscos foram conduzidos em um ambiente controlado de uma fábrica de *software*, cujo PDS foi concebido para atender aos requisitos do nível F do Modelo de Referência MPS para *Software* (MR-MPS-SW), o qual está vinculado ao Programa para Melhoria de Processo de Software e Serviços (MPS.BR) [3].

1.4 METODOLOGIA DO DESENVOLVIMENTO DO TRABALHO

A metodologia de pesquisa utilizada para elaborar esta dissertação de mestrado foi, primeiramente, a revisão da literatura para compreender os trabalhos realizados e a situação atual do GR no desenvolvimento de *software*. A exploração baseou-se na leitura de artigos e relatórios técnicos publicados em anais de conferências e em periódicos nacionais

e internacionais, obtidos nas bases do *Institute of Electrical and Electronics Engineers* (IEEE), *ScienceDirect* e *Association for Computing Machinery* (ACM), principalmente. Tal pesquisa permitiu identificar tanto o que já foi feito quanto as lacunas presentes.

Além do caráter exploratório desta pesquisa, sua natureza pode ser classificada como aplicada, pois pretende-se gerar conhecimentos dirigidos à solução de um problema específico. Quanto ao método científico utilizado, é essencialmente dedutivo, uma vez que a verificação da conclusão se dará por meio da validação das premissas [16] [32]. A Tabela 1.1 expõe, resumidamente, as classificações deste trabalho.

Tabela 1.1 – Classificação da Pesquisa

Característica	**Classificação**
Natureza	Pesquisa Aplicada
Objetivo	Pesquisa Exploratória
Método científico	Dedutivo
Origem dos dados	Múltiplas fontes
Procedimentos técnicos	Pesquisa bibliográfica e Estudo de caso

Por fim, para verificar e validar o *framework* GAIA Riscos, o ambiente de uma fábrica de desenvolvimento *software* foi utilizado como base para coleta de informações sobre as atividades do GR. Os dados obtidos foram utilizados para avaliar as vantagens, desvantagens, utilidades e a eficácia da aplicação do *framework* em um PDS. O estudo de caso completo está descrito na Seção 4 desta dissertação.

1.5 ORGANIZAÇÃO DO TRABALHO

Para expor os conteúdos apresentados neste capítulo o trabalho encontra-se dividido em quatro seções, conforme descrito a seguir:

- A **Seção 1** compreende esta introdução.
- Na **Seção 2** serão apresentados os conceitos teóricos e trabalhos relacionados que compõe esta pesquisa.
- Na **Seção 3** será descrito o *framework* GAIA Riscos e seus componentes.

- Na **Seção 4** será apresentado o estudo de caso realizado em uma empresa de desenvolvimento de *software*.
- Na **Seção 5** serão evidenciadas as conclusões obtidas por meio da realização desta pesquisa, suas contribuições e os trabalhos futuros relacionados ao tema.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção são explicados alguns conceitos que embasam a elaboração deste trabalho. Dada a delimitação da pesquisa, as bases teóricas sobre o gerenciamento de projetos (GP) e gerenciamento de riscos (GR) são fundamentais para formar o corpo de conhecimento necessário ao desenvolvimento do estudo. Para tanto, cada um destes temas terá uma seção específica. Adicionalmente, para estruturar o GAIA Riscos, realiza-se uma breve revisão sobre algumas boas práticas de gerenciamento de serviços e alguns modelos de maturidade.

2.1 GERENCIAMENTO DE PROJETOS

Os projetos são fundamentais para qualquer atividade de geração de produtos ou serviços, envolvendo durante um período de tempo um determinado número de pessoas, as quais geralmente são organizadas em times [13]. O GP, por sua vez, deve criar um equilíbrio entre estes fatores, garantindo a entrega deste produto de acordo com as metas de prazo, custo e qualidade estabelecidas [45].

A gestão de projetos evoluiu constantemente desde meados da década de 1960, devido aos novos desafios do século XX. Nascida na indústria bélica e aeroespacial americana, esta atividade posteriormente foi adotada na construção civil e em outras áreas da engenharia. Atualmente, os conceitos envolvidos passaram a ser compreendidos e aplicados a diferentes setores da economia, inclusive no desenvolvimento de *software* [36].

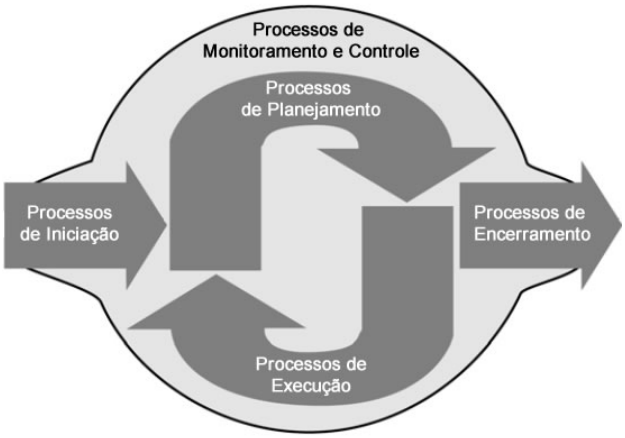
Atualmente, as organizações, comunidades e pessoas envolvidas com a área reconhecem a importância do assunto tanto no setor público quanto no setor privado. Assim, dia após dia, empresas do mundo todo aderem a técnicas e metodologias para gerenciar seus projetos, aumentar a qualidade de seus processos e, consequentemente, atingir os resultados esperados por seus clientes [56].

O órgão pioneiro na divulgação destes conceitos é o *Project Management Institute* (PMI), uma entidade internacional sem fins lucrativos que congrega os profissionais de áreas relacionadas ao GP. Em seu livro *A Guide to the Project Management Body of Knowledge* (PMBOK), atualmente em sua 5ª edição, esta associação descreve conceitos e as melhores práticas das áreas de gerenciamento, padronizando as terminologias e processos utilizados pelos profissionais certificados. Este guia divide-se em 10 áreas de conhecimento, conforme segue:

- **Gerenciamento de integração do projeto:** define os processos para identificar, definir, combinar, unir e coordenar os diversos elementos e atividades do GP;
- **Gerenciamento do escopo do projeto:** descreve os processos para garantir que o projeto contemple todos os aspectos necessário para completar o produto;
- **Gerenciamento de tempo do projeto:** identifica os processos necessários para estabelecer o cronograma das atividades envolvidas na criação do produto;
- **Gerenciamento de custos do projeto:** descreve os processos para estimar e controlar os custos para concluir o projeto dentro do orçamento aprovado;
- **Gerenciamento da qualidade do projeto**: expõe os processos, políticas, objetivos e responsabilidades para garantir que o projeto irá satisfazer os objetivos de qualidade;
- **Gerenciamento de recursos humanos do projeto:** identifica os processos para gerir e organizar os papéis e responsabilidades dos membros da equipe;
- **Gerenciamento das comunicações do projeto:** descreve processos para coletar, transmitir e armazenar as informações relevantes ao projeto;
- **Gerenciamento de riscos do projeto:** define os processos para identificar, analisar e controlar os riscos inerentes ao projeto;
- **Gerenciamento de aquisições do projeto:** identifica os processos envolvidos na compra ou aquisição de produtos e serviços necessários para realizar o trabalho; e
- **Gerenciamento de partes interessadas:** se concentra em gerenciar o comprometimento dos envolvidos com o projeto.

Estas áreas de conhecimento do PMBOK são empregadas nas diferentes fases do projeto, ao longo de seu ciclo de vida. A classificação destes processos, por sua vez, dá-se por meio de 5 grupos: (1) iniciação, (2) planejamento, (3) execução, (4) monitoramento e controle e (5) fechamento do projeto. A Figura 2.1 expõe o relacionamento entre estes grupos de processo.

Figura 2.1 – Relacionamento entre os grupos de processo do PMBOK.



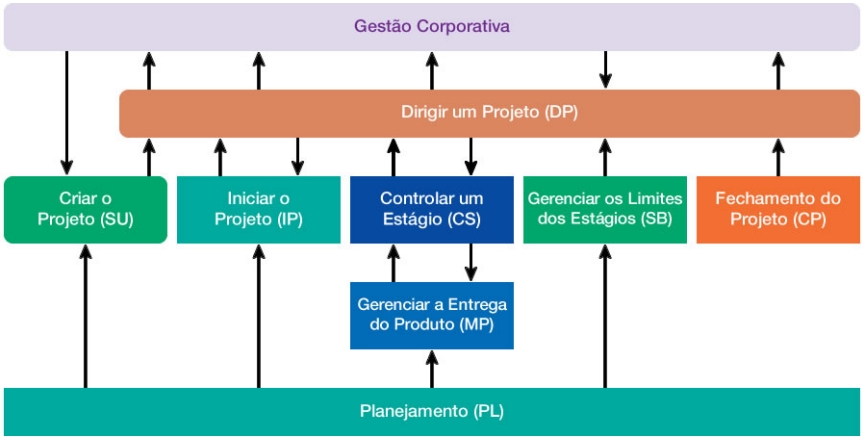
Fonte: Adaptado de [44].

Após o sucesso do PMBOK entre as organizações norte americanas, principalmente, outras associações lançaram guias de melhores práticas para o GP. Na Europa, o *Office of Government Commerce* (OGC) possui o modelo *Projects in Controlled Environments* (PRINCE2), cuja proposta é separar as atividades de gerenciamento da execução do projeto, criando um ambiente adaptável para qualquer projeto da organização [5] [57]. Para tanto, ele divide-se em quatro partes:

- **Princípios:** compreende 7 orientações básicas que devem estar presentes em todos os projetos de um organização, ou seja, são a base para a implantação do modelo;
- **Temas:** conjunto de 7 áreas do projeto que necessitam ser abordadas ao longo de seu ciclo de vida (Qualidade, riscos e mudança, por exemplo);
- **Processos:** são 8 processos necessários para completar um objetivo do GP (Processos de criação do projeto, fechamento do projeto e gerenciamento da entrega de um produto, por exemplo); e
- **Adequação:** conjunto de políticas e práticas que indicam as atividades mais importantes para determinados tipos de projeto.

Assim como o PMBOK, o modelo PRINCE2 também busca o sucesso dos projetos por meio do gerenciamento por grupos de processos, os quais reúnem atividades para iniciar, gerenciar, criar e fechar um projeto, controlar e gerenciar os limites de um estágio e gerenciar a entrega do produto. A Figura 2.2 expõe de maneira simplificada o relacionamento os grupos de processo do modelo PRINCE2.

Figura 2.2 – Relacionamento entre os grupos de processo do modelo PRINCE2



Fonte: Adaptado de [57]

A execução de cada grupo do processo, apresentado na Figura 2.2, dá-se de acordo com os conceitos definidos por Deming [12] sobre o ciclo PDCA (*Plan*, *Do*, *Check e Act*). Cada grupo de processo representa uma atividade do ciclo de vida, que pode ser repetida, ou não, dependendo do projeto, os quais estão descritos abaixo:

- **Criar o Projeto (SU):** atividades para formalizar a criação do projeto, definir a equipe de gerenciamento e gerenciar as expectativas de qualidade.
- **Iniciar o Projeto (IP):** ações para planejar o projeto, obter aprovações dos requisitos e critérios de qualidade.
- **Dirigir um Projeto (DP):** etapa de autorização para iniciar e finalizar um projeto, além de aprovação para começar e terminar os estágios.
- **Controlar um Estágio (CS):** atividades para gerenciar um estágio e aprovar sua finalização.
- **Gerenciar a Entrega do Produto (MP):** ações para realizar o trabalho bem como aprovar a entrega do produto final.
- **Gerenciando os Limites dos Estágios (SB):** fase para registrar as lições aprendidas e obter aprovações necessárias para iniciar o próximo estágio.
- **Fechamento do Projeto (CP):** atividades para verificar se todos os produtos previstos foram entregues e registrar recomendações para os próximos projetos da organização.
- **Planejamento (PL):** etapa de definição do nível de planejamento necessário bem como realização de estimativas e análise de riscos.

2.1.1 Gerenciamento de Projetos no Desenvolvimento de *Software*

Assim como no mercado global, as áreas de desenvolvimento de *software* e tecnologia da informação e comunicação (TIC) seguem a tendência de aderirem a metodologias para controlar seus projetos. Isto deve-se, em parte, pelo entendimento que uma parte significativa do insucesso dos projetos de *software* está relacionada com uma má gestão ou, então, pela completa ausência da mesma [27].

Um projeto de *software*, por sua vez, compreende duas dimensões: a engenharia e o GP [26]. A engenharia aborda a construção do sistema, integrando, verificando, validando e combinando todos os componentes em um produto que será entregue ao cliente. As atividades GP, por sua vez, buscam facilitar as atividades da engenharia, garantindo que a entrega seja feita no prazo estabelecido, atenda aos requisitos estipulados e não apresente defeitos [10].

Em decorrência da complexidade das atividades que cercam o GP, é notória a necessidade de se utilizar metodologias eficientes para administrar os projetos de *software* [56]. Neste contexto, várias metodologias de GP, tradicionais ou específicas para o desenvolvimento de *software* são utilizadas para aumentar a qualidade dos processos, dentre as quais destacam-se o próprio guia do PMBOK, modelo PRINCE2, a norma ISO 15504 [19] e os modelos de melhoria de processo de *software*: *Capability Maturity Model Integration* (CMMI) [52] e o Modelo de Referência MPS para *Software* (MR-MPS-SW) [3]

2.2 GERENCIAMENTO DE RISCOS

O GR faz parte de diferentes campos do conhecimento e a bibliografia a seu respeito geralmente a associa as áreas de gerenciamento de projetos, administração, seguros e financeira [1]. Esta seção busca definir diversos termos utilizados na área, bem como identificar o panorama atual do GR no desenvolvimento de *software* e os modelos de gestão mais relevantes encontrados na literatura.

A palavra risco é utilizada nas mais diferentes áreas de conhecimento e diversas comunidades atribuem diferentes significados a ela [30]. Entretanto, é um senso comum entre as principais abordagens utilizadas pelo mercado que os 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 [21],

[44], [57]. Tais efeitos podem ser classificados de duas formas: especulativos ou danosos [59], tal como exposto pela Tabela 2.1.

Tabela 2.1 – Tipos de riscos, impactos e estratégias para gerenciamento

Tipo	Impacto	Estratégia
Especulativo	Positivo ou negativo	Monitorar
Danoso	Negativo	Evitar

Fonte: Adaptado de [59]

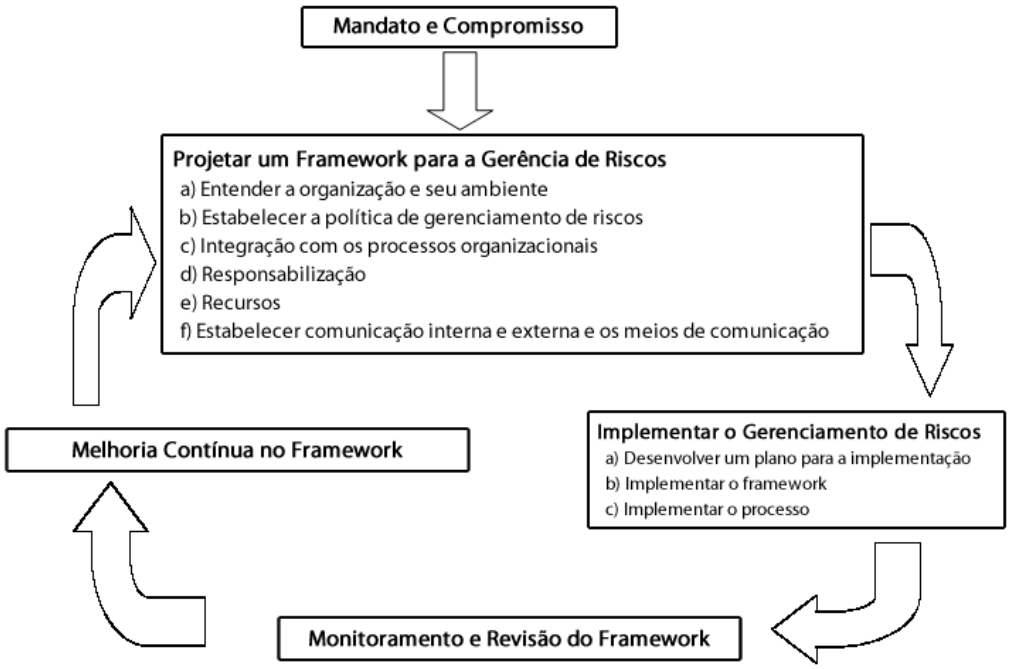
Como é possível observar na Tabela 2.1, os risco especulativos são fatores incertos que podem se concretizar na forma de algo positivo ou negativo, devendo ser monitorados para minimizar a probabilidade de um impacto negativo ocorrer e maximizar a probabilidade um impacto positivo. Os riscos danosos, por sua vez, sempre afetam negativamente os objetivos do projeto, desta forma devem ser mitigados, tendo em vista que os mesmos não oferecem benefícios para o projeto.

Neste contexto, o GR provê um conjunto de políticas, objetivos, planos, responsabilidades, recursos, processos e atividades para identificar, analisar, avaliar e monitorar estes fatores, melhorando continuamente o processo da organização [21], [45] e [57]. Várias são as abordagens que permitem gerir os riscos dos projetos da organização.

A ISO 31000 [21] trata tanto dos aspectos positivos quanto negativos da ocorrência de riscos, com o objetivo de fornecer aos gerentes, princípios, guias e terminologias comuns à área. Por ser uma norma ISO, pode ser utilizada em qualquer organização, independentemente do ramo ou atividade do negócio. Para tanto, a norma compreende um *framework* para implantação e um processo padrão para o GR. Ainda, ela apresenta padrões para integrar o GR entre os diversos setores de uma mesma empresa e metodologias já existentes.

Este *framework* de implantação busca integrar as atividades do processo de GR aos procedimentos da organização. As atividades para adotar a ISO 31000 envolvem ações para compreender a organização e suas reais necessidades, implementar GR e melhorar continuamente os processos organizacionais. A Figura 2.3 representa as cinco principais atividades *framework* de implantação da ISO 31000.

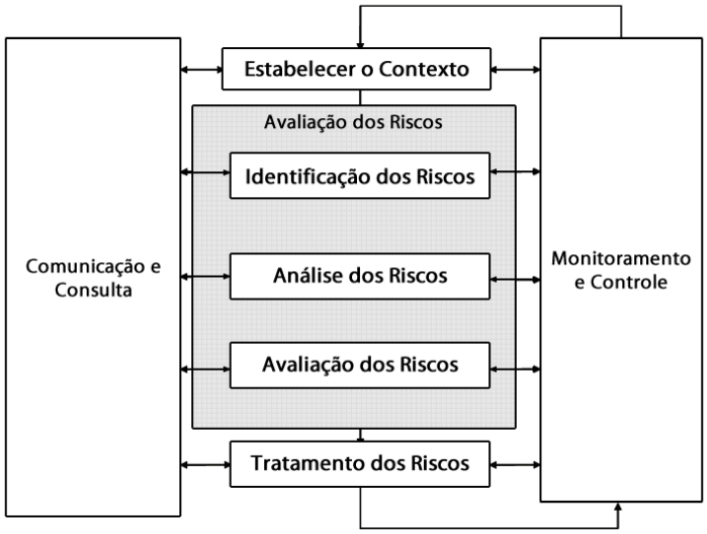
Figura 2.3 – Relacionamento entre os componentes do *framework* para gerenciar riscos



Fonte: Adaptado da ISO 31000 [21]

Conforme mencionado, este *framework* visa integrar o processo padrão de GR oferecido pela norma aos processos organizacionais. Para tanto, ele compreende atividades para comunicar as partes envolvidas, estabelecer o contexto do GR e avaliar e tratar as ameaças, além de possibilitar o monitoramento e controle das mesmas. A Figura 2.4 ilustra a relação entre as atividades do processo de GR da ISO 31000.

Figura 2.4 – Relacionamento entre as atividades do processo de GR da ISO 31000



Fonte: Adaptado da ISO 31000 [21]

De acordo com a ilustração é possível verificar a presença de 5 atividades principais: comunicação e consulta, estabelecer o contexto, avaliação dos riscos, tratamento dos riscos e monitoramento e controle, as quais são executadas da seguinte forma:

- **Comunicação e Consulta:** ocorre paralelamente a todas etapas do GR para garantir que os interesses de todas as partes envolvidas sejam atendidos. Esta atividade deve ser conduzida por um plano de gerenciamento das 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 do gerenciamento de riscos, além dos critérios usados 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 estabelecidos.
- **Monitoramento e Controle:** atividade que deve ser executada de maneira iterativa ou *ad hoc*[1] 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 (BDH) da organização.

Somado ao *framework* de implantação da norma e a seu processo padrão para administrar os riscos do projeto, a ISO disponibiliza aos gerentes o Guia 73 [23], que contém terminologias, acrônimos e siglas comuns à área e também a norma ISO 31010 [22], que descreve um conjunto de ferramentas, técnicas e metodologias úteis para identificar, analisar e avaliar os riscos.

[1] O CMMI-DEV [54] define o termo *ad hoc* como um processo que é executado sempre que necessário para resolver um determinado problema.

Além da ISO 31000, outros modelos para GP que incluem o GR em suas atividades foram pesquisados. O PMBOK possui uma área de conhecimento exclusiva para este tema. Seu principal objetivo é aumentar a probabilidade de ocorrência de eventos positivos e reduzir a probabilidade eventos negativos. As etapas envolvidas no processo de GR do PMBOK são:

- **Planejar o Gerenciamento de Riscos:** consiste em estabelecer as regras que irão nortear as atividades de GR durante todo o ciclo de vida do projeto, estabelecendo critérios, partes envolvidas e suas responsabilidades, orçamento, prazo e métricas de probabilidade ocorrência de um risco.
- **Identificar os Riscos:** etapa de levantamento dos riscos. Ocorre durante todo o ciclo de vida do projeto com o intuito de criar e manter atualizada uma lista descritiva com os riscos que podem afetá-lo. Esta lista deve conter os principais impactos esperados caso a ameaça se concretize, inclusive.
- **Realizar a Análise Qualitativa dos Riscos:** atividade para priorizar os riscos de acordo com os impactos que eles podem causar ao projeto, além de sua probabilidade de ocorrência. O objetivo desta fase é classificar os riscos em grupos e alto, moderado ou baixo impacto.
- **Realizar a Análise Quantitativa dos Riscos:** complementa a análise qualitativa, entretanto o intuito deste processo é mensurar os efeitos que os riscos exercem sobre as metas do projeto, além de colaborar na determinação das prioridades.
- **Planejar as Respostas aos Riscos:** fase de planejamento das medidas que serão tomadas frente aos riscos identificados e analisados, com o objetivo de definir abordagens, reponsabilidades, custos envolvidos, planos de contingência e prazo para realizar o tratamento.
- **Monitorar e Controlar os Riscos:** etapa de acompanhamento dos riscos e implementação dos planos de resposta, com o objetivo de monitorar os riscos residuais, identificar novas ameaças, analisar a eficácia do processo de GR e registrar as lições aprendidas no BDH da organização.

