Universidade Estadual de Londrina

JOÃO VICTOR KAWAZOE NAHRA

GAIA CANOA: MODELO PARA GESTÃO DE RISCO EM GOVERNANÇA DE TI

LONDRINA
2019

JOÃO VICTOR KAWAZOE NAHRA

GAIA CANOA: MODELO PARA GESTÃO DE RISCO EM GOVERNANÇA DE TI

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação da Universidade Estadual de Londrina para obtenção do título de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Rodolfo Miranda de Barros

LONDRINA

2019

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UEL

J89 Nahra, João Victor.
GAIA CANOA : MODELO PARA GESTÃO DE RISCO EM GOVERNANÇA DE TI / João Victor Nahra. - Londrina, 2019.
37 f. : il.

Orientador: Rodolfo Miranda de Barros.
Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade Estadual de Londrina, Centro de Ciências Exatas, Programa de Pós-Graduação em Ciência da Computação, 2019.
Inclui bibliografia.

1. Gestão - TCC. 2. Risco - TCC. 3. Governança de TI - TCC. I. Miranda de Barros, Rodolfo. II. Universidade Estadual de Londrina. Centro de Ciências Exatas. Programa de Pós-Graduação em Ciência da Computação. III. Título.
CDU 519

JOÃO VICTOR KAWAZOE NAHRA

GAIA CANOA: MODELO PARA GESTÃO DE RISCO EM GOVERNANÇA DE TI

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação da Universidade Estadual de Londrina para obtenção do título de Bacharel em Ciência da Computação.

BANCA EXAMINADORA

Orientador: Prof. Dr. Rodolfo Miranda de Barros
Universidade Estadual de Londrina

Prof. Dr. Segundo Membro da Banca
Universidade/Instituição do Segundo Membro da Banca – Sigla instituição

---

Prof. Dr. Terceiro Membro da Banca
Universidade/Instituição do Terceiro Membro da Banca – Sigla instituição

---

Prof. Ms. Quarto Membro da Banca
Universidade/Instituição do Quarto Membro da Banca – Sigla instituição

Londrina, 25 de novembro de 2019.

Este trabalho é dedicado aos meus pais, que souberam me dar apoio e desafios.

AGRADECIMENTOS

Agradeço profundamente a todas as pessoas que me apoiaram nessa graduação, sendo elas meus amigos ou não. Agradeço aos meus pais que me apoiaram durante toda a minha formação. Agradeço ao meu orientador Professor Doutor Rodolfo Miranda de Barros e ao meu veterano Matheus Santana da Silva pela oportunidade do trabalho e pelo aprendizado durante o ano.

"A ship is safe in harbor, but that's not what ships are for."
(John A. Shedd.)

NAHRA, J. K.. **Gaia Canoa: Modelo Para Gestão de Risco em Governança de TI**. 2019. 38f. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade Estadual de Londrina, Londrina, 2019.

RESUMO

A Gestão de Risco (GR) tornou-se importante no cenário onde o volume de informação acaba produzindo incertezas para o Âmbito de Governança. Esses riscos, se tratados com um conjunto de ações estratégicas como o planejamento, a identificação, a análise e o controle do mesmos, são gratificantes. Tal processo permite que a organização tome uma posição preventiva, evitando perdas de recursos e oportunidades, gerando valor aos *stakeholders*, que são muitas vezes quem investe na GR. Este trabalho pretende desenvolver um modelo para gestão seguindo os modelos de melhores práticas, criando uma maneira de lidar com os riscos e originando e conservando um ambiente melhor de Gestão e Governança de TI.

Palavras-chave: Gestão. Risco. Governança de TI.

NAHRA, J. K.. **Gaia Canoa: Model for Risk Management in IT Governance**. 2019. 38p. Final Project (Bachelor of Science in Computer Science) – State University of Londrina, Londrina, 2019.

ABSTRACT

Risk management has become important with the huge volume of data that creates uncertainties for the Governance Scope. If treated using strategies, such as planning, identification, analysis and control, risks become great opportunities, generating value for stakeholder. Furthermore, these strategies allow for organizations to take a preventive position, reducing resource and opportunity losses, and generate value to stakeholders, who often invests in risk management. This work intends to develop a model for risk management following best practices, promoting a way of deal with risks and creating and maintaining a better IT Governance and Management environment.

Keywords: Management. Risk. IT Governance.

LISTA DE ILUSTRAÇÕES

Figura 1 – Criação de valores. Adaptada de [1] 15
Figura 2 – Necessidade de gerenciamento de projetos. Adaptada de [2] 16
Figura 3 – Os modelos de melhores práticas no contexto da Governança de TI. Fonte: [3] 17
Figura 4 – Benefícios da Prática de Gestão de Risco em Softwares. Adaptada de [4] 19
Figura 5 – PGR: *Inputs* e *Outputs*. Adaptado de [4] 19
Figura 6 – Ciclo PDCA. 23
Figura 7 – Modelo: GAIA Canoa. 24
Figura 8 – Subprocesso: Estabelecer o Contexto 25
Figura 9 – Subprocesso: Identificar Riscos 25
Figura 10 – Subprocesso: Analisar / Avaliar Riscos 26
Figura 11 – Exemplo de Gráfico de Burndown. Adaptado de [5] 27
Figura 12 – Subprocesso: Monitorar e Controlar 28
Figura 13 – Resultado da avaliação para a Questão 2 30
Figura 14 – Resultado da avaliação para a Questão 2 30
Figura 15 – Resultado da avaliação para a Questão 3 31
Figura 16 – Resultado da avaliação para a Questão 4 31

LISTA DE TABELAS

Tabela 1 – Tipo de riscos, impactos e estratégias para o gerenciamento. Adaptada de [6] 17
Tabela 2 – Classificação da Pesquisa 23
Tabela 3 – Plano de Respostas à Riscos 27
Tabela 4 – Resultados 32

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
TI	Tecnologia da Informação
GR	Gerenciamento de Risco
UEL	Universidade Estadual de Londrina
ITIL	*Information Technology Infrastructure Library*
CobiT	*Control Objectives For Information end Related Technology*
BS	*British Standard*
ISO	*International Organization for Standardization*
IEC	*International Electrotechnical Commission*
FMEA	*Failure Mode and Effect Analysis*
PMBOK	*Project Management Body of Knowledge*
IBGC	*Instituto Brasileiro de Governança Corporativa*
RMP	*Risk Management Process*

SUMÁRIO

1 INTRODUÇÃO 13

2 FUNDAMENTAÇÃO TEÓRICA 15
2.1 Governança e Gestão de TI 15
2.2 Gerenciamento de Riscos 17
2.3 Trabalhos Correlatos 22

3 GAIA CANOA: MODELO PARA GESTÃO DE RISCO EM GOVERNANÇA DE TI 23
3.1 Modelo 24

4 RESULTADOS 29
4.1 Questão 1 30
4.2 Questão 2 30
4.3 Questão 3 31
4.4 Questão 4 31
4.5 Avaliação Geral 32

5 CONCLUSÃO 33

REFERÊNCIAS 34

APÊNDICES 36

ANEXOS 37

1 INTRODUÇÃO

No cenário atual o volume de informação gerado pelas organizações tem crescido vertiginosamente, junto a importância que as organizações vem dando a ela, sendo esta informação considerada como ativo organizacional; um diferencial competitivo em relação ao mercado. De acordo com [7], a governança denota direção, que inclui a execução legal e regular de recursos institucionais para administrar organizações e estuda os erros relacionados a separação e a segregação da posse.

Nesse cenário, conforme as necessidades aparecem, há uma adaptação por parte da Governança e Gestão de TI, no qual atuam como moderadores dentro da organização, onde a Governança adota as práticas de TI aos objetivos planejados da empresa, sendo a informação o expediente decisivo. Diante disso, tornou-se necessário a criação de instrumentos que auxiliam o trabalho de Governança de TI, como *frameworks* e bibliotecas de processos.

