UNIVERSIDADE FEEVALE

CLEIBER ANDRÉ MUNIZ DA CUNHA

PROPOSIÇÃO DE UM MODELO DE GESTÃO DE RISCOS ORIENTADO À TECNOLOGIA DA INFORMAÇÃO

Novo Hamburgo, Julho de 2011.

CLEIBER ANDRÉ MUNIZ DA CUNHA

cleiberc@terra.com.br

PROPOSIÇÃO DE UM MODELO DE GESTÃO DE RISCOS ORIENTADO À TECNOLOGIA DA INFORMAÇÃO

Professor orientador: Roberto Scheid

Novo Hamburgo, Julho de 2011.

CLEIBER ANDRÉ MUNIZ DA CUNHA

Trabalho de Conclusão do Curso de Sistemas de Informação, com título **Proposição de um modelo de gestão de riscos orientado à tecnologia da informação**, submetido ao corpo docente da Universidade Feevale, como requisito necessário para obtenção do Grau de Bacharel em Sistemas de Informação.

Aprovado por:

_____
Prof. Roberto Scheid
Professor Orientador

_____
Marcelo Carboni Gomes
Professor Avaliador

_____
Luis Roberto Ulbrich
Professor Avaliador

Novo Hamburgo, julho de 2011.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me guiado e dado forças para alcançar mais este objetivo. Aos meus pais que me ensinaram valores essenciais para toda minha vida e a importância do conhecimento.

À minha esposa Letícia pelo apoio e incentivo para a conclusão do curso. Aos nossos filhos, Juan e Gaby pela compreensão nos momentos de ausência e nos momentos difícieis que passamos juntos.

Aos familiares, amigos, colegas acadêmicos, professores, especialmente ao amigo e orientador Roberto Scheid, pela compreensão, apoio e paciência para o desenvolvimento deste trabalho.

À empresa e aos colegas profissionais pela oportunidade e boa vontade que contribuiram de alguma maneira com o desenvolvimento deste trabalho.

RESUMO

A gestão de riscos possui diversas ferramentas que são utilizadas pelas mais diversas empresas, a fim de prevenir impactos aos negócios e contribuir na diminuição das incertezas dos projetos. Na gestão de projetos, o gerente precisa prever o que pode dar errado e quais seriam as respectivas ações para mitigar o(s) problema(s). Assim, a gestão de riscos incide numa ferramenta importante para que os interessados do projeto visualizem de forma clara quais os possíveis riscos que podem surgir durante a execução do mesmo. Em infraestrutura de TI (Tecnologia da Informação), a gestão de riscos traz sua contribuição uma vez que possibilita ao gerente demonstrar para seus superiores – entre outras coisas – os riscos que estão associados aos projetos. Muitas vezes, convencer o empresariado da necessidade de investimentos pode ser uma tarefa complicada, especialmente em TI. Pois, em muitos casos, não é possível mensurar o retorno do mesmo, e isso contribui com a incerteza na tomada de decisão. Portanto, a gestão de riscos consiste numa forma de justificar os investimentos a serem feitos, não apenas pelo valor a ser investido, mas pelas consequências que podem vir ocorrer caso isso não aconteça. Sendo assim, este trabalho tem por objetivo propor um modelo de gestão de riscos para auxiliar a direção das empresas quando da tomada de decisão associada à Tecnologia da Informação. Desta forma, possibilitará que os riscos certos sejam conhecidos e assumidos pela alta direção. A fim de validar a sistemática proposta, a mesma será aplicada da seguinte forma: 1) pesquisa-ação em uma empresa do segmento químico situada na região do Vale dos Sinos – RS; e 2) estudo de caso em 5 (cinco) empresas de diferentes ramos de atividades (indústria calçadista, clínica médica, *software house* e governamental) de diferentes regiões.

Palavras-chave: Governança de TI, Infraestrutura de TI, Gestão de Riscos, Segurança da Informação.

ABSTRACT

Risk management is an useful tool used by most of the companies and its main objective is to prevent impacts on the businesses and also contribute to reduce the uncertainty of the projects. On project management, usually a manager needs to anticipate which risks the company is exposed to and which actions would have to be taken in order to mitigate the risks. Therefore, risk management is an important mechanism that provides a clear view of the possible risks that the companies are exposed to during the time of the project and it should cover all people involved on it. In IT infrastructure (Information Technology Infrastructure), risk management contributes to the manager demonstrates to his superiors – among other things – the risks related to the projects. Usually, it is a difficult task to convince the stakeholders about the needs of investments, especially on IT projects. In fact, at most cases, it is not possible to measure the result of the investment, and this contributes to the uncertainty in decision making. Hence, risk management also consists in a way to justify a possible investment, not only due to the amount that would be spent on it but the consequences that may occur in case you do not do it. Thus, this paper aims to propose a risk management model to help the Business Board when they need to take some important decision related to IT investments. Finally, it will allow that correct risks are known and are assumed by the Board. To vefify the systematic proposed, it will be done: 1) action-research in a Chemical industry located at Vale dos Sinos region, in RS and 2) case study in 5 (five) companies with different activities and different regions.

Keywords: IT Governance, IT infrastructure, Risk Management, Information Security.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ALE	*Annualized Loss Expectancy*
ARO	*Annualized Rate Occurrence*
BI	*Business Inteligence*
CPM	*Corporate Performance Management*
CRM	*Customer Relationship Management*
CIO	*Chief Information Officer*
CMMI	*Capability Maturity Model Integration*
COBIT	*Control Objectives for Information and Related Technology*
EF	*Exposure Factor*
GR	Gestão de Riscos
ISO	*International Organization for Standardization*
ITGI	*Information Technology Governance Institute*
ITIL	*Information Technology Infrastructure Library*
PDCA	*Plan, Do, Check, Act*
PI	Probabilidade e Impacto
PMBOK	*Project Management Body of Knowledge*
PMI	*Project Management Institute*
RH	Recursos Humanos
SI	Segurança da Informação
SLE	*Single Loss Expectancy*
SCM	*Supply Chain Management*
SWOT	*Strengths, Weaknesses, Opportunities, Threats*
TI	Tecnologia da Informação

SUMÁRIO

INTRODUÇÃO

Risco é uma das condições essenciais para a inovação conforme definido por Brown (2005, p. 60). Ele afirma que os riscos devem ser gerenciados; ou seja, alimentados e controlados. A governança de riscos é o conjunto de processos, políticas e estruturas que proporcionam uma visão de nível empresarial de todos os riscos, de maneira que os executivos possam priorizar e investir apropriadamente os recursos (WESTERMAN; HUNTER, 2008, p. 42).

> Os riscos desafiam muitos projetos e negócios por serem complexos e multifacetados. Como resultados dos processos de gerenciamento de riscos são gerados muitos dados e isso facilita a sobrecarga sobre os gerentes ou mesmo a sua fadiga. Este pode ser o principal fator que propicia falha no apontamento dos riscos mais importantes. Ainda mais significante é o fato de que frequentemente é difícil identificar as relações ou dependências entre os riscos, em que a combinação de efeito entre eles poderia ser mais importante do que ele individualmente (HILLSON, 2008, p. 9).

Spohr; Sauvé (2003, p. 6) contextualizam que se faz necessário que as empresas conheçam melhor os recursos, as promessas e a realidade das novas tecnologias, avaliando até que ponto elas devem modificar sua forma de trabalho para adotar alguma destas tecnologias. Sob este contexto, é preciso que qualquer tomada de decisão com relação à adoção de tecnologias novas ou emergentes tenha como objetivo principal o crescimento do negócio.

A palavra risco, normalmente, remete à problemas. Mas, sob a ótica de Slywotzky; Drzik (2005, p. 66), existe também o lado bom, onde a gestão de riscos estratégica permite ao executivo passar da “defesa ao ataque”. Em geral, olha-se para os perigos do risco, e a reação da gerência é de buscar saídas para minimizar a exposição a ele.

Segundo Freemann; Hulme; Buehler (2008, p. 67), sem processos sólidos de gestão de riscos, a empresa pende para um de 2 (dois) extremos:

1) Excesso de exposição; ou

2) Excesso de proteção.

Considerando que nenhuma empresa possa estar completamente livre de riscos, muitos gestores buscam mecanismos para identificar e apresentar aos executivos de negócio aqueles riscos mais significativos (WESTERMAN; HUNTER, 2008, p. 5-12). Os autores complementam ainda que, muitos empresários tratam os riscos de TI por um viés meramente técnico; considerando que o assunto deva ser tratado somente pelo Gerente de TI, que possui conhecimento para tal. O ideal seria administrar os riscos tendo em consideração uma visão comercial integrada ao risco de TI. Os Autores destacam que existem 3 (três) disciplinas

centrais que os gestores de riscos deveriam considerar como base na elaboração do seu plano de gestão:

- “Apagar menos incêndios”, que significa diminuir a quantidade de incidentes no processo de TI;
- Alicerce da TI melhor estruturado, para que a infraestrutura de TI que fornece a sustentação para o negócio seja bem dimencionada e estável às àreas de negócios;
- Transformar riscos em oportunidades.

Seguindo nesta linha de raciocínio, Westerman; Hunter (2008, p. 179) abordam que quando uma empresa vivencia surpresas frequentes, ou tenha atingido o ponto em que o mau desempenho e as falhas de TI já nem a surpreenda, então sua gestão de riscos de TI não está funcionando. Neste caso, é necessário repará-la antes de ter uma surpresa perigosamente significativa.

Sob esta ótica, o objetivo deste trabalho será a elaboração de um modelo de gestão de riscos orientado a TI que possa fornecer argumentos mensuráveis para auxiliar a direção da companhia a conhecer melhor os riscos a que está exposta.

Salienta-se que por questões de tempo, o escopo do presente trabalho não compreenderá a gestão de riscos para desenvolvimento de softwares e *helpdesk*.

Consideram-se como objetivos específicos os apresentados a seguir:

- Comparar abordagens de diferentes autores sobre práticas de gestão de riscos e governança de TI voltados à infraestrutura e segurança da informação;
- Propor um modelo de gestão de riscos orientado a Tecnologia da Informação;
- Pesquisar software(s) *freeware(s)* e proprietário(s) existente(s) que venha(m) atender os requisitos propostos pelo modelo sugerido pelo presente trabalho de maneira que se possa(m) recomendá-lo(s) como sendo boas práticas (*Benchmark*);
- Efetuar um estudo de caso em diferentes empresas, através de questionários, a partir do modelo proposto, com o objetivo de verificar sua aderência. E, efetuar uma pesquisa-ação em uma empresa do segmento químico situada na região do Vale dos Sinos – RS;

1 REVISÃO BIBLIOGRÁFICA

De acordo com o objetivo deste trabalho, propor um modelo de gestão de riscos para a TI foi realisado uma revisão bibliográfica sobre os principais temas desenvolvidos ao longo do trabalho. Primeiramente será apresentado o processo de governança de TI, para explorar àqueles tópicos que serão mais utilizados no decorrer do trabalho. Na seqüência uma aborgagem sobre os conceitos, definições, processos e ferramentas que são aplicadas à gestão de riscos.

1.1 Governança de Tecnologia da Informação

Governança de TI pode ser definida como a especificação dos direitos decisórios e do framework de responsabilidades para estimular comportamentos desejáveis na utilização de TI (MANSUR apud WEILL; ROSS, 2007, p. 2).

Fernandes; Abreu (2008, p. 14) acrescenta que governança de TI representa o compartilhamento de decisões de TI com os demais dirigentes da organização e estabelece as regras, a organização e os processos. Este processo é o que norteia o uso da tecnologia da informação pelos usuários, departamentos, divisões, negócios da organização, fornecedores e clientes. Na visão do autor, a governança de TI deve:

- Garantir o alinhamento da TI ao negócio;
- Garantir a continuidade do negócio contra interrupções e falhas;
- Garantir o alinhamento da TI a marcos de regulação externa.

Na figura 1.1, encontram-se os fatores que motivam a gonvernança de TI. Na figura percebe-se a forte ligação entre TI e negócios.

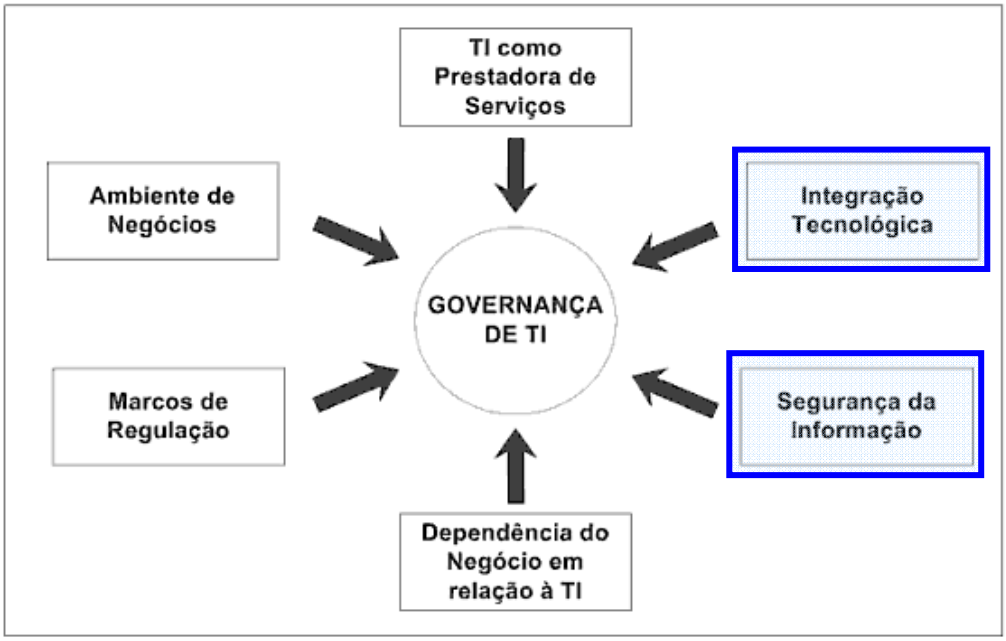


Figura 1.1 – Fatores motivadores da governança de TI
Fonte: Adaptado de Fernandes; Abreu (2008, p. 20)

Conforme a delimitação do presente trabalho, será verificado apenas os fatores referente à infraestrutura de TI e Segurança da informação como destacado na figura 1.1.

1.1.1 Infraestrutura de TI

Para Mansur (2007, p. 2), infraestrutura de TI são basicamente as decisões referente a capacidade atual e planejada de TI disponíveis para o negócio, sob a forma de serviços compartilhados. O autor ilustra ainda que investimentos excessivos em infraestrutura representa desperdício de dinheiro pela depreciação dos ativos; de outro lado, um investimento escasso implica em problemas operacionais e em decisões de investimento emergenciais. Na figura 1.2, pode-se visualizar como é composta a infraestrutura de TI de acordo com a visão do autor.

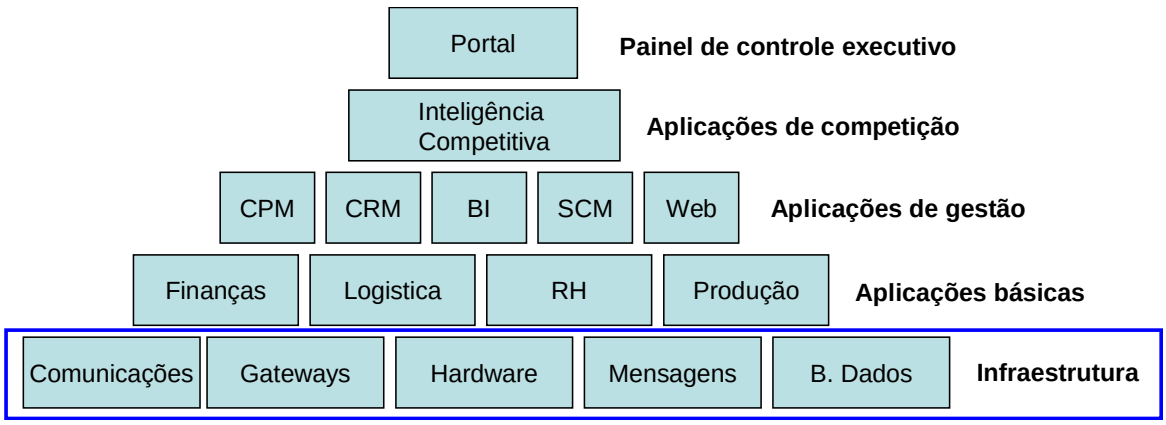


Figura 1.2 – Modelo completo de infraestrutura de TI
Fonte: Adaptado de Mansur (2007, p. 24)

1.1.2 Segurança da Informação (SI)

Nesta seção, procuraram-se trazer informações sobre a segurança da informação, seus principais aspectos e conceitos para o melhor entendimento do trabalho.

A definição de segurança pode ser entendida como o estado de estar livre de perigos e incertezas. Dentro de uma organização, esta segurança costuma se aplicar a tudo aquilo que possui valor e, consequentemente, demanda proteção. Os ativos podem estar categorizados por: 1) tangíveis: que são computadores, impressoras, móveis; 2) intangíveis: a imagem da empresa, marca do produto, etc. Mas também podem estar classificados de outra forma, tais como: 1) lógicos: dados; 2) físicos: fábrica; 3) humano: empregados. Sendo assim, segurança da informação é aquela que visa à proteção de ativos que contêm informações (RAMOS et al, 2006, p. 19).

1.1.2.1 Aspectos de Segurança da Informação

A segurança, para Ramos et al (2006, p. 20), busca a proteção contra situações nas quais os prejuízos são causados por conta de danos diretos aos ativos ou por situações prejudiciais inesperadas. O autor menciona que para evitar que tais situações ocorram, sugere-se que seja dispensada atenção sobre os 3 (três) aspectos da pirâmide ou tríade da SI (figura 1.3).