Complementarmente ao processo de GR, o guia do PMBOK apresenta modelos de documentos de entrada e saída, além de uma vasta coleção de ferramentas e técnicas úteis aos gerentes de projetos nas atividades realizadas no dia-a-dia da organização.

2.2.1 Gerenciamento de Riscos no Desenvolvimento de *Software*

Atualmente, todos os ramos de atividade dependem, de alguma forma, dos sistemas de informação (SI) para operar ou controlar equipamentos e gravar, processar ou gerir suas informações. Neste sentido, vários estudos tem sido realizados na área de GR no processo de desenvolvimento de *software* [25], com o intuito de produzir modelos, processos e ferramentas para aumentar a probabilidade de sucesso dos projetos de *software* [45] [53].

Boehm [7] é um dos pioneiros na área propondo um modelo composto de atividades para identificar, analisar, avaliar, tratar e controlar os riscos. A principal diferença deste para os outros estudos está na classificação dos riscos do projeto, chamada de taxonomia dos riscos, proposta por Boehm. Desde então, várias abordagens tem tratado sobre o GR no desenvolvimento de *software*, das quais destacam-se as baseadas em modelos de processo e modelos de *framework* [4].

Neste contexto, ao longo da década de 90, as metodologias existentes aumentaram gradativamente o enfoque dado as atividades relacionadas ao GR, para as quais passaram a dedicar capítulos exclusivos em seus guias [31]. Ademais, de acordo com Kerzner [28], as atividades de GR associadas ao desenvolvimento de *software* passaram a ter destaque no cenário internacional a partir de 1996, como reflexo da crise do *software* e da necessidade melhoria dos sistemas.

Na seção 2.2.2 são apresentados, analisados e comparados vários modelos de referência e abordagens para gerir riscos de projetos de desenvolvimento de *software*. Os estudos apresentados levam em consideração aspectos relacionados ao tema e à utilização da abordagem ou modelo em ambientes de desenvolvimento de *software*.

2.2.2 Modelos de Gestão de Riscos no Desenvolvimento de *Software*

É possível encontrar na literatura várias metodologias para controlar os riscos dos projetos, entre as quais estão presentes aquelas que se baseiam na criação de uma memória institucional para auxiliar os gerentes em todas as etapas envolvidas nesta gerência

[2], [46] e [47]. Nestes estudos, inclusive, é comum a presença de um repositório de informações sobre os riscos, suas causas e metodologias utilizadas para mitigá-los.

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 [18], [29], [33] e [34]. Dentre as principais características destes modelos está a capacidade de armazenar e disseminar as informações obtidas em decorrência do processo de gestão dos riscos.

Outros modelos para controlar os riscos dos projetos são os processos utilizados pelos métodos ágeis. Nos casos do *Extreme Programming* (XP) [37] e do SCRUM [51], as atividades de gerenciamento são realizadas de maneira iterativa e incremental, dentro de reuniões 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.

Alguns autores, por sua vez, apresentam a gerência de riscos utilizando-se de processos de modelagem e simulação [11], [35]. 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 existem trabalhos que tratam a gerência dos riscos de maneira concorrente e colaborativa entre os vários projetos de uma organização [18] e [58], 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 [58] 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 para casos de terceirização de desenvolvimento de *software* em que o desenvolvimento é realizado nas dependências do cliente, prática denominada *body shop*, Schreiber [50] 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 [1] 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 como este trabalho.

Os processos de gestão de riscos proposto por alguns padrões amplamente utilizados no mercado também foram pesquisados. É comum aos modelos consultados a presença de atividades para identificar, analisar, avaliar, tratar, comunicar e monitorar os riscos [21], [45] e [57]. Este conjunto de atividades, por sua vez, busca 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 desnecessários com retrabalhos.

A Tabela 2.2 apresenta uma análise comparativa detalhada entre os modelos e abordagens apresentadas. Para elaborar os critérios de comparação presentes na tabela foram utilizados os principais aspectos abordados pelas metodologias do GR, bem como as características que esta pesquisa pretende resolver.

Conforme é possível observar na Tabela 2.2, o GAIA Riscos acopla os componentes dos serviços e os níveis de maturidade e indica as diretrizes para utilizar e implementar cada um deles. Destaca-se, ainda, que não foram encontrados modelos que utilizem concomitantemente os níveis de maturidade, os questionários de avaliação diagnóstica e os *checklists* de reavaliação para moldar o processo de GR as necessidades da organização.

Por fim, dentre os modelos pesquisados, destacam-se: (1) a metodologia elaborada por Alhawari [2], a qual utiliza as informações e experiências provenientes de outros projetos bem como o conhecimento obtido pelos membros equipe para auxiliar nas atividades da gerência de riscos, (2) a presença de um *framework* para implantar o processo de GR da ISO 31000 [21], padronizando as atividades necessárias e (3) a constante presença de reuniões no SCRUM [51], as quais tem por objetivo integrar todos envolvidos com o projeto.

Tabela 2.2 – Tabela comparativa com os trabalhos relacionados

CRITÉRIO	PMBOK [44]	ISO 31000 [21]	Leme, L. [34]	Riehle, R. [46]	Alhawari, S. [2]	Gusmão, C. [17]	Islam, S. [25]	SCRUM [51]	GAIA Riscos
Documentação dos Riscos	Sim. O registro dos riscos é gerado de acordo com os documentos do projeto.	Sim. Registro dos riscos é gerado de acordo com os documentos do projeto.	Sim. O registro dos riscos é gerado.	Sim. O registro dos riscos é gerado de acordo com a memória da organização.	Sim. O registro dos riscos é gerado de acordo com os documentos do projeto e experiências da equipe.	Sim. O registro dos riscos é gerado de acordo com os documentos do projeto.	Sim. O registro dos riscos é gerado de acordo com os objetivos do GR.	Sim. O registro dos riscos é gerado de acordo com os dados obtidos em encontros chamados de *sprints*.	Sim. O registro detalhado dos riscos é gerado de acordo com os documentos do projeto e conhecimento da equipe.
Análise/Avaliação dos Riscos	Sim. Os riscos são analisados de maneira qualitativa e quantitativa para determinar as prioridades.	Sim. Os riscos são compreendidos para serem avaliados posteriormente.	Sim. Os riscos são avaliados para identificar a probabilidade de ocorrerem e determinar seu impacto.	Critério não contemplado pelo estudo.	Sim. Os riscos são avaliados de acordo com o conhecimento da equipe.	Sim. Os riscos são avaliados para identificar a probabilidade de ocorrerem e determinar seu impacto.	Sim. Os riscos são avaliados para identificar a probabilidade de ocorrerem e determinar seu impacto.	Sim. Os riscos são avaliados durante as iterações baseando-se no conhecimento obtido e outros projetos.	Sim. Os riscos são avaliados para identificar a probabilidade de ocorrerem e determinar seu impacto.
Tratamento dos Riscos	Sim. Pode-se eliminar, transferir, mitigar ou aceitar os riscos.	Sim. Pode-se evitar, aumentar, remover a fonte, mudar a probabilidade, alterar ou manter os riscos.	Sim. Pode-se pesquisar, aceitar, evitar, transferir, mitigar ou conter os riscos.	Sim. Baseia-se na memória organizacional para ser realizado.	Sim. Pode-se evitar, reduzir, transferir ou conter os riscos.	Sim. Planos para tratar os riscos são elaborados para eliminá-los.	Sim. Os riscos que impedem o sucesso do projeto são eliminados.	Sim. Os riscos são tratados com base em experiências obtidas em outros projetos similares.	Sim. Pode-se evitar, aumentar, remover a fonte, mudar a probabilidade, alterar ou manter os riscos.
Nível de Participação dos *Stakeholders*	Intermediário. Os envolvidos ajudam apenas a identificar os riscos.	Intermediário. Os envolvidos ajudam apenas a identificar os riscos.	Baixo. Apenas os gerentes de projeto e os engenheiros de *software* participam.	Alto. Os envolvidos ajudam a identificar e tratar os riscos do projeto.	Muito alto. Os envolvidos ajudam a identificar, avaliar e tratar os riscos do projeto.	Baixo. Apenas os gerentes de projeto e os engenheiros de *software* participam.	Intermediário. Os envolvidos ajudam apenas a identificar os riscos.	Muito alto. As reuniões a cada iteração tem a participação de todos os envolvidos.	Muito alto. Todos os envolvidos ajudam a identificar, avaliar, controlar e tratar os riscos.

CRITÉRIO	PMBOK [44]	ISO 31000 [21]	Leme, L. [34]	Riehle, R. [46]	Alhawari, S. [2]	Gusmão, C. [17]	Islam, S. [25]	SCRUM [51]	GAIA Riscos
Utilização de BDH de Riscos	Sim. Apenas para a manutenção de uma memória organizacional.	Sim. Apenas para a manutenção de uma memória organizacional.	Sim. Apenas para a manutenção de uma memória organizacional.	Sim. A memória institucional é fator chave para o sucesso do GR.	Sim. A memória institucional é fator chave para o sucesso do GR.	Critério não contemplado pelo estudo.	Critério não contemplado pelo estudo.	Sim. As experiências são registradas para auxiliarem em outros projetos similares.	Sim. A memória institucional é crucial para o sucesso do GR.
Implantação da Gerência de Riscos	Apenas pode ser realizada de maneira completa.	É realizada de maneira progressiva.	Critério não contemplado pelo estudo.	Critério não contemplado pelo estudo.	É realizada de maneira progressiva.	Critério não contemplado pelo estudo.	Critério não contemplado pelo estudo.	É realizada iterativamente até que a metodologia se torne comum entre todos os membros da equipe.	Realizada de maneira completa ou progressiva, de acordo com o interesse da organização.
Níveis de Maturidade	Não	Não	Não	Não	Não	Não	Não	Não	Sim. Os níveis de maturidade determinam quais atividades do GR devem ser implantadas na organização.
Integração com o PDS da Organização	As atividades devem ser incorporadas ao PDS da organização.	As atividades devem ser incorporadas ao PDS da organização por meio da execução de um *framework*.	Critério não contemplado pelo estudo.	O processo de GR deve ser incorporado de maneira progressiva no PDS da organização.	O processo de GR deve ser incorporado ao PDS da organização por meio da aplicação de um *framework*.	O processo de GR deve ser incorporado ao PDS da organização.	O processo de GR deve ser incorporado ao PDS da organização.	Ocorre durante as reuniões realizadas a cada iteração.	Os serviços podem ser executados em qualquer etapa ou então incorporado ao PDS da organização.

CRITÉRIO	PMBOK [44]	ISO 31000 [21]	Leme, L. [34]	Riehle, R. [46]	Alhawari, S. [2]	Gusmão, C. [17]	Islam, S. [25]	SCRUM [51]	GAIA Riscos
Comunicação com os Interessados	Sim. Existe um processo de comunicação comum a todas as áreas da organização.	Sim. Existe um processo específico para a comunicação dos riscos.	Sim. Existe apenas a comunicação interna entre a equipe do projeto.	Critério não contemplado pelo estudo.	Sim. Existe um processo para comunicar todos os envolvidos.	Critério não contemplado pelo estudo.	Critério não contemplado pelo estudo.	Ocorre durante as reuniões realizada a cada iteração.	Sim. Ocorre sempre que necessário por meio do serviço de comunicação e consulta.
Questionário de Avaliação Diagnóstica	Não	Não	Não	Não	Não	Não	Não	Não	Sim. Existe um Questionário Eletrônico para coletar as respostas do usuário.
***Checklists* de Reavaliação**	Não	Não	Não	Não	Não	Não	Não	Não	Sim. Deve ser preenchido a cada iteração do processo de implantação do *framework.*
Instruções de Trabalho	Devem ser bem definidas e priorizar as ferramentas e técnicas do guia.	Devem ser bem definidas e priorizar as ferramentas e técnicas da ISO 31000 e os vocabulários do guia 73.	Critério não contemplado pelo estudo.	Critério não contemplado pelo estudo.	Critério não contemplado pelo estudo.	Devem ser bem definidas, entretanto o autor cita apenas a existência de *templates* de documentos.	Critério não contemplado pelo estudo.	Devem ser bem definidas e utilizar as ferramentas e técnicas mais conhecidas pela equipe.	Devem ser bem definidas e utilizar as ferramentas e técnicas, *templates* e vocabulários presentes no serviço.

2.3 *INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY* (ITIL)

O *Information Technology Infrastructure Library* (ITIL) é um padrão mundialmente aceito que provê as melhores práticas para gerir serviços de TIC, focando sempre em fazer com que eles estejam alinhados aos objetivos organizacionais e agreguem valor ao negócio. Criado no final dos anos 80 pelo governo britânico, o guia atualmente encontra-se em sua 3ª edição (ITIL V3) e é mantido e distribuído pelo *Office of Government Commerce* (OGC) [42]. Em sua última edição lançada em 2011 o ITIL divide-se cinco livros:

- **Estratégia de Serviço:** alinhamento do serviço com os objetivos organizacionais.
- **Desenho de Serviço:** modelagem do serviço, com o intuito de adequá-lo ao ambiente da organização.
- **Transição de Serviço:** implementação do serviço.
- **Operação de Serviço:** execução do serviço de acordo com as determinações das fases anteriores.
- **Melhoria Contínua de Serviço:** identificação e implementação de mudanças conforme as necessidades organizacionais.

Cada um destes livros aborda de maneira ampla e detalhada as fases do ciclo de vida do ITIL. Somado a eles, existe, ainda, um volume introdutório, chamado de *The oficial introduction of the ITIL service lifecycle*, cuja finalidade é apresentar uma visão geral do modelo, sua metodologia de utilização e descrever brevemente cada uma das fases que compõe o ciclo de vida.

Segundo este conjunto de boas práticas, ainda, um serviço pode ser definido como um meio de entregar valor aos clientes, facilitando que eles atinjam os resultados esperados, sem assumir os custos e riscos específicos. Para tanto, o serviço deve responder por um evento específico, ser mensurável e focado nos resultados [42].

Por fim, o gerenciamento dos serviços compreende os métodos, processos, funções, papéis e atividades que possibilitem entregar os serviços aos clientes, considerando todas as etapas envolvidas desde a elaboração de sua estratégia até sua manutenção e melhoria contínua, provendo valor aos clientes em forma de serviços [42].

2.4 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 [3]. 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):** é um padrão criado e mantido pelo PMI e com atividades baseadas no PMBOK cuja função é avaliar e desenvolver capacidades organizacionais para o GP. A metodologia para identificar um nível de maturidade consiste na execução de um processo auto avaliativo sob as áreas de conhecimento do guia do PMBOK [45].
- ***Capability Maturity Model Integration* (CMMI):** é um modelo de avaliação de maturidade mundialmente conhecido, o qual é criado e mantido pelo *Software Engineering Institute* (SEI). A estratégia utilizada para mensurar a maturidade do processo fundamenta-se na comparação das evidências fornecidas pelo processo em questão com as diretrizes do nível de maturidade desejado [14].
- ***Control Objectives for Information and Related Technology* (COBIT):** é uma metodologia criada pelo *IT Governance Institut*e (ITGI) e, atualmente, mantida pelo *Information Systems Audit and Control Association* (ISACA). O método utilizado para estabelecer o grau de maturidade do processo consiste em compará-lo com os critérios específicos de cada nível de maturidade [24].
- **Modelo de Referência MPS para *Software* (MR-MPS-SW):** o desenvolvimento deste modelo é coordenado pela Associação para Promoção da Excelência do *Software* Brasileiro (SOFTEX). A estratégia para avaliar um nível de maturidade consiste em verificar se a organização atende aos resultados de atributos de processo do nível almejado [3].
- ***Maturity Model in Information Security* (MMGRSeg):** modelo criado com base no CMMI e na norma ISO/IEC 27005 [20] por Mayer e Fagundes [38]. 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.

3 GAIA RISCOS

Este capítulo apresenta o *framework* para gerenciar riscos por meio de serviços denominado GAIA Riscos. O objetivo principal deste *framework* é melhorar os processos para estabelecer contexto, identificar, analisar, avaliar, tratar, comunicar e monitorar os riscos por meio de evoluções gradativas e incrementais no Processo de Desenvolvimento de *Software* (PDS) de uma organização.

Para atingir este objetivo foram desenvolvidos, em um primeiro momento, quatro componentes principais, que são: (1) sete serviços, (2) cinco níveis de maturidade, (3) um questionário de avaliação diagnóstica e (4) um processo de implantação. Posteriormente, também integraram o GAIA Riscos quatro *checklists* de reavaliação e indicadores de desempenho, conforme é possível observar por meio da Figura 3.1.

Figura 3.1 – Estrutura do *framework* GAIA Riscos

Conforme ilustrado pela Figura 3.1, em azul, estão os elementos que subsidiaram o desenvolvimento dos componentes do GAIA Riscos, em vermelho. As próximas seções detalham a estrutura e os componentes do *framework*, os quais estão disponíveis para utilização no endereço http://www.gaia.uel.br/gaia_riscos/.

3.1 SERVIÇOS

Conforme exposto na Seção 2.3, os serviços têm como objetivo entregar valor aos clientes, permitindo que eles atinjam seus resultados, de maneira mensurável e sem que eles arquem com os custos e riscos envolvidos. No *framework* proposta, cada serviço

organiza os conhecimentos das melhores práticas de GR disponíveis no mercado, assim como ilustrado pela Figura 3.2.

Figura 3.2 – Componentes do serviço

Como pode-se observar na Figura 3.2, o serviço possui cinco áreas que organizam as informações pertinentes a esta gerência e, inclusive, podem ser customizadas de acordo com as necessidades do projeto, cliente e organização. A seguir descreve-se cada uma das cinco áreas que compõe um serviço:

- **Ferramentas e Técnicas:** retiradas da ISO 31010 [22]. Compreendem instrumentos e metodologias que possibilitam aplicar e incorporar as práticas do GR em uma organização.
- ***Templates* de Documentos:** retirados do PMBOK [44]. Consistem em modelos de documentos com o propósito de padronizar os registros do GR.
- **Indicadores de Desempenho:** fundamentam-se na proposta do *Balanced Scorecard* (BSC) [41]. Definem métricas para mensurar a evolução do GR e incentivar a melhoria contínua desta gerência.
- ***Workflows*:** baseiam-se nas diretrizes da ISO 31000 [21]. Caracterizam os processos padrão para gerir os riscos em uma organização.
- **Vocabulários:** retirados do Guia 73 da ISO [23]. Compreendem terminologias, nomenclaturas e siglas comuns as atividades de cada serviço do *framework*.

Além de organizar as informações relevantes e serem customizadas de acordo com a necessidade, a utilização das áreas de serviço institucionaliza um repositório de políticas, metodologias, práticas, documentos, terminologias, procedimentos e métricas para realizar as atividades do GR. O acesso a estas informações é disponibilizado para os membros da equipe por meio da Internet.

Para obter os serviços que compõe o *framework*, as sete atividades de GR propostas pela norma ISO 31000 (Seção 2.2) foram fragmentadas. A seguir são caracterizados cada um dos serviços do GAIA Riscos:

- **Identificar Riscos:** realização de análises nos planos do projeto para obter uma lista de riscos. Para elaborar o catálogo de riscos realizam-se reuniões de *brainstorming*, análises documentais, entrevistas com os interessados, consultas no BDH da organização e pode-se aplicar a técnica de Wideband Delphi [6] para identificar e estimar os impactos dos riscos em projetos cujo domínio é desconhecido.
- **Estabelecer o Contexto:** definição dos parâmetros que irão nortear as atividades de identificação, análise, avaliação, tratamento e monitoramento dos riscos, bem como comunicação entre os interessados. Para tanto, podem-se realizar reuniões, entrevistas com todos os envolvidos com o projeto, consultas ao BDH da organização e aplica-se a técnica de Wideband Delphi.
- **Analisar Riscos:** compreensão dos riscos identificados para gerar um lista de riscos analisados. O processo de análise consiste em implementar protótipos do produto ou parte dele, montar e analisar árvores de decisão, elaborar de matrizes de probabilidade/impacto e aplicar a técnica denominada “e se” (*what if*) [22].
- **Avaliar Riscos:** comparação dos riscos analisados com os parâmetros estabelecidos para classificar a lista de riscos de acordo com a criticidade do mesmo. Para tanto, pode-se realizar simulações, análises de causa/consequência, análises estatísticas e de informações do BDH da organização.
- **Tratar Riscos:** ações para desenvolver os planos de tratamento dos riscos, planos de contingência e implementar as ações necessárias. Tais

ações resultam em relatórios de desempenho e lições aprendidas, que são armazenadas no BDH da organização.

- **Monitoramento e Controle:** atividades para determinar a eficiência do processo de GR. As informações obtidas resultam de medições realizadas durante a execução dos serviços do *framework*. Tais dados representam a evolução das atividades de GR dentro do PDS da organização.
- **Comunicação e Consulta:** identificação dos envolvidos com o projeto e os meios de comunicação necessários para disseminar as informações entre todos. Esta atividade resulta em indicadores de qualidade e na própria informação transmitida aos interessados.

Baseando-se na estrutura exposta na Figura 3.2 e nas descrições acima apresentadas tem-se os componentes necessários para um serviço do *framework*. Desta forma, para ilustrar as informações que compõe cada uma das áreas, a Figura 3.3 exemplifica alguns dos componentes do serviço de monitoramento e controle.

Figura 3.3 - Componentes do serviço de monitoramento e controle

Por fim, para atingir o objetivo deste estudo, cada serviço do *framework* foi alocado em níveis de maturidade. A próxima seção descreve cada um dos níveis de maturidade mapeando a alocação dos serviços para cada um dos cinco níveis.

3.2 NÍVEIS DE MATURIDADE

Este estudo tem como objetivo apresentar o *framework* GAIA Riscos, o qual é orientado a serviços e tem como foco principal auxiliar os gerentes de projeto a incluírem, de maneira incremental, as atividades do GR. Os níveis de maturidade são um importante componente do GAIA Riscos, pois estabelecem patamares para evoluir esta gestão e também proporcionam às organizações subsídios para adotar, gradativamente, as atividades envolvidas neste processo.

Baseando-se nesta premissa, após a pesquisa realizada na Seção 2.4, o estudo conduzido por Mayer e Fagundes [38] foi utilizado para definir os níveis de maturidade do GAIA Riscos, pois, embora seja voltado à área de Segurança de Informação, seus conceitos estão aderentes ao padrão do CMMI e a norma ISO/IEC 27005 [20], os quais são amplamente aceitos no desenvolvimento de *software*. Assim, ao evoluir seu grau de maturidade, uma organização passa por três estágios:

- **Imaturidade:** estágio em que os processos organizacionais são inexistentes ou não são seguidos.
- **Maturidade:** etapa na qual os processos organizacionais são definidos e começam a ser padronizados e controlados.
- **Excelência:** estágio em que os processos organizacionais são definidos, padronizados e controlados em busca da melhoria contínua.