A palavra risco é derivada do latim *risico* e *riscu* significando incerteza. No qual os primeiros registros sobre riscos estão relacionados à teoria de probabilidades aplicada em jogos de azar, ambiente onde há chance de se perder ou ganhar valor. Neste caso, a informação permite uma maior previsibilidade do resultado, influenciando no valor adquirido/perdido. Neste cenário, onde a Tecnologia da Informação (TI) está presente em toda a organização; as alterações são mais rápidas e necessitam de um planejamento à TI mais bem estruturada. Essas alterações quando influenciam regras de negócio ou regulamentações, compõem riscos que resultando em sucessos ou insucessos.

O gerenciamento de risco (GR), procura identificar riscos, e a partir de uma análise, gerar contramedidas para maneja-los. Estes riscos quando tratados, podem ser aproveitados de maneira propícia para redução de gastos, e inicialmente o que poderia causar estragos dentro de uma organização, passa a ser uma das fontes para o crescimento dela. Desta forma, o objetivo deste trabalho é desenvolver um modelo para implantação de gestão de risco seguindo os princípios de *Information Technology Infrastructure Library* (ITIL) [8] e o *Control Objectives For Information end Realated Technology* (COBIT) [9], onde informações serão extraídas e analisadas para uma identificação do risco, seguido por uma análise, uma avaliação e posteriormente por um monitoramento, possuindo como uma das bases o modelo BS ISO/IEC 27005:2008[10]. Incorporando o GR, é esperado que problemas indesejados sejam evitados através do tratamento desses riscos, consequentemente as atividades do GR devem possibilitar que os clientes se sintam seguros em relação a tais riscos. Neste trabalho, as expressões 'gerenciamento de risco' e 'gestão de risco' são ambas usadas. Em geral, 'gerenciamento de risco' refere se a arquitetura usada para gerenciar o risco efetivamente, enquanto que 'gestão de risco' refere-se a aplicação dessa arquitetura

em riscos determinados. O presente trabalho apresenta um modelo para implantação da gestão de riscos em governança de TI, que através do preparo e planejamento, analisa os riscos organizacionais de TI, fazendo o papel de documentá-los e controlá-los, utilizando algumas práticas de modelos como PRINCE2 [11], a ISO 31000:2009 [12] e novamente ITIL [8] e COBIT [9] citados anteriormente.

Nomeado GAIA Canoa, o trabalho almeja através de um desenvolvimento de um modelo que a gestão de riscos permita uma melhora a atuação da governança. Será delimitado o campo de estudo para: riscos em governança de TI, com o intuito de cumprir o cronograma e objetivos propostos onde as pesquisas e experimentos serão propostos no laboratório GAIA da Universidade Estadual de Londrina (UEL).

Em seguida, o Capítulo 2 aborda os conceitos fundamentais para a assimilação do tema, tal como trabalhos correlatos e suas aplicações. No Capítulo 3, é apresentado o modelo proposto e sua função, no Capítulo 4 será abordado os resultados em relação a aplicação do modelo e uso, e por fim, no Capítulo 5 é apresentado a conclusão sobre o trabalho e seus alcances.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Governança e Gestão de TI

Para CobiT [9], empreendimentos existem para criar ou gerar valor à seus *stakeholders*, onde, criar valor entende-se como gerar benefícios com custo de recurso otimizando-se o risco. Deste modo, o objetivo da governança está ligado diretamente a criação de valores. A Figura 1 ilustra a criação de valor para um *stakeholder*.

Figura 1 – Criação de valores. Adaptada de [1]

Estes valores ou benefícios podem tomar formas diferentes, como financeiro para empresas, e de serviço público para governos. Segundo [9], uma organização tem muitos *stakeholders* com perspectivas diferentes de criação de valor. Desta forma, a governança atua como mediador de negociações e decisões entre diferentes *stakeholders*. Deste modo, para o Instituto Brasileiro de Governança Corporativa (IBGC) [13], a Governança Corporativa tem o papel de direcionar, monitorar e estimular, com o intuito de alinhar os interesses com boas práticas, gerando valores e permitindo a continuidade da empresa.

O crescimento do volume de informações demandou a criação de novas formas para o processamento dessa informação, que possibilitou com que a área de TI que até então era apenas fonte de despesa, tornasse uma área importante dentro de qualquer organização, pois possibilita uma melhora significativa no processamento de informações, auxiliando na tomada de decisão, sendo válido ressaltar que o valor adquirido é estimado por um *stakeholder* de acordo com sua necessidade. Deste modo para Vargas [14], existem sete fatores que determinam a necessidade ou não, do gerenciamento de um projeto, conforme o diagrama com os critérios propostos por Cleland [2]:

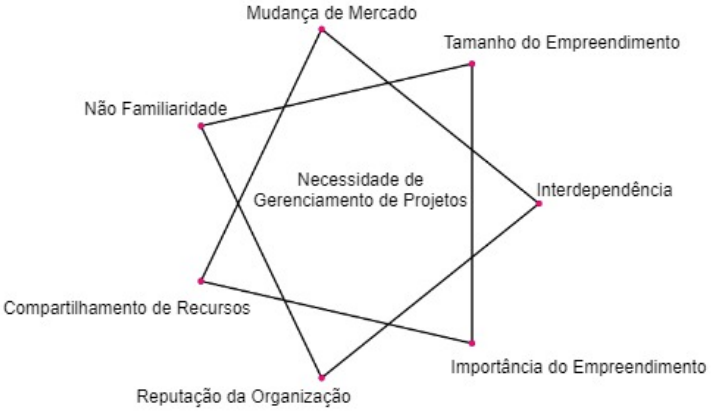

Figura 2 – Necessidade de gerenciamento de projetos. Adaptada de [2]

Ainda segundo Vargas [14], não é necessário que todos esses fatores sejam pertinentes, e basta que um desses fatores seja determinante para que o modelo de gerenciamento seja indispensável. Desta forma, há necessidade que a gestão de TI funcione como um facilitador para a Governança de TI, exercendo o mesmo papel dentro da Governança Corporativa, abrangendo processos de TI dentro da organização.

A Gestão de TI é regularizada pela ISO/IEC 20000 [15], que discorre sobre especificações e práticas de serviços na gerência de TI. Todavia, conforme Fernandes [3] nas últimas duas décadas vem surgindo uma série de modelos de melhores práticas para o auxílio do gerenciamento na governança de TI. Entre estes, são citados modelos como: ISO/IEC 38500, CobiT[9], ITIL[8], ISO 31000, PRINCE2[11], Project Management Body of Knowledge (PMBOK), SCRUM, etc. A figura 3 ilustra como os modelos de melhores práticas atuam na Governança de TI:

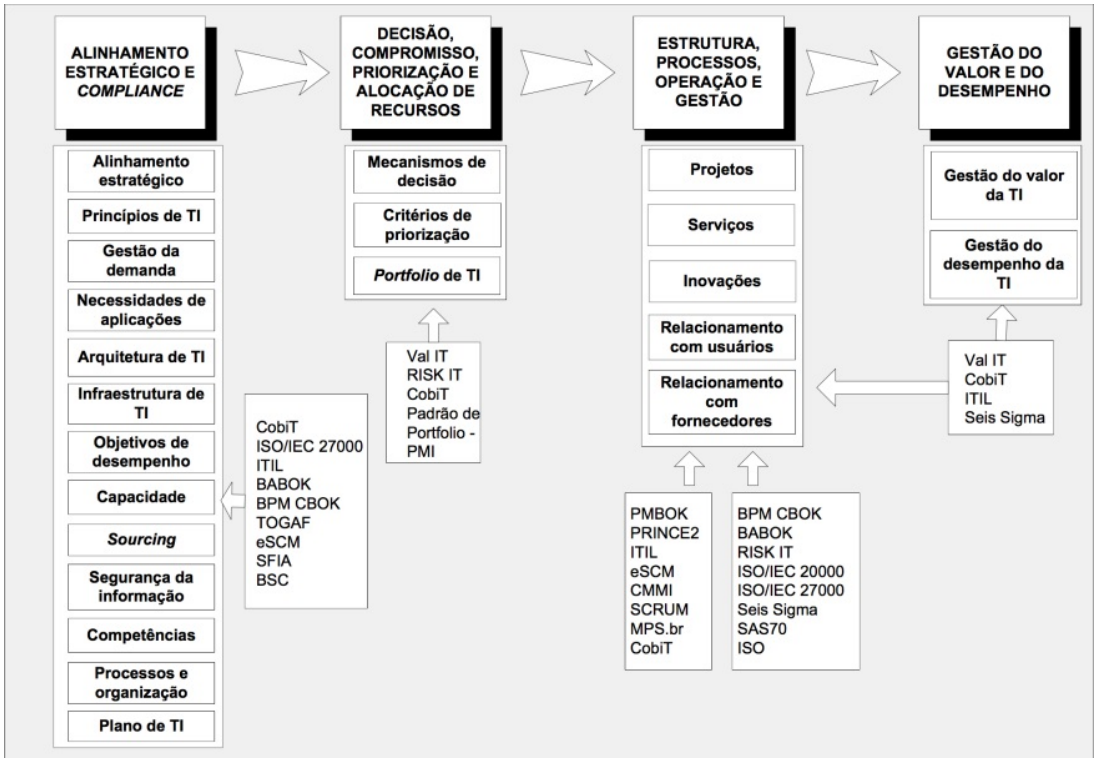

Figura 3 – Os modelos de melhores práticas no contexto da Governança de TI. Fonte: [3]

Segundo Fernandes [3], entre estes domínios e componentes utilizados por estes modelos, o alinhamento estratégico da TI busca determinar qual deve ser o alinhamento da TI em termos da arquitetura, infraestrutura, aplicações, processos e organização com as necessidades presentes e futuras do negócio; sendo os princípios de TI as regras a serem seguidas no âmbito da empresa, e que contribuem na tomada de decisão acerca da arquitetura e infraestrutura de TI, aquisição e desenvolvimento de aplicações, uso de padrões, gestão dos ativos de TI; a arquitetura reforça a padronização de processos, dados e tecnologias de negócio e dos valores e credos da organização.

2.2 Gerenciamento de Riscos

Para [16], risco é a combinação da probabilidade de um evento acontecer, acompanhado de sua consequência. Conforme CobiT [9], um risco de TI é relacionado a eventos de TI, que podem causar impacto no negócio.

Como o objetivo do modelo é fazer a gestão de riscos, é importante ressaltar as classificações de acordo com a Tabela 1 adaptada de Young[6].

Tabela 1 – Tipo de riscos, impactos e estratégias para o gerenciamento. Adaptada de [6]

Tipo	**Impacto**	**Estratégia**
Especulativo	Positivo ou negativo	Monitorar
Danoso	Negativo	Evitar

Desta forma, os riscos especulativos devem ser monitorados a fim de minimizar a as chances do evento negativo ocorrer, podendo assim aproveitar um impacto positivo. Já os riscos danosos devem ser evitados ou reduzidos levando em consideração que os resultados são indubitavelmente ruins.

No modelo *The Risk IT Framework* criado por [1], o risco pode ser categorizado da seguinte forma:

- *IT benefit/value enablement risk*—Associado a oportunidades perdidas em relação do uso da tecnologia a fim de melhorar a eficiência ou a efetividade dos processos de negócios ou servir de facilitador para novas iniciativas de negócios.
- *IT programme and project delivery risk*—Associado a contribuição da TI para novas ou melhores soluções de negócios, usualmente na forma de projetos ou programas como parte do portfólio de investimento.
- *IT operations and service delivery risk*—Associado a todos os aspectos dos negócios para uma performance usual de sistemas e serviços de TI, que podem acabar ou reduzir o valor do empreendimento.

Para Schwalbe [4], o gerenciamento de riscos é como a arte e ciência de identificar, analisar, e responder o risco em toda a vida de um projeto com os melhores interesses para alcançar o objetivo do projeto. Desta forma, o gerenciamento de risco tem um impacto positivo em projetos apurados. Como prova, Schwalbe [4] realizou uma pequisa com 260 empresas de TI e apresentou os seguintes resultados:

- 90% dos participantes possuem procedimentos para identificar e avaliar riscos.
- 80% antecipam e evitam problemas como benefício primário do gerenciamento de risco.
- 70% das organizações definiram os processos de desenvolvimento de software.
- 60% possuem escritório de gerenciamento de projeto.

Desta forma a Figura 4 revela graficamente os benefícios da prática de gerenciamento de risco das organizações que participaram das pesquisadas anteriormente.

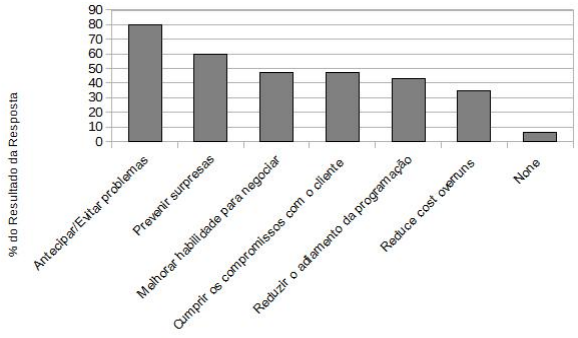

Figura 4 – Benefícios da Prática de Gestão de Risco em Softwares. Adaptada de [4]

Segundo Joia [17], o gerenciamento de riscos deve começar com um planejamento. Esta é uma das preocupações principais e deve acontecer na fase inicial das atividades e funciona como uma reflexão sobre como lidar com os riscos do projeto ao longo de sua concepção e desenvolvimento.

Deve-se um termo de abertura do projeto, estimativas de custos (prazo e tempo) e documentações respeitando as políticas corporativas. E já nessa fase ocorre decisões de *go/ no-go* de um projeto ou proposta. Na metodologia usada em [18], um plano de gerenciamento de risco(PGR) é criado em um processo de planejamento, que define como conduzir uma gestão de risco para um projeto.

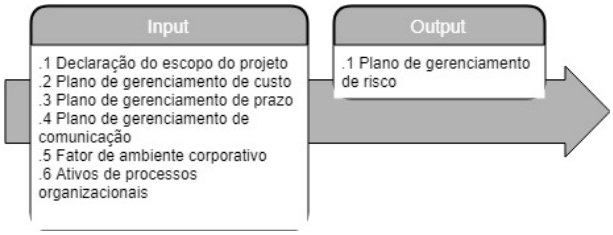

Figura 5 – PGR: *Inputs* e *Outputs*. Adaptado de [4]

A Figura 5 mostra um procedimento paralelo à de Schwalbe [4] no qual o ciclo de gerenciamento é divido em seis processos principais, dada a seguinte ordem:

1. **Planejamento do gerenciamento de risco** inclui a decisão de como abordar e planejar as atividades de gerenciamento de risco para um projeto. Revê o plano de gerenciamento do projeto, o termo de abertura do projeto, o registro do *stakeholder*, fatores ambientais da empresa e o ativo de processo organizacional. Equipes de projetos podem discutir e analisar a atividade de gerenciamento de risco para projetos particulares. Este processo tem como fruto um PGR;

2. **Identificação dos riscos** envolve estabelecer qual risco pode afetar cada projeto. Uma documentação é feita com o perfil de cada risco. Este processo permite uma

abertura de um registro de riscos;

3. **Análise qualitativa do risco** abrange priorizar os riscos baseado na probabilidade de ocorrer e a repercussão. Após a identificação dos riscos, equipes de projetos usam ferramentas e técnicas para classificar os riscos e atualizar os dados no registro de riscos. Este processo faz uma atualização dos documentos do projeto;

4. **Análise quantitativa do risco** envolve estimar a escala numérica do efeito que um risco pode provocar no objetivo do projeto. Este processo faz uma atualização dos documentos do projeto;

5. **Planejamento de respostas ao risco** inclui criar um preparo para melhorar oportunidades e reduzir os indícios aos objetivos do projeto. Equipes de projetos utilizam os resultados dos processos de gerenciamento que precedem este, para desenvolver estratégias de resposta aos riscos que muitas vezes resultam em atualizações no plano de gerenciamento de projeto e outros documentos do projeto;

6. **Controle do risco** envolve riscos residuais e identificados por monitoramento, revelando novos riscos, executando planos de respostas ao risco e avaliando a efetividade das estratégias ao longo da vida do projeto. Este processo produz informações de desempenho no trabalho, pedidos de mudanças e atualizações no plano de gestão do projeto, outros documentos do projeto e ativos de processo organizacional.