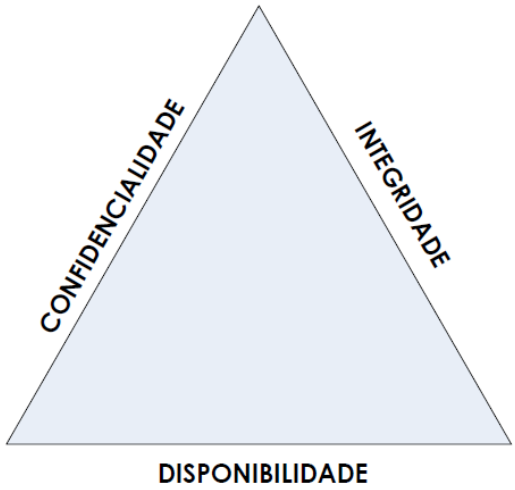


Figura 1.3 – Pirâmide ou tríade da SI
Fonte: Ramos et al (2006, p. 21)

- ***Confidencialidade*** – significa garantir que apenas pessoas que devem ter conhecimento a respeito de uma informação possam acessá-la;

- ***Integridade –*** a preservação da integridade envolve proteger as informações contra alterações em seu estado original, intencional ou não;
- ***Disponibilidade*** – é aquela informação que pode ser acessada por aqueles que dela necessitam, no momento em que precisam.

1.1.3 Utilização das melhores práticas de TI

A combinação das metodologias (ITIL, CobiT, ISO, Six Sigma, etc.) reflete em um processo de governança de TI mais forte com o objetivo de atender a gestão de riscos demandada pelo mercado. Concomitantemente, as métricas claras e objetivas permitem mediar a real contribuição da área em relação aos lucros, redução dos custos, a melhoria dos serviços (MANSUR, 2007, p. 8).

A seguir, no quadro 1.1, pode-se verificar que existem diversos modelos e metodologias que a TI pode utilizar a seu favor em relação a gestão de riscos.

Quadro 1.1 – Melhores práticas de TI voltado à gestão de riscos

Modelo de melhores práticas	***Escopo do Modelo***
CobiT – *Control Objectives for Information and related Technology.*	Modelo abrangente aplicável para a auditoria e controle de processos de TI, desde o planejamento da tecnologia até a monitoração e auditoria de todos os processos.
CMMI – *Capability Maturity Model Integration (for development)*	Desenvolvimento de produtos e projetos de sistemas e software.
ITIL – *Information Technology Infrastructure Library*	Infraestrutura de tecnologia da informação (definição da estratégia, desenho, transição, operação e melhoria contínua do serviço).
ISO/IEC 27001 e ISO/IEC 27002 – Código de prática para a gestão da segurança da informação.	Segurança da informação.
PMBOK – *Project Management Body of Knowledge.*	*Base de conhecimento em gestão de projetos.*

Fonte: Adaptado de Fernandes; Abreu (2008, p. 164).

Nas duas últimas décadas, vem surgindo e sendo elaborada uma série de modelos de melhores práticas para TI conforme demonstrado no quadro 1.1. Alguns desses modelos são originais e outros são derivados e/ou evoluídos de outros modelos (FERNANDES; ABREU, 2008, p. 164). Em gestão de riscos, segundo referencial bibliográfico pesquisado, nota-se as orgenizações têm adotado o uso de metologias como “melhores práticas” de TI. As mais citadas, estão no quadro 1.1 acima. Para tanto é necessário que se conheça os conceitos de risco, como podem gerenciados através de técnicas de identificação, análise e planos de resposta aos mesmos.

1.2 Riscos

A palavra risco deriva do italiano antigo “riscare”, que significa “ousar”. Os riscos, de acordo com Baraldi, são os elementos incertos e as expectativas que agem constantemente sobre os meios estratégicos (pessoas, processos, informação e comunicação) e sobre o ambiente podendo provocar desastres financeiros e morais. Os riscos devem ser avaliados quanto à relevância de seus impactos e probabilidades de suas ocorrências, ajustados pelos efeitos dos respectivos controles internos (BARALDI, 2005).

De fato, riscos são incertezas. Quanto mais breve os riscos e incertezas são conhecidos, melhor preparada sua organização estará para lidar com o mesmo, caso ocorram. É necessário encontrar o ponto no quais as partes interessadas estão dispostas a enfrentar o risco com base nos benefícios que eles podem trazer (HELDMAN, 2009).

Risco deve ser considerado como a probabilidade de uma ameaça explorar uma – ou várias – vulnerabilidades causando prejuízos. Em termos gerais, o risco pode estar associado a algo negativo ou positivo (RAMOS et al, 2006, p. 48-49).

> Minimizar o impacto negativo sobre a organização e a segurança na tomada de decisão são as razões fundamentais para que as organizações implementem um processo de gerenciamento de risco de TI (NIST, 2002).

1.2.1 Termos e definições relacionados a riscos

De acordo com a bibliografia estudada, identificaram-se diversos termos que podem ser relevantes e fascilitar o entendimento das próximas seções. Sendo assim a seguir está uma lista de termos e suas respectivas definições:

- ***Ativo*** – qualquer coisa que tenha valor para a organização;
- ***Escopo*** – conjunto de ativos, ameaças e vulnerabilidades que serão cobertos pelo sistema de gestão de riscos;
- ***Ameaça*** – tudo aquilo que tem potencial de causar algum dano a um ativo e, consequentemente, a uma organização;
- ***Vulnerabilidade***:
  - São as circunstâncias que levam um ou mais ativos a ficarem expostos a uma ou mais ameaças;
  - *Análise x avaliação*.
- ***Proteção***:
  - *Prevenção* – evita que o incidente ocorra;

- *Desencorajamento* – desencoraja a prática de ações não desejadas e/ou autorizadas;
- *Limitação* – delimita o (s) dano (s) causado (s);
- *Monitoramento* – monitora o estado e funcionamento;
- *Detecção* – detecta a ocorrência de um incidente;
- *Reação* – reage a um determinado incidente;
- *Correção* – corrige uma falha explorada por alguma vulnerabilidade;
- *Recuperação* – repara os danos causados por incidentes.

O risco pode ser composto por três componentes básicos: 1) evento que é a causa da origem do risco; 2) probabilidade é a possibilidade de o risco ocorrer; e 3) impacto ocorrerá caso o risco aconteça (HELDMANN, 2009).

Diante das abordagens apresentadas pelos autores das bibliografias “visitadas”, observa-se a possível necessidade de implementação do processo de gestão de riscos para identificar, analizar, responder e monitorar os ativos da organização. Sendo assim é necessário conhecer como é estruturado o processo de gestão de riscos desde o planejmento até o plano de respostas aos riscos.

1.2.2 Gestão de Riscos (GR)

Gestão de riscos é um conjunto de atividades que tem por objetivo, de uma forma economicamente racional, maximizar o efeito dos fatores de risco positivos e minimizar o efeito dos negativos (SCHMITZ, 2005). Heldman (2009, p. 236) acrescenta que é neste processo onde se especifica como os riscos serão definidos, controlados e monitorados.

O processo de gestão de risco é um ciclo constante com pontos de checagem periódicos, e não um esforço momentâneo conforme pode visualizar na figura 1.4. Os riscos evoluem com o tempo, conforme a empresa e seu ambiente mudam; as prioridades e a política de risco evoluem em resposta (WESTERMAN; HUNTER, p. 104).

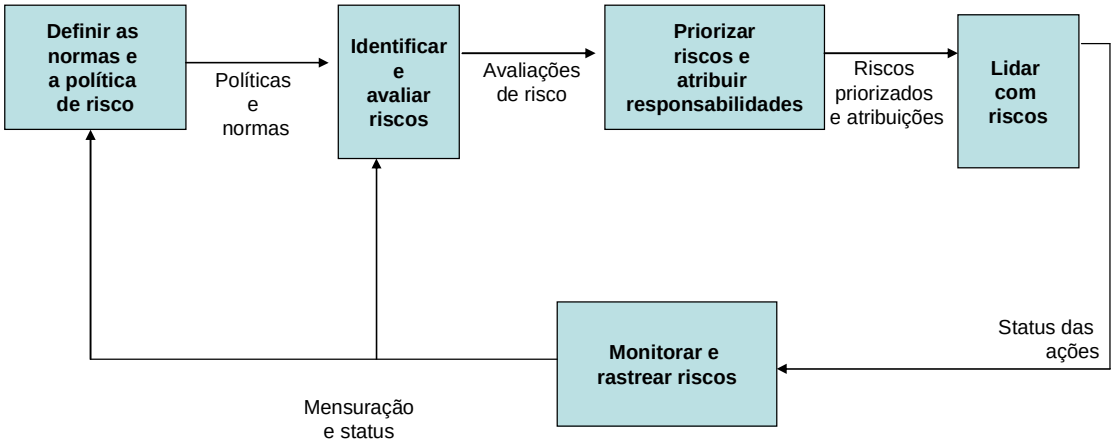


Figura 1.4 – Passos no processo de governança do risco de TI
Fonte: Westerman; Hunter (2008, p. 104)

De acordo com CMMI, o gerenciamento de risco em projetos está contemplado no segundo nível de maturidade (Gerenciado) através de duas áreas de processo: Planejamento do Projeto pelo “SP Identificar os Riscos do Projeto” apartir “SG Desenvolvimento do Plano do Projeto”; e Monitoração e controle do projeto através da “SP Monitorar os Riscos do Projeto” dentro da “SG Monitorar o Projeto de Acordo com o Plano”. Contudo, esta atuação é feita reativamente, ou seja, o foco está na identificação dos riscos para conscientização e reação à medida que eles ocorram. No terceiro nível – nivel de maturidade (definição) - é onde o gerenciamento de riscos está efetivamente tratado pela área de processo de gerência de riscos. Esta área de processo age de forma proativa com o objetivo de minimizar os impactos dos riscos nos objetivos do projeto.

Os processos de gestão de riscos possuem uma estrutura similar, dentre os autores pesquisados. Na figura 1.5 foi desenvolvido um comparativo dos processos sugeridos por cada autor estudado.

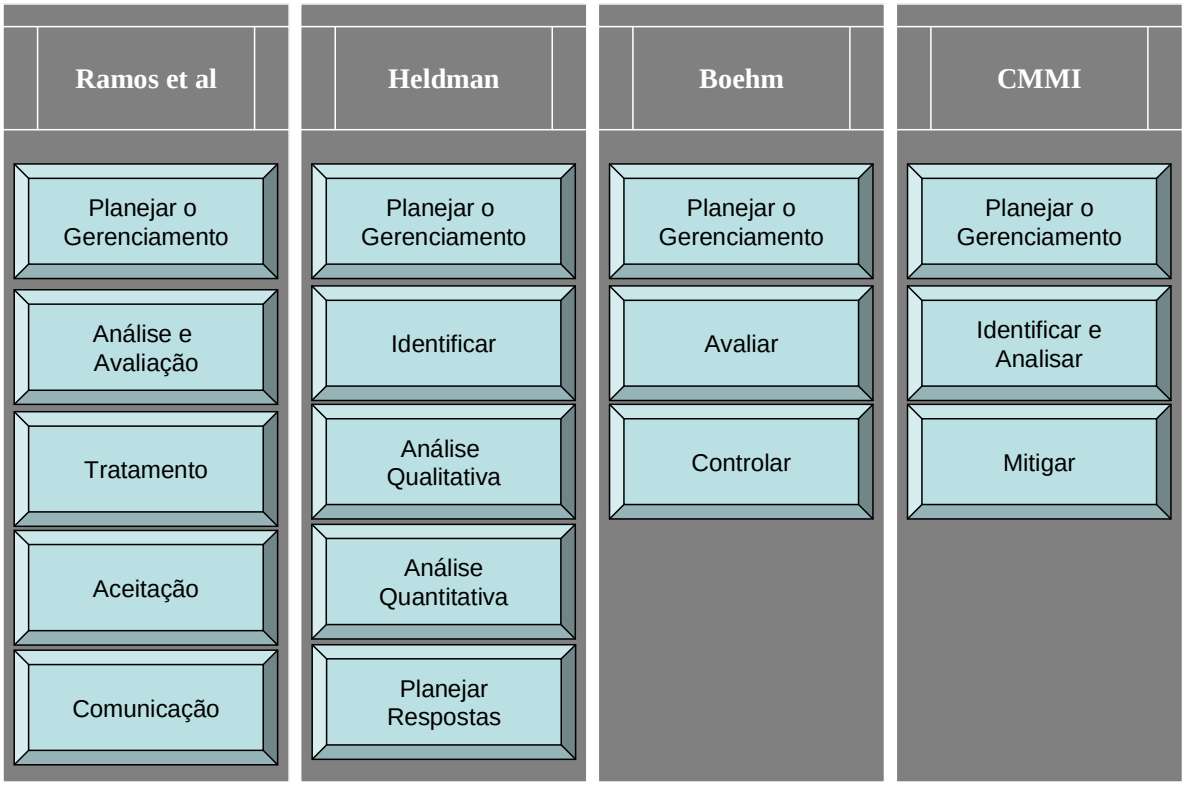


Figura 1.5 – Comparativo de gestão de riscos (Ramos et al x Heldman x Boehm x CMMI
Fonte: Autoria propria (2011)

Observando-se a figura 1.5 é possível perceber que os processos de gestão de riscos dos autores citados são deferentes na estrutura, porém, o resultado dos processos parecem convergir para um mesmo modelo:

- ***Gerenciar de riscos***
- ***Identificar e avaliar***
- ***Analisar***
- ***Planejar respostas***

1.2.3 Plano de gerenciamento de riscos

Sua finalidade de acordo com Heldman (2009) é criar um “plano de gerencimento de riscos”, que especifique como os riscos serão definidos, monitorados e controlados ao logo do projeto.

O objetivo específico “preparar-se para a gerência de riscos”, através das suas 3 (três) práticas, tem a função de estabelecer uma estratégia para identificar, analisar e mitigar riscos, que deverão ficar documentadas no plano de gerenciamento de riscos (HELDMAN, 2009).

O plano de gerenciamento de riscos detalha como os processos de gerenciamento de riscos (incluindo identificar os riscos, realizar a análise qualitativa de riscos, realizar a análise quantitativa, planejar respostas a riscos, monitorar e controlar os riscos) serão implementados, monitorados e controlados por todo o ciclo de vida de um determinado projeto. Heldman apud PMBOK Guide (2009), afirma que para este processo devem-se incluir os seguintes elementos:

- ***Metodologia*** – refere-se aos procedimentos de execução do gerenciamento de riscos, incluindo métodos, ferramentas e a localização dos dados sobre os riscos a serem utilizados em futuros processos;
- ***Funções e responsabilidades*** – descrevem a equipe responsável pela administração dos riscos identificados e respectivos repostas;
- ***Elaboração do orçamento –*** o orçamento para o gerenciamento de riscos;
- ***Cronologia –*** a cronologia dos processos de gerencimento de riscos;
- ***Categorias de riscos –*** representam uma forma de identificar sistematicamente os riscos e servem de base para a sua compreensão. O uso dessas categorias ajuda a melhorar o processo de determinação e identificação de riscos, pois estabelece uma linguagem comum de descrição dos riscos para todos os envolvidos;
- ***Definições de probabilidade e impacto dos riscos –*** ao escrever o plano de gerenciamento de riscos, o autor recomenda documentar as definições dos níveis de probabilidade e impacto uma vez que eles se relacionam a potenciais eventos de riscos negativos e seus impactos;
- ***Índice da matriz de probabilidade –*** a matriz de probabilidade e impacto prioriza a combinação de destes dois fatores, que irá ajudar a determinar os riscos que precisam de planos de respostas detalhados;
- ***Tolerência das partes interessadas revisadas –*** significa extamente o que o nome sugere. Com o avançar dos processos de gerenciamento de riscos, as tolerâncias a riscos podem mudar;
- ***Relatório de formatos –*** explicita o conteúdo do registro de riscos e a forma desse documento;
- ***Monitoramento –*** inclui uma descrição de como a história das atividades de risco no presente projeto deve ser documentado e como se dará a auditoria dos processos de risco.

Heldman (2009, p. 237) menciona que as catecterísticas de riscos serão utilizadas durante o processo de identificação dos riscos e devem ser identificadas e documentadas no respectivo plano de gerenciamento. Essas categorias irão ajudar a certificar-se de que o próximo processo, identificar os riscos, seja executado efetivamente e gere uma saída de qualidade.

Durante o processo de análise e avaliação de riscos é que serão feitos todos os levantamentos em relação às ameaças, vulnerabilidades, probabilidades e impacto aos quais os ativos estão sujeitos. Por conta disso, esse é provalvemente o processo mais trabalhoso e de maior duração (RAMOS et al, 2006, p. 67).

De acordo com Heldman apud PMI (2009) é na fase de planejamento que o processo de gestão de riscos é feito, e assim é possível demonstrar como identificar e planejar as atividades de gerência de riscos do projeto. Na figura 1.6, o autor apresenta o processo completo.

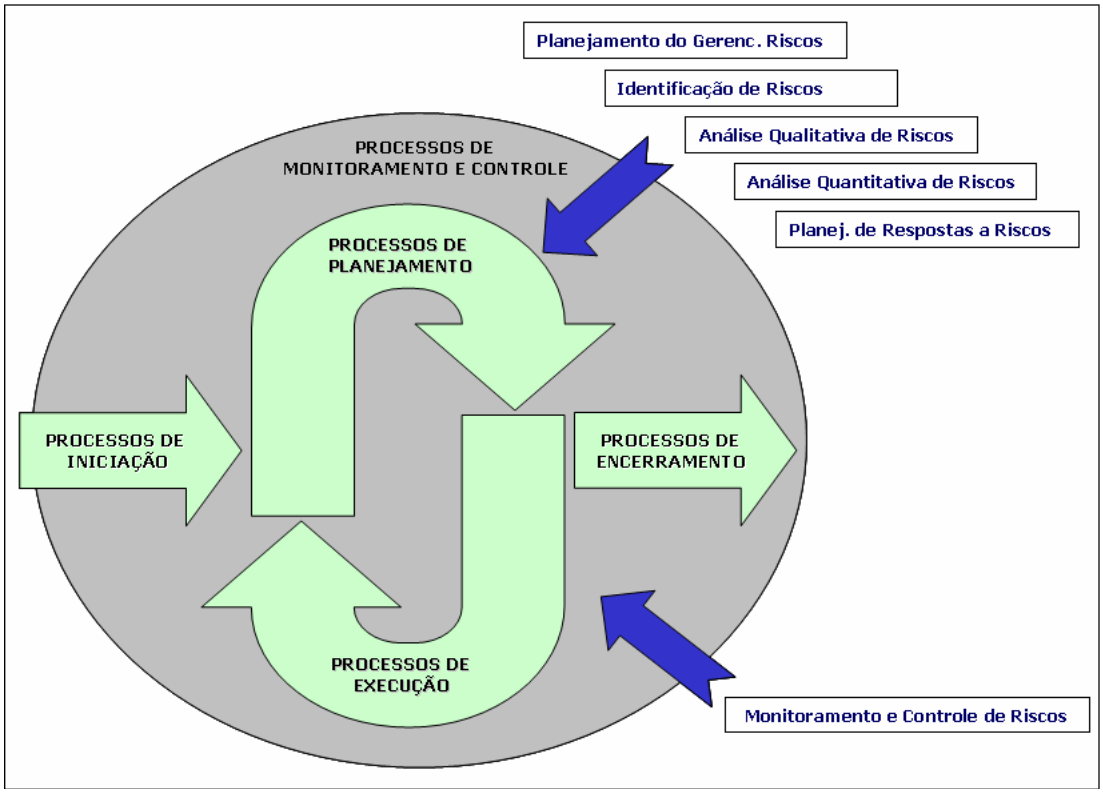


Figura 1.6 – Processo da gerência de riscos segundo o PMI
Fonte: (HELDMAN, 2009)

1.2.4 Avaliação de riscos

Para o *National Institute of Standards and Technology* (NIST, 2002, p. 8), a avaliação de riscos é usada nas organizações para determinar a extensão da potencial ameaça e o risco associado com um sistema de TI. A saída deste processo auxilia na identificação de

controles apropriados para reduzir ou eliminar o risco durante o processo de mitigação de riscos.