Cada um destes três estágios compreende um ou mais níveis de maturidade que, por sua vez, contém um ou mais serviços. A alocação dos serviços em um nível de maturidade foi realizada para possibilitar a evolução gradativa do GR. Nos níveis iniciais foram alocados os processos fundamentais para realizar esta gerência [7], enquanto os níveis mais elevados destinaram-se aos serviços mais complexos. Os estágios, níveis de maturidade e serviços do GAIA Riscos são ilustrados pela Figura 3.4.

Figura 3.4 - *Framework* GAIA Riscos

Como pode-se observar na Figura 3.4, o GAIA Riscos compreende três estágios e cinco níveis de maturidade, os quais representam os caminhos para melhoria do processo de uma organização. Cada nível busca estabelecer um conjunto de serviços que devem ser adotados pela organização para aderir a um determinado nível. Os cinco níveis de maturidade do *framework* são:

- **Nível 1 – Inicial:** as organizações pertencentes a este nível de maturidade podem não conhecer o GR, ou então executá-lo de maneira *ad hoc*. Este nível caracteriza uma organização pela falta de preparo dos envolvidos com o projeto nas atividades desta gerência. Além disso, a existência deste nível de maturidade é essencial para englobar todas as organizações, até mesmo as que não executam o GR.
- **Nível 2 – Conhecido:** para atingir este nível de maturidade as empresas devem executar atividades para gerir os riscos do projeto, mesmo que de maneira embrionária. Este nível caracteriza-se pela ênfase no processo de identificação dos riscos, ponto inicial das atividades.
- **Nível 3 – Padronizado:** a partir do processo de identificação dos riscos, as organizações que desejam alcançar este nível de maturidade devem

executar atividades para definir formalmente os parâmetros do GR e também adotar processos para analisar, avaliar e tratar os riscos.

- **Nível 4 – Gerenciado:** com base nas atividades desenvolvidas para aderir aos níveis 2 e 3 do GAIA Riscos, as empresas necessitam adotar metodologias para monitorar e controlar o GR. Este nível caracteriza-se, principalmente, pela possibilidade de identificar novos riscos ao longo do desenvolvimento do projeto de software, bem como identificar desvios nos parâmetros previamente estabelecidos.
- **Nível 5 – Otimizado:** com a evolução do processo de GR torna-se necessário comunicar e consultar os clientes sobre os assuntos pertinentes a esta gerência. Assim, para aderir a este nível uma organização deve adotar práticas específicas para troca de informações entre os envolvidos com o projeto.

3.3 QUESTIONÁRIO DE AVALIAÇÃO DIAGNÓSTICA

A função do Questionário de Avaliação Diagnóstica (QAD) é identificar, por meio das respostas fornecidas pelo usuário, o grau de maturidade com que o PDS que está sob avaliação atende aos serviços do *framework* GAIA Riscos. Para tanto, o questionário organiza-se em 7 Grupos de Questões (GQ), os quais compreendem questões objetivas sobre cada um dos serviços do GAIA Riscos. Para estar alinhado à ISO 31000, os questionamentos respondem as assertivas da norma. O QAD bem como seus componentes encontram-se disponíveis no Apêndice A desta dissertação.

As questões são de múltipla escolha e possuem um conjunto de alternativas que traduzem objetivamente as situações ocorridas no dia-a-dia das organizações, com o intuito de simplificar o preenchimento do questionário pelos usuários. Além disso, cada alternativa possui um Fator Multiplicativo (FM), o qual quantifica seu impacto em relação à questão que pertence, conforme a proposta de Briganó e Barros [9]. Estes fatores auxiliam no cálculo da taxa de atendimento do serviço, conforme Tabela 3.1.

Tabela 3.1 – Modelo de questão

Questão: As políticas, normas, regulamentações e guias que interferem no sucesso do projeto são documentados?		
Alternativa		**FM**
A	Sempre que necessário ocorre a documentação de políticas, normas, regulamentações e guias. Tais dados são utilizados durante todo desenvolvimento do projeto.	3
B	Sempre que necessário ocorre a documentação de políticas, normas, regulamentações e guias, no entanto estas informações são raramente utilizadas.	2
C	Desconheço esta informação	0
D	Raramente ocorre a documentação de políticas, normas, regulamentações e guias.	-2
E	Não existe documentação de políticas, normas, regulamentações e guias são definidos e documentados de maneira clara e objetiva.	-3

Além da relação entre a questão e suas alternativas, que são os FM, exemplificados na Tabela 3.1, outro importante componente do QAD é o relacionamento entre as questões e os serviços do *framework* GAIA Riscos, o qual é dado por Pesos. Desta forma, uma mesma questão pode influenciar um ou vários serviços ao mesmo tempo. A Tabela 3.2 apresenta a matriz de relacionamento entre uma questão e os pesos que ela pode exercer.

Tabela 3.2 – Peso da questão nos serviços

Questão: As políticas, normas, regulamentações e guias que interferem no sucesso do projeto são documentados?		
Serviço	**Justificativa**	**Peso**
Estabelecer Contexto	A existência destes documentos caracteriza a existência do contexto do GR.	4
Identificar Riscos	Armazenar estes documentos não indica que os riscos são identificados.	0
Analisar Riscos	Recolher estes documentos caracteriza que eles podem ser úteis para compreender os riscos.	1
Avaliar Riscos	A existência destes documentos evidencia que eles podem ser úteis para classificar os riscos.	1
Tratar Riscos	Armazenar estes documentos indica que podem haver restrições a implementação das soluções, logo, evidencia a realização do tratamento.	1
Monitoramento e Controle	O surgimento destes documentos pode ocorrer ao longo de todo ciclo de vida, logo, armazená-los indica que o monitoramento e controle é realizado.	1
Comunicação e Consulta	Recolher os documentos que podem interferir no GR não indica a troca de informações entre as partes.	1

Por meio da associação das Tabelas 3.1 e 3.2 é possível verificar que a questão tomada como exemplo exerce forte influência sobre os serviços *Estabelecer Contexto* e *Identificar Riscos*. Além disso, esta mesma questão afeta moderadamente os serviços *Avaliar Riscos* e *Monitoramento e Controle* e influencia fracamente os serviços de *Avaliar Riscos*, *Tratar Riscos* e de *Comunicação e Consulta*.

A primeira versão do QAD contém 50 questões, sendo 2 subjetivas para coletar informações sobre número de funcionários e faturamento da organização e 48 objetivas, as quais são alocadas no GQ no qual exercem maior influência. Caso uma questão possua mesmo peso para dois grupos, o critério de alocação é aleatório. Para elaborar as respostas do questionário, as diretrizes da ISO 31000 foram fundamentais, pois fornecem os casos ideias esperados para o GR. Os objetivos de cada GQ são melhor detalhados abaixo:

- **GQ1 – Estabelecer o Contexto:** mensurar a existência de elementos como políticas, critérios, métodos, premissas e restrições do GR.

- **GQ2 – Identificar Riscos:** aferir a presença de atividades para identificar as fontes de risco, suas causas, probabilidade de ocorrência e áreas de impacto, bem como sua correta documentação.
- **GQ3 – Analisar Riscos:** avaliar a presença de atividades para filtrar os riscos identificados, mantendo apenas os relevantes aos critérios e parâmetros estabelecidos.
- **GQ4 – Avaliar Riscos:** medir o grau com que as atividades para quantificar os riscos e classificá-los de acordo com sua probabilidade de ocorrência e criticidade estão presentes no PDS.
- **GQ5 – Tratar Riscos:** avaliar a presença e atividades para elaborar e implementar os planos de tratamento, bem como determinar os níveis de aceitação de riscos residuais.
- **GQ6 – Monitoramento e Controle:** aferir a existência de atividades para garantir que o GR está relevante e efetivo frente aos critérios pré-estabelecidos.
- **GQ7 – Comunicação e Consulta:** mensurar o grau com que atividades para garantir que os interesses e os conhecimentos de todos os envolvidos com o projeto sejam entendidos e considerados estão presentes no PDS.

Baseado nas informações coletadas pelas respostas do QAD e seguindo o modelo de questão exposto na Tabela 3.1 e 3.2 obtém-se 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 FM relacionado a alternativa selecionada. A pontuação final, por sua vez, é obtida pela somatória destes produtos para cada serviço.

Para calcular o percentual de atendimento sobre cada serviço, a pontuação final deve ser ajustada com base nos valores extremos do questionário, que determinam o intervalo entre seu maior (VMax) e menor (VMin) valor possível. Para calcular VMax deve-se multiplicar o maior FM de cada questão pelo peso em cada um dos serviços. Para obter o valor total de VMax, somam-se os valores alcançados para cada serviço. Para o exemplo apresentado nas Tabelas 3.1 e 3.2, o maior FM é +3, assim o VMax é calculado conforme a Tabela 3.3.

Tabela 3.3 - Exemplo de cálculo de VMax

Serviço	FM	Peso	Cálculo	Resultado
Estabelecer Contexto	3	4	3 x 4	12
Identificar Riscos	3	0	3 x 0	0
Analisar Riscos	3	1	3 x 1	3
Avaliar Riscos	3	1	3 x 1	3
Tratar Riscos	3	1	3 x 1	3
Monitoramento e Controle	3	1	3 x 1	3
Comunicação e Consulta	3	1	3 x 1	3

De maneira semelhante à exposta na Tabela 3.3, para calcular o VMin deve-se multiplicar o menor FM de cada questão pelo peso em cada um dos serviços. Para obter o valor total de VMin, somam-se os valores alcançados para cada serviço. Para o exemplo, o menor FM é -3, assim o VMin é calculado conforme a tabela 3.4.

Tabela 3.4 – Exemplo de cálculo de VMin

Serviço	FM	Peso	Cálculo	Resultado
Estabelecer Contexto	-3	4	-3 x 4	-12
Identificar Riscos	-3	0	-3 x 0	0
Analisar Riscos	-3	1	-3 x 1	-3
Avaliar Riscos	-3	1	-3 x 1	-3
Tratar Riscos	-3	1	-3 x 1	-3
Monitoramento e Controle	-3	1	-3 x 1	-3
Comunicação e Consulta	-3	1	-3 x 1	-3

Após calcular os valores máximos e mínimos possíveis para cada serviço, faz-se necessário definir uma Faixa de Pontuação (FP), a qual é obtida pela diferença de VMax e VMin. Além disso, o resultado final deve ser ajustado por um Fator de Ajuste (FA) que se dá pela diferença entre 0 e VMin. As Tabelas 3.5 e 3.6 exemplificam FP e FA com base no exemplo apresentado nas Tabelas 3.2 e 3.3.

Tabela 3.5 - Exemplo de FP

Serviço	Cálculo	FP
Estabelecer Contexto	12-(-12)	24
Identificar Riscos	0-0	0
Analisar Riscos	3-(-3)	6
Avaliar Riscos	3-(-3)	6
Tratar Riscos	3-(-3)	6
Monitoramento e Controle	3-(-3)	6
Comunicação e Consulta	3-(-3)	6

Tabela 3.6 - Exemplo de FA

Serviço	Cálculo	FA
Estabelecer Contexto	0-(-12)	12
Identificar Riscos	0-0	0
Analisar Riscos	0-(-3)	3
Avaliar Riscos	0-(-3)	3
Tratar Riscos	0-(-3)	3
Monitoramento e Controle	0-(-3)	3
Comunicação e Consulta	0-(-3)	3

Com isso, torna-se possível calcular o resultado da avaliação diagnóstica, o qual é orientado ao percentual com que a organização atende a cada serviço do *framework*. Assim, realiza-se a somatória do produto entre o peso da questão – para cada serviço – e o FM da alternativa selecionada. Supondo que a alternativa escolhida na questão exposta na Tabela 3.1 tenha sido a B, cujo FM é 2 e os pesos estejam de acordo com a Tabela 3.2, a Tabela 3.7 expõe o cálculo do resultado (R) do FM pelo peso.

Tabela 3.7 - Exemplo de cálculo de resultado

Serviço	Cálculo	R
Estabelecer Contexto	2 x 4	8
Identificar Riscos	2 x 0	0
Analisar Riscos	2 x 1	2
Avaliar Riscos	2 x 1	2
Tratar Riscos	2 x 1	2
Monitoramento e Controle	2 x 1	2
Comunicação e Consulta	2 x 1	2

Para finalizar o cálculo da taxa de atendimento, calcula-se o Resultado Final (RF) do questionário, por serviço. Para tanto, divide-se a somatória das respostas com os FA pela FP. No caso de FP possuir resultado igual a 0 o RF também é 0, visto que a divisão por 0 não existe. A Tabela 3.8 demonstra o RF obtido com base nas Tabelas 3.1, 3.2 e 3.7.

Tabela 3.8 - Exemplo de cálculo de resultado final

Serviço	Cálculo	RF
Estabelecer Contexto	$\frac{8+12}{24} x\,100\%$	83%
Identificar Riscos	$PP = 0$	0%
Analisar Riscos	$\frac{2+3}{6} x\,100\%$	83%
Avaliar Riscos	$\frac{2+3}{6} x\,100\%$	83%
Tratar Riscos	$\frac{2+3}{6} x\,100\%$	83%
Monitoramento e Controle	$\frac{2+3}{6} x\,100\%$	83%
Comunicação e Consulta	$\frac{2+3}{6} x\,100\%$	83%

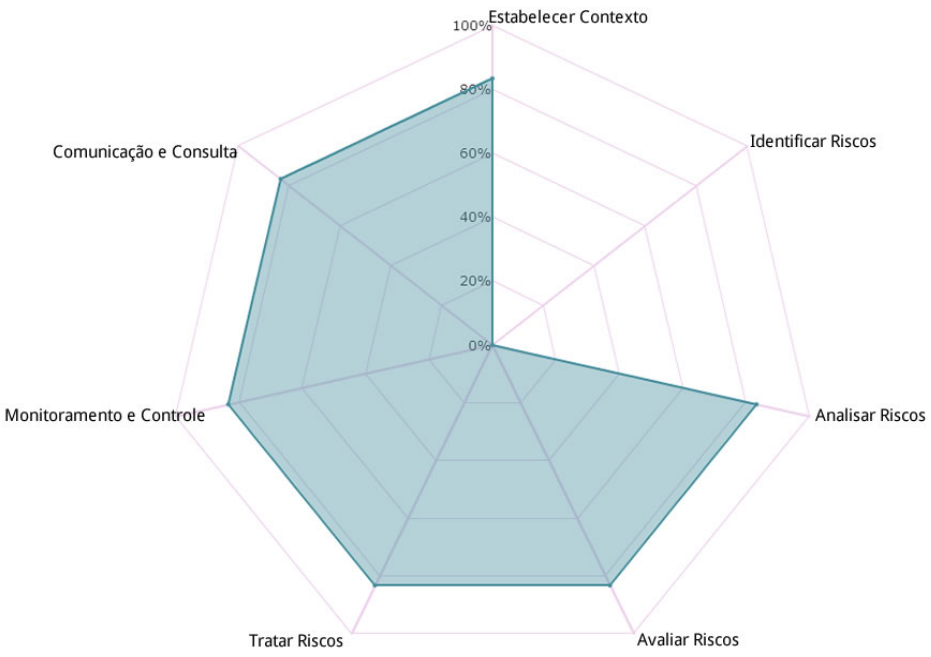
Uma vez determinado o RF de cada serviço, aquele que obteve menor percentual de atendimento determina o grau de maturidade do processo de GR da organização. A Tabela 3.9 expõe os critérios de conversão, os quais foram definidos linearmente e poderão ser alterados futuramente com base nos dados históricos obtidos com a execução do *framework*.

Tabela 3.9 – Tabela de conversão de percentual em nível de maturidade

Nível de Maturidade	Intervalo de Percentual
Nível 1 – Inicial	$0 \leq RF(\%) \leq 20$
Nível 2 – Conhecido	$20 < RF(\%) \leq 40$
Nível 3 – Padronizado	$40 < RF(\%) \leq 60$
Nível 4 – Gerenciado	$60 < RF(\%) \leq 80$
Nível 5 – Otimizado	$80 < RF(\%) \leq 100$

Para demonstrar os resultados obtidos com a aplicação do QAD utiliza-se um gráfico de radar, cujos eixos representam os serviços do *framework* e sua área define os percentuais de atendimento. Desta maneira, tem-se uma visão global sobre os mesmos, facilitando a visualização dos usuários. O gráfico representado pela Figura 3.5 ilustra a conversão dos RFs, conforme citado anteriormente.

Figura 3.5 - Exemplo de gráfico de radar



Para o exemplo adotado, observando-se os RFs expostos na Tabela 3.8, a classificação dos níveis de maturidade da Tabela 3.9 e o gráfico de radar apresentado na Figura 3.5, é possível afirmar que, embora praticamente todos os serviços tenham atendido aos requisitos dos níveis superiores, a baixa aderência ao serviço de *identificação dos riscos* foi determinante para caracterizar o PDS no primeiro nível de maturidade. Para este exemplo hipotético, aderir ao serviço de identificação dos riscos representaria a evolução da organização ao 5º nível de maturidade do GAIA Riscos.

Ressalta-se, ainda, que o exemplo apresentado compreende apenas uma questão, se houvesse outras, valores como VMax, VMin, FP, FA e R seriam acumulados por serviço e alterariam consideravelmente o RF e o gráfico obtidos. Um modelo real de aplicação do QAD está disponível no estudo de caso (Seção 4) desta dissertação.

Para automatizar a coleta das respostas do QAD, o processo de coleta das informações, cálculo do resultado e geração o gráfico de radar um Sistema de Avaliação Diagnóstica (SAD) foi desenvolvido no âmbito da Fábrica de Projetos de Tecnologia de Informação GAIA. A fábrica GAIA é composta por equipes de alunos dos cursos de graduação e pós-graduação do curso de Ciência da Computação do Departamento de Computação (DC) da Universidade Estadual de Londrina (UEL).

O processo de desenvolvimento utilizado na fábrica é prescritivo e foi concebido de forma a atender ao nível F de maturidade do modelo de referência MR-MPS-

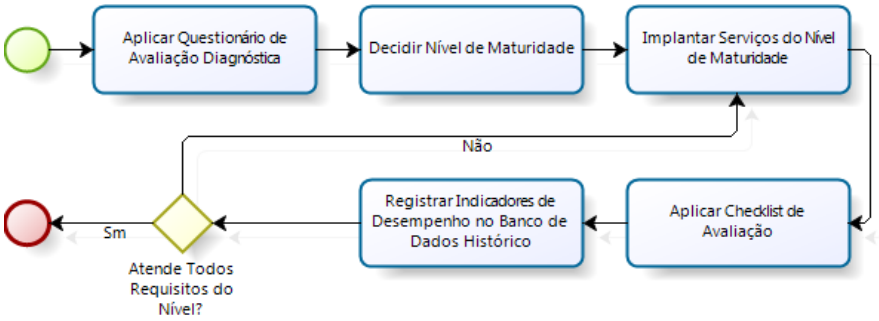
SW [3], com o intuito de padronizar seus processos, aumentar a qualidade do *software* produzido, satisfação do cliente e a produtividade da equipe.

O SAD encontra-se disponível no portfólio de projetos da fábrica e pode ser acessado pelo endereço http://www.gaia.uel.br/gaia_ad/.

3.4 PROCESSO DE IMPLANTAÇÃO

Para aplicar o *framework* GAIA Riscos em um PDS algumas atividades devem ser seguidas. Tais procedimentos buscam determinar o nível de maturidade do PDS, reavaliar sua aderência a um determinado nível e mensurar sua capacidade de evolução para níveis superiores. As atividades que compõe o Processo de Implantação (PI) do GAIA Riscos são ilustradas pela Figura 3.6.

Figura 3.6 - Processo de implantação do GAIA Riscos



Conforme pode-se observar na Figura 3.6, a entrada do PI é o preenchimento do QAD, o qual é deve ser respondido eletronicamente por meio do SAD. Após esta etapa, decide-se o nível de maturidade com base nos critérios expostos na Tabela 3.9 e implantam-se os serviços necessários para o nível alcançado. Para avaliar se todos os serviços foram atendidos, aplica-se o *checklist* de avaliação.

O *checklist* de avaliação, por sua vez, possui uma série de questões que devem ser atendidas com Totalmente Implementado (T), Parcialmente Implementado (P) ou Não Implementado (N). Mediante a escala obtida durante o preenchimento desta lista de verificação, caso a escala obtida seja P ou N, necessita-se rever o PDS para incorporar as atividades remanescentes, caso contrário o PDS atende aos requisitos. Os *checklists* encontram-se disponíveis nos apêndices B à E deste trabalho.

Como, além de implantar o GR em um PDS o GAIA Riscos também busca garantir a melhoria contínua das atividades, uma vez aplicado o *checklist* de avaliação,

indicadores de desempenho devem ser registrados. Além disso, por meio deles é possível criar um Banco de Dados Histórico (BDH) da organização sobre a evolução do processo de GR neste PDS. A Tabela 3.10 exemplifica a estrutura dos indicadores de desempenho, a qual se baseia nas diretrizes do BSC [41].

Tabela 3.10 – Indicador de total de riscos identificados por pontos de caso de uso

Característica	**Descrição**
Identificador:	TRI
Nome:	Total de Riscos Identificados por pontos de caso de uso
Objetivo da Medição:	Acompanhar o número absoluto de riscos identificados em cada nível de maturidade.
Objetivo de Negócio Associado:	Detectar o maior número possível de riscos.
Fórmula:	TRI = Número Total de Riscos Identificados.
Interpretação da Medição:	Quanto mais riscos identificados menor a chance de surpresas ao longo do ciclo de vida do projeto.
Responsável pela Medição:	Gerente de Projeto
Frequência da Medição:	Sempre, após a aplicação do *checklist* de avaliação.
Fonte de Dados:	Lista de riscos identificados.
Unidade de Medida:	Número inteiro
Meta:	Detectar o maior número possível de riscos.
Público Alvo:	As medições devem ser apresentadas a todos *stakeholders*.
Frequência de Análise:	Sempre que houver a medição do TRI
Responsável pela Análise:	Gerente de Projeto
Método de Análise:	Analisar o TRI comparando-o com os dados do banco de dados histórico da organização.