Para Chapman [19], os ganhos de valores estão relacionados à aplicar o *Risk Management Process* (RMP) que inclui estimular a efetiva integração do plano de gerenciamento de custos, facilitar considerações de atividades extras e focar nos próximos processos e erros de desempenho do produto. Assim, para que o modelo seja integralmente efetivo, o GR precisa encaminhar o *Project Life Cycle* (PLC) inteiro ao invés de trechos, deste modo guiando e informando cada fase do PLC. Ainda segundo Chapman [19], existem sete objetivos que caracterizam uma aproximação minimalista em relação ao custo-beneficio nas escolhas do RMP:

1. **Entender incertezas em termos gerais:** entender incertezas deve ir além da variabilidade e dados disponíveis. E deve corrigir ambiguidades com o foco em gerar melhores decisões possíveis para dados e informações e compreensão da estrutura;

2. **Entender fontes de incertezas e respostas(erros):** é importante a necessidade de compreender fontes de incertezas, pois algumas maneiras de administrar nem sempre são específicas de suas fontes e implicações de respostas que devem ser entendidas para avaliar os impactos;

3. **Determinar o que precisa quantificar apropriadamente:** distinguir o que é útil quantificado, ou melhor tratado como suposição ou condição em termos de eficácia para a tomada de decisão é extremamente importante;

4. **Gerenciar processos iterativos efetivamente e eficientemente:** para o melhor discernimento e aprendizagem, incertezas devem ser introduzidas em termos de processo iterativo, junto aos objetivos do processo que mudam nas consecutivas iterações. Uma vez que os subsequentes passos estão focados em melhorar as avaliações para conduzir o que importa. Desta forma, o último passo deve convencer os outros de que o interesse está sendo apropriadamente conduzido;

5. **Passar uma estimativa e avaliação minimalista inicialmente:** uma abordagem minimalista inicial é necessária uma vez que otimiza o processo e é mais fácil devido a falta de dados, permitindo evitar o uso de matriz de probabilidade simplista inicialmente;

6. **Evitar vieses otimistas para gerenciar expectativas efetivamente:** o viés otimista para maioria das abordagens à estimativa e avaliação necessita de uma atenção para gerenciar as expectativas de maneira efetiva. Quanto mais sofisticado o processo utilizado, mais otimista será o viés, prejudicando a credibilidade do GR na organização. Se isso levar a uma falha na aplicação do GR, pode precipitar a falha da organização;

7. **Simplicidade na complexidade construtiva:** já que a simplicidade é uma virtude importante em si, não apenas em relação a eficiência de uma abordagem minimalista de primeiro acesso, mas porque pode ampliar a clareza e aprofundar o discernimento. Porém, um nível apropriado de complexidade, também é importante, pelas mesmas razões. Obter o melhor equilíbrio é em parte uma questão de estrutura e processo, em parte uma questão de habilidades que podem ser aprendidas através de um processo que é projetado para melhorar a aprendizagem.

Segundo [20] os modelos para gestão de risco tem uma relevância significativa dentro de uma organização uma vez que aumentam a segurança dentro de um processo de maneira financeira e permitem reduzir as chances de insucesso dentro de um ciclo de processo. Atuam também como documento de comunicação dentro de uma organização, permitindo o rastreamento que envolve coletar, atualizar, monitorar e o controlar os riscos.

Dando proveito aos conhecimentos adquiridos, o trabalho visa desenvolver o Gaia Canoa, que é um modelo para implantação de gerenciamento de risco, promovendo uma maior segurança e convívio em relação aos riscos de uma Gestão e Governança de TI.

2.3 Trabalhos Correlatos

Após a abordagem inicial sobre GR, é sabido dizer que os modelos de gerenciamento de risco, seguem processos que devem ser adaptados para gerenciar os riscos de uma organização, desta maneira existem processos customizados para diferentes tipos de negócio.

Enquanto COBIT [9] possui uma visão macro empresarial, onde é tratado a estrutura organizacional, a infraestrutura, a cultura e a ética, Santos [21] afirma que a metodologia usada em *Failure Mode and Effect Analysis* (FMEA) define um sistema a ser analisado e constrói digrama de blocos para identificar as potenciais falhas e listar as ponteciais causas da imperfeição.

O PMBOK [22] divide o GR em seis processos: o planejamento do GR, a identificação do risco, a analise qualitativa do risco, a analise quantitativa do risco, plano de resposta ao risco e controle e monitoramento de risco. Ainda segundo Santos [21], o objetivo dos projetos é gerar um produto desconhecido, o que acaba envolvendo riscos durante o desenvolvimento, e afirma que no PMBOK [22] o 'risco' está em quarto lugar na lista de área citadas na literatura de pesquisas sobre gerenciamento de projetos.

Estes modelos são usados em escala global, e promovem uma segurança quanto aos riscos nos quais se buscam prevenir. Porém, não é garantido que um modelo de sucesso dentro de uma organização, possa ser bem sucedido em outra organização, uma vez que a complexidade ou até os fatores de um empreendimento varia conforme a organização. Desta forma, é esperado a aplicação do modelo mais apropriado a realidade da mesma.

3 GAIA CANOA: MODELO PARA GESTÃO DE RISCO EM GOVERNANÇA DE TI

Este trabalho aplica práticas de pesquisas empregues em trabalhos predecessores desenvolvidos no laboratório GAIA UEL e faz a classificação da pesquisa seguindo os padrões de Gaffo [23], desta forma sua natureza é aplicada, pois o conteúdo gerado é dedicado à um problema exclusivo, e o método científico é dedutivo, uma vez que a verificação da conclusão se dará por meio da validação das premissas. A seguir na Tabela 2 encontra-se as classificações sugeridas.

Tabela 2 – Classificação da Pesquisa

Característica	**Classificação**
Natureza	Pesquisa Aplicada
Objetivo	Pesquisa Exploratória
Método Científico	Dedutivo
Origem dos Dados	Múltiplas fontes
Procedimento técnicos	Pesquisa bibliográfica e Estudo de caso

Assim sendo, a fim de validar o modelo GAIA Canoa, o processo inicial foi utilizar o ciclo PDCA (Plan, Do, Check e Act)/roda de Deming formado por grupo de processos, ilustrados na Figura 6.

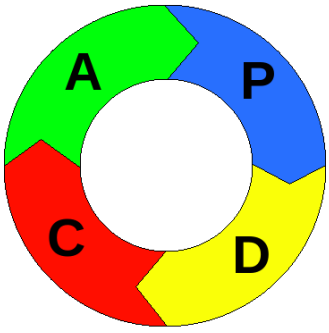

Figura 6 – Ciclo PDCA.

Estes grupos de processo são descritos a seguir:

- **Plan:** Determina as metas por meio de um foco e esclarecimento do objetivo para estabelecer expectativas do resultado. Nesta etapa são estabelecidas algumas regras para obtenção de metas;
- **Do:** Implementa o que foi planejado anteriormente, executando cada processo;

- **Check:** Faz uma análise da execução obtida com o planejamento, verificando se o processo cumpre o que foi proposto. É a etapa de verificação de erros ou desvios no processo;
- **Act:** De acordo com a etapa de *Check*, age para corrigir os erros ou desvio, para o progresso do que foi planejado.

3.1 Modelo

O modelo GAIA Canoa foi desenvolvido com o objetivo de ampliar processos, no qual a ferramenta utilizada para modelagem foi o Bizagi e sua estrutura é baseada no Gaia Riscos de Gaffo [23], sendo ilustrada na etapa inicial o estabelecimento do contexto, seguido respectivamente pela identificação dos riscos, análise ou avaliação, e o tratamento dos riscos. O monitoramento é feito a todo momento sobre as etapas de identificação, análise ou avaliação, e por fim realizar a mitigação caso exista uma necessidade do erro ser tratado, o processo é ilustrado na Figura 7 desenvolvida na ferramenta citada anteriormente.