O objetivo específico “identificar e analisar riscos” tem a função de identificar os riscos e categorizá-los para obter o seu nível de probabilidade e impacto a fim de priorizá-los quanto ao seu grau de criticidade (HELDMAN, 2009). Para avaliar os riscos e sua probabilidade de ocorrência, podem-se utilizar as análises quantitativas e qualitativas, conforme definições a seguir.

1.2.4.1 Análise qualitativa

Este processo visa, de modo geral, descobrir a probabilidade de um evento de risco e determinar seu impacto (ou consequências) caso venham ocorrer (HELDMAN, 2009, p. 237-263).

No método qualitativo, explica Ramos et al (2006, p. 72), ao invés de usar valores numéricos para estimar os componentes do risco, trabalha-se com mensões mais subjetivas como alto, médio e baixo. Sendo assim, não há a necessidade de gerar valores numéricos para os componentes do risco, o que torna o processo muito mais rápido. O processo de Análise qualitativa de riscos, que acontece na fase de planejamento, avalia e classifica os riscos identificados em relação aos seus impactos e probabilidades de ocorrência e os prioriza de acordo com seus potenciais efeitos sobre o desempenho do projeto (HELDMAN, 2009, p. 250).

As ferramentas e técnicas abordadas por Heldman (2009, p. 250) que fazem parte desse processo são utilizadas para atribuir uma pontuação aos riscos – uma maneira de classificar sua probabilidade e impacto. Está compreendida em:

- ***Avaliação da probabilidade e impacto dos riscos*** – é chance de um evento ocorrer. Pode ser dificil avaliar a probabilidade de um risco, o que costuma ser feito por meio da opinião especializada. Em termos leigos, isso significa que se procura adivinhar (ou que um especialista adivinhe) a probabilidade de ocorrência de determinado evento de risco;
- ***Matriz de probabilidade e impacto (PI)* –** é quantidade de danos (ou ganhos) que um evento de risco representa para um projeto. A escala de impacto de riscos pode ser relativa (também conhecida como escala ordinal) na qual se atribuem valores como alto, médio ou baixo (ou alguma combinação desses), ou um escala numérica conhecida como escala cardinal. Ramos et al (2006, p. 73), também sugere o mesmo método, só que divide a **probabilidade** em 2 (dois) componentes:

Ameaça e vulnerabilidade. Na figura 1.7, está o diagrama sugerido por Ramos et al.

Risco Baixo	De 1 a 6
Risco Médio	De 7 a 12
Risco Alto	De 13 a 27

Níveis	**Alto**	**Médio**	**Baixo**
Valores	3	2	1
Risco = Vulnerabilidade x Ameaça x Impacto			

Ameaça		**Alta**			**Média**			**Baixa**		
Vulnerabilidade		**B**	**M**	**A**	**B**	**M**	**A**	**B**	**M**	A
Impacto ou Valor do Ativo	**A**	**1**	**2**	**3**	**2**	**4**	**6**	**3**	**6**	**9**
	M	**2**	**4**	**6**	**4**	**8**	**12**	**6**	**12**	**18**
	B	**3**	**6**	**9**	**6**	**12**	**18**	**9**	**18**	**27**

Figura 1.7 – Exemplo de método qualitativo do cálculo da tabela de PI
Fonte: Adaptado de Ramos et al (2006, p. 73)

- ***Análise de qualidade dos dados sobre riscos*** **–** envolve a especificação da utilidade dos dados coletados para a avaliação dos riscos, que deve levar em conta:
  - Qualidade dos dados usados;
  - Disponibilidade dos dados relacionados aos riscos;
  - Até que ponto o risco é compreendido;
  - Confiabilidade e integridade dos dados;
  - Precisão dos dados.
- ***Categorização dos riscos*** **–** é utilizada para determinar os efeitos dos riscos;
- ***Avaliação da urgência dos riscos*** **–** determina a antecipação com que os eventos de riscos podem ocorrer e define respostas para aqueles que forem acontecer em breve.
- ***Opinião especializada*** **–** como este processo determina valores qualitativos, pela sua própria natureza precisa-se confiar na opinião especializada para determinar o nível de probabilidade, impacto e outras informações.

1.2.4.2 Análise quantitativa

A métrica do risco é feita através de uma metodologia na qual se busca quantificar em termos numéricos os componentes associados ao risco. Como resultante, o risco é representado em termos de possíveis perdas financeiras (RAMOS et al, 2006, p. 53).

- O processo, realizar a análise quantitativa dos riscos avalia os impactos e quantifica a exposição aos riscos por meio de atribuição de probabilidades numéricas a cada um e aos seus impactos sobre os objetivos do projeto (HELDMAN, 2009). Neste mesmo processo, que acontece na fase de planejamento, analisam-se numericamente os riscos mais significantes estabelecidos durante a análise, e a interação entre eles, com o objetivo de estimar uma combinação de possíveis resultados para o projeto como um todo. Parafraseando Heldman apud PMBOK Guide (2009, p. 257), as finalidades desse processo são:
  - Quantificar os possíveis resultados e probabilidades;
  - Determinar a probabilidade de atingir os objetivos do projeto;
  - Identificar riscos que requeiram maior atenção, quantificando sua contribuição para o risco geral do projeto;
  - Identificar metas de cronograma, custos ou escopo realistas e viáveis;
  - Tomar as melhores decisões possíveis de gerenciamento do projeto quando os resultados forem incertos.

Exitem diversas ferramentas que são utilizadas e recomendadas em sistemas da qualidade tais como Brainstorming; SWOT; Ishikawa; 5W2H e PDCA que podem contribuir para a gestão de riscos, pois com o uso destas ferramentas é possível avaliar alguns aspectos bastante importantes, como por exemplo, se o risco avaliado também pode ser uma oportunidade. (HELDMAN, 2009).

1.2.5 Ferramentas da qualidade e gestão de riscos

A seguir destacam-se as principais ferramentas e técnicas sugeridas pelos autores para identificação de riscos:

1.2.5.1 Brainstorming

Provavelmente essa é a técnica mais usada da identificação de riscos. Esta ferramenta implica em reunir em uma sala, especialistas no assunto em questão, integrantes da equipe, membros da equipe de gerenciamento de riscos e quem mais puderem contribuir para o processo e pedir que comecem a identificar possíveis eventos de risco. O segredo é a idéia de um pode inspirar outra idéia e assim por diante, de modo que, até o final da sessão, se tenha identificado todos os riscos possíveis (HELDMAN, 2009, p. 243).

1.2.5.2 Análise SWOT

É uma ferramenta utilizada para fazer análises de cenário (ou análise de ambiente), sendo usada com base para a gestão e o planejamento estratégico de uma organização. É um sistema simples para posicionar ou verificar a posição estratégica da empresa no ambiente em questão (DAYCHOUW, 2007, p. 7). O termo SWOT é uma sigla oriunda do idioma inglês. Significa um anagrama de forças (*Strengths*), fraquezas (*Weaknesses*), oportunidades (*Opportunities*) e ameaças (*Threats*):

- ***Strengths (pontos fortes)*** – vantagens internas;
- ***Weaknesses (pontos fracos)*** – desvantagens internas;
- ***Opportunities (oportunidades)*** – aspectos positivos da envolvente com o potencial de fazer crescer a vantagem competitiva da organização;
- ***Threats (ameaças)*** – aspectos negativos da envolvente com o potencial de comprometer a vantagem competitiva da organização.

As forças e fraquezas são determinadas pela posição atual da organização e se relacionam, quase sempre, a fatores internos. Já as oportunidades e ameaças são antecipações do futuro e estão relacionadas a fatores externos. A figura 1.8 ilustra como se utiliza a análise SWOT.

SWOT	AJUDA (Na conquista de objetivos)	ATRAPALHA (Na conquista de objetivos)
AMBIENTE INTERNO (Atributos da organização)	Forças	Fraquezas
AMBIENTE EXTERNO (Atributos do ambiente)	Oportunidades	Ameaças

Figura 1.8 – Modelo esquemático da análise SWOT.
Fonte: (DAYCHOUW, 2007, p. 8)

1.2.5.3 Diagrama causa-e-efeito ou *Ishikawa*

Foi desenvolvido pelo engenheiro japonês Kaoru Ishikawa, visando identificar, explorar e ressaltar todas as causas possíveis de um problema ou questão específica. No lado direito do diagrama coloca-se o problema ou o efeito que se pretende analisar e no esquerdo são listadas as diversas causas que contribuem para o seu aparecimento, agrupadas segundo hierarquia de importância, descendo-se até o nível de detalhe que se entenda necessário

(VERGUEIRO, 2002, p. 57). Normalmente podem-se avaliar as causas separadas por 2 (duas) categorias:

- ***Operacional*** **–** 5M (método, mão-de-obra, material, máquina e manutenção);
- ***Gerencial*** **-** 5P (políticas, procedimentos, preço, pessoal, planta ou layout).

O uso dessas categorias basicas, argumenta Vergueiro (2002, p. 58), deve ser visto sempre dentro do contexto que se pretende analisar, podendo-se utilizar qualquer classificação que se entenda mais conveniente como ponto de partida para análise de um problema específico. O diagrama de causa-e-efeito é útil para separar as verdadeiras causas de um problema dos efeitos que eles acarretam, evitando-se um equívoco facilmente cometido no dia-a-dia e mudando-se o foco da análise, que passa a concentrar-se no problema em si.

Para elaborar um diagrama de causa-e-efeito recomanda-se partir de uma definição que descreva de forma precisa o problema selecionado, deixando claro o que ele é, onde e quando ocorre, bem como a sua extensão. A partir daí pesquisar as causas construindo um diagrama com o problema à direita e as categorias à esquerda, conforme ilustrado na figura 1.9.

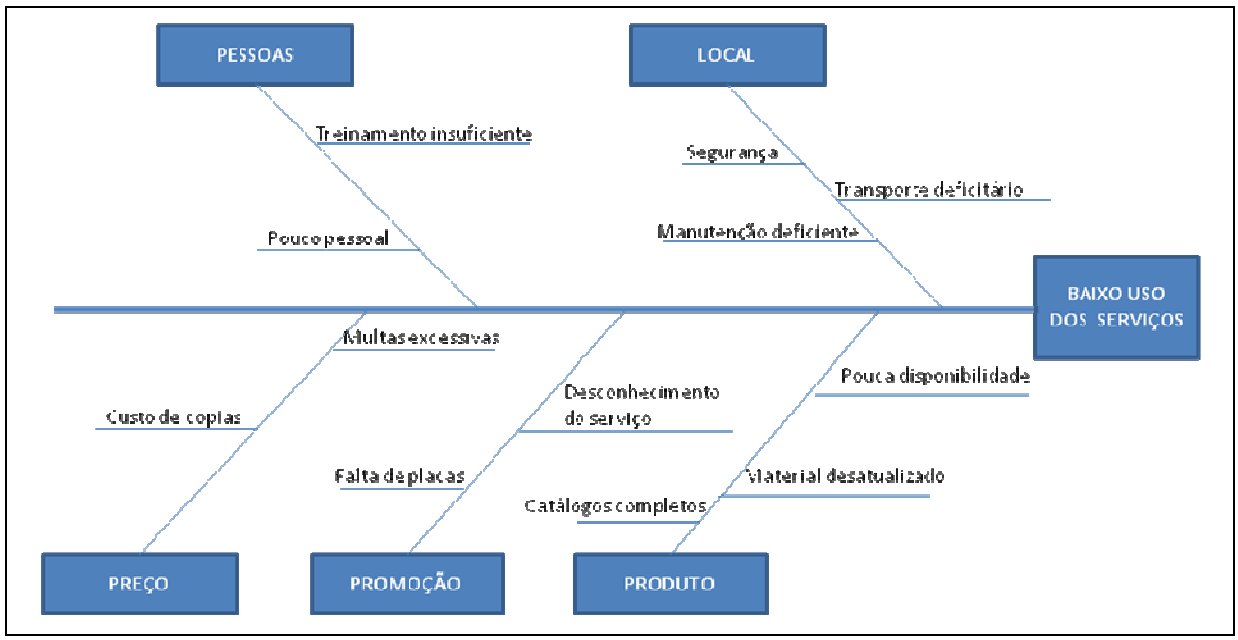


Figura 1.9 – Diagrama de causa-e-efeito
Fonte: (VERGUEIRO, 2002, p. 58)

1.2.5.4 Método 5W2H

Este método consiste basicamente em fazer perguntas no sentido de obter as informações primordiais que servirão de apoio ao planejamento de uma forma geral. A terminologia 5W2H tem origem nos termos da língua inglesa *What, Who, Why, Where, When, How, How much/How many*. Esta ferramenta pode ser utilizada em diversas áreas de

conhecimento, inclusive, no planejamento de riscos. Em planejamento de riscos, 5W2H é utilizada para identificar quais os riscos a serem considerados, quando implementar uma ação de contingência e quando disponibilizar para a mitigação ou transferência dos riscos (DAYCHOUW, 2007, p. 73).

5W2H	
WHAT?	O Que? / Que? / Qual?
WHO?	Quem?
WHY?	Por que?
WHERE?	Onde?
WHEN?	Quando?
HOW?	Como?
HOW MANY? / HOW MUCH?	Quantos? / Quanto?

Figura 1.10 – Método 5W2H
Fonte: (DAYCHOUW, 2007, p. 73)

1.2.5.5 Ciclo PDCA

O ciclo PDCA, também conhecido como “cicle of Shewhart” ou ciclo de Deming, foi introduzido no Japão após a guerra. Foi idealizado por Shewhart, mas foi Deming quem o divulgou e efetivamente o aplicou (DAYCHOUW, 2007, p. 132). O ciclo de Deming tem por princípio tornarem mais claros e ágeis os processos envolvidos na execução da gestão. Na gestão da qualidade está dividido em quatro principais passos que são os seguintes:

- ***Plan (planejamento)*** – estabelecer missão, visão, objetivos (metas), procedimentos e processos (metodologias) necessários para o atingimento dos resultados;
- ***Do (execução)*** – realizar, executar as atividades;
- ***Check (verificação)*** – monitorar e avaliar periodicamente os processos e resultados, confrontando-os com o planejado, os objetivos, as especificações e o estado desejado, consolidando as informações e, eventualmente, confeccionando relatórios;
- ***Act (ação)*** – agir de acordo com o avaliado e de acordo com os relatórios. Eventualmente determinar e confeccionar novos planos de ações, de forma a

melhorar a qualidade, a eficiência e a eficácia, aprimorando a execução e corrigindo eventuais falhas.

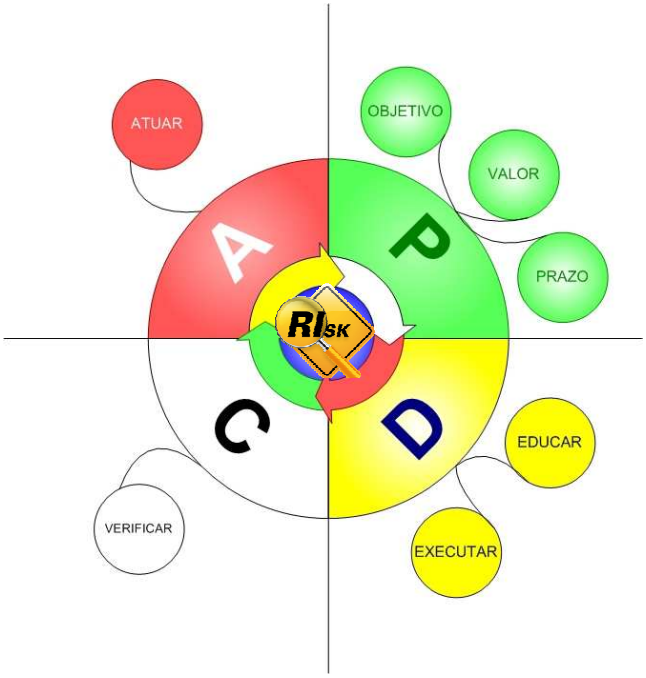


Figura 1.11 – Fluxo PDCA
Fonte: Autoria própria (2011)

1.2.6 Plano de respostas aos riscos

O plano de resposta de riscos especifica as medidas a serem tomadas para reduzir ameaças e tirar proveito das oportunidades encontradas nos processos de análise de riscos. Heldman (2009, p. 264) sugere desenvolver planos de resposta aos riscos para aqueles riscos com uma combinação de alta probabilidade de ocorrênia e impacto significativo ao projeto, aqueles com uma pontuação alta (ou vermelhos) na matriz de probabilidade/impacto ou aqueles com uma pontuação alto como resultado de realizar a análise quantitativa de riscos. O autor complementa ainda que o processo de planejamento de respostas a riscos, que acontece na fase de planejamento, desenvolve procedimentos e técnicas para ampliar as oportunidades e reduzir as ameaças aos objetivos do projeto, assegurando que os riscos identificados serão tratados adequadamente.