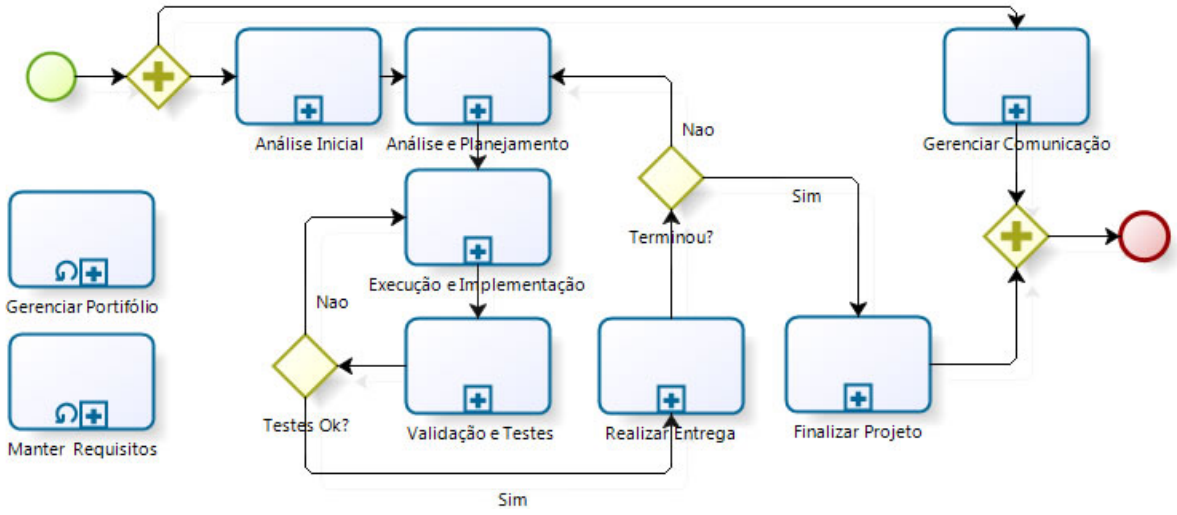
Fonte: Elaborada pelos autores com base na proposta de Niven [41].

Por fim, ao término do PI verifica-se o *checklist* preenchido. Caso existam objetivos não contemplados, torna-se necessário adotar medidas para atendê-los. Ao atingir todas as exigências o usuário pode realizar uma nova iteração do PI para aderir a um novo nível de maturidade do GAIA Riscos.

4 ESTUDO DE CASO

Para verificar e validar o *framework* GAIA Riscos, seu Processo de Implantação (PI) foi executado, iterativamente, até que o Processo de Desenvolvimento de *Software* da Fábrica GAIA (PDSG) da UEL alcançasse o quinto nível de maturidade, ou seja, a excelência. As atividades foram desenvolvidas em quatro iterações realizadas durante a implementação de dois projetos em um período de seis meses. A Figura 4.1 ilustra os componentes do PDSG.

Figura 4.1 - Processo de Desenvolvimento de *Software* da Fábrica GAIA (PDSG)



Fonte: Retirado de [15]

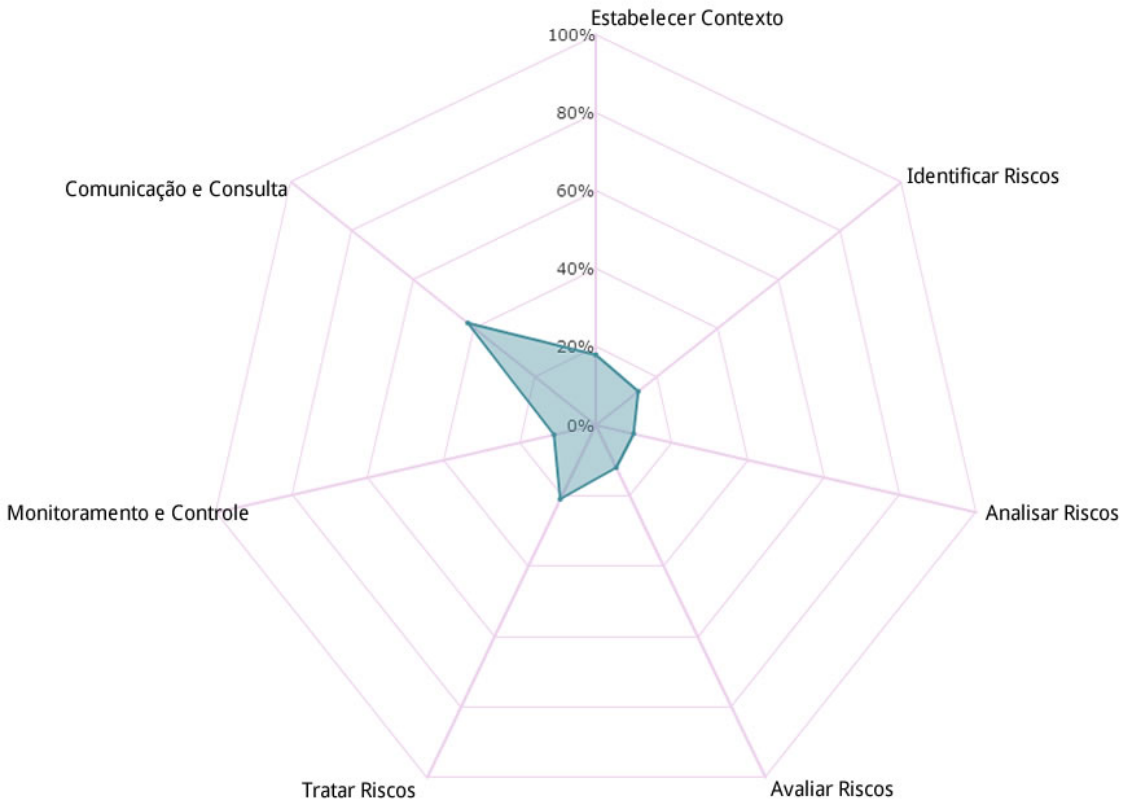
Conforme a representação gráfica do PDSG na Figura 4.1, é possível verificar a presença de nove atividades, cada qual composta por fluxos de trabalho, papéis e artefatos. Tais atividades envolvem ações para identificar as premissas do projeto, expandir sua estrutura, estimar prazos e custos, elaborar os planos de gerenciamento, gerir a troca de informações, identificar novos requisitos, implementar as entregas, testar e validar o *software*, integrar as partes desenvolvidas e administrar o portfólio de produtos da organização.

Como o objetivo deste estudo de caso foi verificar e validar o *framework* GAIA Riscos, as atividades realizadas foram conduzidas em ambiente acadêmico e contaram com participação direta do autor desta dissertação. Desta forma, as alterações realizadas no PDSG limitaram-se ao tempo para conclusão do programa de Mestrado, não representando os esforços necessários para implantar o GAIA Riscos em um ambiente real de produção.

Para iniciar a aplicação do GAIA Riscos, o PDSG foi submetido a uma avaliação do Sistema de Avaliação Diagnóstica (SAD), conforme indicado no PI. As

informações coletadas indicaram a ausência de atividades para administrar os riscos do projeto, ou seja, de acordo com os níveis de maturidade do GAIA Riscos o processo da fábrica encontrava-se no primeiro nível de maturidade. A Figura 4.2 expõe o gráfico obtido por meio da análise realizada.

Figura 4.2 - Gráfico com resultado obtido na primeira execução do SAD



Como ilustrado pela Figura 4.2, o maior nível alcançado foi para o serviço de comunicação e consulta. Este resultado evidencia que o PDSG já contempla atividades para comunicar os interessados sobre o andamento do projeto, as quais atendem aos requisitos do Gerenciamento de Riscos (GR). A Tabela 4.1 expõe os percentuais obtidos para cada serviço.

Tabela 4.1 - Taxa de atendimento obtida na avaliação inicial do PDSG

Serviço	Taxa de Atendimento
Estabelecer o Contexto	18%
Identificar os Riscos	14%
Analisar os Riscos	10%
Avaliar os Riscos	12%
Tratar os Riscos	21%
Monitoramento e Controle	11%
Comunicação e Consulta	42%

Conforme é possível observar na Tabela 4.1, os percentuais para os demais serviços não obtiveram taxa de atendimento superior a 42%. Embora este índice, obtido pelo serviço de comunicação e consulta, seja suficiente para alcançar o terceiro nível, o PDSG encontra-se no primeiro nível de maturidade do GAIA Riscos, uma vez que o serviço com menor taxa de atendimento determina o nível de maturidade de todo o processo.

Neste contexto, para validar os níveis de maturidade do *framework*, primeiramente, um projeto para registrar as interações dos alunos em objetos de aprendizagem foi utilizado, nesta etapa as alterações foram realizadas para que o PDSG evoluísse do primeiro para o segundo nível de maturidade. Para isso, referências ao serviço de identificação dos riscos foram adicionadas nas instruções de trabalho da atividade de Análise e Planejamento. Os indicadores coletados no PI foram armazenados no banco de dados histórico da organização.

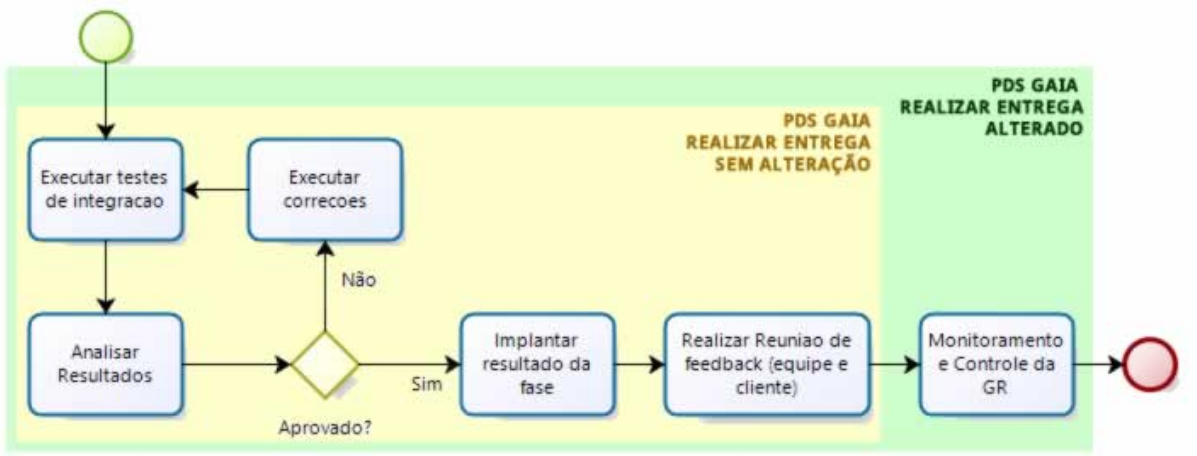
No entanto, após realizar as modificações no processo da fábrica, a equipe percebeu a necessidade de atividades para compreender, avaliar e tratar os riscos. Como consequência, a progressão para terceiro nível de maturidade fez-se necessária. Para tanto, um projeto para controle dos associados e submissão e avaliação de artigos, desenvolvido para a Associação Brasileira de Ensino Odontológico (ABENO) foi utilizado (disponível em http://sistema.abeno.org.br/).

Novamente, o PDSG foi submetido a uma nova iteração do PI do GAIA Riscos. Como resultado, a inclusão de três novas atividades foi sugerida. Primeiramente, a atividade de Análise Inicial foi alterada para referenciar-se ao serviço de Estabelecimento do Contexto. Em seguida, as referências previamente adicionadas a etapa de Análise e Planejamento foram substituídas por uma atividade específica para Identificar, Analisar e Avaliar os Riscos. Por conseguinte, uma atividade para Tratar os Riscos do projeto foi

adicionada à etapa de Execução e Implementação. Ao término desta iteração do PI os indicadores de desempenho foram registrados.

A partir das alterações realizadas as etapas básicas para gerenciar os riscos estavam presentes no PDSG. Contudo, após realizar algumas iterações, observou-se a necessidade de métricas comparativas para demonstrar a efetividade do GR. A progressão para o quarto nível de maturidade fez-se necessária. A Figura 4.3 representa a modificação realizada para incluir o monitoramento e controle do GR ao PDSG, a qual foi executada na etapa denominada Realizar Entrega.

Figura 4.3 – Alteração realizada na atividade Realizar Entrega do PDSG



Após realizar esta modificação no PDSG, a equipe observou a necessidade de melhorar a integração entre a equipe do projeto e o cliente, tanto para informar o andamento das ações quanto para esclarecer e trocar informações sobre os riscos do projeto. Deste modo, iniciaram-se as ações para evoluir o PDSG para o quinto nível de maturidade do GAIA Riscos. Como resultado, referências para o serviço de Comunicação e Consulta foram adicionadas as instruções de trabalho da etapa Gerenciar Comunicação. A Tabela 4.2 sintetiza todas as alterações realizadas no PDSG.

Tabela 4.2 - Síntese das alterações realizadas no PDSG

Atividade do PDSG	Tipo de Alteração	Serviços Referenciados
Análise Inicial	Instrução de Trabalho	Estabelecer o Contexto
Análise e Planejamento	Inclusão de Atividade	Identificar, Analisar e Avaliar os 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

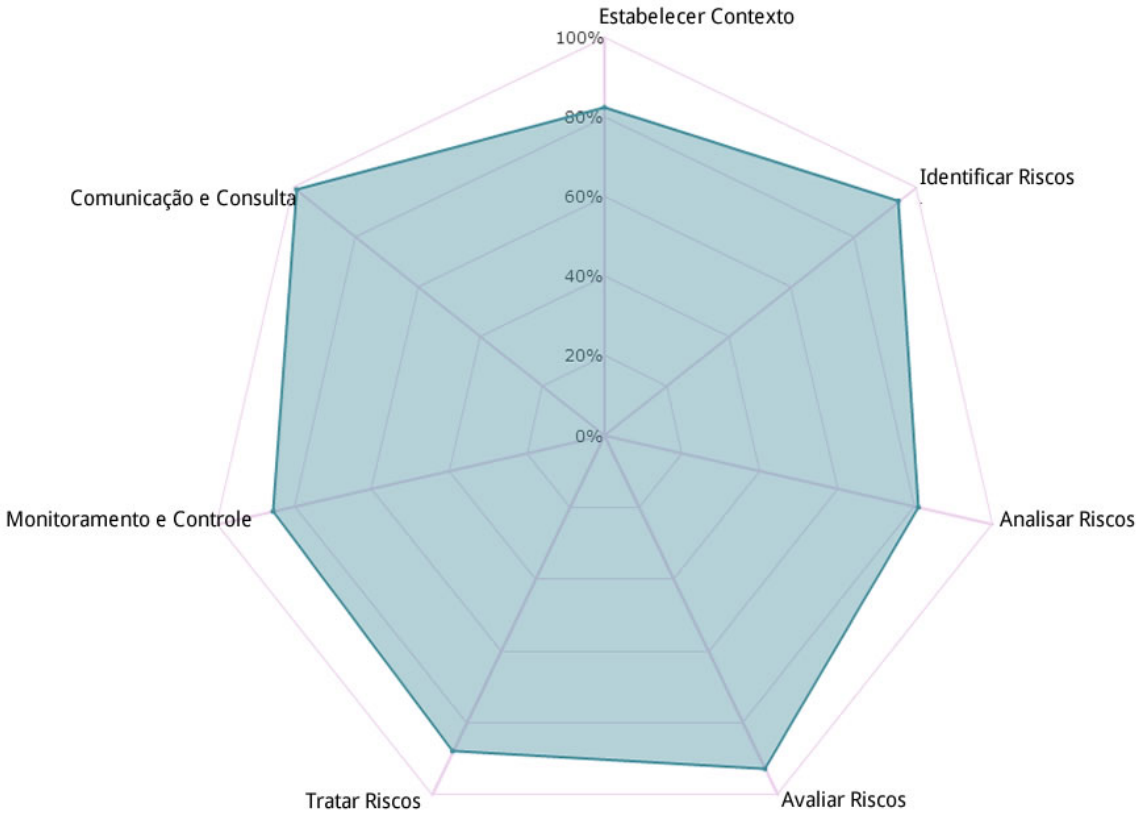
Após realizar todas as alterações expostas na Tabela 4.2 e com o intuito de identificar se os esforços realizados alcançaram o objetivo de evoluir o PDSG à excelência na gestão dos riscos, uma nova avaliação foi conduzida no SAD. A Tabela 4.3 apresenta a evolução em Pontos Percentuais (p.p.) entre os dados iniciais e finais obtidos.

Tabela 4.3 - Comparação entre a taxa de atendimento inicial e final.

Serviço	Taxa Inicial	Taxa Final	Evolução
Estabelecer o Contexto	18%	82%	64 p.p.
Identificar os Riscos	14%	94%	80 p.p.
Analisar os Riscos	10%	80%	70 p.p.
Avaliar os Riscos	12%	92%	80 p.p
Tratar os Riscos	21%	87%	66 p.p.
Monitoramento e Controle	11%	85%	74 p.p.
Comunicação e Consulta	42%	98%	56 p.p.

A partir dos dados expostos na Tabela 4.3, é possível verificar que, por meio das mudanças realizadas, o PDSG passou a atender, com mais de 80%, todos os serviços do GAIA Riscos, aderindo assim ao quinto nível de maturidade do *framework*, ou seja, a excelência no GR. A Figura 4.4 ilustra o gráfico de radar obtido por meio da avaliação final.

Figura 4.4 - Gráfico de resultado obtido após as alterações realizada no PDSG



Para aderir a um nível de maturidade, os *checklists* de reavaliação precisaram ser preenchidos a cada iteração do PI. No total, quatro listas de verificação precisaram ser preenchidas, uma para cada etapa de evolução. No entanto, a evolução do segundo para o terceiro nível de maturidade foi considerada a mais problemática, uma vez que alterou várias atividades do PDSG. Por fim, para somar a este estudo de caso, as seções 4.1 e 4.2 apresentam os principais riscos identificados e os indicadores de desempenho coletados durante este estudo de caso, respectivamente.

4.1 GERENCIAMENTO DE RISCOS E DISCUSSÕES

No decorrer da elaboração desta dissertação dois projetos da fábrica GAIA foram utilizados para verificar e validar o estudo, o primeiro consiste em uma aplicação para registrar interações em objetos de aprendizagem (Projeto A) e o segundo um *software* para controlar os associados da ABENO (Projeto B). Por meio das mudanças implementadas, foi possível coletar e armazenar diversos riscos, os quais podem ser visualizados na Tabela 4.4.

Tabela 4.4 - Principais riscos coletados nos Projetos A e B

	ID - Risco
Projeto A	A1 - Falta de familiaridade com as ferramentas e tecnologias envolvidas
	A2 - Membros da equipe que abandonaram o projeto
	A3 - Rotatividade de alunos dentro da equipe
	A4 - Prazo curto para entrega do sistema
Projeto B	B1 - Atrasos nos compromissos por parte do cliente
	B2 - Falta de infraestrutura no ambiente de implantação do cliente
	B3 - Dificuldade do cliente em expressar suas necessidades.
	B4 - Inexperiência do cliente na utilização de recursos computacionais
	B5 - Membros da equipe não familiarizados com as regras de negócio do cliente
	B6 - Baixa produtividade devido ao não conhecimento das regras de negócio
	B7 - Desmotivação da equipe
	B8 - Conhecimento centrado em poucos membros da equipe
	B9 - Mudanças nos alunos da equipe do projeto
	B10 - Prazo curto para entrega do sistema
	B11 - Mudança de escopo do projeto
	B12 - Mudanças contínuas de requisitos
	B13 - Requisitos mal entendidos ou definidos
	B14 - Necessidade de integração entre sistemas com tecnologias diferentes

De acordo com os dados apresentados na Tabela 4.4, é possível verificar que vários foram os riscos identificados durante as etapas da aplicação do GAIA Riscos sob o PDSG, demonstrando a importância desta gerência independentemente do tamanho do projeto. Desta forma, também é possível verificar que os riscos identificados afetaram diversas áreas do projeto, passando por escopo, tempo, recursos humanos e requisitos, principalmente.

Durante a aplicação do GAIA Riscos alguns riscos se concretizaram, dentre os quais destacam-se a mudança do escopo do projeto por mais de uma vez e as mudanças contínuas nos requisitos pelo cliente, fatos que geraram retrabalhos indesejados, prejudicaram o cronograma e o orçamento do projeto. Outro problema verificado foi o mal entendimento dos requisitos tanto pelos gerentes quanto pela equipe de desenvolvimento.

Contudo, ao adotar metodologias para troca de informações sobre os riscos, o entendimento entre as partes e o número de retrabalhos realizados melhorou

consideravelmente. Ressalta-se, ainda, que a mudança contínua nos requisitos era esperada e foi prevista aos planos do projeto, uma vez que a ABENO possui membros e representantes espalhados em várias cidades e instituições de ensino do Brasil.

No decorrer da execução do Projeto B, ainda, a equipe notou a necessidade de compreender as influências dos riscos sob o projeto, classificando-os de acordo com sua probabilidade de ocorrência e impacto previstos. Para completar o GR também foi necessário monitorar os riscos em cada iteração do PDSG bem como trocar informações com as partes interessadas sempre que necessário.

A partir das ações desenvolvidas para aderir ao GAIA Riscos, novas atividades e algumas referências foram adicionadas ao PDSG. Como resultado, a fábrica GAIA passou a utilizar planilhas para analisar a probabilidade e impacto dos riscos, atas de reuniões, relatos de entrevistas, relatórios de acompanhamento dos riscos e evidências da troca de informações entre os interessados. Tais ações trouxeram mais segurança para a equipe e para o cliente, diminuindo a incidência de retrabalhos, conforme pode ser observado pelos indicadores apresentados na Seção 4.2.

4.2 INDICADORES DE DESEMPENHO

Ao término de cada iteração do PI do GAIA Riscos, os indicadores de desempenho foram armazenados. O primeiro indicador representa o total de riscos tratados/mitigados nos Projetos A e B. A Tabela 4.5 apresenta as especificações deste indicador de desempenho.

Tabela 4.5 – Indicador de riscos tratados/mitigados

Característica	Descrição
Identificador:	RTM.
Nome:	Riscos Tratados ou Mitigados.
Objetivo da Medição:	Definir a porcentagem de riscos que, depois de identificados, são tratados/mitigados para servir de base para estimativas em novos projetos da organização e manter informações sobre a efetividade do processo de tratamento dos riscos.
Objetivo de Negócio Associado:	Identificar o percentual de riscos tratados/mitigados durante o planejamento e a execução dos projetos da organização.
Fórmula:	TRI = Total de Riscos Identificados; TTM = Total de Riscos Tratados/Mitigados; O resultado é dado por: R = TTM / TRI.
Interpretação da Medição:	São vários os riscos coletados ao longo do planejamento e execução de um projeto. Neste ponto, o indicador resulta na porcentagem de riscos que são efetivamente tratados/mitigados. Assim, quanto maior o resultado obtido, mais eficiente é o tratamento dos riscos.
Responsável pela Medição:	Gerente do projeto.
Frequência da Medição:	A medição deverá ser realizada a cada iteração do processo de desenvolvimento de *software.*
Fonte de Dados:	Plano de gerenciamento de riscos; Documentos de análise e avaliação dos riscos; Relatórios de Tratamentos dos Riscos.
Unidade de Medida:	Porcentagem.
Meta:	Tratar ou mitigar o maior número possível de riscos.
Tolerância:	A tolerância é influenciada por diversos fatores do projeto como cliente, equipe ou tecnologias envolvidas. Não recomenda-se que a porcentagem de riscos tratados/mitigados seja inferior a 50%.
Público-alvo:	As medições devem ser disponibilizadas aos gerentes de projeto, membros da equipe e cliente.
Frequência da Análise:	A análise dos dados coletados deve ser realizada a cada iteração do processo de desenvolvimento de *software.*
Responsável pela Análise:	Gerente do projeto.
Método da Análise:	A porcentagem obtida será analisada pelo gerente do projeto e disponibilizada em um gráfico de barras para o público-alvo.