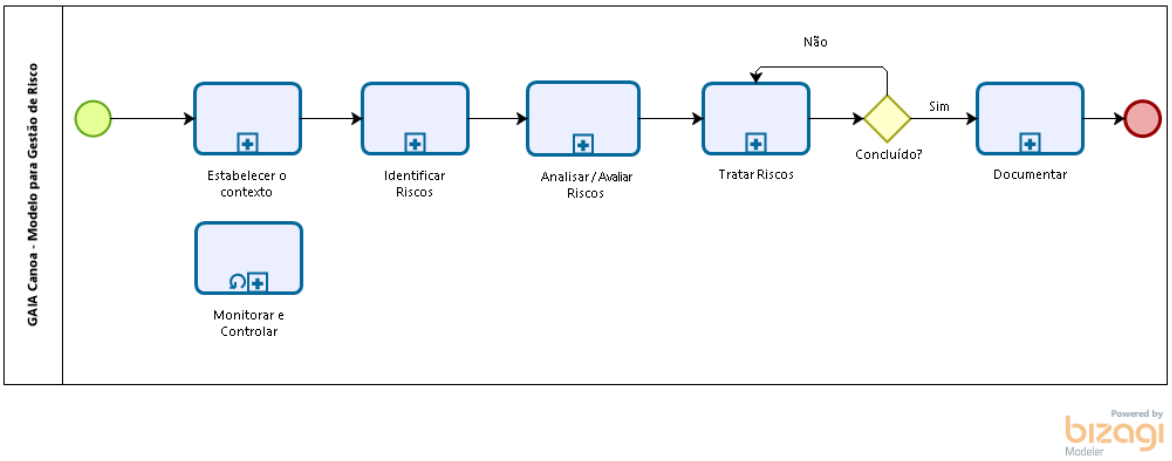

Figura 7 – Modelo: GAIA Canoa.

Após uma breve análise da figura 7, é possível atribuir uma especificação adequada para cada etapa do processo para uma compreensão melhor do modelo.

O Estabelecer o contexto: nesta etapa, é feita a avaliação da política do processo, seguida por critérios estabelecidos, métodos sugeridos e restrições do processo respectivamente, por fim ao verificar o cumprimento da premissa, o processo é documentado. A figura 8 ilustra o subprocesso para estabelecer o contexto:

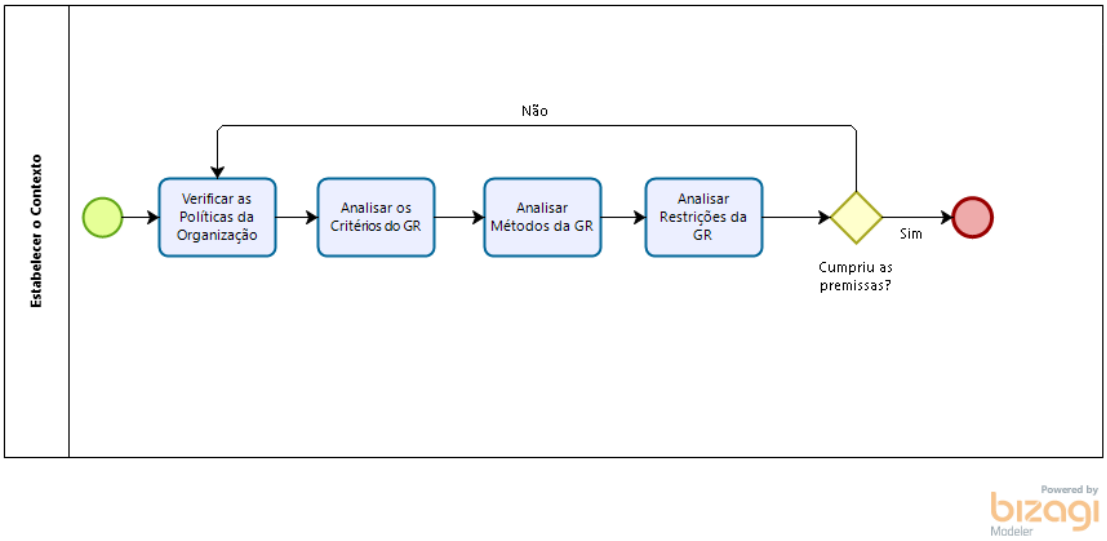

Figura 8 – Subprocesso: Estabelecer o Contexto

Identificar riscos: nesta etapa, é feita a verificação das fontes de risco, possibilitando o estudo de suas causas, desta forma é feito o cálculo da probabilidade de ocorrência, e é estimado possíveis prejuízos. Para finalizar a etapa, é feito a documentação do risco identificado. A figura 9 ilustra o subprocesso para identificar riscos:

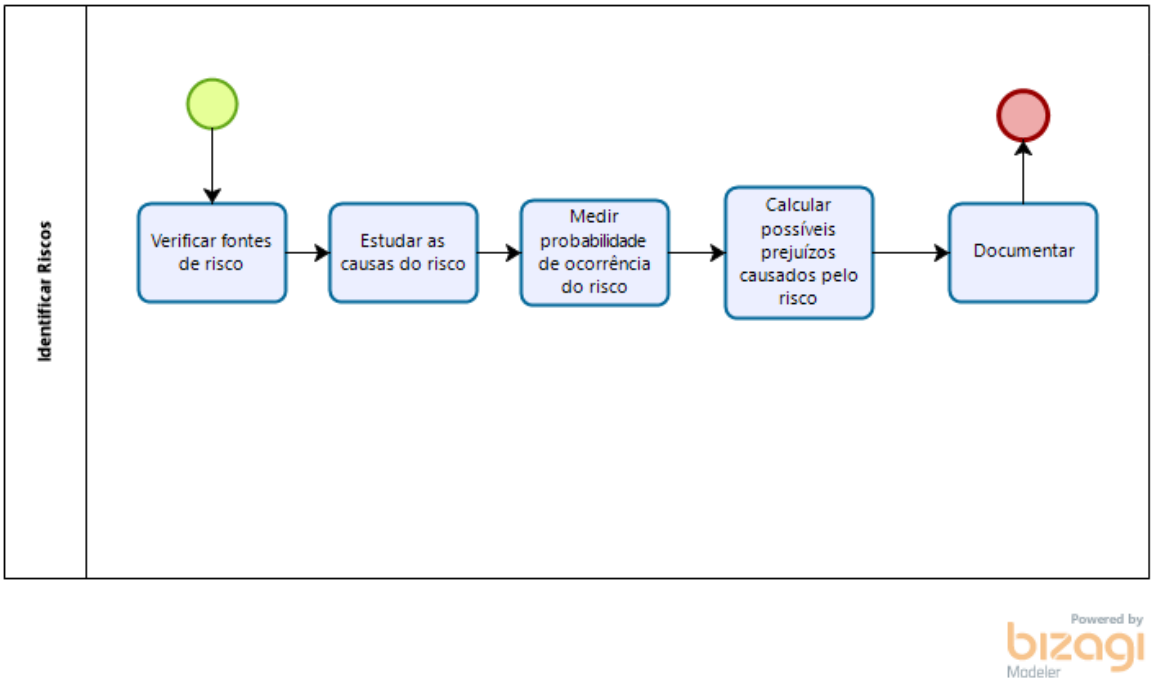

Figura 9 – Subprocesso: Identificar Riscos

Analisar/Avaliar Riscos: no início desta etapa é feito a filtragem dos riscos, define-se a quantificação da probabilidade e criticidade, logo em seguida é feita a classificação para finalmente documentar este processo. A figura 10 ilustra o subprocesso para analisar ou avaliar riscos:

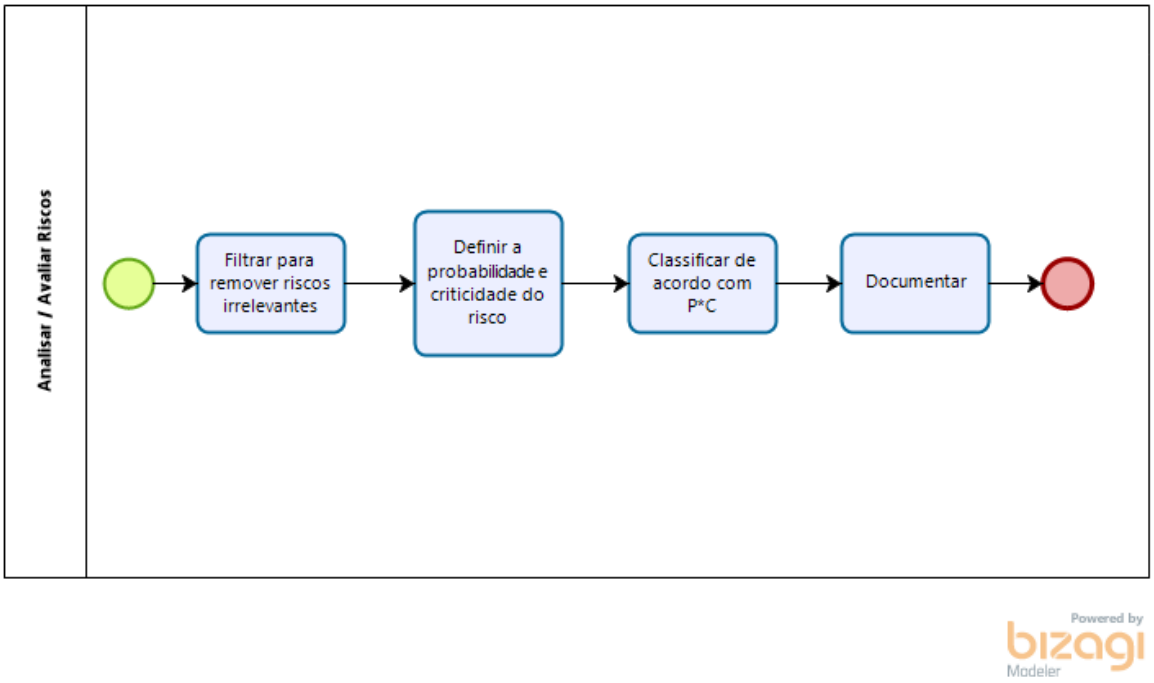

Figura 10 – Subprocesso: Analisar / Avaliar Riscos

Tratar Riscos: é nesta etapa que ficam presente as atividades e planos de tratamento, assim como a aprovação de riscos residuais uma vez que podem ser desprezíveis. A Tabela 3 foi gerada à partir do plano comumente utilizado para organizar e definir o tratamento do risco, e deve ser completada respectivamente com:

- **Risco:** esta área da tabela deve ser preenchida com o título ou o nome dado ao risco.
- **P:** esta área da tabela deve ser preenchida com a probabilidade em uma escala de 1(baixa) a 10(alta) de ocorrer o risco.
- **I:** esta área da tabela deve ser preenchida com o impacto de 1(pequeno) a 10(grande) do risco.
- **P*I:** esta área da tabela deve ser preenchida com o valor resultante da multiplicação da probabilidade P pelo impacto I. Quanto maior o valor resultante, maior a prioridade para que o risco seja resolvido.

- **Estratégia:** esta área da tabela deve ser preenchida com as estratégias uma das estratégias: aceitar, transferir, mitigar ou evitar.
- **Resposta ao Risco:** esta área da tabela deve ser preenchida com o plano definido pela empresa com o intuito de resolver o problema causador do risco.
- **Custo de Resposta:** esta área da tabela deve se preenchida com o valor que define o custo para colocar em prática o plano descrito na sessão *Resposta ao Risco* da Tabela 3.

A seguir a ilustração da Tabela 3:

Tabela 3 – Plano de Respostas à Riscos

Risco	P	I	P * I	Estratégia	Resposta ao Risco	Custo para

Monitoramento: Fiscaliza as atividades que garantem a relevância e a efetividade do GR com relação aos critérios estabelecidos. O monitoramento é executado em paralelo com as outras etapas do modelo em período integral e é utilizado o *Burndown Chart* ou Gráfico de *Burndown*, que é ilustrado na Figura 11:

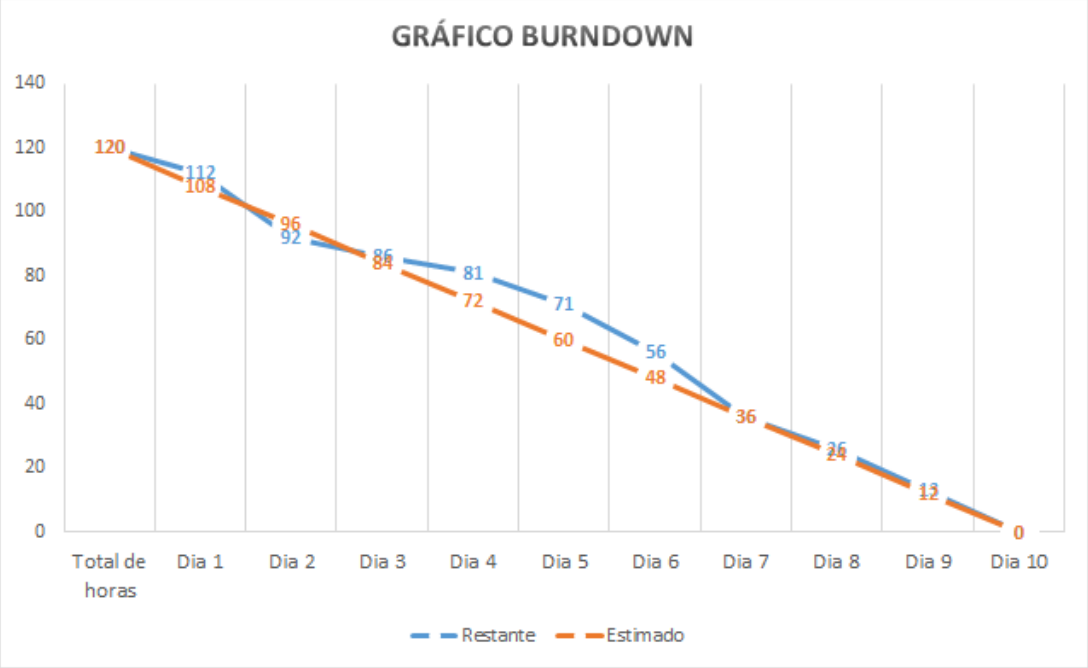

Figura 11 – Exemplo de Gráfico de Burndown. Adaptado de [5]

O gráfico de *Burndown* é formado por dois eixos: o eixo Y (vertical), que representa a demanda de risco a ser resolvido; e o eixo X (horizontal), que representa o tempo - a quantidade de tempo ou horas de trabalho para queimar(resolver) a demanda. Esse gráfico é representado com duas linhas: uma linha reta de cima para baixo que percorre da esquerda para a direita do gráfico, onde fica a previsão de conclusão de um processo; e a segunda linha que é a real, que revela como a organização agiu com relação a projeção de uso do tempo para a demanda. Para estimarmos a linha ideal, são levados em consideração a identificação de cada risco, com a probabilidade de ocorrer o risco, e o impacto do risco. A organização deve utilizar métodos como o *sprint* para tratar os riscos, desta forma, a linha ideal deve ser tracejada a cada determinado período com o objetivo de se tornar a meta para o tratamento de riscos. O mesmo serve para a linha real, no qual o valor de y na linha é aumentado quando o risco aumenta ou deixa de ser resolvido.