1.2.6.1 Estratégias para riscos negativos ou ameaças

Na maioria dos casos, a forma preferida de lidar com um risco de TI é reduzir sua probabilidade ou seu impacto. Muitos riscos de TI associados com a precisão são inevitáveis em termos regulamentares; riscos associados com o acesso ficam cada vez mais perigosos, por isso não podem ser aceitos e é difícil transferi-los; riscos associados com a agilidade não

podem em geral ser transferidos, mas também não podem ser aceitos nem evitados pela maioria das empresas (WESTERMAN; HUNTER, 2008, p. 112). Um exemplo associado à contexto seria: *"Não ter um plano de contingência para o caso de falhas de um sistema, e com isso, aceitou na prática um risco de baixa probabilidade, mas de impacto potencialmente desastroso"*. Dado que o potencial impacto de uma falha no sistema, independentemente da probabilidade, era muito alto, a organização teria a ganhar com um plano que reconhecesse o impacto e descrevesse contingências.

Na quadro 1.2 há um comparativo das estratégias adotadas pelos autores: Ramos et al (2006), Heldman (2009), Werterman; Hunter (2008) que nota-se certa semelhança de estratégias. O que difere Ramos et al (2006) dos demais, é que eles consideram a estratégia de mitigar riscos como medidas que diminuam **apenas os impactos.**

Quadro 1.2 – Comparativo sobre estratégias para tratar os riscos identificados

ESTRATÉGIA	RAMOS et al	HELDMAN	WESTERMAN; HUNTER
Evitar/Eliminar	X	X	X
Transferir	X	X	X
Aceitar/Reter	X	X	X
Reduzir	X	X	X
Mitigar	X		

Fonte: Autoria própria (2011).

A seguir estão as definições de cada estratégia que são adotadas pelos autores:

- ***Evitar/eliminar* –** implica em evitar os riscos por completo, eliminando a causa dos eventos destes define Heldman (2009, p. 264). Com a eliminação do risco, basicamente os erradica por meio da extinção de sua causa;
- ***Transferir* –** consiste em deslocar o risco e suas consequencias para terceiros. Ele não é eliminado, mas a responsabilidade pelo seu gerenciamento é transferida explica Heldman (2009, p. 265-266). A transferência do risco pode ocorrer de várias formas: seguros; terceirização; garantias; fianças e bonificações por desempenho.

- ***Mitigar*** – procura reduzir a probabilidade de ocorrência e o impacto de um evento de risco para níveis aceitaveis. O objetivo específico "Mitigar Riscos", tem a função de minimizar os riscos quanto a sua probabilidade de ocorrência e o seu impacto aos objetivos do projeto (HELDMAN, 2009, p. 266).

De acordo com *National Institute of Standards and Technology* (NIST, 2002, p. 27), mitigação de riscos defini-se como sendo o segundo processo do gerenciamento de riscos, que envolve priorizar, avaliar e implementar controles apropriados para reduzi-los apartir do processo de avaliação de riscos. Como a eliminação de riscos é normalmente impraticável ou próximo do impossível, é responsabilidade da direção, funcionários e gerentes de negócios usarem uma abordagem para obter o menor custo e implementar o maior número de controles a fim de diminuir o risco para um nível aceitável, com o mínimo impacto adverso aos recursos da organização.

O objetivo e missão da organização devem ser preservados pela seleção daquelas opções de mitigação de riscos. A prioridade pode ser dada pelas ameaças e pelas vulnerabilidades que tem a causa potencial dos impactos significantes (IBM, 2008, p. 28).

> Mitigação é uma estratégia muito parecida com a direção defensiva: ao avistar o obstáculo na estrada, você pensa nas suas opções e toma as medidas necessárias para contorná-la, prosseguindo com segurança em sua jornada (HELDMAN, 2009, p. 266).

- ***Aceitar/reter*** **–** para Heldman (2009, p. 266) é utilizada quando não é possível eliminar todas as ameaças. É uma estratégia que pode ser empregada em ameaças quanto com aqueles que representam oportunidades. Existem duas formas de aceitação de riscos:
  - *Passiva* **–** significa que não irá criar nenhum plano para tentar evitar ou mitigar o risco;
  - *Ativa* **–** envolve a criação de reservas de contingências de modo a lidar com os riscos caso eles venham a ocorrer.

1.3 Riscos relacionados à infraestrutura de TI

Para IBM (2008, p. 2), riscos é parte inerente dos negócios em, que devem ser considerados praticamente todos os aspectos dos negócios modernos que estão ligados a TI. A resiliência depende cada vez mais da capacidade da empresa gerenciar, com eficiência, os riscos que se apresentam em sua infraestrutura física, de TI e em seus processos. Um bom gerenciamento de riscos no atual ambiente de negócios, que é altamente interconectado, exige que líderes de TI enxerguem e compreendam os riscos relacionados aos investimentos de negócios e as vantagens financeiras que podem obter.

Uma estrutura de governança conciente de riscos facilita essa perspectiva mais ampla de negócios, pois proporciona uma visão mais completa dos riscos e dos retornos potenciais aos tomadores de decisão de toda a organização.

Segundo IBM (2008, p. 6), não é possível realizar um bom gerenciamento dos riscos de TI sem uma estrutura de governança robusta. Assim, ela sugere a adoção de padrões abertos desenvolvidos pelo *IT Governance Institute* (ITGI), que são orientações excelentes e globalmente aceitas. *Control Objectives for Information and related Technology* (COBIT) proporciona as melhores práticas para governança de tecnologia e infraestrutura, incluíndo o gerenciamento dos riscos. Processos estruturados como esses, melhoram a percepção proativa dos riscos da empresa e sua capacidade de preparação, análise e resposta às ameaças. Entretanto, a complexidade organizacional pode dificultar sua implementação. À medida que o gerenciamento dos riscos se torna parte cada vez mais integral do trabalho do *Chief Secutiry Officer* (CIO) e o número de riscos dentro da esfera de controle da TI aumenta, os CIOs devem assumir um papel de liderança para a execução desses processos:

- Alocando o financiamento e os ***recursos adequados*** para iniciativas de análise de riscos;
- Proporcionando ***orientação***, por meio de diálogos entre as partes interessadas, e garantindo o alinhamento contínuo com os objetivos de negócios e a conformidade com políticas de governança;
- Buscando ***melhoria contínua*** para os processos;
- Ajudando a incorporar uma melhor percepção dos ***riscos à governança*** geral de negócios da empresa;
- Estabelecendo ***políticas de gerenciamento*** dos riscos para orientar a execução das atividades.

1.3.1 Barreiras para o gerenciamento de riscos

De acordo com IBM (2008, p. 8), além de observar os processos acima listados, a organização deve considerar algumas barreiras: pessoas, organização e automação, afim propiciar um gerenciamento de riscos de TI eficaz.

1.3.1.1 Pessoas

Para ser realmente eficaz, o gerenciamento de riscos deve estar profundamente integrado a mentalidade corporativa da força de trabalho. As empresas precisam desenvolver uma cultura de consiência dos riscos que esteja em sintonia com a ampla gama de ameaças

aos negócios, assim como com as estratégias de resposta aos riscos para mitigá-las. Todos os funcionários devem se sentir capazes de manter e gerar valor para os negócios.

1.3.1.2 Organização

O apoio executivo ao gerenciamento dos riscos da TI é garantido, mas sua eficácia não. Os processos de gerenciamento dos riscos como os do COBIT, devem ser combinados às diretrizes de continuidade de negócios e a uma governança conciente dos riscos, hierarquicamente de cima para baixo.

1.3.1.3 Automação

A automação pode facilitar o gerenciamento dos riscos de TI de 2 (duas) maneiras importantes. Primeiro, ela pode aliviar a complexidade associada a análises e relatórios de riscos cruciais. Esses processos se tornam cada vez mais complicados à medida que a organização cresce e mais mudanças tecnológicas e de negócios são introduzidas. Segundo, a automação facilita a avaliação e a redução dos riscos reais para operações reais. Aplicativos de gerenciamento de serviços e atividades de negócios, assim como aplicativos de segurança e monitoramento de controles, reduzem a sobrecarga nos recursos por meio de diagnósticos de causa-raiz e funções de previsão de resposta. Eles podem ajudar a identificar ameaças, proporcionar avisos antecipados, simplificar e reduzir custos de respostas aos riscos, e melhorar a consistência dos processos de gerenciamento dos riscos.

Normalmente, melhorias são necessárias em uma ou mais dessas áreas; entretanto, todas as 3 (três) devem estar sempre em equilíbrio conforme relata a IBM (2008, p. 9). Na figura 1.12, pode-se observar de forma completa todo o processo de gerenciamento de riscos de TI.

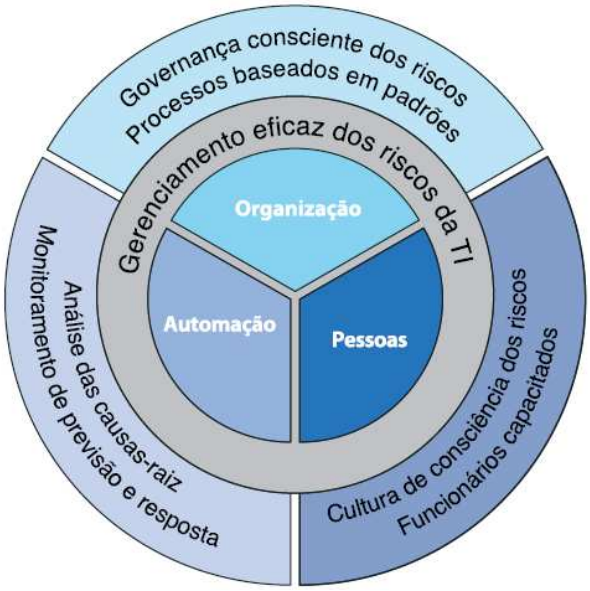


Figura 1.12 – Esquema do gerenciamento eficaz da TI sugerido pela IBM.
Fonte: (IBM, 2008, p. 10)

A partir do refencial teórico, verifca-se a necessidade de implementação de um modelo para gestão de riscos. No próximo capítulo, será apresentado um modelo proposto para a gestão de riscos orientada à Tecnologia da Informação.

2 MODELO PROPOSTO

O obejtivo principal deste trabalho é propor um modelo de gestão de riscos orientado a TI. Desta forma, este capítulo apresentará a modelagem do software buscando atender aos requisitos da gestão de riscos conforme abordado no referencial teórico estudado. A modelagem foi construída utilizando a linguagem *Unified Modeling Language* (UML). Existe a intensão de porteriormente desenvolver o sistema do modelo proposto. Como a empresa em que o modelo foi concebido é uma multinacional, a modelagem de dados foi gerada no idioma Inglês para facilitar a comunicação e o entendimento entre todos os sites ao redor do mundo em que o sistema poderá ser implementado.

2.1 Modelagem do sistema de gestão de riscos

De acordo com Furlan (1998, p. 33), UML é linguagem padrão para especificar, visualizar, documentar e construir artefatos de um sistema. Pode ser utilizada com todos os processos ao longo do ciclo de desenvolvimento e através de diferentes tecnologias de implementação. Fowler (2005, p. 25) complementa que a mesma pode ser definida como uma família de notações gráficas, que auxilia na descrição e no projeto de sistemas de software. Especialmente, aqueles construídos utilizando o estilo Orientado a Objetos (OO). Fowler acrescenta ainda que, UML é um padrão relativamente aberto, controlado pela OMG (*Object Management Group)*, um consórcio aberto de empresas.

A UML consolida um conjunto de essências para modelagem visual de conceitos que geralmente são acordados por vários métodos atuais e ferramentas do mercado (FURLAN, 1998, p. 34). Uma linguagem de modelagem visual apresenta alguns benefícios como:

1. ***Visualização*** – os relacionamentos existentes entre os diversos componentes da aplicação podem ser visualizados de forma a antever o produto final;
2. ***Gerenciamento da complexidade*** – cada aspecto do sistema é desenhado à parte em um modelo específico para que se possa estudar e compreender a estrutura, o comportamento e os possíveis particionamentos físicos, bem como identificar oportunidades de reutilização de componentes;
3. ***Comunicação*** – através da utilização de símbolos padrões tornam-se possível uma comunicação direta e não ambígua entre os participantes do projeto com relação aos detalhes de comportamento do sistema;
4. ***Fornecer mecanismos de extensibilidade e de especialização para apoiar conceitos essenciais*** – a UML será ajustada conforme novas necessidades

venham à tona para domínios específicos. Para tanto, os usuários devem ser capazes de: construir modelos que usem conceitos essenciais sem usar mecanismos de extensão para a maioria das aplicações normais; somar conceitos novos e notação para assuntos não cobertos pela essência; escolher dentre as interpretações variantes de conceitos existentes quando não há um consenso claro e especializar conceitos, notações e restrições para domínios de aplicação particulares;

5. ***Ser independente*** de linguagens de programação e processos de desenvolvimento;
6. ***Prover uma base formal*** para entender a linguagem de modelagem;
7. ***Encorajar o crescimento*** no número de ferramentas orientadas a objeto no mercado;
8. ***Suportar conceitos*** de desenvolvimento de nível mais elevado tais como colaborações, estrutura de trabalho, padrões e componentes;
9. ***Integrar as melhores práticas.***

O fluxo do processo foi desenhado através de diagramas UML. Na próxima seção serão abordadas as técnicas utilizadas para a construção do modelo proposto pelo presente trabalho.

2.1.1 Requisitos funcionais e não funcionais

Os requisitos são coleções de sentenças que devem descrever de modo claro, sem ambiguidades, conciso e consistente todos os aspectos significativos do sistema proposto. Os mesmos devem conter informações suficientes para permitir que os implementadores construam um sistema que satisfaça os requerentes, e nada mais (SOMMERVILLE, 2003, p. 83).

Pressman (1995) define que a análise de requisitos é o primeiro passo técnico do processo de engenharia de software. Afirma que é nesse ponto que uma declaração geral do escopo do software é aprimorada e que se torna a base para as atividades de engenharia de software que irão compor determinado projeto. O autor complementa ainda que, a especificação de requisitos de software é desenvolvida como uma consequência da análise, ilustrando ainda que “a análise deve concentrar-se nos domínios funcionais, comportamentais e de informação de um problema.”

As atividades de análise concentram-se na identificação, especificação e descrição dos requisitos do sistema de *software*. Em síntese, requisito é uma necessidade que o *software* deve cumprir. A análise do presente estudo teve por objetivo levantar os requisitos – a partir da revisão bibliográfica – mínimos necessários à modelagem do sistema de gestão de riscos orietado à infraestrtura de TI.

O detalhamento dos principais requisitos pode ser analisado no APÊNDICE A do trabalho. No quadro 2.1, é possível visualizar 1 (um) exemplo de requisitos, com o intuito de demonstrar a metodologia utilizada na descrição dos mesmos.

Quadro 2.1 – Requisito de cadastro de unidades de negócio

F2 Cadastro de unidade de negócio			Oculto ( )
Descrição: Este requisito visa disponibilizar ao administrador do sistema a inclusão e alteração de Unidades de negócio. A unidade de negócio possui um usuário responsável pela gestão de riscos.			
Requisitos Não Funcionais			
Nome	**Restrição**	**Categoria**	**Formato**
NF 2.1 – Cadastro de unidade de negócio	A unidade de negócio deve estar identificada para que os demais processos sejam relacionados à mesma.	Confiabilidade	Permanente
NF 2.2 – Idioma unidade de negócio	Obrigatoriamente deverá ser informado o idioma utilizado na unidade de negócio a fim de permitir a validação das pessoas que irão se relacionar com a mesma.	Confiabilidade	Permanente

Fonte: Autoria própria (2011).

2.1.2 Diagrama de classes

Um diagrama de classe exibe conjunto de classes, interfaces e colaborações, bem como seus relacionamentos. Esses diagramas são encontrados com maior frequência em sistemas de modelagem orientados a objeto e abrangem uma visão estática da estrutura do sistema (BOOCH; RUMBAUCH; JACOBSON, 2000, p. 25). O diagrama proposto está na figura 2.2.

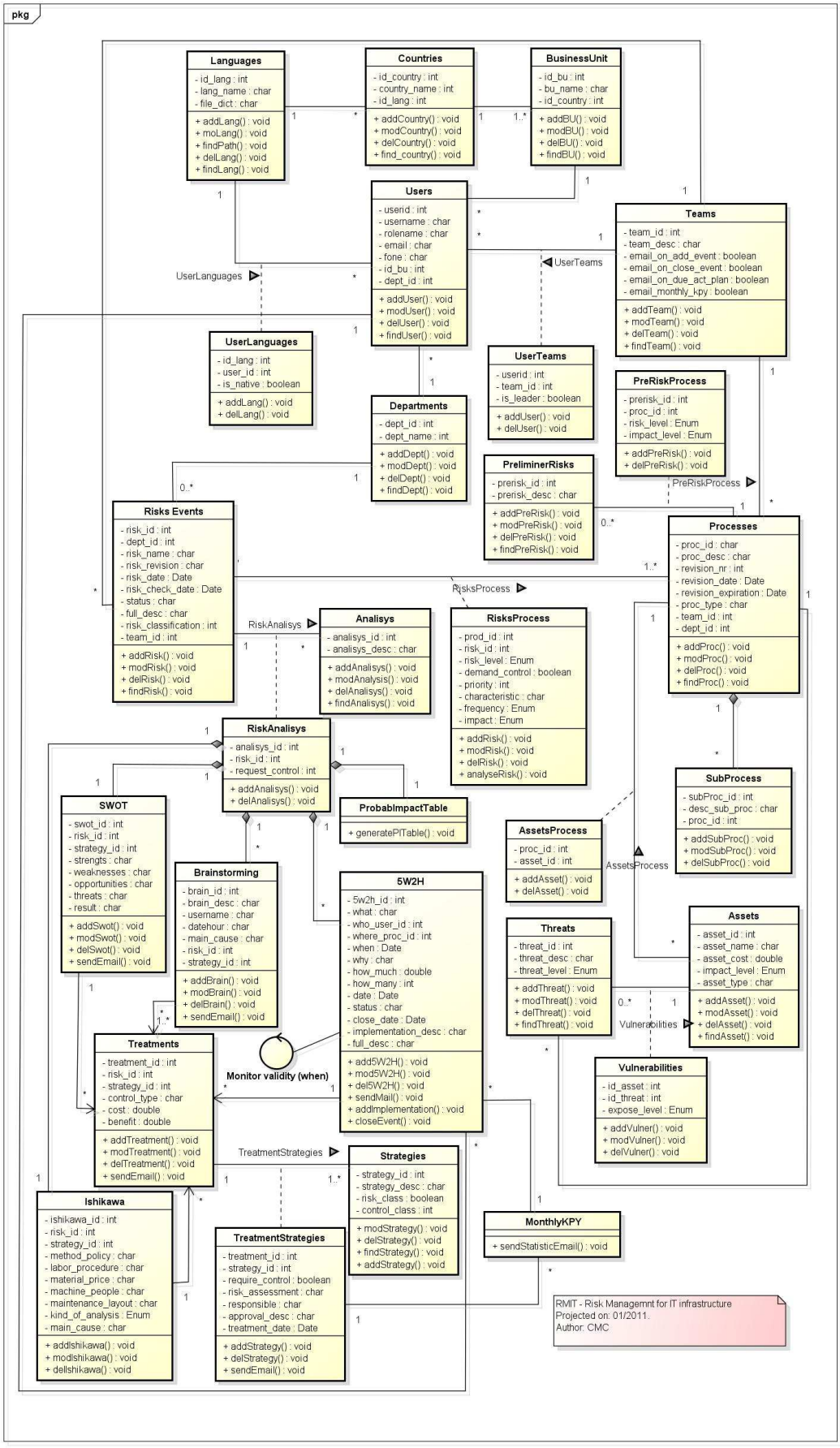


Figura 2.1 – Diagrama de classes
Fonte: Autoria própria (2011).