Além do percentual dos riscos tratados/mitigados também foram coletados outros indicadores, os quais possuem especificações semelhantes as apresentadas na Tabela 4.5. O de total de riscos aceitos/transferidos, especificado na Tabela 4.6, indica a porcentagem do riscos que não foram tratados/mitigados.

Tabela 4.6 – Indicador de total de riscos aceitos/transferidos

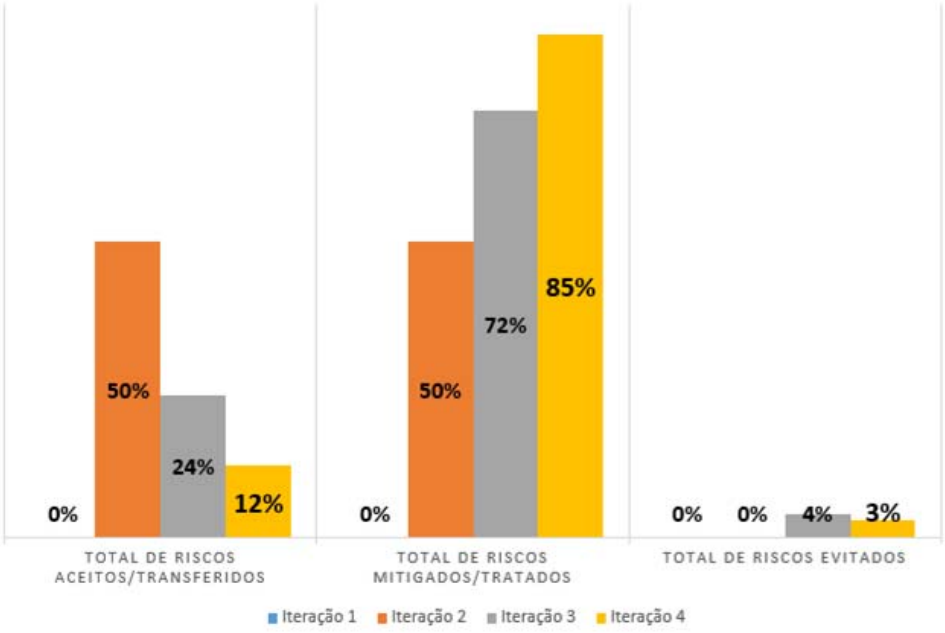
Característica	**Descrição**
Identificador:	RAT.
Nome:	Riscos Aceitos ou Transferidos.
Objetivo da Medição:	Definir a porcentagem de riscos que, depois de identificados, são aceitos/transferidos para servir de base para estimativas em novos projetos da organização e manter informações sobre a efetividade do processo de tratamento dos riscos.
Objetivo de Negócio Associado:	Identificar o percentual de riscos aceitos/transferidos durante o planejamento e a execução dos projetos da organização.
Fórmula:	TRI = Total de Riscos Identificados; TAT = Total de Riscos Aceitos/Transferidos; O resultado é dado por: R = TAT / TRI.
Interpretação da Medição:	São vários os riscos coletados ao longo do planejamento e execução de um projeto. Neste ponto, o indicador resulta na porcentagem de riscos que são aceitos/transferidos. Assim, quanto menor o resultado obtido, mais eficiente é o processo de tratamento dos riscos.
Responsável pela Medição:	Gerente do projeto.
Frequência da Medição:	A medição deverá ser realizada a cada iteração do processo de desenvolvimento de *software.*
Fonte de Dados:	Plano de gerenciamento de riscos; Documentos de análise e avaliação dos riscos; Relatórios de Tratamentos dos Riscos.
Unidade de Medida:	Porcentagem.
Meta:	Aceitar ou Transferir o menor número de riscos possível.
Tolerância:	A tolerância é influenciada por diversos fatores do projeto como cliente, equipe ou tecnologias envolvidas. Não recomenda-se que a porcentagem de riscos aceitos/transferidos seja superior a 10%.
Público-alvo:	As medições devem ser disponibilizadas aos gerentes de projeto, membros da equipe e cliente.
Frequência da Análise:	A análise dos dados coletados deve ser realizada a cada iteração do processo de desenvolvimento de *software.*
Responsável pela Análise:	Gerente do projeto.
Método da Análise:	A porcentagem obtida será analisada pelo gerente do projeto e disponibilizada em um gráfico de barras para o público-alvo.

Outro indicador de grande relevância para validar a efetividade do GR é o indicador de riscos evitados que, por sua vez, apresenta a porcentagem de mudanças realizadas nos planos do projeto. A Tabela 4.7 especifica este indicador.

Característica	Descrição
Identificador:	RE.
Nome:	Riscos Evitados.
Objetivo da Medição:	Definir a porcentagem de riscos que foram evitados por meio de alterações nos planos do projeto, com o intuito de servir de base para estimativas em novos projetos da organização e manter informações sobre a efetividade do processo de tratamento dos riscos.
Objetivo de Negócio Associado:	Identificar o percentual de riscos evitados durante o planejamento e a execução dos projetos da organização.
Fórmula:	TRI = Número Total de Riscos Identificados; TE = Número Total de Riscos Evitados; O resultado é dado por: R = TE / TRI.
Interpretação da Medição:	São vários os riscos coletados ao longo do planejamento e execução de um projeto. Neste ponto, o indicador resulta na porcentagem de riscos que são evitados por meio de mudanças realizadas nos planos do projeto. Assim, quanto menor o resultado obtido, menor é o número de mudanças e mais eficiente é o tratamento dos riscos.
Responsável pela Medição:	Gerente do projeto.
Frequência da Medição:	A medição deverá ser realizada a cada iteração do processo de desenvolvimento de *software.*
Fonte de Dados:	Plano de gerenciamento de riscos; Documentos de análise e avaliação dos riscos; Relatórios de Tratamentos dos Riscos.
Unidade de Medida:	Porcentagem.
Meta:	Evitar o menor número de riscos possível.
Tolerância:	A tolerância é influenciada por diversos fatores do projeto como cliente, equipe ou tecnologias envolvidas. Não recomenda-se que a porcentagem de riscos evitados seja superior a 5%.
Público-alvo:	As medições devem ser disponibilizadas aos gerentes de projeto, membros da equipe e cliente.
Frequência da Análise:	A análise dos dados coletados deve ser realizada a cada iteração do processo de desenvolvimento de *software.*
Responsável pela Análise:	Gerente do projeto.
Método da Análise:	A porcentagem obtida será analisada pelo gerente do projeto e disponibilizada em um gráfico de barras para o público-alvo.

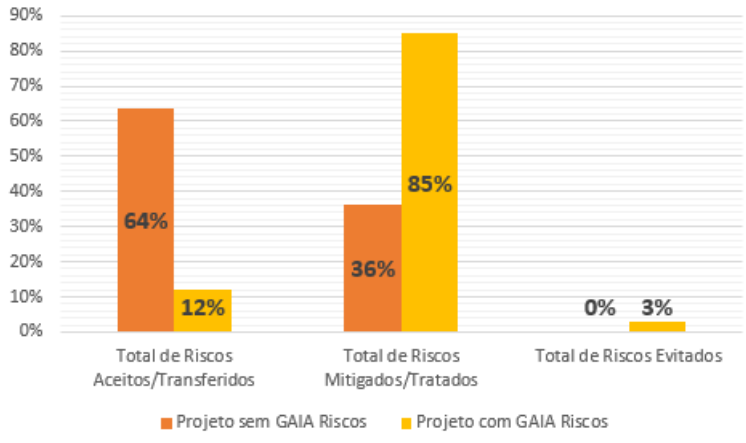
Para ilustrar a evolução dos indicadores especificados nas Tabelas 4.5, 4.6 e 4.7, os percentuais obtidos em cada iteração do PI do GAIA Riscos foram confrontados. O resultado ilustrado pela Figura 4.5 representa a evolução do PDSG obtida durante a realização deste estudo de caso.

Figura 4.5 - Comparativo dos indicadores de desempenho coletados



Por fim, para evidenciar as contribuições que a adoção do GAIA Riscos trouxe ao PDSG, os indicadores de riscos tratados/mitigados, aceitos/transferidos e evitados foram confrontados com dados do banco de dados histórico da fábrica GAIA. A Figura 4.5 apresenta o resultado desta análise comparativa.

Figura 4.6 - Comparativo entre projetos com e sem o GAIA Riscos



De acordo com os dados expostos no gráfico apresentado na Figura 4.5, é possível constatar que antes de adotar as práticas propostas pelo GAIA Riscos, em média 11 riscos eram identificados, dos quais apenas 36% eram mitigados/tratados e 64% aceitos/transferidos. Após a implementação do *framework*, em um projeto com dimensões semelhantes, 33 riscos foram identificados, dos quais 85% foram tratados/mitigados, 12% aceitos/transferidos e 3% evitados.

5 CONCLUSÕES E TRABALHOS FUTUROS

Este capítulo relata as conclusões obtidas por meio da realização desta pesquisa, assim como as principais contribuições e resultados alcançados para a área de Gerenciamento de Riscos (GR) no Processo de Desenvolvimento de *Software* (PDS) – Seções 5.1 e 5.2. Em seguida, a Seção 5.3, apresenta os trabalhos futuros relacionados a continuidade do estudo. Por fim, na Seção 5.4, são feitas as considerações finais desta dissertação.

5.1 CONCLUSÕES

Adotar metodologias para gerir os riscos dos projetos em uma organização de desenvolvimento de *software* é imprescindível frente aos desafios impostos pelo mercado atual. Desta forma, implementar estas ações não só protege a empresa como também evita problemas de especificação do produto, retrabalhos desnecessários, atrasos no cronograma ou até o cancelamento do projeto.

Além disso, mesmo com as abordagens encontradas na literatura (expostas na Seção 2), existem lacunas que permitem evoluir os modelos existentes apresentando um conjunto de serviços, questionamentos e *checklists* de reavaliação para descobrir o grau de maturidade do GR, possibilitando a implantação das atividades, de maneira gradativa e incremental dentro de uma organização de desenvolvimento de *software*.

Neste contexto, esta dissertação teve como finalidade preencher estas deficiências apresentando o *framework* para gerenciar riscos denominado GAIA Riscos, o qual baseia-se em serviços e níveis de maturidade para facilitar a implantação desta gerência. Este *framework* é resultado direto do estudo realizado e permite que os gerentes de projeto avaliem um PDS, obtenham serviços relacionados ao nível de maturidade alcançado e desenvolvam planos para evoluir para os próximos níveis.

Por meio da análise dos resultados obtidos com o estudo de caso realizado (Seção 4), pode-se afirmar que esta pesquisa atingiu o objetivo delimitado na Seção 1, representando uma excelente alternativa para aplicar as atividades do GR a um PDS, possibilitando avaliar os processos desta gerência para classificá-los em uma escala de cinco níveis de maturidade. Portanto, a elaboração deste modelo vai diretamente de encontro ao objetivo estabelecido para este trabalho.

5.2 CONTRIBUIÇÕES

A contribuição de maior relevância desta pesquisa é a elaboração de uma estrutura inovadora, denominada GAIA Riscos, cuja principal característica é a capacidade de permitir a melhoria contínua no GR em uma organização de desenvolvimento de *software*, aumentando a chance de sucesso dos projetos. Também são contribuições importantes do trabalho:

- Os sete Serviços (*Estabelecer o Contexto do GR*, *Identificar Riscos*, *Analisar Riscos*, *Avaliar Riscos*, *Tratar Riscos*, *Monitoramento e Controle* e *Comunicação e Consulta*) que compõe o GR, bem como a organização das áreas de conhecimento provenientes de guias e normas amplamente utilizados pela comunidade de gerenciamento de projetos.
- Um Questionário de Avaliação Diagnóstica (QAD) composto de 50 questões, sendo 48 objetivas e 2 subjetivas, que abrange as atividades do processo de GR e que possibilita identificar as deficiências do PDS avaliado.
- Os cinco níveis de maturidade (*Inicial*, *Conhecido*, *Padronizado*, *Gerenciado* e *Otimizado*) que representam os patamares de evolução do PDS e possibilitam a implantação total ou parcial das atividades desta gerência, de acordo com os interesses da organização.
- Um Processo de Implantação (PI) definido que estabelece uma sequência lógica para incorporar as atividades de GR ao PDS da organização, possibilitando, inclusive, a coleta de métricas.
- Quatro *checklists* de reavaliação que permitem revisar a aderência do PDS a um determinado nível de maturidade, bem como identificar as áreas de serviço que necessitam ser incorporadas para atender a um nível específico.

5.3 TRABALHOS FUTUROS

Muitas atividades e pesquisas foram desenvolvidas no decorrer da elaboração desta dissertação, as quais focaram-se em identificar as atividades necessárias para constituir um *framework* para gerenciar riscos por meio de serviços e que ajude as

organizações a reduzirem o número de falhas dentro do ambiente de desenvolvimento de *software*. No entanto, ainda existem trabalhos a serem realizados:

- Realizar estudos de caso em empresas de desenvolvimento de *software* de pequeno, médio e grande porte, com a finalidade de aprimorar a estrutura do *framework*, serviços, áreas de serviço, QAD e Sistema de Avaliação Diagnóstica (SAD).
- Investigar formas para adaptar o *framework* GAIA Riscos e seus componentes em outros domínios que não o desenvolvimento de *software*, como, por exemplo, a Governança de Tecnologia da Informação e Comunicação (TIC).
- Investigar e avaliar o GAIA Riscos sob a ótica das metodologias ágeis, bem como trabalhar a agilidade no GR dentro de ambientes de desenvolvimento de *software*.
- Realizar melhorias no SAD para permitir a comparação dos resultados obtidos com as informações armazenadas no banco de dados do sistema, além de incrementar novos relatórios gerenciais.

5.4 CONSIDERAÇÕES FINAIS

O processo de GR compreende atividades imprescindíveis para as organizações modernas, aumentando sua capacidade em lidar com os riscos inerentes aos projetos. De uma forma geral, atualmente, poucas são as empresas que investem seus recursos para capacitar suas equipes e aderir à metodologias para administrar os riscos, criando, assim, estigmas ao setor de desenvolvimento de *software*.

A medida em que as organizações que desenvolvem produtos de *software* se conscientizarem desta realidade, a relação custo-benefício para implantar estas atividades tornar-se-á favorável, uma vez que os custos envolvidos serão ínfimos se comparados aos benefícios que protegerão seus recursos humanos, materiais, financeiros e ambientais.

Somado a isto, a crescente ênfase dada ao termo desenvolvimento sustentável, o qual revela a necessidade de conciliar o desenvolvimento econômico com a redução de desperdícios e aumento da proteção dos recursos humanos e ambientais, torna evidente o quanto o GR pode contribuir para o setor de desenvolvimento de *software*. É necessário investir em prevenção de falhas para tornar as organizações mais competitivas.

Portanto, é necessário investir em metodologias que possibilitem antever o acontecimento de erros ou falhas, tornando assim as organizações mais competitivas, ou seja, empregar metodologias para gerenciar os riscos dos projetos de *software*.

REFERÊNCIAS

[1] ALDENUCCI, M. G. **Um modelo de maturidade para processos de gerenciamento de riscos em projetos**. Dissertação (Mestrado em Engenharia de Produção e Sistemas) – Pontifícia Universidade Católica do Paraná, Curitiba, 2009.

[2] ALHAWARI, S.; KARADSHEH, L.; TALET, A. N. Knowledge-Based Risk Management Framework for Information Technology Project. In: **Fifith International Conference on Knowledge**, p. 203-204. 2009.

[3] Associação para Promoção da Excelência do Software Brasileiro. **Guia Geral de Software**. Brasília: SOFTEX. Agosto, 2012.

[4] BANNERMAN, P. L. Risk and risk management in software projects: A reassessment. **Journal of Systems and Software**, v. 81, n. 12, 2008. p. 2118-2133.

[5] BENTLEY, C. **PRINCE2:** a practical handbook. 3 ed. Burlington, Elsevier: Butterworth-Heinemann, 2012.

[6] BOEHM, B. W. **Software engineering economics**. 1 ed. Nova Iorque: Prentice Hall. 1981. 767p.

[7] BOEHM, B. W. **Software risk management:** principles and practices. IEEE Software. IEEE Computer Society Press. 1989.

[8] BOEHM, B. W.; DE MARCO, T. **Software Risk Management**. IEEE Software. IEEE Computer Society Press. 1997. p. 17-19.

[9] BRIGANO, G. U.; BARROS, R. M. Aprendizado de TI: Um modelo para melhorar o aprendizado de TI nas organizações. In: VII SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO. **Anais…** 2011.

[10] CHEMUTURY, M.; CAGLEY JUNIOR, T. M. **Mastering software project management:** Best Practices, Tools and Techniques. 2 ed. Fort Lauderdale: J. Ross Publishing. 2010.

[11] CHINBAT, U.; TAKAKUWA, S. *Using* Simulation Analysis for Mining Project Risk Management. In: **Proceedings of the 2009 Winter Simulation Conference**. 2009. p. 2612-2623.

[12] DEMING, J. E. **Out of the Crisis.** Cambridge: Cambridge University Press, 1986.

[13] DINSMORE, C.; CAVALIERI, A. **Como se Tornar um Profissional em Gerenciamento de Projetos:** livro-base de "preparação para certificação pmp". Rio de Janeiro: Qualitymark, 2003.

[14] EHSAN, N.; PERWAIZ, A.; ARIF, J. CMMI / SPICE Based Process Improvement. In: **International Conference in Management of Innovation and Technology**. P 859-862. 2010.

[15] GAFFO, F. H.; BARROS, R. M. GAIA Risks – A service-based framework to manage Project risks. In: 2012 XXXVIII CONFERENCIA LATINOAMERICANA EN INFORMATICA (CLEI), Medellin. **Anais...** 2012.

[16] GIL, A. C. **Como elaborar projetos de pesquisa.** 4 ed. São Paulo: Atlas, 2006.

[17] GUSMÃO, C. **Um modelo de processo de gestão de riscos para ambientes de múltiplos projetos de desenvolvimento de software**. Dissertação (mestrado) – Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Pernambuco, Recife. 2007.

[18] HAN, S. H; KIM, D. Y.; KIM, H. A web-based integrated system for international project risk management. In: **Automation in Construction**. 2008. p. 342-356.

[19] International Organization for Standardization. **ISO 15504:** Information Technology – Proccess Assessment – Part I – Concepts and Vocabulary. Geneve: ISO, 2003.

[20] _____. **ISO 27005:** Information Technology – Security Techniques – Information Security Risk Management. Geneve: ISO, 2008.

[21] _____. **ISO 31000:** Risk Management - Principles and Guidelines. Geneve: ISO, 2009.

[22] _____. **ISO 31010:** Risk Management - Risk Assessment Techniques. Geneve: ISO 2009.

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

[24] Information Technology Governance Institute. **CobiT 4.1.** Rolling Meadows, Illinois: IT Governance Institute, 2007.

[25] ISLAM, S.; DONG, W. **Human Factors in Software Security Risk Management**. 2008. p. 13-16.

[26] JALOTE, P. **Software Project Management in Practice**. 1 ed. Boston: Pearson Education, 2002.

[27] JOHNSON, J. **Micro Projects Cause Constant Change**. Standish Group Inc. Disponível em: http://cf.agilealliance.org/articles/system/article/file/1053/file.pdf. Acesso em: 01 nov. 2012.

[28] KERZNER, H. **Applied project management: best practices on implementation**. Nova Iorque: John Willey & Sons Inc, 2000.

[29] KESHLAF, A. A.; RIDDLE, S. Risk Management for Web and Distributed Software Development Projects. In: **Fifth International Conference on Internet Monitoring and Protection**. 2010. p. 22-28.

[30] KLOMAN, H. F.; **Risk management agonists**. Risk Analysis. v. 10. Issue 2. P 201-205. 1990.

[31] KNOB, F. et al, *RiskFree* – Uma Ferramenta de Gerenciamento de Riscos Baseada no PMBOK e Aderente ao CMMI. In: V SIMPÓSIO BRASILEIRO DE QUALIDADE DE SOFTWARE (SBQS). p. 203-217. **Anais...** 2006.

[32] LAKATOS, E. M.; MARKONI, M. A. **Fundamentos de Metodologia Científica.** 6 ed. São Paulo: Atlas, 2005.

[33] LAMERSDORF, A. et al. A Risk-Driven Model for Work Allocation in Global Software Development Projects. In: **IEEE Sixth International Conference on Global Software Engineering**. 2011. p. 15-24.

[34] LEME, L. H. R. **Uma estratégia para apoiar o gerenciamento de riscos em um ambiente distribuído de desenvolvimento de software.** Dissertação (Mestrado em Ciência da Computação) – Universidade Estadual de Maringá, 2007.

[35] LIU, D.; WANG, Q.; XIAO, J. The role of software process simulation modelling in software risk management: a systematic review. In: **3rd international symphosium on empirical software engineering and measurement**. 2009. p. 302-311.

[36] MARTINS, J. C. C. **Gerenciando projetos de desenvolvimento de software com PMI, RUP e UML**. 5 ed. Rio de Janeiro: Brasport, 2010.

[37] MATHKOUR, H.; ASSASSA, G; BAIHAN, A. A Risk Management Tool for Extreme Programming. In: **International Journal of Comouter Science and Network Security**. v. 8. n. 8. 2008. p. 326-333.

[38] MAYER, J.; FAGUNDES, L. L. 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.

[39] MCMANUS, J. **Risk Management in Software Development Projects**. Burlington, Elsevier: Butterworth-Heinemann, 2004.

[40] MÓDULO SECURITY. **10ª Pesquisa Nacional Sobre Segurança da Informação**. São Paulo: Módulo Security. Disponível em: <http://www.modulo.com.br>. Acesso em: 19 dez. 2012.

[41] NIVEN, P. R. **Balanced scorecard passo-a-passo**. Rio de Janeiro: Qualitymark. 2007. 425p.

[42] Office of Government Commerce (OGC). **An introductory overview of ITIL V3**, 2007.

[43] PRIKLADNICKI, R.; AUDY, J. L. N. Uma Análise Comparativa de Práticas de Desenvolvimento Distribuído de Software no Brasil e no Exterior. In: XX SIMPÓSIO BRASILEIRO DE ENGENHARIA DE SOFTWARE. **Anais...** Florianópolis, UFSC/IDESTI, 2006. p. 255-270.

[44] PROJECT MANAGEMENT INSTITUTE. **A Guide to the Project Management Body of Knowledge.** 5 ed. Newton Square, Pennsylvania: Project Management Institute Inc, 2012.

[45] _____. **Organizational project management maturity model (OPM3)**. 4 ed. Newton Square, Pennsylvania: Project Management Institute Inc, 2008.