A figura 12 ilustra os subprocessos integrados no monitoramento que é realizado em tempo integral:

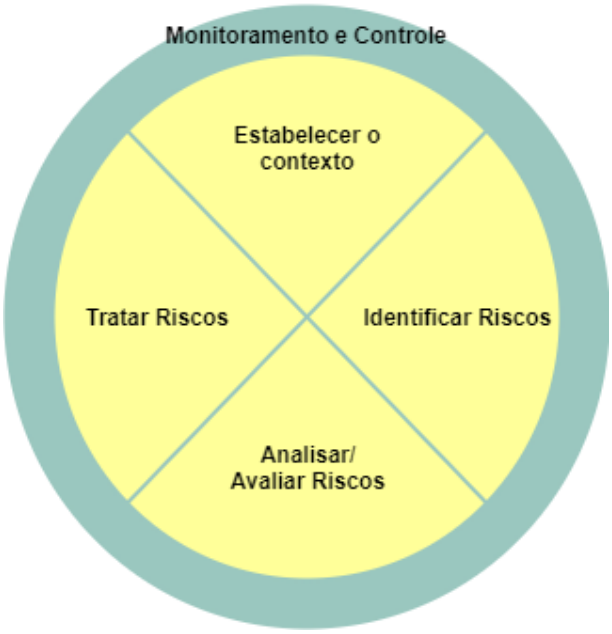

Figura 12 – Subprocesso: Monitorar e Controlar

4 RESULTADOS

A avaliação para este trabalho seguirá o método adotado por trabalhos do laboratório GAIA UEL, sendo proposto à um grupo de profissionais que atuam na área de governança em Londrina e região, sendo aplicado um questionário compostos por três questões objetivas e uma questão dissertativa que é utilizada como meio de *feedback*:

1. Os processos retratados no GAIA Canoa: Modelo para Gestão de Risco, cobrem todos os processos dentro de uma gestão de risco?
2. Na sua opinião, O Gaia Canoa: Modelo para Gestão de Risco é um modelo escalonável?
3. Na sua opinião, o GAIA Canoa: Modelo para Gestão de Risco contribui para a segurança em relação aos riscos dentro de uma organização?
4. Na sua opinião, o que pode ser melhorado no Gaia Canoa: Modelo para Gestão de Riscos?

As questões objetivas tem todas o mesmo formato, sendo atribuído a cada resposta uma nota no padrão que se segue:

1. Discordo Totalmente
2. Discordo
3. Indiferente
4. Concordo
5. Concordo Totalmente

Cada questão deve ser avaliada individualmente, assim como o modelo será avaliado como um todo. O modelo foi apresentado a especialistas composto basicamente por mestrandos, doutorandos e profissionais que atuam na área de Governança e Gestão de TI, gerando resultados interessantes.
Os profissionais atuam em diferentes empresas em Londrina e região, sendo bastante diversificados os ramos de atuação e também o porte das empresas. É importante salientar que todos os participantes atuantes no mercado de trabalho ocupam cargos de gerência e diretoria em suas respectivas empresas.

4.1 Questão 1

A Figura 13 mostra a avaliação recebida pela questão 1:

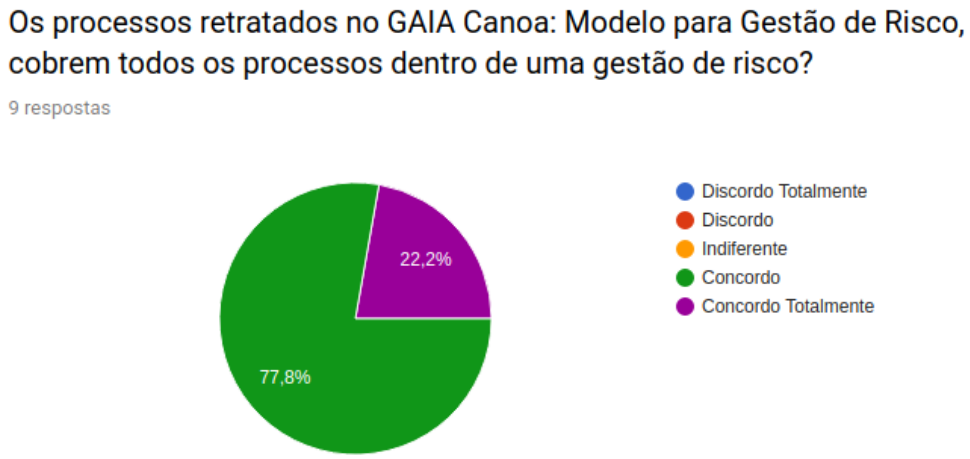

Figura 13 – Resultado da avaliação para a Questão 2

Analisando a avaliação, é possível afirmar que de acordo com os profissionais participantes da pesquisa, o GAIA Canoa cobriu todos os processos dentro de uma gestão de risco, tendo uma boa aceitação por parte destes profissionais.

4.2 Questão 2

A Figura 14 mostra a avaliação recebida pela questão 2:

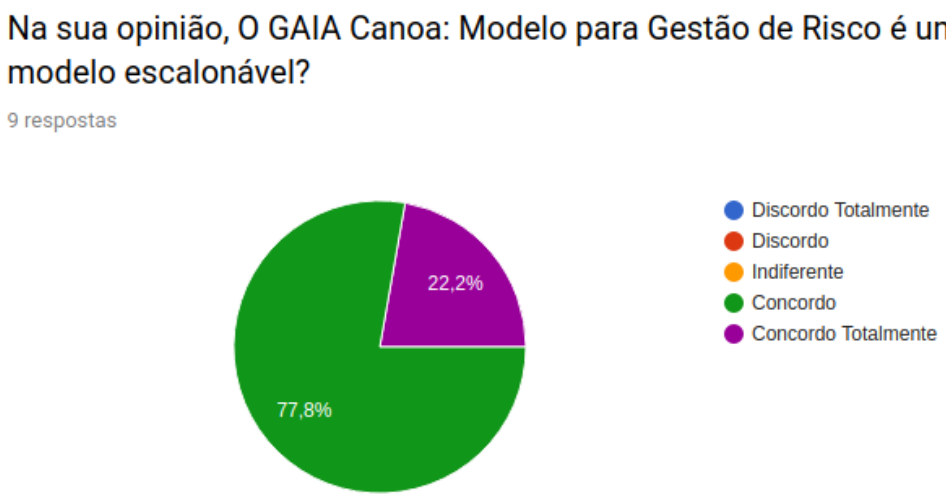

Figura 14 – Resultado da avaliação para a Questão 2

De fato ainda que muito positivo, o resultado é semelhante a questão 1, pois os participantes da pesquisa concordaram que o GAIA Canoa é um modelo escalonável, uma

vez que o modelo em si apresentou tais características.

4.3 Questão 3

A Figura 15 mostra a avaliação recebida pela questão 3:

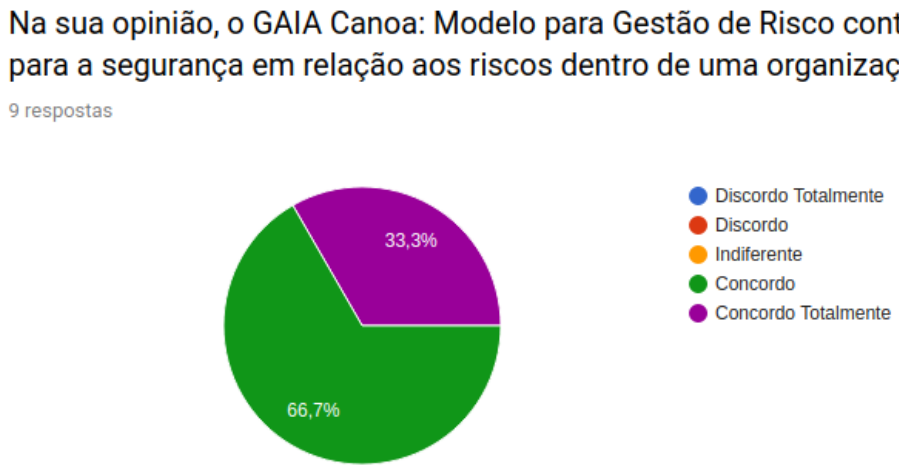

Figura 15 – Resultado da avaliação para a Questão 3

Analisando os resultados, é possível verificar que a avaliação obteve um resultado com valor médio aproximado de 4.86, afirmando que o modelo GAIA Canoa contribui para a segurança, mostrando efetividade na gestão de risco.