2.1.3 Diagrama de casos de uso

Este diagrama exibe um conjunto de caso de uso e atores (um tipo especial de classe) e seus relacionamentos. Diagramas de caso de uso abrangem a visão estática de casos de uso do sistema (BOOCH; RUMBAUCH; JACOBSON, 2000, p. 26). O Diagrama de caso de uso está apresentado na figura 2.2.

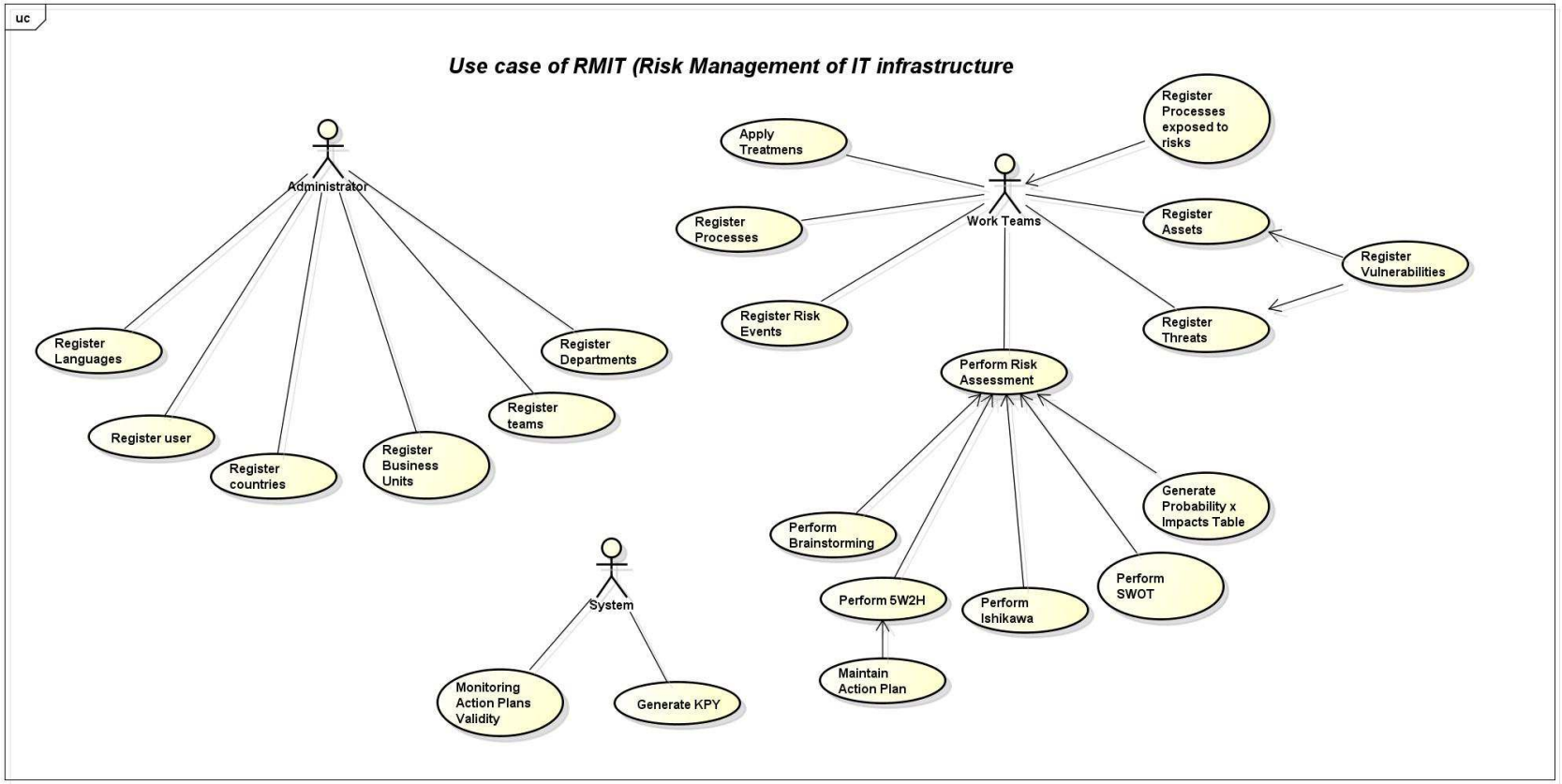


Figura 2.2 – Diagrama de caso de uso
Fonte: Autoria própria (2011).

2.1.4 Diagrama de atividades

O diagrama de atividade (figura 2.3) é um tipo especial de diagrama de gráfico de estado, exibindo o fluxo de uma atividade para outra. Abrange a visão dinâmica do sistema e é importante principalmente para a modelagem da função de um sistema e dá ênfase ao fluxo de controle entre objetos (BOOCH; RUMBAUCH; JACOBSON, 2000, p. 26). A figura 2.3, apresenta o diagrama de atividade referente ao caso de uso “Registrar Eventos de Risco”.

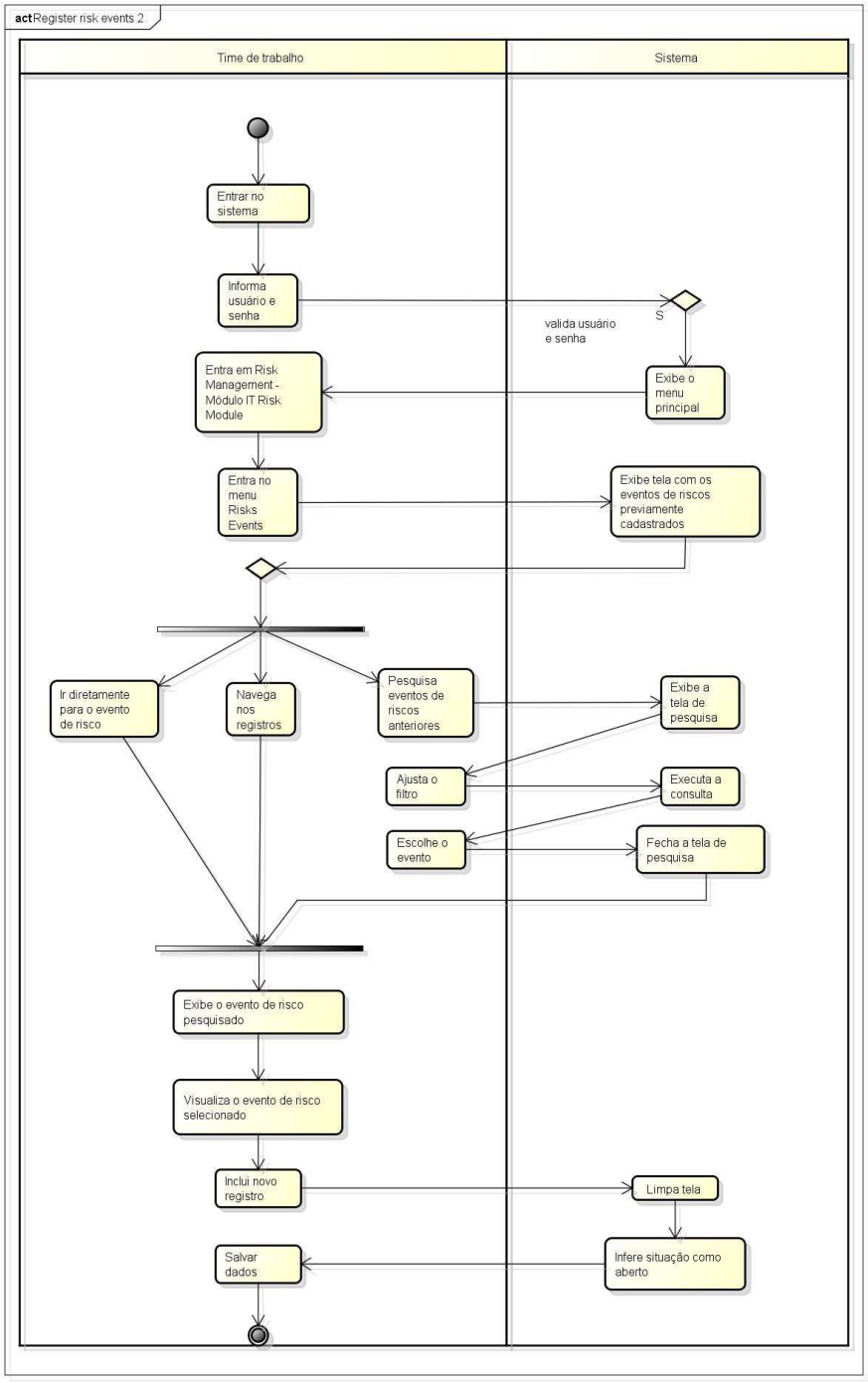


Figura 2.3 – Diagrama de atividades
Fonte: Autoria própria (2011).

2.1.5 Descrição dos casos de uso

A partir dos requisitos funcionais e não funcionais detalhados anteriormente e também com base no driagrama de caso de uso serão detalhados nesta seção, as interações dos usuários com o sistema de maneira descritiva.

O detalhamento dos principais casos de uso está apresentado no APÊNDICE B do presente trabalho. No quadro 2.2, segue a descrição do caso de uso Registrar eventos de risco, para exemplificar a metodologia utilizada na descrição destes casos de uso:

Quadro 2.2 – Descrição do caso de uso "Registrar eventos de risco".

1 – Registrar eventos de risco (*Register risk events*)
Atores: Time de trabalho
Pré-condição: Os usuários e time de trabalho precisam estar cadastrados e parametrizados previamente.
Objetivo: Registrar os eventos de riscos que será o marco inicial do processo de gestão do risco em questão.
Fluxo de eventos: 1. O ator entra no sistema de gestão de riscos; 2. O sistema solicita usuário e senha do usuário que deve estar cadastrado; 3. O ator informa o nome de usuário e senha e clica em OK para validar os dados; 4. O sistema vefirica se o usuário de senha informado é válido; 5. O sistema exibe o menu principal do sistema; 6. O ator entra no menu Risk Management – IT Risk Module; 7. O ator entra no menu Tasks, Risk events; 8. O sistema deve exibir a tela com os eventos de riscos previamente cadastrados; 9. O ator pode pesquisar eventos de riscos anteriores através do botão pesquisa (lupa); 9.1. O ator ajusta o filtro de acordo com o que deseja pesquisar; 9.2. O sistema executa a consulta no banco de dados e exibe o resultado; 9.3. O ator escolhe o evento de risco que deseja visualizar e clica bo botão OK; 10. O sistema fecha a tela de pesquisa e exibe os dados completos do evento de risco; 11. O ator visualiza o risco consultado; 12. O ator poderá incluir novo evento de risco através do botão New; 13. O sistema limpa os dados dos campos para permitir a inclusão das informações do novo evento de risco; 14. O ator preenche os dados do novo evento de risco e salva os dados através do botão Save; 15. O sistema infere a situação do novo evento de risco como aberto (open);
Fluxo alternativo 1: **1.** No item 12, o ator poderá copiar o risco pesquisado para uma nova ocorrência através do botão copiar; **2.** O sistema efetua a cópia do evento selecionado para um novo evento de risco e habilita a edição dos dados; **3.** O ator poderá alterar os dodos do evento de risco e salvar o registro através do botão Save; 4. O sistema infere a situação do novo evento de risco como aberto (open); **Fluxo alernativo 2:** **1.** No item 12, o ator poderá modificar o risco pesquisado caso o registro tenha sua situação como aberto (open); **2.** O ator poderá alterar os dados do evento de risco e salvar o registro através do botão Save; **3.** O sistema infere a situação do novo evento de risco como aberto (open); **Fluxo alernativo 3:** **1.** No item 9, o ator poderá ir direto ao evento de risco desejado caso já saiba o código do evento através do botão Ir Para; **2.** O ator clica no botão Ir Para; **3.** O sistema exibe uma tela para digitação do código do evento de risco; **4.** O ator digita o código do evento e clica no botão OK; **5.** O sistema exibe os dados completos do evento de risco;

Fluxo alternativo 4: **1.** No item 9, o ator poderá navegar nos eventos de riscos já cadastrados através dos botões de navegação que está na parte superior da tela; O sistema exibe o evento de risco corrente.
Pontos de extensão: Não se aplica
Casos de uso incluídos: Register user.

Fonte: Autoria própria (2011).

Para facilitar o endendimento do sistema, foram criadas algumas imagens para representar as telas do mesmo. Estas imagens são chamadas de protótipos de interface.

2.1.6 Protótipo de telas

Na figura 2.4, está ilustrado o protótipo da tela de registro dos eventos de riscos.

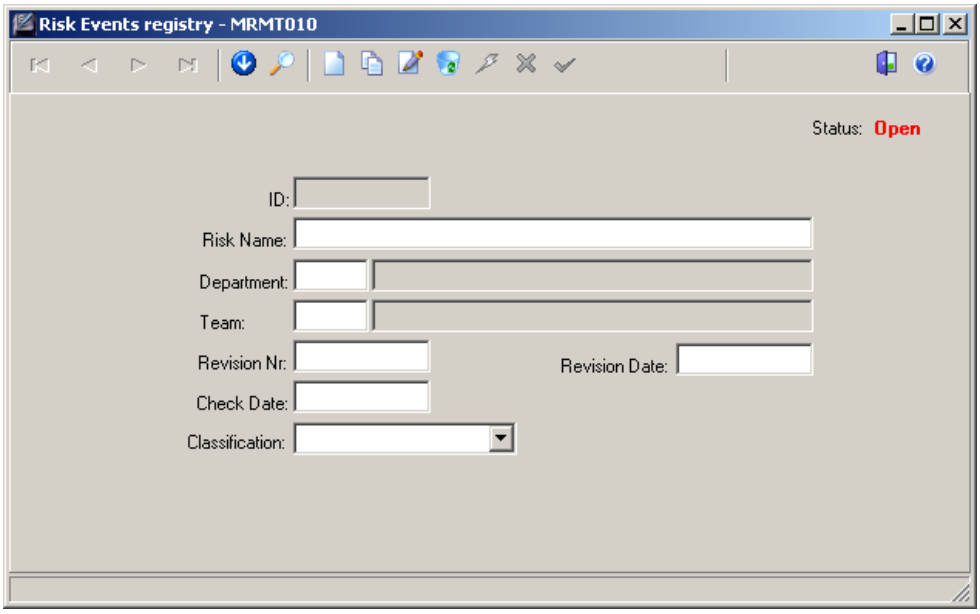


Figura 2.4 – Protótipo da tela de registro de eventos de risco.
Fonte: Autoria própria (2011).

Na figura 2.5, é apresentado o protótipo da tela de registro da análise de risco. Na parte inferior da imagem, é possível visualizar alguns botões que podem ser descritos como:

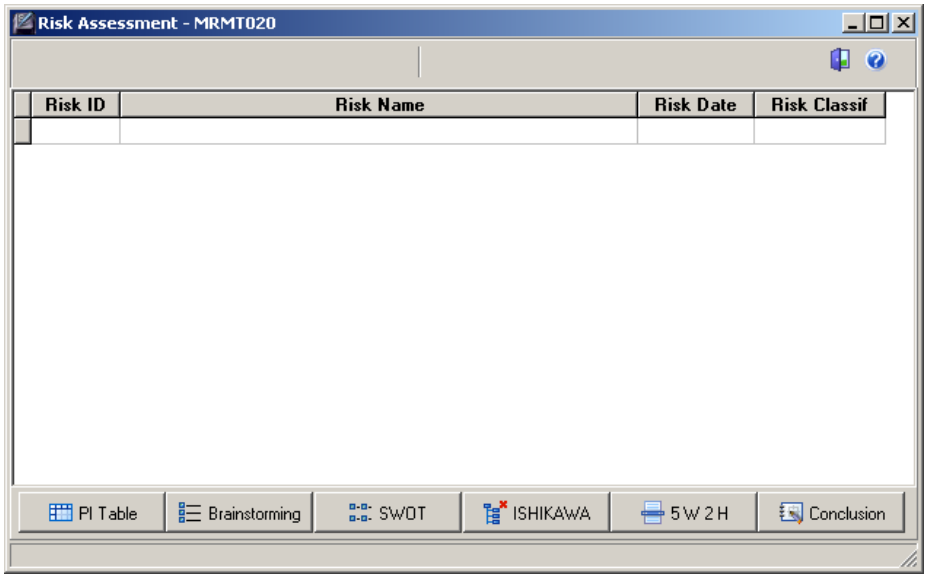


Figura 2.5 – Protótipo da tela de análise de riscos.
Fonte: Autoria própria (2011).

- ***Botão PI Table*** – ao clicar neste botão, o sistema buscará os dados que foram informados no registro do evento de risco, as ameaças e as vulnerabilidades, a fom de gerar a matriz de probabilidade e impacto;
- ***Botão Brainstorming*** – ao clicar neste botão, o sistema irá apresentar a tela para permitir a inclusão dos dados do método *Brainstorming;*
- ***Botão SWOT*** – ao clicar neste botão, o sistema exibirá a tela com os campos da análise SWOT (forças, fraquezas, oportunidades e ameaças);
- ***Botão Ishikawa*** – ao clicar neste botão, o sistema exibirá a tela com o método Ishikawa ou causa-e-efeito, com os respectivos campos para preeenchimento.
- ***Botão 5W2H*** – ao clicar neste botão, será apresentada a tela com do método escolhido, e possibilitá a geração de planos de ação, relacionando o usuário e a data de vencimento de cada ação;
- ***Botão Conclusion*** – ao clicar neste botão, será apresentada a tela com o campo para registro da conclusão da análise do evento de risco.