[46] RIEHLE, R. Institucional memory and risk management. In: **ACM SIGSOFT Software Engineering Notes**, v. 32, n. 6, 2007.

[47] ROSSELET, U.; WENTLAND, M. Knowledge management framework for IT project portfolio risk management. In: **Fifth International Conference on Knowledge**, p. 203-204, 2009.

[48] SALLES JUNIOR, C. A. C. **Gerenciamento de Riscos em Projetos**. 2 ed. Rio de Janeiro: Editora FGV, 2010.

[49] SANTOSO, L. W. Key Factors of Project Human Resources Management for Sucessful Software Engineering. In: **Proceedings of information technology, communication and multimedia seminar.** Surabaya, Indonesia. 2008. p. 1-7.

[50] SCHREIBER, D. GARCIA, C. S.; DOMINGOS, D. Terceirização de Desenvolvimento de Software em Body Shop: uma proposta para diminuir os riscos. In: X SIMPÓSIO BRASILEIRO DE QUALIDADE DE SOFTWARE. **Anais…** 2010. p. 8.

[51] SCHWABER, K.; SUTHERLAND, J. **The Definitive Guide to SCRUM:** The Rules of the Game. 2011.

[52] Software Engineering Institute. **CMMI A-Specification – Version 1.7 for CMMI Version 1.2.** Pittsburg, Pennsylvania: Software Engineering Institute, Carnegie Mellon University, 2007.

[53] _____. **CMMI – Capability Maturity Model Integration – Version 1.1**. Pittsburg, Pennsylvania: Software Enigneering Institute, Carnegie Mellon University, 2001.

[54] _____. **CMMI for Development (CMMI-DEV) – Version 1.2 – Technical Report.** Pittsburg, Pennsylvania: Software Engineering Institute, Carnegie Mellon University, 2006.

[55] The Standish Group. **Chaos manifesto 2013:** think big, act small. Disponível em <www.standishgroup.com/sample_research/index.php>. Acesso em: 20 set. 2013.

[56] TORREAO, P. G. B. C. **Project management knowledge learning environment:** ambiente inteligente de aprendizado para educação em gerenciamento de projetos.

[57] TURLEY, F. **The PRINCE2 training manual:** a common sense approach to learning and understanding PRINCE2. 2010.

[58] WANQING, L.; YONG, Z. Study on Risk Management System for Construction Enterprises Based on Projects. In: **4th international conference on wireless communications**, Networking and Mobile Computing. 2008. p. 1-5.

[59] YOUNG, P. C.; TIPPINS, S. C. **Managing business risk**. Nova Iorque: American Management Association. 2001.

APÊNDICES

APÊNDICE A

QUESTIONÁRIO DE AVALIAÇÃO DIAGNÓSTICA

Questionário: Gerenciamento de Riscos (Versão 1.0).
Descrição: Questionário de Avaliação Diagnóstica sobre o Gerenciamento de Riscos no Processo de Desenvolvimento de Software.

Dados da Organização

1. Número de Funcionários: _____
2. Faturamento da Empresa: _____

Questões

3. Existem critérios e parâmetros bem definidos para identificar os riscos presentes em seus projetos?		
Alternativa		**FM**
A	A organização possui critérios e parâmetros bem definidos e eles são conhecidos por todos.	3
B	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 existem critérios e parâmetros para gerenciar os riscos, as atividades são realizadas de maneira intuitiva.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	A boa definição de parâmetros indica que esta atividade é realizada.	4
Identificar Riscos	Definir parâmetros evidencia a busca por riscos.	2
Analisar Riscos	Estabelecer parâmetros caracteriza a presença de atividades para compreender os riscos.	1
Avaliar Riscos	Os parâmetros definem métricas para classificar os riscos, comprovando a presença desta atividade, a qual depende dos parâmetros para tomar decisões.	3
Tratar Riscos	A definição de parâmetros indica que as ameaças são tratadas, embora não comprove isso.	1
Monitoramento e Controle	O monitoramento e controle avalia a eficácia do GR comparando-a com os parâmetros, logo, definir parâmetros evidencia a realização desta atividade.	2

Comunicação e Consulta	Possuir parâmetros não indica que a comunicação entre as partes é realizada.	0

4. O objetivo do gerenciamento de riscos em um projeto é definido?		
Alternativa		**FM**
A	Os objetivos são bem definidos e conhecidos por todos.	3
B	A organização possui objetivos bem definidos, entretanto eles não são divulgados para todos os membros da equipe.	2
C	Desconheço esta informação.	0
D	A organização possui alguns objetivos, os quais não são conhecidos por todos.	-2
E	Não há a definição clara dos objetivos do gerenciamento de riscos, as atividades são realizadas de maneira intuitiva ou à medida que os problemas aparecem.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	Definir os objetivos do GR caracteriza o contexto desta gerência.	4
Identificar Riscos	Ter objetivos definidos para o GR indica que os riscos do projeto são identificados.	2
Analisar Riscos	Possuir objetivos estabelecidos para o GR evidencia a presença da análise, uma vez que ela é realizada para compreender um problema específico.	2
Avaliar Riscos	Definir os objetivos do GR caracteriza a presença da avaliação, pois os riscos são classificados de acordo com eles.	2
Tratar Riscos	Ter objetivos definidos para o GR indica que o tratamento é realizado, uma vez que tal atividade é realizada para resolver um problema específico.	2
Monitoramento e Controle	Possuir objetivos para o GR não evidencia a presença de atividades para monitorá-lo.	0
Comunicação e Consulta	Definir os objetivos do GR não indica a presença de troca de informações entre os envolvidos.	0

5. O escopo do gerenciamento dos riscos de um projeto é caracterizado?		
Alternativa		**FM**
A	O escopo é bem definido, documentado e conhecido por todos.	3
B	O escopo é bem definido e documentado, porém não disseminado para todos os membros da equipe.	2
C	Desconheço esta informação.	0
D	O escopo é definido, mas não é documentado nem disseminado para os membros da equipe.	-2

E	Não há definição do escopo do gerenciamento de riscos.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	O contexto do GR compreende as informações sobre o escopo do problema a ser resolvido.	4
Identificar Riscos	Determinar o escopo do GR indica que a organização procura resolver os problemas, logo, deve realizar atividades para identificar os riscos.	1
Analisar Riscos	Caracterizar o escopo do GR evidencia a presença de informações úteis para compreender os riscos.	1
Avaliar Riscos	Especificar o escopo do GR indica a presença de informações úteis para classificar os riscos.	1
Tratar Riscos	Definir o escopo do GR caracteriza a existência de atividades para tratar os riscos.	2
Monitoramento e Controle	Determinar o escopo do GR não evidencia a presença de atividades de monitoração.	0
Comunicação e Consulta	Caracterizar o escopo do GR não indica que a comunicação entre os envolvidos é realizada.	0

6. Os responsáveis pelas atividades do gerenciamento de riscos são designados?		
Alternativa		**FM**
A	Existem responsáveis por cada fase do GR e todos conhecem suas atribuições.	3
B	Existem responsáveis para cada fase do GR, mas nem todos conhecem suas atribuições.	2
C	Desconheço esta informação.	0
D	Embora existam responsáveis pelo gerenciamento de riscos não há plena consciência de suas atribuições.	-2
E	Não há responsáveis estabelecidos para as atividades do gerenciamento de riscos.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	Determinar papéis e responsabilidades indica a presença do contexto para o GR.	4
Identificar Riscos	Definir os responsáveis evidencia a presença da identificação dos riscos.	1
Analisar Riscos	Estabelecer responsáveis caracteriza a presença da análise dos riscos.	1
Avaliar Riscos	Determinar responsáveis indica a presença da avaliação dos riscos.	1
Tratar Riscos	Definir responsáveis evidencia a presença do tratamento dos riscos.	1

Monitoramento e Controle	Eleger responsáveis evidencia a presença da monitoração dos riscos.	1
Comunicação e Consulta	Estabelecer os responsáveis é o primeiro passo para realizar a comunicação entre os envolvidos.	2

7. As políticas, normas, regulamentações e guias que interferem no sucesso do projeto são documentados?		
Alternativa		**FM**
A	Sempre que necessário ocorre a documentação de políticas, normas, regulamentações e guias. Tais dados são utilizados durante todo desenvolvimento do projeto.	3
B	Sempre que necessário ocorre a documentação de políticas, normas, regulamentações e guias, no entanto estas informações são raramente utilizadas.	2
C	Desconheço esta informação	0
D	Raramente ocorre a documentação de políticas, normas, regulamentações e guias.	-2
E	Não existe documentação de políticas, normas, regulamentações e guias são definidos e documentados de maneira clara e objetiva.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	A existência destes documentos caracteriza a existência do contexto do GR.	4
Identificar Riscos	Armazenar estes documentos não indica que os riscos são identificados.	0
Analisar Riscos	Recolher estes documentos caracteriza que eles podem ser úteis para compreender os riscos.	1
Avaliar Riscos	A existência destes documentos evidencia que eles podem ser úteis para classificar os riscos.	1
Tratar Riscos	Armazenar estes documentos indica que podem haver restrições a implementação das soluções, logo, evidencia a realização do tratamento.	1
Monitoramento e Controle	O surgimento destes documentos pode ocorrer ao longo de todo ciclo de vida, logo, armazená-los indica que o monitoramento e controle é realizado.	1
Comunicação e Consulta	Recolher os documentos que podem interferir no GR não indica a troca de informações entre os envolvidos.	1

8. As metodologias para avaliar os riscos são definidas e registradas?		
Alternativa		**FM**
A	As metodologias para avaliar os riscos são bem definidas, documentadas e disseminadas entre os membros da equipe.	3

B	As metodologias para avaliar os riscos são bem definidas e documentadas, porém não são bem disseminadas entre os membros da equipe.	2
C	Desconheço esta informação.	0
D	Os membros da equipe utilizam algumas metodologias para gerenciar os riscos, no entanto elas não são documentadas.	-1
E	São utilizadas algumas metodologias para gerenciar os riscos, contudo elas não são documentadas nem disseminadas entre os membros da equipe.	-2
F	Não são utilizadas metodologias para avaliar os riscos.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	As metodologias para avaliar os riscos devem ser registradas no contexto do GR.	4
Identificar Riscos	A presença de metodologias para avaliar riscos indica que uma lista de riscos é gerada com o intuito de ser analisada e avaliada.	2
Analisar Riscos	Possuir metodologias para avaliar riscos evidencia que uma lista de riscos é gerada com o intuito de ser analisada e avaliada.	2
Avaliar Riscos	Dispor de metodologias para avaliar os riscos caracteriza a presença desta atividade.	3
Tratar Riscos	A presença de metodologias para avaliar os riscos não indica que eles são tratados.	0
Monitoramento e Controle	Possuir metodologias para avaliar os riscos não caracteriza a monitoração do GR.	0
Comunicação e Consulta	Dispor de metodologias para avaliar os riscos não evidencia a comunicação entre os envolvidos.	0

9. Os níveis de aceitação ou tolerância para um determinado risco são fixados?		
Alternativa		**FM**
A	Existem níveis de tolerância para os riscos e, quando possível, todos são mitigados até desaparecer ou atingir um nível aceitável.	3
B	Desconheço esta informação.	0
C	Não existem níveis de tolerância dos riscos e todos são mitigados até desaparecerem.	-2
D	Não existem níveis de tolerância dos riscos e todos são mitigados até atingirem níveis que achamos ideais.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Estes níveis são documentados pelo contexto do GR.	4
Identificar Riscos	Estes níveis de aceitação/tolerância indicam a presença	1

	de atividades para identificar os riscos.	
Analisar Riscos	Os níveis de aceitação/tolerância caracterizam atividades para analisar os riscos.	2
Avaliar Riscos	Os níveis de aceitação/tolerância evidenciam atividades para avaliar os riscos.	3
Tratar Riscos	Estes níveis não indicam a presença de atividades para tratar os riscos.	0
Monitoramento e Controle	Estes níveis indicam a presença de atividades de monitoração pois devem ser controlados durante o ciclo de vida do projeto.	2
Comunicação e Consulta	Os níveis de aceitação/tolerância não indicam a presença de atividades de comunicação entre os envolvidos.	0

10. A metodologia para determinar probabilidade de ocorrência de um risco é caracterizada?

	Alternativa	**FM**
A	Existem metodologias definidas e documentadas para determinar a probabilidade que um risco tem para ocorrer.	3
B	Existem metodologias definidas para determinar a probabilidade que um risco tem para ocorrer, no entanto elas não são documentadas.	2
C	Desconheço esta informação.	0
D	Sempre são utilizadas diferentes metodologias para determinar a probabilidade de ocorrência de um risco.	-2
E	A probabilidade que um risco tem de ocorrer não é levada em consideração pela equipe do projeto.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	Estas metodologias devem estar documentadas no contexto do GR.	4
Identificar Riscos	A presença destas metodologias indica que os mesmos são identificados para posteriormente serem analisados e avaliados.	1
Analisar Riscos	Estas metodologias evidenciam a presença de atividades para identificar, analisar e avaliar os riscos.	3
Avaliar Riscos	A existência destas metodologias caracteriza a presença de atividades de análise no PDS.	2
Tratar Riscos	A existência destas metodologias não caracteriza que os riscos são tratados.	0
Monitoramento e Controle	Estas metodologias podem sofrer modificações/melhorias durante o ciclo de vida do projeto.	1

Comunicação e Consulta	A existência destas metodologias não caracteriza a comunicação entre os envolvidos.	0

11. As decisões necessárias para o caso de um risco se concretizar são estipuladas?		
Alternativa		**FM**
A	Existem diferentes ações documentadas para os grupos de riscos que o projeto possui.	3
B	Existem diferentes ações documentadas para alguns grupos de riscos que o projeto possui.	2
C	Desconheço esta informação.	0
D	Existem algumas ações documentadas para alguns grupos de riscos que o projeto possui.	-2
E	Não existem ações documentadas, se um risco se concretizar as decisões necessárias serão tomadas na hora.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	As principais decisões possíveis devem estar documentadas no contexto do GR.	4
Identificar Riscos	Estas decisões não influenciam o processo de identificação dos riscos.	0
Analisar Riscos	Estas decisões podem auxiliar na compreensão de um risco, evidenciando esta atividade.	1
Avaliar Riscos	Estas decisões podem auxiliar na classificação de um riscos, evidenciando esta atividade.	1
Tratar Riscos	As decisões a serem tomadas caso um risco se concretizar indicam a realização do tratamento dos mesmos.	3
Monitoramento e Controle	As possíveis decisões que serão tomadas caso o risco se concretize ou então iniciar o processo de tratamento emergencial.	2
Comunicação e Consulta	Estas decisões não indicam que a comunicação entre os interessados é realizada.	0

12. As premissas e as restrições do processo de gerenciamento de riscos são definidas?		
Alternativa		**FM**
A	As premissas existem, são documentadas e disponibilizadas para todos os membros da equipe.	3
B	As premissas existem e são documentadas, contudo não são disponibilizadas para os membros da equipe.	2
C	Desconheço esta informação.	0

D	As premissas existem, porém não são documentadas nem disponibilizada para todos os membros da equipe.	-2
E	Não ocorre a definição das premissas para o gerenciamento de riscos.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Estas premissas são documentadas no contexto do GR.	4
Identificar Riscos	As premissas são utilizadas para compreender, classificar e tratar os riscos, logo, evidenciam a criação de uma lista dos mesmos.	1
Analisar Riscos	Estas premissas caracterizam esta atividade pois são utilizadas para compreender os riscos	2
Avaliar Riscos	As premissas indicam a existência desta atividade pois são utilizadas para classificar os riscos.	2
Tratar Riscos	As premissas estabelecem, inclusive, as restrições do GR, portanto influenciam no tratamento dos riscos.	1
Monitoramento e Controle	A presença de premissas não indica que o GR é monitorado e controlado.	0
Comunicação e Consulta	Estas premissas não evidenciam a presença de atividades de comunicação entre os envolvidos.	0

13. A organização busca identificar as fontes causadoras de riscos?		
Alternativa		**FM**
A	Além dos riscos, suas causas também são identificadas.	3
B	Desconheço esta informação.	0
C	Somente ocorre a identificação dos riscos.	-2
D	Não ocorre nem identificação dos riscos nem de suas causas.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Buscas estas fontes não indica que o contexto do GR é estabelecido.	0
Identificar Riscos	Buscar fontes de risco indica que a organização realiza a identificação dos riscos.	4
Analisar Riscos	A busca pelas fontes de risco não influencia na análise dos mesmos.	0
Avaliar Riscos	Buscar fontes de risco não altera a avaliação dos mesmos.	0
Tratar Riscos	A busca por fontes de risco não atinge no tratamento dos mesmos.	0
Monitoramento e Controle	Buscar fontes de risco deve ser realizada ao longo de	1

	toda o GR.	
Comunicação e Consulta	Buscar fontes de risco não evidencia a presença de comunicação entre os envolvidos.	0

14. Ocorre a criação de uma lista formal com os riscos identificados bem como suas descrições?		
Alternativa		**FM**
A	A lista gerada contém todos os riscos do projeto bem como suas descrições.	3
B	Desconheço esta informação.	0
C	A lista gerada contém apenas uma relação dos riscos, os quais não são descritos.	-2
D	Não existe uma lista formal de riscos.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	A lista de riscos não evidencia o estabelecimento do contexto.	0
Identificar Riscos	A lista de riscos indica que a identificação dos riscos é realizada.	4
Analisar Riscos	A elaboração da lista de riscos é o primeiro passo para realizar a análise dos riscos.	1
Avaliar Riscos	A criação da lista de riscos é a etapa inicial para a realizar da avaliação dos riscos.	1
Tratar Riscos	A lista de riscos é o primeiro passo para realizar o tratamento dos riscos.	1
Monitoramento e Controle	A lista de riscos não evidencia a monitoração do GR.	0
Comunicação e Consulta	A lista de riscos não prova que a comunicação entre os envolvidos é realizada.	0

15. Se necessário, a organização busca auxílio em outras pessoas com conhecimentos apropriados sobre o projeto?		
Alternativa		**FM**
A	Não se aplica nesta organização.	0
B	Consultas são realizadas com especialistas em assuntos relevantes ao sucesso do projeto.	3
C	A organização tenta resolver internamente quando não conhece minúcias do projeto, em último caso realizam-se consultas com especialistas.	-1
D	A organização sempre resolve internamente quando não conhece detalhes do projeto.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Consultar terceiros não evidencia o estabelecimento do contexto do GR.	0
Identificar Riscos	Buscar auxílio a terceiros para entender o projeto em busca de riscos indica que a identificação dos mesmos é realizada.	4
Analisar Riscos	Buscar conhecimentos com especialistas colabora com a compreensão dos riscos identificados, evidenciando a realização desta atividade.	1
Avaliar Riscos	Buscar auxílio com terceiros auxilia na avaliação dos riscos identificados, indicando a realização desta atividade.	1
Tratar Riscos	Buscar informações com especialistas ajuda no tratamento dos riscos, caracterizando a execução desta atividade.	1
Monitoramento e Controle	Consultar informações com especialistas não evidencia a atividade de monitoramento e controle.	0
Comunicação e Consulta	Consultar terceiros indica que algumas atividades de comunicação são realizadas no processo.	1

16. As ameaças atreladas a um determinado risco são documentadas?		
Alternativa		**FM**
A	Sempre que houver riscos ligados à riscos todos são documentados.	3
B	Os riscos são documentados. Se houverem riscos atrelados a eles faz-se apenas uma observação.	1
C	Desconheço esta informação.	0
D	Apenas os riscos são documentados.	-2
E	Nenhum risco é documentado.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Documentar riscos decorrentes de outros riscos não indica que o contexto é estabelecido.	0
Identificar Riscos	Se a organização documenta riscos provenientes de outros riscos indica que a identificação dos riscos é realizada.	4
Analisar Riscos	Documentar riscos oriundos de outros riscos indica que uma breve análise é realizada na lista de riscos.	2
Avaliar Riscos	Se a organização documenta riscos decorrentes de outros riscos caracteriza que uma breve avaliação é realizada na lista de riscos.	2

Tratar Riscos	Documentar riscos provenientes de outros riscos não evidencia que o tratamento é realizado.	0
Monitoramento e Controle	Documentar riscos oriundos de outros riscos não indica que o monitoramento e controle é realizado.	0
Comunicação e Consulta	Documentar riscos decorrentes de outros riscos não indica que a comunicação entre os envolvidos ocorre.	0

17. As informações utilizadas para identificar os riscos sempre estão atualizadas?		
Alternativa		**FM**
A	Todos os documentos utilizados corresponde a última versão disponível.	3
B	Sempre que possível utiliza-se a última versão dos documentos.	2
C	Desconheço esta informação.	0
D	Raramente a equipe que cuida dos riscos do projeto tem acesso a última versão dos documentos.	-2
E	Os arquivos utilizados para identificar os riscos sempre estão desatualizados.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	Estas informações não evidenciam que o contexto do GR é estabelecido.	0
Identificar Riscos	Estas informações indicam que a identificação dos riscos sempre se baseia nos melhores dados disponíveis.	4
Analisar Riscos	Estas informações não caracterizam a realização desta atividade.	0
Avaliar Riscos	Estas informações não indicam a realização desta atividade.	0
Tratar Riscos	Estas informações não evidenciam a realização do tratamento dos riscos.	0
Monitoramento e Controle	Estas informações caracterizam o monitoramento e controle dos documentos do projeto.	2
Comunicação e Consulta	Estas informações não indicam a realização desta atividade.	0

18. Se necessário, a organização utiliza ferramentas e técnicas específicas para identificar os riscos do projeto?		
Alternativa		**FM**
A	Não se aplica nesta organização.	0
B	Sempre que necessário são utilizadas ferramentas e técnicas específicas, as quais estão documentadas nos planos de gerenciamento de riscos.	3
C	Sempre que necessário são utilizadas ferramentas e técnicas específicas, no entanto	2

	elas não estão documentadas nos planos de gerenciamento de riscos.	
D	Não são utilizadas ferramentas e técnicas para identificar riscos.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	A utilização destas ferramentas evidencia o estabelecimento do contexto, uma vez que devem ser documentadas.	1
Identificar Riscos	A utilização destas ferramentas caracteriza a realização desta atividade.	4
Analisar Riscos	A presença destas ferramentas não indica a realização da análise dos riscos.	0
Avaliar Riscos	A utilização destas ferramentas não evidencia a realização da avaliação dos riscos.	0
Tratar Riscos	A presença destas ferramentas não indica a realização do tratamento dos riscos.	0
Monitoramento e Controle	A utilização destas ferramentas não caracteriza a realização do monitoramento e controle do GR.	0
Comunicação e Consulta	A presença destas ferramentas não evidencia a realização da comunicação entre os envolvidos.	0

19. Quando um risco é documentado, as áreas de impacto, suas causas e possíveis consequências complementam a lista de riscos identificados?		
Alternativa		**FM**
A	Sempre que um risco é registrado na lista de riscos leva-se em conta seu impacto, suas causas e consequências para o projeto.	3
B	Na maioria das vezes em que um risco é registrado na lista de riscos considera-se seu impacto, suas causas e consequências para o projeto.	2
C	Desconheço esta informação.	0
D	Raramente um risco identificado contém informações sobre seu impacto, suas causas e consequências.	-1
E	Não há complementação de informações na lista de riscos, que contém apenas a relação de riscos identificados.	-2
F	Não existe lista de riscos.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Esta documentação não indica que o contexto é estabelecido.	0
Identificar Riscos	Esta documentação evidencia que os riscos são identificados.	4
Analisar Riscos	Esta documentação caracteriza que uma análise básica é	1

	realizada sobre os riscos.	
Avaliar Riscos	Esta documentação evidencia que algumas etapas da avaliação são realizadas.	2
Tratar Riscos	Esta documentação não indica que o tratamento do riscos é realizado.	0
Monitoramento e Controle	Esta documentação não caracteriza que revisões no GR são conduzidas.	0
Comunicação e Consulta	Esta documentação não evidencia que a comunicação entre os envolvidos realmente ocorre.	0

20. A organização busca compreender o risco após a identificação do mesmo?		
Alternativa		**FM**
A	Os riscos identificados sempre são compreendidos após o processo de identificação.	3
B	Na maioria das vezes ocorre a compreensão dos riscos após o processo de identificação.	2
C	Desconheço esta informação.	0
D	Raramente os riscos são compreendidos após o processo de identificação.	-2
E	Os riscos identificados não são compreendidos.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	A compreensão dos riscos não evidencia o estabelecimento do contexto para o GR.	0
Identificar Riscos	A compreensão dos riscos é desenvolvida após a identificação dos mesmos, portanto evidencia esta atividade.	1
Analisar Riscos	A análise dos riscos consiste na compreensão dos mesmos.	4
Avaliar Riscos	A compreensão dos riscos não configura a realização da avaliação dos mesmos.	0
Tratar Riscos	A compreensão dos riscos não caracteriza o tratamento dos mesmos.	0
Monitoramento e Controle	A compreensão dos riscos não evidencia o monitoramento e controle do GR.	0
Comunicação e Consulta	A compreensão dos riscos não indica a realização da comunicação entre os envolvidos.	0

21. Quando um risco é compreendido, suas causas, impactos, consequências e probabilidade de ocorrência são levadas em consideração?