4.4 Questão 4

A questão 4 foi respondida com o seguinte *feedback* conforme é ilustrado na Figura 16:

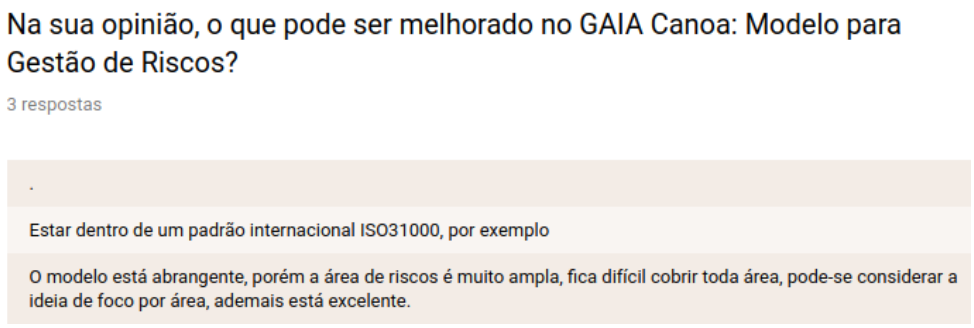

Figura 16 – Resultado da avaliação para a Questão 4

Entre as respostas, a segunda e a terceira respostas podem ser aproveitadas em uma futura implementação, permitindo uma padronização e criando um foco em uma área determinada para o GR.

4.5 Avaliação Geral

Tabela 4 – Resultados

	Resultados					
Avaliação:	5	4	3	2	1	Média Parcial
Questão 1	2	7	-	-	-	≈ 4.22
Questão 2	2	7	-	-	-	≈ 4.22
Questão 3	3	6	-	-	-	≈ 4.33
Média Total	≈ 4.26					

A Tabela 4 apresenta os resultados para cada questão, permitindo gerar uma média parcial e uma média total para as mesmas. Desta forma, com o resultado aproximado de 4.26 pode se dizer que o GAIA Canoa: Modelo para Gestão de Risco atingiu um bom nível de aceitação dos profissionais consultados, gerando indícios de uma aplicação prática bem sucedida.

5 CONCLUSÃO

No contexto apresentado, conclui-se que o cenário atual para organizações é repleto de projetos que muitas vezes pela quantidade ou qualidade, elevam a complexidade quando postos em prática, simultaneamente aumentando os riscos. Desta forma, o Gerenciamento de Riscos(GR) tem o papel fundamental de trabalhar com os riscos que há nos processos, identificando-os, e após a análise, tratando-os para reduzir os riscos em termos de probabilidade ou impacto, potencializando a ocorrência de ganhos para o *stakeholder*. Assim, o GR acaba se tornando essencial para a organização, uma vez que possui um forte alinhamento com o interesse da Governança.

Com a visão de montar estratégias para tratar os riscos que o modelo Gaia Canoa apresenta propostas para atender estrategicamente os projetos, viabilizando o custo e a segurança em relação aos riscos que vão surgindo, e através das documentações integra o histórico de riscos aumentando a confiabilidade no tratamento.

Por isso, o modelo GAIA Canoa é sugerido a ser adaptado e implantado em diversas áreas de uma organização, seguindo as etapas do GR, podendo prevenir e atuar no tratamento de riscos que podem ser prejudiciais à organização. Deste modo, pode se afirmar que com a análise dos processos e adequação às etapas do GR permite uma introdução do modelo desenvolvido.

REFERÊNCIAS

[1] ISACA. Cobit 5 for risk. In: ISACA. [S.l.], 2013.

[2] D.L., I. L. C. *Project Management: Strategic Design and Implementation*. Fourth edition. [s.n.], 2002. ISBN 0071393102,9780071393102,0071229698,9780071229692,9780071459143. Disponível em: <http://gen.lib.rus.ec/book/index.php?md5=8F5F75B4566D23BB7E60D2D62BC2C0E4>.

[3] FERNANDES, A. A.; ABREU, V. F. D. *Implantando a Governançaa de TI-: Da estratégia à Gestão de Processos e Serviços*. [S.l.]: Brasport, 2014.

[4] SCHWALBE, K. *Information technology project management*. [S.l.]: Cengage Learning, 2015.

[5] RIEPER. *Gráfico Burndown Scrum Excel*. [S.l.], 2016. Disponível em: <https://www.guiadoexcel.com.br/grafico-burndown-scrum-excel/>.

[6] YOUNG, P. C.; TIPPINS, S. C. *Managing business risk: an organization-wide approach to risk management*. [S.l.]: Amacom New York, 2001.

[7] TARANTINO, D. A. *The Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices*. Wiley, 2008. ISBN 047009589X. Disponível em: <http://gen.lib.rus.ec/book/index.php?md5=597FF52337E974AC42A860B4030E4BF8>.

[8] AXELOS. *Information Technology Infrastructure Library*. [S.l.], 2011. Disponível em: <https://www.axelos.com/best-practice-solutions/itil/>.

[9] ISACA. *Modelo Corporativo para Governança e Gestão de TI da Organização Personal(COBIT 5)*. [S.l.], 2012. Disponível em: <http://www.isaca.org/COBIT/Pages/default.aspx>.

[10] BSI. *BS ISO IEC 27005:2008 Information technology – Security techniques – Information security risk management*. [s.n.]. ISBN 9780580545139. Disponível em: <http://gen.lib.rus.ec/book/index.php?md5=CC5395203AC5DB06CFB3BD029DF88D65>.

[11] AXELOS. *PRojects IN Controlled Environments*. [S.l.], 2009. Disponível em: <https://www.axelos.com/best-practice-solutions/prince2>.

[12] ISO. *Norma Internacional ISO 31000:2018*. ISO, 2018. Disponível em: <http://gen.lib.rus.ec/book/index.php?md5=1fcc4363ce725e27ebb91d9cdf6beaba>.

[13] IBGC. *Governança Corporativa*. [S.l.], 2014. Disponível em: <https://www.ibgc.org.br/conhecimento/governanca-corporativa>.

[14] VARGAS, R. V. *Gerenciamento de Projetos (6a edição)*. [S.l.]: Brasport, 2005.

[15] STANDARDIZATION. *ISO/IEC 20000-1:2011*. [S.l.], 2011. Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso-iec:20000:-1:ed-2:v1:en>.

[16] GUIDE, I. 73: 2009. *Risk management—Vocabulary*, v. 551, p. 49, 2009.

[17] JOIA, L. A. *Gerenciamento de riscos em projetos*. [S.l.]: Editora FGV, 2015.

[18] GUIDE, A. Project management body of knowledge (pmbok® guide). In: *Project Management Institute*. [S.l.: s.n.], 2001.

[19] CHAPMAN, C.; WARD, S. *Project risk management: processes, techniques, and insights*. [S.l.]: Wiley, 2003.

[20] Perera, J.; Holsomback, J. An integrated risk management tool and process. In: *2005 IEEE Aerospace Conference*. [S.l.: s.n.], 2005. p. 129–136.

[21] SANTOS, F. R. S. d.; CABRAL, S. Fmea and pmbok applied to project risk management. *JISTEM-Journal of Information Systems and Technology Management*, SciELO Brasil, v. 5, n. 2, p. 347–364, 2008.

[22] PMI. *PMBOK® Guide* . [S.l.], 2017. Disponível em: <https://www.pmi.org/pmbok-guide-standards/foundational/pmbok>.

[23] GAFFO, F. H.; BARROS, R. M. D. Gaia risks-a service-based framework to manage project risks. In: IEEE. *2012 XXXVIII Conferencia Latinoamericana En Informatica (CLEI)*. [S.l.], 2012. p. 1–10.

Apêndices

Anexos

TRABALHOS PUBLICADOS PELO AUTOR