Na figura 2.6, está demonstrado o protótipo da tela do método de análise do 5W2H, no qual tem a intensão de disponibilizar uma visão mais clara do mesmo.

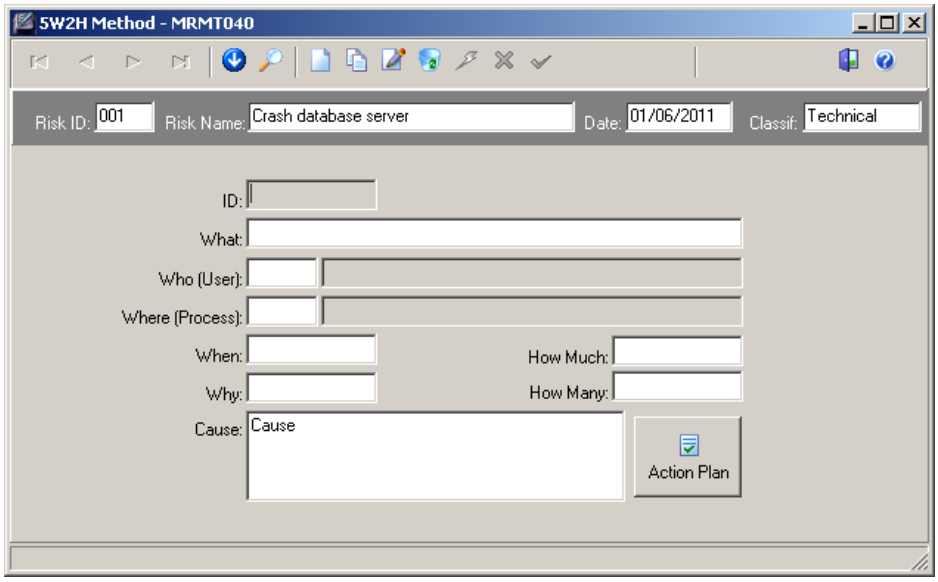


Figura 2.6 – Protótipo da tela de análise 5W2H.
Fonte: Autoria própria (2011).

Na figura 2.7, pode verificar como seria a tela de registro dos processos que estão expostos ao evento de risco selecionado.

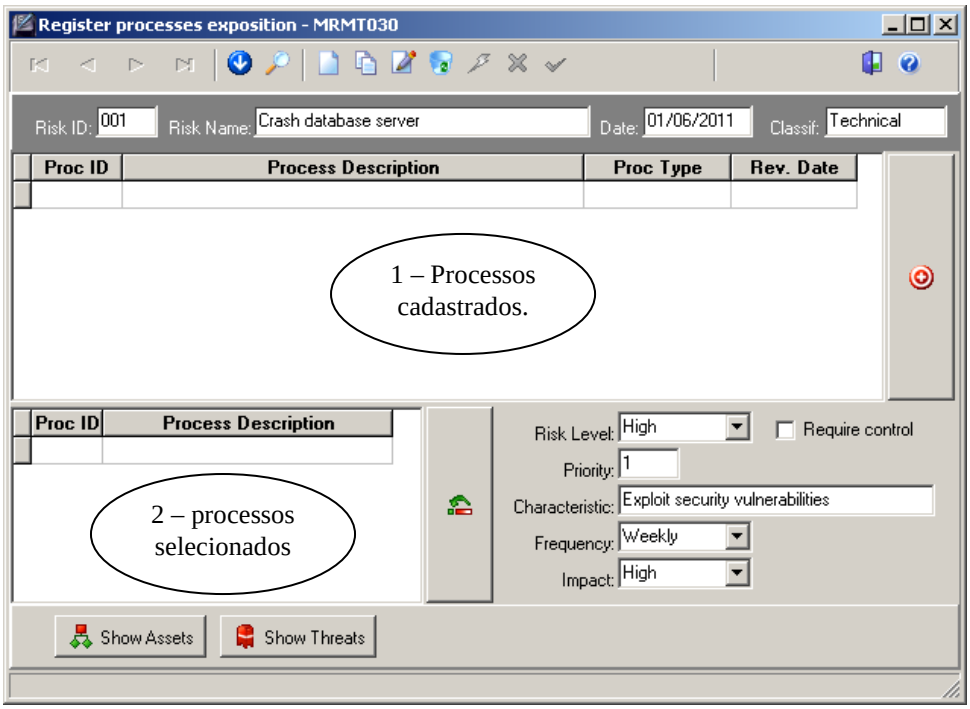


Figura 2.7 – Protótipo da tela de registro de processos expostos ao evento de risco.
Fonte: Autoria própria (2011).

A partir do modelo sugerido, indentificou-se a necessidade de fazer um *benchmarking* para tentar identificar ferramentas existentes no mercado, com o objetivo de verificar as “melhores práticas” adotadas em outros sistemas de gestão de riscos. No capítulo 3 pode-se visualizar o processo de bechmarking que foi efetuado.

3 BENCHMARKING

De acordo com Daychouw (2007, p. 37), *benchmarking* é um processo de medição e comparação sistemática dos processos de negócios de uma organização com os líderes naqueles processos em qualquer parte do mundo para obter informações que ajudarão esta organização a implementar ações para melhorar seu desempenho.

O objetivo principal do benchmarking é "aprender". Mas é necessário assumir uma postura de "organização que aprende" para que se possa justificar o esforço investido no processo (DAYCHOUW, 2007, p. 37). O quadro 3 apresenta uma analogia com o que é e o que não é benchmarking.

Quadro 3.1 – Analogia do Benchmaking.

Benchmarking é...	Benchmarking não é...
Um processo contínuo.	Um evento isolado.
Uma investigação que fornece informações valiosas.	Uma investigação que fornece respostas simples e "receitas".
Um processo de aprendizado com outros.	Cópia ou imitação.
Um trabalho intensivo, consumidor de tempo, que requer disciplina.	Rápido e fácil.
Uma ferramenta viável a qualquer organização e aplicável a qualquer processo.	Mais um modismo da administração.

Fonte: (DAYCHOUW, 2007, p. 40).

Em suma, benchmarking é, em grande parte, uma oportunidade para uma empresa aprender com a experiência de outras. É um instrumento que oferece fontes de estímulos e *insights* sobre a empresa e desafia sua metodologia habitual de trabalho. A implementação dos resultados e descobertas depende da vontade de mudar e de adaptar-se a novas formas de fazer as coisas (ZAIRI; LEONARD, 1995, p. 46-47). Os autores mencionam que existem tipos diferentes de benchmarking.

3.1 Tipos de Benchmarking

O benchmarking começou como um estudo continuado e profundo da melhor concorrência, uma engenharia reversa detalhada dos produtos e processos tecnológicos concorrentes, o que eles conseguiram e como fizeram (ZAIRI; LEONARD, 1995, p. 71). Os 4 (quatro) tipos de benchmarking são:

1. ***Benchmarking competitivo* –** pode ser utilizado como um modo de informar às pessoas quão bem ou mal eles estão se saindo contra a concorrência direta. A essência do benchmarking é o entendimento de como resultados melhores são atingidos e qual caminho foi delineado para atingí-los;
2. ***Benchmarking funcional* –** é usado para comparar funções específicas, como por exemplo: distribuição, logística, serviço, etc... Com o melhor do setor e o melhor entre

empresas de porte similar. Uma grande vantagem desta abordagem é a maior facilidade de ganhar acesso a informações de empresas que não competem diretamente por representarem menores ameaça;

3. ***Benchmarking interno* –** Benchmarking não significa necessariamente comparação com outra empresa. Para muitas multinacionais, uma pesquisa interna intensiva é o ponto de partida para qualquer exercício de benchmarking. É o esforço contínuo de estabelecer a boa prática em várias operações do negócio como um todo;
4. ***Benchmarking genérico* –** é similar ao funcional em vários aspectos, exceto pelo fato de que focalizam processos de negócio multifuncionais – os processos que estão no coração dos negócios.

A partir do entendimento dos conceitos sobre benchmarking, foi efetuado um processo de benchmarking funcional de um software de gestão de riscos que está apresentado na seção seguinte.

3.2 Aplicação do Benchmarking

Foram pesquisadas algumas empresas como a Modulo Security e a Soft Expert. Na Módulo Security envio-se o pedido para disponibilização da versão de demonstração para avaliação via seu *website*, mas não houve resposta. A Soft Expert disponibilizou uma apresentação, no qual possibilitou a visualização e ter uma noção de como funciona seu sistema.

Também foi efetuado pesquisas na internet por ferramentas *freeware* (grátis). Existem diversas ferramentas freeware na internet, mas que atendem apenas parte do processo de gestão de riscos. A maioria delas são ferramentas para fazer a análise de riscos, que é somente uma das etapas do processo.

A partir da pesquisa, identificou-se um software *opensource* (código aberto) para gestão de projetos que contém o lenvantamento de riscos sobre o projeto. Contudo, nota-se que o mesmo apenas relaciona os riscos, a probabilidade e impacto proveniente de um determinado projeto, como pode ser visualizado na figura 3.1.

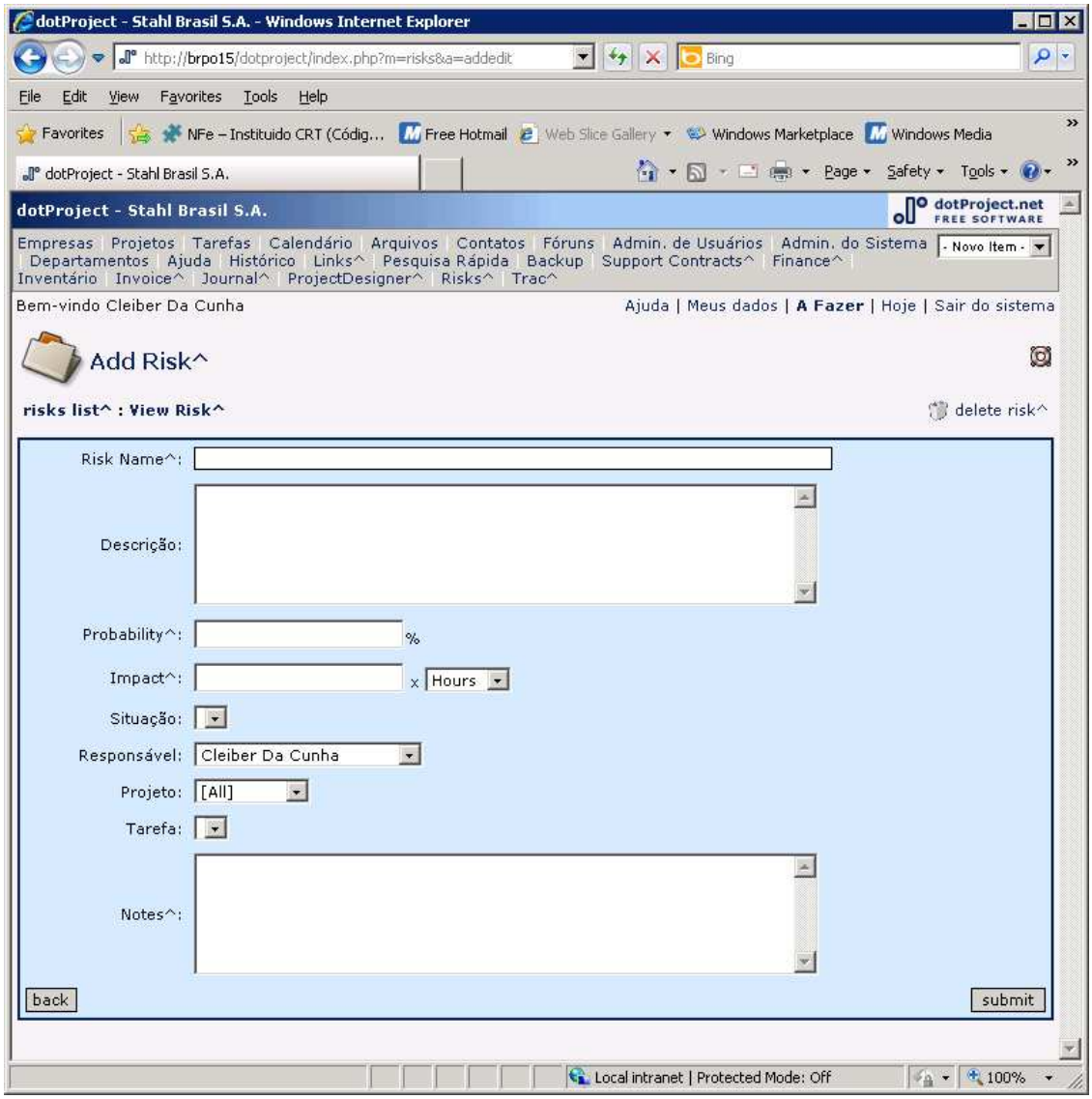


Figura 3.1 – Riscos de projetos existente na dotProject
Fonte: Material interno da empresa Stahl Brasil S.A adaptado da dotProject.net

Das duas empresas contatadas, Soft Expert e Módulo Security, apenas a Soft Expert forneceram material informacional sobre sua solução integrada de gestão de riscos. Sendo assim, o estudo focou em mais detalhes no material fornecido pela Soft Expert.

3.2.1 Empresa Soft Expert

É uma empresa lider na América Latina no desenvolvimento de soluções para a gestão integrada da excelência e conformidade empresarial. Com 14 (quatorze) anos de atuação no mercado, a empresa está presente em mais de 25 (vinte e cinco) países, nos cinco continentes, com uma carteira de mais de 1.800 clientes. É possível perceber na imagem 3.2,

que a empresa vem num crescente bastante agressivo o que torna o processo de benchmarking interessante.

Figura 3.2 – Evolução de crescimento da Soft Expert.
Fonte: Material fornecedido pela SoftExpert - Corporate_Demo_SoftExpert_PT_v2.exe (2011)

3.2.2 SoftExpert ERM Suite

Enterprise Risk Management é o nome do módulo de gestão de riscos da SoftExpert. Segundo a empresa, o processo está definido conforme a figura 3.3.

Figura 3.3 – Enterprise risk management da SoftExpert.
Fonte: Material fornecedido pela SoftExpert - Demo_ERM_BR.exe (2011).

Na figura 3.4, está descrito cada fase do processo de gestão de riscos.

Figura 3.4 – Processo de gestão de riscos
Fonte: Material fornecedido pela SoftExpert - Demo_ERM_BR.exe (2011).

Em cada uma das etapas da gestão de riscos conforme a figura 3.4, a SoftExpert apresentou telas ilustrativas da sua solução.

3.2.2.1 Estabelecer contexto

A figura 3.5 contém a primeira etapa do processo de gestão de riscos, no qual será inserido e definido o contexto a ser análisado.

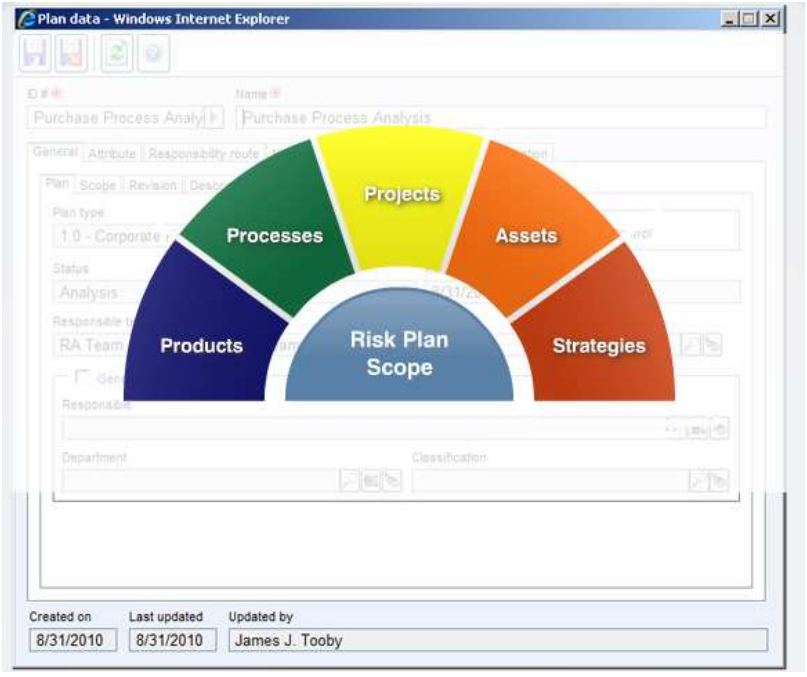


Figura 3.5 – Estabelecer contexto.
Fonte: Material fornecedido pela SoftExpert - Demo_ERM_BR.exe (2011).

3.2.2.2 Identificar

Nesta seção é gerada uma lista preliminar com os possíveis riscos de acordo com o contexto definido anteriormente, listando as causas e potenciais consequências (figura 3.6).

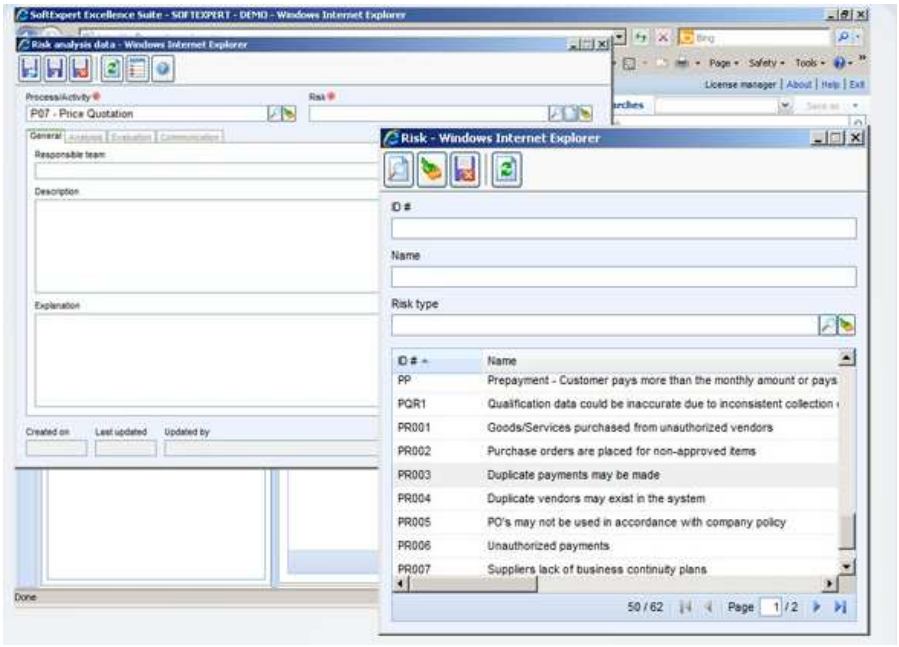


Figura 3.6 – Inclusão de riscos preliminares
Fonte: Material fornecedido pela SoftExpert - Demo_ERM_BR.exe (2011).