Alternativa		FM
A	Todos os fatores que podem influenciar a ocorrência de um risco são levados em consideração.	3
B	Desconheço esta informação.	0
C	Os fatores que podem influenciar a ocorrência de um risco não são levados em consideração.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Estes fatores não indicam que o contexto do GR é estabelecido.	0
Identificar Riscos	Para obter estes fatores é necessário identificar os riscos, portanto indica a realização desta atividade.	1
Analisar Riscos	Compreender as causas, impactos, consequências e probabilidade de ocorrência caracteriza esta atividade.	4
Avaliar Riscos	Estes fatores não indicam que os riscos são analisados.	0
Tratar Riscos	Estes fatores não evidenciam que os riscos são tratados.	0
Monitoramento e Controle	Estes fatores não caracterizam a realização do monitoramento e controle do GR.	0
Comunicação e Consulta	Estes fatores não indicam que a comunicação entre os interessados é realizada.	0

22. Riscos com maior probabilidade de ocorrer ou que com maiores impactos ao projeto são analisados de maneira especial?

Alternativa		FM
A	Todos os riscos com alta probabilidade de ocorrência são analisados com um maior grau de detalhamento.	3
B	Apenas alguns riscos com alta probabilidade de ocorrência são analisados com um maior grau de detalhamento.	2
C	Desconheço esta informação.	0
D	Raramente um risco com alta probabilidade de ocorrência é analisado com um maior grau de detalhamento.	-2
E	Todos os riscos são analisados da mesma forma.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	As métricas de aceitação ou não de um riscos evidenciam o contexto do GR.	1
Identificar Riscos	Para analisar estas informações os riscos precisam ser identificados, portando indicam a existência desta atividade.	2

Analisar Riscos	A análise dos riscos é a atividade responsável por verificar os impactos e a probabilidade dos riscos ocorrerem.	4
Avaliar Riscos	Uma vez que critérios de probabilidade e impacto são obtidos evidencia-se algumas etapas da atividade de avaliação dos riscos.	1
Tratar Riscos	Estes critérios não indicam que o tratamento seja realizado no PDS.	0
Monitoramento e Controle	Estes critérios não caracterizam a atividade de monitoramento e controle.	0
Comunicação e Consulta	Estes critérios não evidenciam a presença de atividade para comunicar as partes envolvidas.	0

23. A organização documenta de maneira clara e completa a lista dos riscos analisados?		
Alternativa		**FM**
A	As informações obtidas com a análise dos riscos complementam a lista dos riscos identificados.	3
B	Desconheço esta informação.	0
C	As informações obtidas com a análise dos riscos não são utilizadas para complementar a lista dos riscos identificados.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	Esta documentação não caracteriza o estabelecimento do contexto do GR.	0
Identificar Riscos	Para documentar os riscos analisados é necessário identificá-los, portanto evidencia a presença desta atividade.	1
Analisar Riscos	Esta atividade é responsável por documentar os riscos.	4
Avaliar Riscos	Documentar os riscos analisados é a primeira etapa do processo de avaliação dos mesmos, o que evidencia a realização desta atividade.	2
Tratar Riscos	O registro dos riscos analisados não caracteriza seu tratamento.	0
Monitoramento e Controle	A documentação dos riscos analisados não indica que o GR é monitorado.	0
Comunicação e Consulta	Documentar os riscos analisados não evidencia a troca de informações entre os interessados.	0

24. Se novos riscos surgirem durante a análise de uma ameaça eles são inclusos na lista de riscos identificados?	
Alternativa	**FM**

A	Sempre que novos riscos surgem eles são inclusos na lista de riscos identificados para posteriormente serem avaliados.	3
B	Geralmente quando um novo risco surge ele é incluso na lista de riscos identificados para ser posteriormente analisado.	2
C	Desconheço esta informação.	0
D	Raramente que novos riscos surgem eles são inclusos na lista de riscos identificados para posteriormente serem avaliados.	-2
E	Os riscos que surgirem durante o processo de análise não são adicionados à lista dos riscos.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	A documentação dos riscos decorrentes da análise não evidencia o estabelecimento do contexto.	0
Identificar Riscos	O registro dos riscos decorrentes da análise caracteriza a realização da identificação de riscos.	2
Analisar Riscos	A análise dos riscos tem como objetivo compreender melhor os riscos e documentar os resultados obtidos.	4
Avaliar Riscos	A inclusão dos riscos provenientes da análise indica uma avaliação, mesmo que básica dos mesmos.	1
Tratar Riscos	Esta documentação não evidencia a realização do tratamento dos riscos.	0
Monitoramento e Controle	O registro dos riscos decorrentes da análise não caracteriza o monitoramento e controle do GR.	0
Comunicação e Consulta	A documentação dos riscos provenientes da análise não indica a comunicação entre os envolvidos.	0

25. Análises quantitativas, qualitativas ou uma combinação das duas são realizadas para determinar o impacto de uma ameaça?		
Alternativa		**FM**
A	Todas as análises são realizadas e estão documentadas nos planos de gerenciamento de riscos.	3
B	Todas as análises são realizadas, contudo elas não estão documentadas nos planos de gerenciamento de riscos.	2
C	Desconheço esta informação.	0
D	As análises não são realizadas.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	A presença destas metodologias não evidencia que o contexto do GR é estabelecido.	0
Identificar Riscos	Estas metodologias não indicam que a identificação dos	0

	riscos é realizada.	
Analisar Riscos	Estas metodologias caracterizam a realização de análises nos riscos do projeto.	4
Avaliar Riscos	A presença destas metodologias evidencia uma análise, mesmo que básica dos riscos.	1
Tratar Riscos	Estas metodologias não indicam que os riscos do projetos são tratados.	0
Monitoramento e Controle	A presença destas metodologias não caracteriza o monitoramento e controle do GR.	0
Comunicação e Consulta	Estas metodologias não evidenciam a troca de informações entre os envolvidos com o projeto.	0

26. A análise dos riscos leva em consideração a documentação do projeto?		
Alternativa		**FM**
A	Sempre que um risco é analisado as informações são obtidas na documentação do projeto.	3
B	Desconheço esta informação.	0
C	Os riscos são analisados apenas de acordo com a lista de riscos, que não leva em consideração os dados presentes na documentação do projeto.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	Considerar os documentos do projeto não indica que o contexto é estabelecido.	0
Identificar Riscos	Levar em consideração esta documentação não caracteriza a identificação dos riscos.	0
Analisar Riscos	Os documentos do projeto devem ser considerados pelo processo de análise dos riscos.	4
Avaliar Riscos	Considerar esta documentação não caracteriza a análise dos riscos.	0
Tratar Riscos	Levar em consideração os documentos do projeto não indica o tratamento dos riscos.	0
Monitoramento e Controle	Os documentos do projeto são constantemente atualizados, portanto utilizá-los evidencia o monitoramento e controle do GR.	1
Comunicação e Consulta	Considerar estes documentos não caracteriza a troca de informações entre os envolvidos.	0

27. A organização utiliza os dados da análise de riscos para determinar se um risco será aceito ou não?	
Alternativa	**FM**

A	Os dados obtidos na análise do risco são de extrema importância para determinar se ele será aceito ou não.	3
B	Geralmente os dados obtidos na análise do risco são utilizados determinar se ele será aceito ou não.	1
C	Desconheço esta informação.	0
D	Raramente os dados obtidos na análise do risco são utilizados para determinar se ele será aceito ou não.	-2
E	Não há análise dos riscos para gerar dados.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	A compreensão dos riscos não indica que o contexto do GR é estabelecido.	0
Identificar Riscos	Para analisar os riscos é necessário identificá-los, portanto evidencia a presença desta atividade.	1
Analisar Riscos	A obtenção de dados provenientes da análise indica que esta atividade é realizada.	2
Avaliar Riscos	Avaliar os riscos baseando-se na análise realizada indica caracteriza a realização desta atividade.	4
Tratar Riscos	Estes dados não indicam que o tratamento dos riscos é realizado.	0
Monitoramento e Controle	Utilizar os dados obtidos com a análise dos riscos não evidencia a presença do monitoramento do GR.	0
Comunicação e Consulta	Os dados da análise não caracterizam a comunicação entre os envolvidos.	0

28. Os dados da análise de riscos são utilizados para estabelecer os riscos com maior prioridade?		
Alternativa		**FM**
A	Os dados obtidos na análise do risco influenciam diretamente na determinação das prioridades.	3
B	Geralmente os dados obtidos na análise do risco influenciam na determinação das prioridades.	2
C	Desconheço esta informação.	0
D	Raramente os dados obtidos na análise do risco influenciam na determinação das prioridades.	-2
E	Não há análise dos riscos para gerar dados.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Os dados da análise de riscos não indicam que o contexto do GR é estabelecido.	0

Identificar Riscos	Para analisar os riscos é necessário identificá-los, portanto caracteriza a presença desta atividade no PDS.	1
Analisar Riscos	A utilização de dados decorrentes da análise evidencia a presença desta atividade.	2
Avaliar Riscos	Utilizar os dados para definir as prioridades indica que a avaliação dos riscos é realizada.	4
Tratar Riscos	Estabelecer as prioridades não caracteriza o tratamento dos riscos.	0
Monitoramento e Controle	Estes dados não indicam que o monitoramento e controle é realizado.	0
Comunicação e Consulta	Os dados da análise de riscos não evidenciam a comunicação entre os interessados.	0

29. Os dados obtidos durante a análise de riscos são comparados com os parâmetros e critérios estabelecidos?		
Alternativa		**FM**
A	Sempre que a avaliação dos riscos é realizada os dados são comparados com os parâmetros estabelecidos.	3
B	Na maioria das vezes em que a avaliação dos riscos é realizada os dados são comparados com os parâmetros estabelecidos.	2
C	Desconheço esta informação.	0
D	Raramente durante a avaliação dos riscos os dados são comparados com os parâmetros estabelecidos.	-2
E	A avaliação dos riscos não leva em consideração os parâmetros estabelecidos.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	A existência de parâmetros indica o estabelecimento do contexto do GR.	2
Identificar Riscos	Para obter dados da análise é necessário identificar os riscos, portanto há a caracterização desta atividade.	1
Analisar Riscos	A existência de dados comparativos indica a realização da análise dos riscos.	2
Avaliar Riscos	A comparação dos dados evidencia a realização da análise dos riscos.	4
Tratar Riscos	Comparar os dados não indica que o tratamento dos riscos é realizado.	0
Monitoramento e Controle	A existência de dados comparativos não caracteriza a presença do monitoramento das atividades do GR.	0
Comunicação e Consulta	Os dados comparativos não evidenciam a comunicação entre os envolvidos.	0

30. Existe algum processo para avaliar as opções de tratamento de um determinado risco?		
Alternativa		**FM**
A	Existe um processo padrão e genérico que é utilizado para avaliar todas as opções de tratamento de um risco.	3
B	Existe um processo padrão, o qual pode ser utilizado para apenas para alguns tipos de riscos.	2
C	Desconheço esta informação.	0
D	Existe um processo padrão e genérico, o qual não é utilizado.	-2
E	Não existe um processo padrão para avaliar as opções de tratamento de riscos.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	A existência deste processo não indica o estabelecimento do contexto do GR.	0
Identificar Riscos	A presença deste processo não evidencia a identificação dos riscos.	0
Analisar Riscos	A existência deste processo não caracteriza a presença de atividades para analisar os riscos.	0
Avaliar Riscos	A presença deste processo não indica a existência de atividades para avaliar os riscos.	0
Tratar Riscos	As opções de tratamento evidenciam a realização desta atividade.	4
Monitoramento e Controle	A presença deste processo não indica a realização de monitoramentos no GR.	0
Comunicação e Consulta	A existência deste processo não caracteriza a troca de informações entre os envolvidos.	0

31. Os riscos residuais são avaliados para determinar se seus níveis de aceitação são toleráveis ou não?		
Alternativa		**FM**
A	Após cada tratamento realiza-se uma análise nos riscos residuais para determinar o nível de aceitação é tolerável ou não.	3
B	Desconheço esta informação.	0
C	Após o tratamento não são realizadas análises para determinar se os riscos residuais são aceitáveis ou não.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Avaliar os riscos residuais não influencia no contexto do GR.	0

Identificar Riscos	Avaliar riscos residuais não indica que a identificação dos riscos é realizada.	0
Analisar Riscos	Avaliar os riscos residuais não exerce influência sobre a análise dos riscos.	0
Avaliar Riscos	Avaliar os riscos residuais indica que atividades para classificá-los são realizadas.	2
Tratar Riscos	Os riscos residuais são obtidos após o tratamento das ameaças.	4
Monitoramento e Controle	Medir o grau de riscos residuais indica que os mesmos devem ser monitorados ao longo do ciclo de vida do projeto.	1
Comunicação e Consulta	Avaliar riscos residuais não caracteriza a comunicação entre os envolvidos.	0

32. Caso um risco residual não seja tolerável, a organização possui um processo de tratamento desta ameaça?

	Alternativa	**FM**
A	Todos os riscos residuais que não atinge um nível de aceitação tolerável são tratados.	3
B	Desconheço esta informação.	0
C	Os riscos residuais são tratados apenas se reaparecerem em outro ponto do projeto.	-2
D	Os riscos residuais não são tratados.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	O tratamento de riscos residuais não indica que o contexto do GR é estabelecido.	0
Identificar Riscos	Tratar riscos residuais não caracteriza a identificação dos riscos.	0
Analisar Riscos	O tratamento de riscos residuais não evidencia a análise dos mesmos.	0
Avaliar Riscos	Tratar riscos residuais não indica que a avaliação dos mesmos é realizada.	0
Tratar Riscos	Tratar riscos residuais evidencia que as soluções dos riscos são implementadas.	4
Monitoramento e Controle	O tratamento dos riscos residuais ocorre sempre que seu nível torna-se insatisfatório, portanto deve ser monitorado ao longo do ciclo de vida.	2
Comunicação e Consulta	Tratar riscos residuais não indica a comunicação entre os envolvidos.	0

33. A efetividade do tratamento realizado é avaliada?		
Alternativa		**FM**
A	A avaliação da efetividade do tratamento de riscos baseia-se em evidências, como por exemplo o nível de riscos residuais.	3
B	Desconheço esta informação.	0
C	A avaliação da efetividade do tratamento é determinada com base no conhecimento da equipe sobre o assunto.	-2
D	Não são realizadas avaliações da efetividade do tratamento do risco.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Avaliar a efetividade do tratamento indica que o contexto do GR é estabelecido.	0
Identificar Riscos	Avaliar a efetividade do tratamento evidencia a realização da identificação dos riscos.	0
Analisar Riscos	Avaliar a efetividade do tratamento indica a presença de atividades para analisar os riscos.	0
Avaliar Riscos	Avaliar a efetividade do tratamento caracteriza que esta atividade é realizada no PDS.	1
Tratar Riscos	Avaliar a efetividade do tratamento evidencia que as soluções são implementadas.	4
Monitoramento e Controle	A efetividade do tratamento deve ser constantemente reavaliada durante o ciclo de vida do projeto, portanto caracteriza a monitoração do GR.	2
Comunicação e Consulta	Avaliar a efetividade do tratamento não indica a presença de atividades de comunicação.	0

34. Se houverem dados decorrentes da avaliação de efetividade do tratamento, estes são armazenados em um banco de dados histórico?		
Alternativa		**FM**
A	Todas as experiências obtidas com o tratamento do risco são armazenadas, as quais posteriormente passam por uma triagem.	3
B	Apenas novas experiências obtidas com o tratamento do risco são armazenadas.	2
C	Desconheço esta informação.	0
D	Apenas informações julgadas interessantes pela equipe do projeto são armazenadas.	-2
E	Não há armazenamento de informações sobre o gerenciamento de riscos.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Armazenar informações no banco de dados histórico não indica que o contexto do GR é realizado.	0

Identificar Riscos	Armazenar estas informações não caracteriza a existência de atividades para identificar os riscos.	0
Analisar Riscos	Registrar estas informações não garante a realização da análise dos riscos.	0
Avaliar Riscos	Registrar estas informações não indica a presença de atividades para avaliar os riscos.	0
Tratar Riscos	Estas informações são geradas no processo de tratamento de riscos.	4
Monitoramento e Controle	O armazenamento de informações no banco de dados histórico não evidencia a presença do monitoramento do GR.	0
Comunicação e Consulta	Registrar estas informações indica a presença de mecanismos para armazenar os dados decorrentes do tratamento dos riscos.	2

35. A organização define um cronograma para tratamento dos riscos?		
Alternativa		**FM**
A	Todas as atividades do gerenciamento de riscos possuem cronograma para serem realizadas.	3
B	Apenas algumas atividades principais do gerenciamento de riscos possuem cronograma para serem realizadas.	2
C	Desconheço esta informação.	0
D	Existe um cronograma que não compreende as atividades do gerenciamento de riscos.	-2
E	Não existe cronograma.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	O cronograma indica a presença de um contexto estabelecido para gerenciar riscos.	2
Identificar Riscos	O cronograma não indica a presença de atividades para identificar os riscos.	0
Analisar Riscos	O cronograma não evidencia atividades para compreender os riscos.	0
Avaliar Riscos	O cronograma não caracteriza a presença de atividades para determinar as prioridades de tratamento.	0
Tratar Riscos	Estabelecer um cronograma para tratar os riscos evidencia a realização das atividades para implementar as soluções.	4
Monitoramento e Controle	O cronograma não caracteriza a realização do monitoramento e controle do GR.	0

Comunicação e Consulta	O cronograma não indica a realização de troca de informações entre os envolvidos.	0

36. A organização elabora planos de contingência para ser executado caso um risco se concretize?		
Alternativa		**FM**
A	Existem planos de contingência para todos os riscos identificados, analisados e avaliados.	-3
B	Existem planos de contingência apenas para os riscos determinados como mais críticos.	2
C	Desconheço esta informação.	0
D	Existem apenas alguns planos de contingência, os quais não são totalmente confiáveis.	-2
E	Não existem planos de contingência.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	Os planos de contingência não indicam que o contexto do GR é estabelecido.	0
Identificar Riscos	Os planos de contingência evidenciam atividades para identificar os riscos.	0
Analisar Riscos	Os planos de contingência não caracterizam a existência da análise de riscos.	0
Avaliar Riscos	Os planos de contingência não indicam a presença de atividades para avaliar os riscos.	0
Tratar Riscos	Estabelecer planos de contingência evidencia a presença de atividades para tratar os riscos.	4
Monitoramento e Controle	Os planos de contingência devem ser implementados, quando necessário, ao longo do ciclo de vida do projeto, indicando a existência de atividades para monitorar e controlar o GR.	2
Comunicação e Consulta	Os planos de contingência não caracterizam a comunicação entre os envolvidos com o projeto.	0

37. Os dados do tratamento são utilizados para avaliar a eficácia e eficiência do gerenciamento de riscos?		
Alternativa		**FM**
A	Todos os dados obtidos durante o tratamento de um risco são utilizados para avaliar a eficiência deste gerenciamento.	3
B	Os dados do tratamento são coletados, no entanto não são plenamente utilizados	1

	para avaliar a eficiência da gerência de riscos.	
C	Desconheço esta informação.	0
D	Alguns dados são coletados, entretanto não são suficientes para avaliar a eficácia do gerenciamento de riscos.	-2
E	Não há coleta de informações sobre o tratamento de riscos.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Estes dados não indicam a presença de atividades para estabelecer o contexto do GR.	0
Identificar Riscos	Estes dados não evidenciam atividades para identificar os riscos.	0
Analisar Riscos	Estes dados não caracterizam a presença de atividades para analisar os riscos.	0
Avaliar Riscos	Estes dados não indicam atividades para avaliar os riscos.	0
Tratar Riscos	Se há dados provenientes do tratamento, há indícios que esta atividade é realizada.	2
Monitoramento e Controle	Os dados coletados ao longo do ciclo de vida evidenciam a presença do monitoramento e controle.	4
Comunicação e Consulta	Estes dados não indicam a troca de informações entre os envolvidos com o projeto.	0

38. Há preocupação com mudanças no contexto interno e externo do projeto?		
Alternativa		**FM**
A	Existem preocupações e elas são levadas em consideração na hora de estabelecer as atividades do gerenciamento de riscos.	3
B	Existem preocupações, contudo elas não são levadas em consideração na hora de estabelecer as atividades do gerenciamento de riscos.	1
C	Desconheço esta informação.	0
D	Não existem preocupações, a gerência dos riscos não depende do contexto interno ou externo do projeto.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Preocupar-se com mudanças no contexto do GR evidencia que está atividade é realizada.	2
Identificar Riscos	Mudar o contexto do GR não indica que a identificação dos riscos é realizada.	0