Após são listadas as medidas de controle existentes (figura 3.7). É possível identificar que o software prevê riscos positivos e negativos através dos campos “Cost” e “Benefit” supracitado por (SCHMITZ, 2005, p.63; HELDMAN, 2009, p. 266).

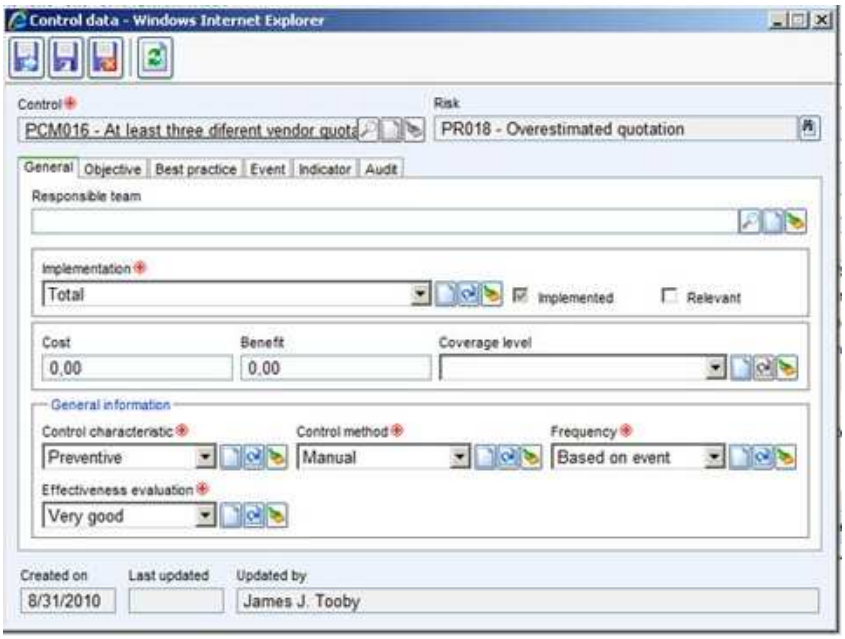


Figura 3.7 – Medidas de controle
Fonte: Material fornecedido pela SoftExpert - Demo_ERM_BR.exe (2011).

3.2.2.3 Analisar e avaliar

Nesta etapa (figura 3.8), é onde será determinada a severidade e probabilidade para que se possa decidir se o risco deve ser tratado. O processo é feito porr meio de uma análise que se definiu na idendificação do risco (seção 3.2.2.2).

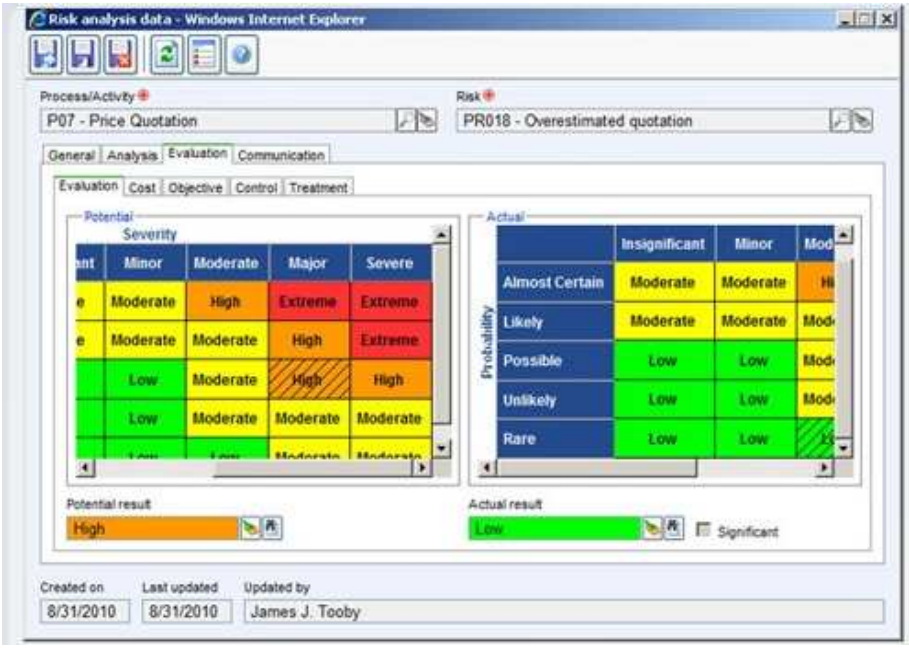


Figura 3.8 – Medidas de controle
Fonte: Material fornecedido pela SoftExpert - Demo_ERM_BR.exe (2011).

Pode-se utilizar nessa fase, ferramentas como Ishikawa para avaliar os desvios referentes ao processo analisado (figura 3.9).

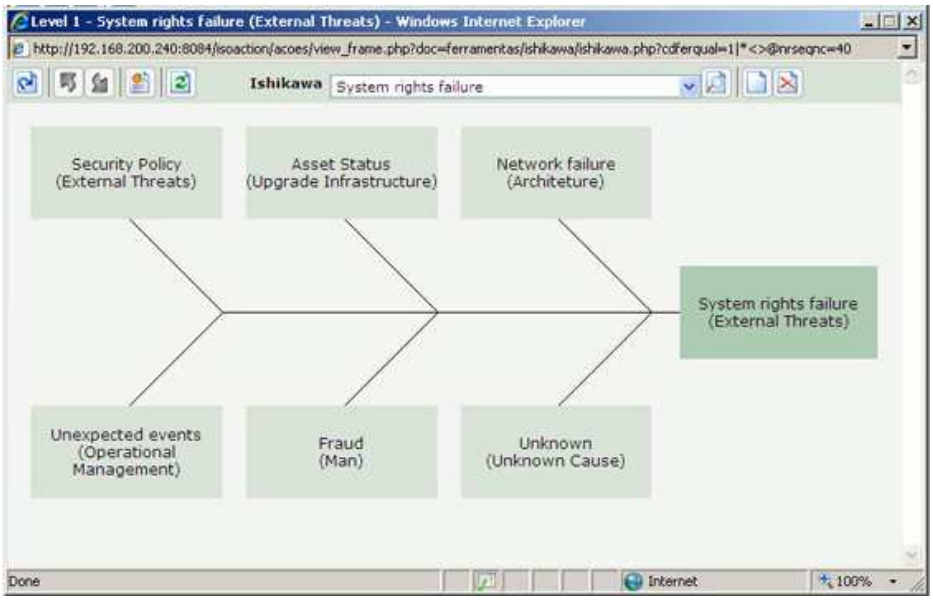


Figura 3.9 – Diagrama de Ishikawa
Fonte: Material fornecedido pela SoftExpert - Demo_ERM_BR.exe (2011).

3.2.2.4 Tratar

Este é o momento (figura 3.10) onde será informado ao sistema de que forma serão implementados os tratamentos e a forma que será feito o monitoramento da execução, definindo as opções e métodos (plano de ação, *workflow*, projeto).

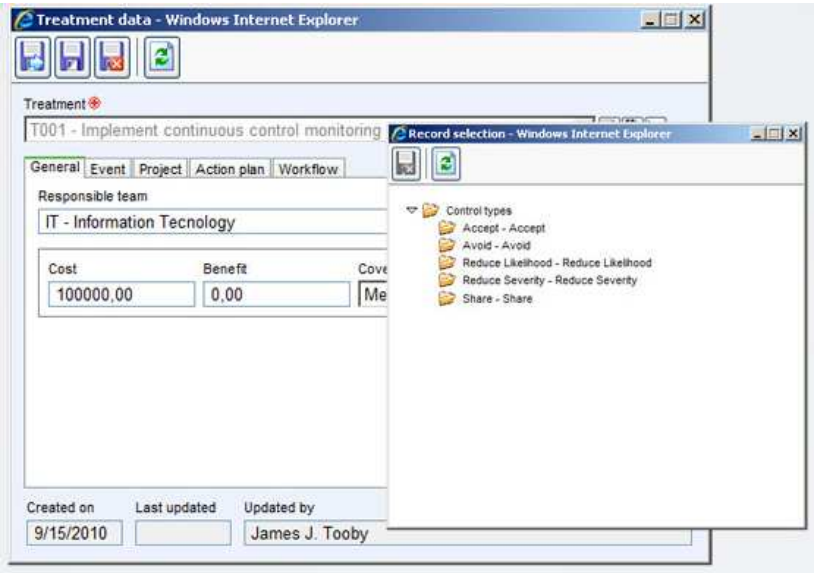


Figura 3.10 – Implementação do tratamento
Fonte: Material fornecedido pela SoftExpert - Demo_ERM_BR.exe (2011).

3.2.2.5 Comunicar e consultar

Durante todo o processo de gestão de riscos, os grupos de pessoas selecionados (figura 3.11) serão informados e comunicados. Desta forma, participarão do processo do início ao fim.

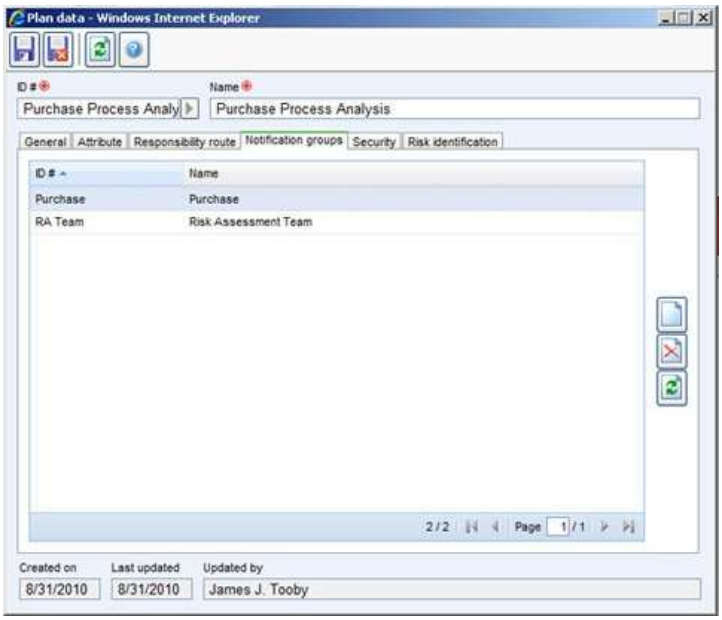


Figura 3.11 – Comunicação
Fonte: Material fornecedido pela SoftExpert - Demo_ERM_BR.exe (2011).

Nesta fase também é fornecida diversas formas de visualizações (figura 3.12) para facilitar a execução das atividades e manter o processo sobre controle.

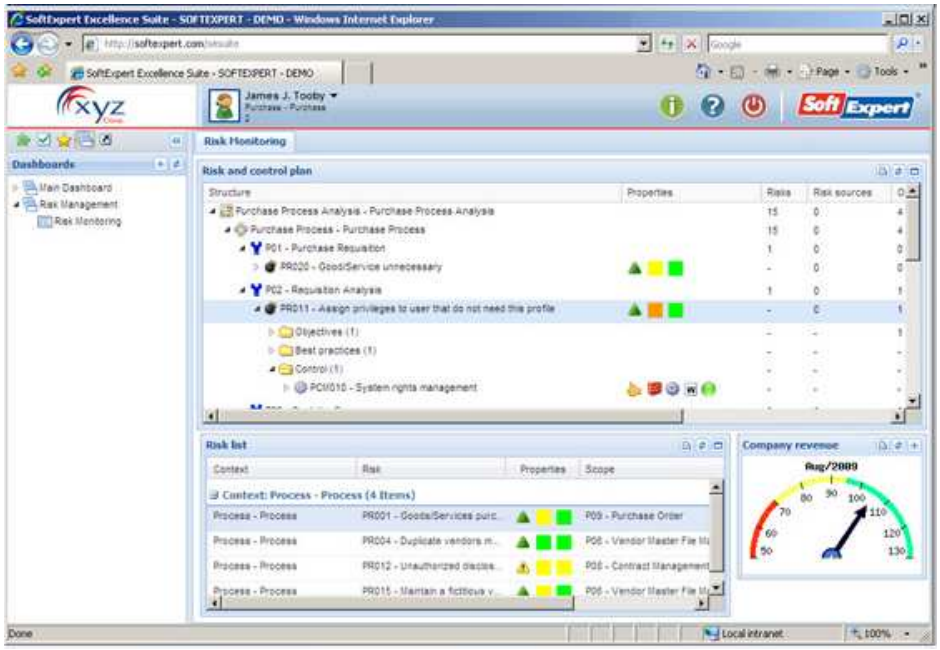


Figura 3.12 – Monitoramento
Fonte: Material fornecedido pela SoftExpert - Demo_ERM_BR.exe (2011).

Com o processo de benchmarking foi possível constatar que a solução proposta pela Soft Expert possui diversas ferramentas para a gestão de riscos, inclusive para o escopo de TI. O sistema abrange todas as etapas sugeridas pelos autores (quadro 1.2, p. 31). O que poderia inviabilizar sua adoção, em algumas organizações, é que a mesma possui um custo de aquisição, acrescida de manutenção mensal. Sendo assim, para sua implementação, será necessário submeter o projeto à aprovação financeira para que seja avaliado o custo-benefício de sua implantação.

No próximo capítulo, será abordada a metodologia utilizada para efetuar a pesquisa do presente trabalho.

4 METODOLOGIA

O método de pesquisa descreve o conjunto de regras para que um pesquisador possa desenvolver um trabalho de investigação e produzir conhecimento, garantindo que as etapas do trabalho e resultados obtidos possam ser entendidas, interpretados e até repetidos por terceiros se praticados em condições similares a original (MALHOTRA, 2006, p. 290).

Neste capítulo apresenta-se o método de pesquisa, bem como as técnicas de coleta e análise de dados que a pesquisa se propôs.

4.1 Método de pesquisa

Para a elaboração deste trabalho foram adotadas as seguintes metodologias:

- ***Pesquisa-ação*** – os principais objetivos de uma pesquisa-ação, de acordo com Coughlan; Coughlan (2002, p. 152) são a geração de conhecimento científico e o desenvolvimento de uma solução para um problema prático existente em uma organização por meio de um processo cíclico que envolve planejamento, ação, avaliação dos resultados para re-planejamento. Assim, a escolha da metodologia se justifica visto que o autor deste trabalho interage na área de atuação da solução. Além disso, procura-se que o resultado esperado seja um processo que promova a melhoria contínua e conte com a participação das pessoas da organização.
- ***Estudo de Caso*** – é definido como aquele que examina um fenômeno em seu ambiente natural, pela aplicação de diversos métodos de coleta de dados, visando a obter informações de uma ou mais entidades. Essa estratégia de pesquisa possui caráter exploratório, sem nenhum controle experimental ou de manipulação. Além disso, as fronteiras do fenômeno não são evidentes (POZZEBON; FREITAS, 1998, p. 145).

Por conseguinte, foi adotada a pesquisa descritiva que, segundo Gil (2006, p. 42), objetiva primordialmente a descrição das características de determinada população ou fenômeno, ou, então, o estabelecimento de relações entre variáveis. São inúmeros os estudos que podem ser classificados sob este título e uma de suas características mais significativas está na utilização de técnicas padronizadas de coleta de dados, tais como questionários e a observação sistemática.

Pozzebon; Freitas (1998, p. 144) definem que, entre os métodos qualitativos, pode-se destacar a importância potencial que o estudo de caso e a pesquisa-ação podem vir a desempenhar na área de sistemas de informação.

O foco da pesquisa tem como objetivo propor um modelo de gestão de riscos orientado a TI, usando como base as respostas extraídas da pesquisa-ação e do estudo de caso.

A definição da área-alvo da pesquisa está descrita na seção que segue.

4.2 Definição da área alvo da pesquisa

Como foram adotadas duas metodologias (pesquisa-ação e estudo de caso) a fim de agregar valor à pesquisa, a áreas alvo foi subdividida em duas:

- ***Pesquisa-ação***: a empresa foco deste estudo é uma multinacional de capital aberto dedicada à oferta de produtos químicos para tratamento e acabamento em couros e sintéticos. Seus produtos, combinados com a excelência de atendimento, são capazes de gerar maior ganho de produtividade, além de produtos de altíssimo valor agregado. Ela é uma indústria química situada em Portão-RS no [1] Vale dos Sinos. Sua matriz está situada na Holanda, onde atua a mais de 50 (cinquenta) anos no ramo químico. No Brasil, possui 120 funcionários nas unidades de Portão (115) e Franca – SP (5). A unidade de Portão, atualmente, é a centralizadora da América do Sul, onde são produzidos os produtos e distribuídos nas demais unidades: Argentina, Uruguai e Colombia. A escolha da organização para aplicação da pesquisa-ação foi definida em função dos seguintes items:
  - Identificação da possibilidade de implantação do gerenciamento de riscos sobre a infraestrutura de TI;
  - Facilidade de obtenção dos dados a serem coletados; e
  - Interesse de sua Matriz em implementar a gestão de riscos em TI
- ***Estudo de caso*** – foram pesquisadas 5 (cinco) empresas de ramos de atividades diferentes que são: 1) indústria calçadista; clínica médica; *software-house;* governamental e indústria de alimentos;

A partir desta definição, foram selecionados os sujeitos que estão dispostos na próxima seção.

4.2.1 Seleção dos sujeitos

Os sujeitos da pesquisa são as pessoas que irão fornecer os dados necessários, aqueles que irão responder o questionário elaborado para efetuar a pesquisa-ação (VERGARA, 2007, p. 53). Os sujeitos selecionados para a pesquisa estão descritos no quadro 4.1:

Quadro 4.1 – Sujeitos da pesquisa

Metodologia aplicada	Tipo da empresa	Cargo
ESTUDO DE CASO	*Softwarehouse* & Provedor de Internet	Gerente de Projetos.
	Indústria de alimentos	Gerente de TI.
	Indústria de calçados	Analista de TI.
	Clínica médica	Analista de TI.
	Governamental	Analista de TI.
PESQUISA-AÇÃO	Indústria química	Diretor mundial de TI (CIO) Gerente de TI (Cingapura) Gerente de TI (Índia)

Fonte: Autoria própria (2011).