Analisar Riscos	Alterações nos parâmetros e critérios do GR não caracteriza a realização da análise dos riscos.	0
Avaliar Riscos	Desvios no contexto do GR não comprovam a realização da avaliação dos riscos.	0
Tratar Riscos	Preocupar-se com alterações nos parâmetros e critérios do GR não demonstra a realização do tratamento dos riscos.	0
Monitoramento e Controle	As mudanças de contexto do GR devem ser observadas ao longo do desenvolvimento do projeto.	4
Comunicação e Consulta	Desvios no parâmetros e critérios do GR não caracterizam que a comunicação é realizada.	0

39. Reavaliações constantes são realizadas nos planos do projeto para identificar novos riscos?

	Alternativa	FM
A	Periodicamente são realizadas reavaliações nos planos do projeto em busca de novos riscos.	3
B	As reavaliações são realizadas, entretanto não tem um prazo fixo para ocorrer.	2
C	Desconheço esta informação.	0
D	Não são realizadas reavaliações nos planos do projeto, à medida que novos problemas acontecem eles são solucionados.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Reavaliar os planos de projeto não indica que o contexto do GR é estabelecido.	0
Identificar Riscos	Reavaliar os planos do projeto em busca de novos riscos caracteriza a identificação dos mesmos.	2
Analisar Riscos	Reavaliar estes planos não indica que a análise dos riscos é realizada.	0
Avaliar Riscos	Reavaliar os planos do projeto não evidencia que a avaliação dos riscos é realizada.	0
Tratar Riscos	Reavaliar os planos do projeto não caracteriza atividades para tratar os riscos.	0
Monitoramento e Controle	As reavaliações indicam a realização de atividades para monitorar o GR.	4
Comunicação e Consulta	Reavaliar os planos do projeto não caracterizam que a comunicação é realizada.	0

40. Existem métodos para armazenar e recuperar as informações do gerenciamento de riscos?

Alternativa		FM
A	Existem métodos bem definidos e conhecidos por todos os membros da equipe.	3
B	Existem métodos bem definidos, porém o conhecimento centraliza-se em apenas alguns membros da equipe.	2
C	Desconheço esta informação.	0
D	Existem métodos bem definidos, entretanto eles não são utilizados.	-2
E	Não existem métodos bem definidos para armazenar e recuperar informações do gerenciamento de riscos.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	A presença destes métodos não caracteriza a existência de atividades para estabelecer o contexto do GR.	0
Identificar Riscos	Estes métodos não indicam a presença da identificação dos riscos no PDS.	0
Analisar Riscos	Estes métodos não caracterizam a realização da análise dos riscos.	0
Avaliar Riscos	Estes métodos não evidenciam atividades para avaliar os riscos.	0
Tratar Riscos	Estes métodos não indicam a existência do tratamento dos riscos.	0
Monitoramento e Controle	Manter as informações atualizadas caracteriza a realização de atividades para monitorar e controlar o GR.	4
Comunicação e Consulta	Estes métodos indicam que as informações são mantidas no banco de dados histórico da organização para servirem de conhecimento para outros projetos.	2

41. As informações sobre custos e esforços necessários para manter o gerenciamento de riscos são armazenadas?

Alternativa		FM
A	As informações são armazenadas e todos os membros do projeto tem acesso.	3
B	As informações são armazenadas, contudo somente o responsável pelo projeto tem acesso.	2
C	Desconheço esta informação.	0
D	As informações são armazenadas, mas não são utilizadas.	-2
E	Não existem informações sobre os custos do gerenciamento de riscos.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Armazenar estes dados não evidencia o estabelecimento do contexto.	0

Identificar Riscos	Registrar estes dados não indica a realização de atividades para identificar os riscos.	0
Analisar Riscos	Armazenar estas informações não indica que a análise dos riscos é executada no PDS.	0
Avaliar Riscos	Registrar estas informações não caracteriza a presença da avaliação dos riscos.	0
Tratar Riscos	Armazenar estes dados não indica que os riscos são tratados.	0
Monitoramento e Controle	O registro destas informações busca manter atualizados os dados do GR, portanto evidencia a presença desta atividade no PDS.	4
Comunicação e Consulta	As informações precisam ser armazenadas em um repositório, indicando que consultas são realizadas no banco de dados histórico da organização.	2

42. Existem políticas que determinam por quanto tempo a informação deve ser mantida no banco de dados histórico do gerenciamento de riscos?		
Alternativa		**FM**
A	As políticas são bem definidas e existe um prazo máximo e mínimo para manter as informações.	3
B	As políticas são bem definidas, porém não existe um prazo mínimo ou máximo para manter as informações.	2
C	Desconheço esta informação.	0
D	Não existem políticas e as informações são antigas e desatualizadas.	-2
E	Não há o armazenamento de informações no banco de dados histórico do gerenciamento de riscos.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Estas políticas estão armazenadas no contexto do GR, portando indicam que está atividade é realizada.	3
Identificar Riscos	Estas políticas não indicam que a identificação dos riscos é realizada.	0
Analisar Riscos	Estas políticas não evidenciam a presença de atividades para analisar os riscos.	0
Avaliar Riscos	Estas políticas não caracterizam a realização de atividades para avaliar os riscos.	0
Tratar Riscos	Estas políticas não garantem a presença do tratamento dos riscos no PDS.	0
Monitoramento e Controle	As informações e as políticas mudam constantemente, portanto evidenciam a presença desta atividade no PDS.	4

Comunicação e Consulta	As informações são armazenadas, portanto há a presença de atividades para consultar o banco de dados histórico da organização.	1

43. Os dados armazenados são utilizados para incentivar os *stakeholders* para melhorar continuamente o gerenciamento de riscos?		
Alternativa		**FM**
A	Os colaboradores que produzem informações de qualidade recebem bonificações.	3
B	Os colaboradores que produzem informações de qualidade são elogiados.	2
C	Desconheço esta informação.	0
D	Os colaboradores que produzem informações de qualidade não recebem incentivos.	-2
E	Não há armazenamento de informações.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	Estes dados não indicam que o contexto do GR é estabelecido.	0
Identificar Riscos	Estas informações não evidenciam que a identificação dos riscos está presente no PDS.	0
Analisar Riscos	Estas informações não caracterizam a realização da análise dos riscos.	0
Avaliar Riscos	Estes dados não indicam que atividades para avaliar os riscos são realizadas.	0
Tratar Riscos	Estas informações não caracterizam a presença do tratamento dos riscos no PDS.	0
Monitoramento e Controle	O armazenamento das informações ocorre ao longo do ciclo de vida, portanto evidencia a realização desta atividade.	4
Comunicação e Consulta	Estas informações necessitas ser armazenadas, portanto indicam a presença de atividades para consultar o banco de dados histórico da organização.	1

44. As partes interessadas são comunicadas para estabelecer o contexto do gerenciamento de riscos?		
Alternativa		**FM**
A	As partes interessadas são comunicadas periodicamente de acordo com um plano de comunicação.	3
B	As partes interessadas são comunicadas em algumas situações específicas.	2

C	Desconheço esta informação.	0
D	As partes interessadas raramente são comunicadas.	-2
E	Não há comunicação entre as partes interessadas.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	A comunicação entre os envolvidos para estabelecer o contexto do GR evidencia esta atividade.	2
Identificar Riscos	Esta comunicação não indica que os riscos são identificados.	0
Analisar Riscos	A comunicação entre os envolvidos não garante que a análise dos riscos é executada no PDS.	0
Avaliar Riscos	A troca de informações entre os interessados não evidencia a presença de atividades para avaliar os riscos.	0
Tratar Riscos	Esta comunicação não indica que os riscos são tratados no PDS.	0
Monitoramento e Controle	A comunicação entre os envolvidos não caracteriza o monitoramento das atividades do GR.	0
Comunicação e Consulta	A troca de informações entre os envolvidos caracterizar a comunicação e consulta.	4

45. Os interesses dos envolvidos são entendidos e considerados?		
Alternativa		**FM**
A	Todos os interesses dos interessados são plenamente entendidos e considerados.	3
B	Os interesses são entendidos e considerados, contudo nem sempre são atendidos.	2
C	Desconheço esta informação.	0
D	Os interesses raramente são entendidos e considerados.	-2
E	Os interesses não são entendidos e considerados.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Considerar estes interesses não indica que o contexto é estabelecido.	0
Identificar Riscos	Considerar estes interesses não caracteriza a presença de atividades para identificar os riscos no PDS.	0
Analisar Riscos	Considerar estes interesses não evidencia atividades para analisar os riscos.	0
Avaliar Riscos	Considerar estes interesses não indica a presença de atividades para avaliar os riscos.	0
Tratar Riscos	Considerar estes interesses não caracteriza a realização do tratamento dos riscos.	0

Monitoramento e Controle	Considerar estes interesses não evidencia o monitoramento e controle.	0
Comunicação e Consulta	A troca de informações para atender os interesses dos envolvidos indica a presença da comunicação e consulta no PDS.	4

46. O conhecimento de diferentes áreas são agregados para auxiliar o processo de análise dos riscos?		
Alternativa		**FM**
A	Os conhecimentos presentes no banco de dados histórico sempre são utilizados para auxiliar na análise dos riscos.	3
B	Os conhecimentos presentes no banco de dados histórico geralmente são utilizados para auxiliar na análise dos riscos.	2
C	Desconheço esta informação.	0
D	Os conhecimentos presentes no banco de dados histórico raramente são utilizados para auxiliar na análise dos riscos.	-2
E	Não existem conhecimentos armazenados no banco de dados histórico.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	Agregar estes conhecimentos não evidencia a presença de atividades para estabelecer o contexto do GR.	0
Identificar Riscos	Estes conhecimentos não garantem que atividades para identificar os riscos são realizadas no PDS.	0
Analisar Riscos	Estes conhecimentos são utilizados para analisar os riscos, portanto indicam a realização desta atividade.	2
Avaliar Riscos	Estes conhecimentos não indicam que atividades para avaliar os riscos estão presentes no PDS.	0
Tratar Riscos	Estes conhecimentos não evidenciam o tratamento dos riscos.	0
Monitoramento e Controle	Estes conhecimentos não garantem que o monitoramento e controle é realizado no PDS.	0
Comunicação e Consulta	A obtenção destes conhecimentos caracteriza a comunicação entre os interessados.	4

47. Existe um plano que rege a comunicação entre as partes interessadas?		
Alternativa		**FM**
A	Existe um plano bem definido e documentado para garantir a comunicação entre as partes interessadas.	3
B	Existe um plano documentado, no entanto ele não pode ser utilizado para garantir a comunicação entre as partes interessadas	1

C	Desconheço esta informação.	0
D	Existe documentado, o qual está desatualizado.	-2
E	Não existe plano de comunicação.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	A presença de um plano que rege a comunicação indica que o contexto é estabelecido.	2
Identificar Riscos	Este plano não garante que atividades para identificar riscos estão presentes no PDS.	0
Analisar Riscos	Este plano não indica a realização de análises nos riscos do projeto.	0
Avaliar Riscos	A presença deste plano não evidencia a presença de atividades de avaliação de riscos.	0
Tratar Riscos	Este plano não caracteriza a realização do tratamento dos riscos.	0
Monitoramento e Controle	Este plano não indica que o monitoramento e controle é realizada	0
Comunicação e Consulta	A presença deste plano para reger a comunicação entre os envolvidos evidencia a troca de informações entre os interessados.	4

48. O conhecimento de diferentes áreas são utilizados para auxiliar na tomada de decisão?		
Alternativa		**FM**
A	O conhecimento de outras áreas do projeto sempre é levado em consideração durante o processo de tomada de decisão.	3
B	Sempre que necessário o conhecimento de outras áreas do projeto é levado em consideração durante o processo de tomada de decisão.	2
C	Desconheço esta informação.	0
D	Raramente o conhecimento de outras áreas do projeto é levado em consideração durante o processo de tomada de decisão.	-2
E	O conhecimento de outras áreas do projeto não é levado em consideração durante o processo de tomada de decisão.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Estes conhecimentos não indicam que o contexto GR é estabelecido.	0
Identificar Riscos	A presença destes conhecimentos não evidencia a presença de atividades para identificar os riscos no PDS.	0
Analisar Riscos	Estes conhecimentos não garantem que a análise dos	0

	riscos é realizada.	
Avaliar Riscos	Estes conhecimentos auxiliam a determinar as prioridades da lista de riscos, portanto evidenciam esta atividade.	2
Tratar Riscos	A presença destes conhecimentos não garante que os riscos são tratados no PDS.	0
Monitoramento e Controle	Estes conhecimentos não indicam que o monitoramento e controle é realizado.	0
Comunicação e Consulta	A interligação das diferentes áreas caracteriza a comunicação entre os envolvidos com o projeto.	4

49. Existem meios para comunicar os assuntos referente aos riscos?		
Alternativa		**FM**
A	Existem vários meios documentados para garantir a comunicação das parte envolvidas.	3
B	Existem alguns meios disponíveis para comunicar os interesses das partes envolvidas.	2
C	Desconheço esta informação	0
D	Existe apenas um meio disponível para comunicar os envolvidos.	-2
E	Não existem meios de comunicação definidos.	-3

Eixo	**Justificativa**	**Peso**
Estabelecer Contexto	Os meios de comunicação devem ser documentados, evidenciando o estabelecimento do contexto no PDS.	1
Identificar Riscos	Os meios de comunicação não indicam que os riscos são identificados.	0
Analisar Riscos	Os meios de comunicação não evidenciam a análise dos riscos.	0
Avaliar Riscos	Os meios de comunicação não garantem que os riscos são avaliados.	0
Tratar Riscos	Os meios de comunicação não indicam a presença de atividades para tratar os riscos no PDS.	0
Monitoramento e Controle	Os meios de comunicação não evidenciam atividades para monitorar e controlar o GR.	0
Comunicação e Consulta	Os meios de comunicação são os canais pelos quais a comunicação é realizada, evidenciando a presença desta atividade no PDS.	4

50. As informações relevantes são distribuídas a todos os membros da equipe, respeitando os dados confidenciais e a integridade do conteúdo?

Alternativa		FM
A	As informações são distribuídas de acordo com os níveis de acesso de cada usuário.	3
B	As informações são distribuídas sem controlar níveis de acesso dos usuários.	2
C	Desconheço esta informação.	0
D	As informações são distribuídas e de livre acesso à todos.	-2
E	Não são distribuídas informações.	-3

Eixo	Justificativa	Peso
Estabelecer Contexto	Os domínios e limites para definir uma informação como relevante está presente no contexto do GR, portanto indica que o PDS possui atividades para estabelece-lo.	1
Identificar Riscos	A distribuição das informações não indica a realização de atividades para identificar os riscos.	0
Analisar Riscos	Disseminar as informações aos interessados não garante que os riscos sejam analisados.	0
Avaliar Riscos	Distribuir as informações aos interessados não caracteriza atividades para avaliar os riscos.	0
Tratar Riscos	A disseminação das informações não indica a presença de atividades para tratar os riscos no PDS.	0
Monitoramento e Controle	A distribuição das informações não garante que atividades de monitoramento e controle sejam realizadas.	0
Comunicação e Consulta	Disseminar as informações aos interessados indica que o PDS possui atividades para comunicar e consultar os envolvidos.	4

APÊNDICE B

Checklist de Avaliação – Nível 2

Checklist de Reavaliação

Projeto: *<Nome do Projeto>*
Nível atual: GAIA Riscos Nível 1 - Inicial
Nível almejado: GAIA Riscos Nível 2 – Conhecido

Requisito/Necessidade	**N**	**P**	**T**
Os riscos são identificados?			
Além dos riscos, suas fontes causadores são identificadas?			
Existe um lista de riscos?			
Há descrição dos riscos presentes na lista?			
A descrição de um risco contempla possíveis ameaças atreladas a ele?			
Consultas são realizadas com especialistas caso existam dúvidas sobre um determinado assunto?			
A organização baseia-se nas melhores informações disponíveis para identificar os riscos?			
Existem ferramentas, técnicas ou metodologias para identificar os riscos do projeto?			
Estas ferramentas, técnicas ou metodologias estão documentadas no projeto?			
Quando um risco é identificado existem informações complementares, por exemplo, suas causas e possíveis consequências?			

Legenda:
N - Não implementado.
P - Parcialmente implementado.
T - Totalmente Implementado.

APÊNDICE C

Checklist de Avaliação – Nível 3

Checklist de Reavaliação

Projeto: *<Nome do Projeto>*
Nível atual: GAIA Riscos Nível 2 - Conhecido
Nível almejado: GAIA Riscos Nível 3 – Padronizado

Requisito/Necessidade	**N**	**P**	**T**
Existem critérios e parâmetros bem definidos e documentados para o gerenciamento de riscos?			
Existem premissas e restrições definidas para o GR?			
O objetivo do GR é estabelecido e disseminado para toda organização?			
O escopo do GR é definido, documentado e conhecido por todos os membros da equipe?			
Existem papéis e responsabilidades estabelecidos, documentados e conhecidos por todos?			
Quando existem regulamentações, normas, políticas ou guias que interferem no sucesso do projeto eles são documentados e servem de base para as outras atividades do GR?			
Existem documentos que evidenciam a utilização de metodologias para analisar, avaliar, tratar, monitorar ou comunicar os riscos?			
Há a presença de documentos que indiquem a presença de níveis de aceitação ou tolerância para os riscos?			
Há evidências que comprovem a presença de ações ou decisões necessárias no caso da concretização de um risco?			
Existem ações desenvolvidas com o intuito de compreender um risco?			
As causas, impactos e probabilidade de ocorrência de um risco são definidas?			
Riscos denominados com alta probabilidade de ocorrer ou com maior potencial de impacto são analisados de maneira especial?			
Existem documentos que evidenciem a documentação do processo de compreensão dos riscos?			
Riscos são identificados e documentados a partir da análise?			
Existem indícios que ferramentas, técnicas ou metodologias para avaliar os riscos são utilizadas?			
Os dados obtidos com a análise dos riscos são utilizados no			

processo decisório da organização?			
A lista de riscos é classificada, ou seja, são estabelecidos riscos prioritários?			
Há comparação entre os dados obtidos com a análise dos riscos e os parâmetros estabelecidos?			
Caso um risco seja aceito, a organização monitora este nível para mantê-lo sob controle?			
Existem processos ou documentos que evidenciam a realização de atividades para corrigir os riscos?			
Há registros que comprovem a presença de atividades para avaliar a implementação das soluções?			
As informações são armazenadas em um repositório comum, o qual representa o banco de dados histórico do GR dentro da organização?			
Há um cronograma que rege as atividades?			
Há evidências que comprovem a existência de planos de contingência			

Legenda:
N - Não implementado.
P - Parcialmente implementado.
T - Totalmente Implementado.

APÊNDICE D

Checklist de Avaliação – Nível 4

Checklist de Reavaliação

Projeto: *<Nome do Projeto>*
Nível atual: GAIA Riscos Nível 3 - Padronizado
Nível almejado: GAIA Riscos Nível 4 – Gerenciado

Requisito/Necessidade	**N**	**P**	**T**
Há métricas que comprovem a avaliação da eficácia do tratamento dos riscos ao longo do ciclo de vida?			
Existem atividades que policiem mudanças nos planos do projeto ou no contexto do GR?			
Existem dados que indiquem a realização de reavaliações nos documentos do projeto em busca de novos riscos?			
As informações provenientes do gerenciamento dos riscos sempre são atualizadas no repositório?			
Os custos e o cronograma do projeto são monitorados durante a execução das atividades?			
Existem documentos que comprovam a manutenção das informações por um tempo mínimo no banco de dados histórico?			
Existem registros que indiquem a validade de uma informações, ou seja, por quanto tempo ela é considerada atualizada?			
Existem indícios que o gerenciamento de riscos é utilizado como fator motivacional para a equipe do projeto?			
Há atividades que indiquem a realização de atividades para melhorar continuamente a gerência de riscos?			

Legenda:
N - Não implementado.
P - Parcialmente implementado.
T - Totalmente Implementado.

APÊNDICE E

Checklist de Avaliação – Nível 5

Checklist de Reavaliação

Projeto: *<Nome do Projeto>*
Nível atual: GAIA Riscos Nível 4 - Gerenciado
Nível almejado: GAIA Riscos Nível 5 – Otimizado

Requisito/Necessidade	N	P	T
Existem registros que evidenciam a troca de informações entre as partes para estabelecer os parâmetros do gerenciamento de riscos?			
Existe um documento que caracterize o plano de gerenciamento de comunicação?			
Há indícios da realização periódica da troca de informações?			
Os conhecimentos de outras áreas do projeto são consultados?			
As informações provenientes de outras áreas do projeto são utilizada para auxiliar na tomada de decisão?			
Existem documentos que evidenciam a presença de meios de comunicação definidos?			
Existem registros que indique que as informações são distribuídas entre todos os envolvidos?			
As informações são distribuídas apenas para os usuários que possuem permissões para acessá-las?			

Legenda:
N - Não implementado.
P - Parcialmente implementado.
T - Totalmente Implementado.

TRABALHOS PUBLICADOS PELO AUTOR

1. HORITA, F. E. A.; HISATOMI, M.; GAFFO, F. H.; BARROS, R. M. A Process Model using Maturity Model and Lesson Learned to improve the Quality of Organizational Knowledge and Human Resources Management in Software Development. In: **25th International Conference on Software Engineering and Knowledge Engineering (SEKE)**, Boston, USA, 2013 (Qualis CC 2012, B1).

2. GAFFO, F. H.; BARROS, R. M. **Metodologia para Avaliar o Grau de Maturidade da Gerência de Riscos**. In: IX SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO, JOÃO PESSOA. **Anais...** 2013 (Qualis CC 2012, B4).

3. GAFFO, F. H.; BRIGANO, G. U.; HORITA, F. E. A.; BARROS, R. M. Ferramenta para Avaliar o Grau de Maturidade da Gerência de Riscos de um Processo de Desenvolvimento

de *Software*. In: 8ª Conferência Ibérica de Sistemas e Tecnologias de Informação, 2013, Lisboa, **Anais...** 2013 (Qualis CC 2012, B4).

4. GAFFO, F. H.; BARROS, R. M. GAIA Risks: a risk management framework. In: **ISCA 25th international conference on computer applications in industry and engineering**, New Orleans, Louisiana, USA, 2012 (Qualis CC 2012, B4).

5. GAFFO, F. H.; BARROS, R. M. GAIA Risks – a service-based framework to manage Project risks. In: 2012 XXXVIII CONFERENCIA LATINOAMERICANA EN INFORMATICA (CLEI), Medellin. **Anais...** 2012 (Qualis CC 2012, B4).

6. GAFFO, F. H.; BRANCHER, J. D.; BARROS, R. M. Aplicação da Proposta da ISO 31000 em Ambientes de Desenvolvimento de Software**. Cairu em Revista**, v. 1, p. 36-50, 2012 (Qualis CC 2013, C).