Os entrevistados foram selecionados considerando suas características e conhecimento, de forma que pudessem contribuir para o processo da pesquisa.

4.3 Plano de coleta de dados

A etapa de coleta de dados envolve a escolha da técnica a ser utilizada para captura das percepções acerca do assunto (GIL, 2006, p. 163). O questionário é um instrumento utilizado para coleta de dados formada por uma série ordenada de perguntas, que devem ser respondidas por escrito e sem a presença do entrevistador (LAKATOS, 1999, p. 100).

Vergara (2007, p. 54) orienta que ao efetuar uma coleta de dados, o leitor deve ser informado de como o entrevistador pretende obter as informações que precisa para conseguir responder o problema.

Os questionários (APÊNDICE C – em português; APÊNDICE D – em inglês) foram desenvolvidos a partir da análise de conteúdo do referencial bibliográfico pesquisado. Berelson apud Gil (2007, p.165) cita que a análise de conteúdo significa “uma técnica de pesquisa para a descrição objetiva, sistemática e quantitativa do conteúdo evidente da comunicação”. A utilização desta técnica permite analisar o conteúdo de livros, revistas, jornais, discursos, películas cinematográficas, propaganda de rádio e televisão, etc (LAKATOS; 1999, p. 130-131).

O objetivo dos questionários é buscar responder o objetivo geral e os específicos deste trabalho. Outro sim consiste em traduzir os objetivos em questões a serem respondidas. As questões constituem, pois, o elemento fundamental do questionário (GIL, 2007, p. 129). O mesmo deve ser limitado em extensão e finalidade. Se for muito extenso causa desinteresse por parte da pessoa que irá respondê-lo; se curto demais, corre o risco de não oferecer suficientes informações. Lakatos (1999, p. 101) recomenda que deva conter de 20 (vinte) a 30 (trinta) perguntas e que não deve demorar mais de 30 (trinta) minutos para ser respondido. Este número não é fixo, vai depender do tema da pesquisa e dos informantes.

Todas as questões que compõe a pesquisa foram aplicadas a todos os sujeitos relacionados anteriormente na seção 4.2.1. Num primeiro momento, foi realizado um pré-teste com 04 (quatro) pessoas, sendo 2 (dois) administratores de rede e 2 (duas) pessoas ligadas ao processo de gestão de riscos de outras áreas (financeiro). O pré-teste foi realizado com o objetivo de garantir a clareza das questões e objetividade das respostas. O mesmo foi composto por 22 (vinte e duas) questões. Para Lakatos (1999, p. 102), o pré-teste serve para verificar se o questionário apresenta 3 (três) importantes elementos: 1) fidedignidade – qualquer pessoa que o aplique obterá sempre os mesmos resultados; 2) validade – os dados recolhidos são necessários à pesquisa; e 3) operatividade – vocabulário acessível e significado claro. A partir desta ação identificaram-se as seguintes necessidades:

- Maior clareza e delimitação das perguntas;
- Inclusão de conceitos junto às perguntas para facilitar a compreensão da pergunta.

4.4 Plano de Análise de dados

No plano de análise de dados, procura-se explicar como se pretende tratar os dados coletados, explicando o motivo pelo qual a análise será adequada para o propósito do estudo (VERGARA, 2005, p. 59).

A partir dos dados obtidos através do questionário, utilizou-se a técnica de análise de conteúdo para responder ao seguinte objetivo específico: ***propor um modelo de gestão de riscos***. Chizzotti (1991, p.98) define a análise conteúdo como “um método de tratamento e análise de informações para coleta de dados em texto”. Para realizar a análise de conteúdo, os autores sugerem seguir as seguintes etapas: 1) definição do universo; 2) categorização do universo estudado; 3) escolha das unidades de análise; e 4) quantificação (figura 4.1).

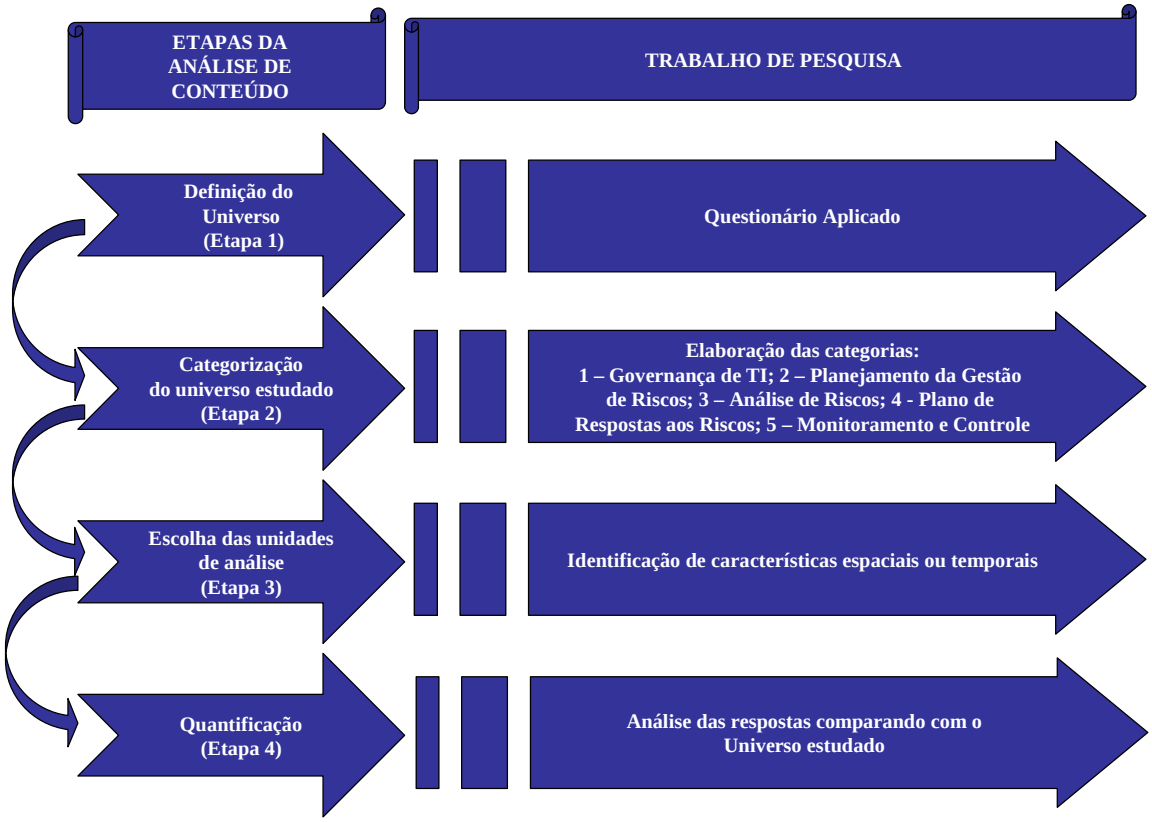


Figura 4.1 – Etapas da análise de conteúdo
Fonte: Adaptado de Freitas; Janissek (2000, p. 45).

- ***Etapa 1 (definição do universo)* –** delimita e define o universo a ser estudado. Apresenta o que está e o que não está na análise de conteúdo. O universo selecionado nesse estudo foi delimitado pelas respostas obtidas no questionário aplicado na pesquisa;
- ***Etapa 2 (categorização do universo estudado)* –** as categorias definidas foram apuradas a partir do referencial bibliográfico e a também das palavras-chave oriúndas das respostas dos questionários aplicado. Gil (2007, p. 168-169) relata que a análise tem como objetivo organizar e sumarizar os dados de tal forma que possibilitem o fornecimento de respostas ao problema proposto para investigação. As respostas fornecidas pelos elementos da pesquisa tendem a ser mais variados. Para que as respostas possam ser adequadamente analisadas, torna-se necessário organizá-las em grupos identificados como categorias. Aquelas que apresentaram as mesmas palavras-chaves foram agrupadas na mesma categoria. Assim sendo, as palavras-chave foram divididas em 5 (cinco) categorias:

1. *Governança de TI* – nesta categoria, foram abordadas questões relativas à governança de TI e práticas utilizadas na organização do entrevistato;
2. *Planejamento da gestão de riscos* **–** objetiva conhecer se existe gestão de riscos, visando identificar pontos favoráveis ou não, para a implementação da gestão de riscos;
3. *Análise de riscos* – procura analisar como os riscos são analisados e tratados na organização.
4. *Plano de respostas aos riscos* – teve como objetivo elucidar as possibilidades de resposta aos riscos da organização, com o intúito de perceber se o entrevistado está contemplanto o processo de gestão de riscos em sua íntegra;
5. *Monitoramento e controle* – visou identificar se os entrevistados já possuem, ou gostariam de implementar, um sistema de modelo de riscos orientado à TI.

- ***Etapa 3 (identificação de características espaciais ou temporais)* –** para Freitas; Janissek (2000, p. 47), esta etapa implica em relacionar especificidades das respostas evidenciando o conjunto total das idéias apresentadas. Sendo assim, todas as categorias foram investigadas em profundidade observando as características espaciais ou temporais.
- ***Etapa 4 (quantificação)* –** nesta etapa foi realizada a análise e interpretação dos dados relacionando com o universo estudado. O resultado das interpretações e análises está disposto no capítulo 5.

5 ANÁLISE DOS DADOS

A análise dos dados é o que possibilita a revisão crítica de um conceito ou modelo, ressaltam Pozzebon; Freitas (1998, p. 166). Bardin (2004, p. 31) complementa que neste período, o analista codifica o conteúdo com interesse não na sua descrição, mas sim no que poderá ensinar depois de receber tratamento.

Roesch (2006, p. 174) indica que em uma pesquisa de caráter qualitativo, após o encerramento da coleta dos dados, o pesquisador se depara com uma grande quantidade de depoimentos, respostas em formato de texto, as quais terão que organizar para depois interpretar. Procura-se utilizar técnicas que seguem os padrões quantitativos, ou seja, tem o propósito de contar a frequência de um fenômeno. Costuma-se denominar o conjunto destas técnicas de análise de conteúdo.

Neste trabalho foi utilizadas questões do tipo abertas (qualitativas) e fechadas (quantitativas). Para as qualitativas, a técnica de análise de conteúdo e para as quantitativas, as questões foram analisadas através de tabulação de dados. Na figura 5.1, é possível verificar o modelo adotado na extração e análise dos dados.

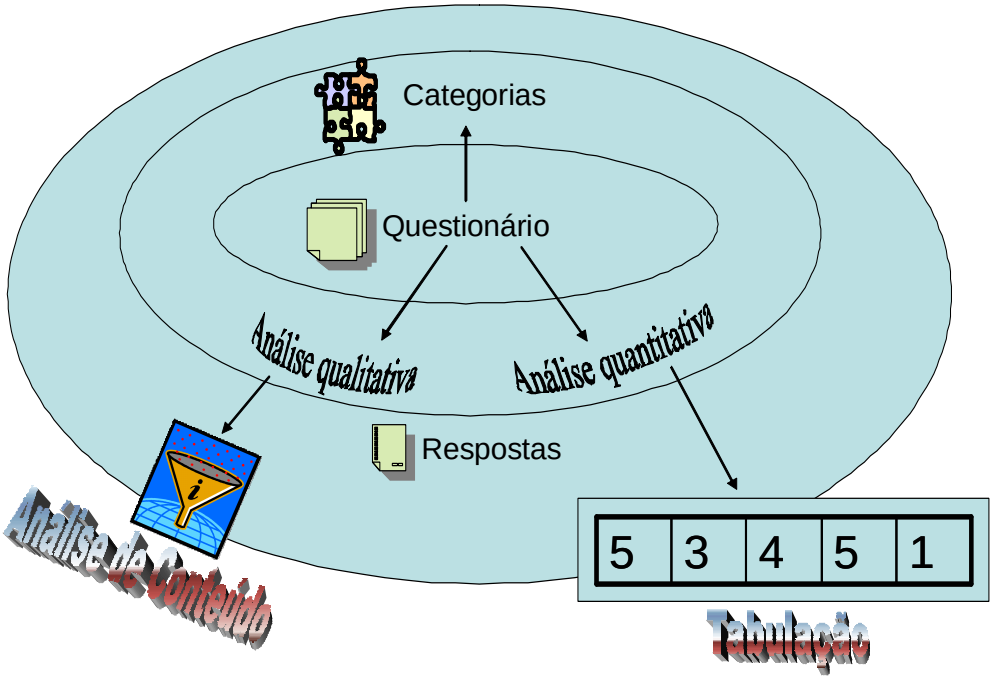


Figura 5.1 – Esquema para apuração dos dados
Fonte: Autoria própia (2011)

5.1 Análise de conteúdo

De acordo com a figura 4.1, a partir dos questionários foram extraídos 5 (cinco) categorias as quais foram subdivididas em mais três respectivamente:

- Categoria inicial – composta pela síntese da pergunta;

- Categoria intermediária – obtida das respostas obtidas;
- Categoria final – uma análise comparativa extraída das respostas e comparada ao referencial bibliográfico (APÊNDICES E, F, G, H, I).

Após a identificação das categorias, foi efetuada a escolha das unidades de análise. As categorias definidas foram investigadas em profundidade, pois apresentam características espaciais ou temporais que implicam em relacionar especificidades das respostas evidenciando o conjunto total das ideias apresentadas (Freitas; Janissek, 2000, p. 47).

A última etapa foi à tabulação das respostas combinadas ao universo estudado, conforme demonstrado no quadro 5. As perguntas de cada categoria foram analisadas suas respectivas respostas fornecidas na seguinte estrutura:

a) ***Pergunta*** **-** questões que compõe o questionário aplicado na pesquisa de verificação;

b) ***Análise*** **–** síntese elaborada pelo autor a partir das respostas coletadas através do questionário;

c) ***RT*** **–** referencial teórico que permite validar ou não, a análise efetuada em relação às respostas obtidas;

d) ***Parecer*** **–** Em relação ao objetivo geral do presente trabalho.

Quadro 5.1 – Análise qualitativa

Nº da pergunta APÊNDICE C	Estrutura de análise
1	**Pergunta:** Considerando que Tecnologia da Informação é o processo de transformação dos conceitos, conhecimentos e equipamentos das áreas de informática e telecomunicações, em aplicações úteis a todas as outras áreas em todo e qualquer contexto, onde ela (a TI) possa ser efetivamente aplicada (SPOHR; SAUVÉ, 2003, p. 240), é necessário que as empresas estejam atentas a importância de sua infraestrutura de TI. De acordo com esta situação, cite 3 (três) fatores que você considera importante na gestão da Tecnologia da Informação. **Análise:** Na pesquisa, segurança da informação, plano de continuidade e melhoria contínua são fatores considerados como sendo importantes pelos entrevistados. **RT:** De acordo com os resultados apurados, nota-se que as respostas dos entrevistados possuem relação com o referencial teórico do presente trabalho. **Parecer:** ***A partir do referencial teórico estudado e das respostas obtidas dos questionários, é possível concluir que é indicado a implementação da gestão de riscos na área de Tecnologia da Informação.***
5	**Pergunta:** De acordo com Spohr; Sauvé (2003, p. 6) é necessário que as empresas conheçam melhor os recursos, as promessas e a realidade das novas tecnologias, avaliando até que ponto elas devem modificar sua forma de trabalho para adotar alguma destas tecnologias. Diante desta afirmação, você acredita que a gestão de riscos poderia contribuir em que situação. **Análise:** Conhecer suas limitações; conhecer os riscos na adoção de novas tecnologias e ter uma visão completa do processo de gestão de riscos para transformar uma incerteza em oportunidade foi consenso em 87,5% dos respondentes da pesquisa. **RT:** Ficou evidenciada a relação entre o mencionado por Spohr; Sauvé e as respostas fornecidas no questionário. **Parecer:** ***Recomanda-se que seja implementado a gestão de riscos a fim de que as organizações identifiquem e conheçam suas limitações. Principalmente, na adoção de novas tecnologias a fim de transformar a incerteza em uma possível oportunidade.***
6	**Pergunta:** Segundo Heldman (2009, p. 233), o plano de gerenciamento de riscos assegura que a quantidade apropriada de recursos e o tempo apropriado são dedicados ao gerenciamento de riscos. Diante desta afirmação, qual sua opinião sobre o processo de gestão de riscos? **Análise:** Há um consenso comum de 100% dos entrevistados: que o processo de gestão de riscos aumenta a assertividade nos projetos; diminuindo as incertezas. **RT:** A função mais importante do plano de gerenciamento de riscos é ser uma linha de base acordada para avaliar os riscos dos projetos (HELDMAN, 2009, p. 233). **Parecer:** ***Sugere-se a implementação da gestão de riscos a fim de nortear a organização e buscar maior assertividade nos projetos.***
7	**Pergunta:** Para Westerman; Hunter (2008, p. 182), a ***governança de riscos de TI*** deveria estar embutida nos mais importantes processos decisórios da organização, onde a empresa evita deixar-se "cegar" e consegue assumir mais riscos, e, portanto, mais oportunidades, com maior confiança. Você concorda com esta afirmação? Por quê? **Análise:** O processo de governança de riscos de TI auxilia as áreas de negócios da organização em conhecer suas limitações e seus pontos fracos. Mas também, possibilita identificar os pontos fortes, podendo identificar as oportunidades que não são visualizadas pelos concorrentes. **RT:** Nesta análise, verificou-se que 7 (*sete*) entrevistados mencionaram que concordam que a gestão de risco deveria estar embutida nos mais importantes processos decisórioas da organização. Portanto, é possível afirmar que há uma relação entre a bibliografia estudada com a percepção dos entrevistados na prática. **Parecer:** ***Quanto à este quesito, é essencial que a governança de riscos de TI seja abordada no nível estratégico das organizações para assegurar que***

	suas limitações sejam inferiores às suas oportunidades no momento da tomada de decisão.
9	**Pergunta:** Qual sua opinião sobre gestão de riscos de ***infraestrutura de TI***? **Análise:** Dentre as opiniões apresentadas como resposta a esta pergunta, destaca-se: • Preocupação com a Segurança da Informação; • Preocupação com a continuidade dos negócios e • Alinhamento da TI com os negócios. **RT:** De acordo com Ramos et al (2006, p. 20), a segurança da informação busca a proteção contra situações nas quais os prejuízos são causados por conta de danos diretos aos ativos ou por situações prejudiciais inesperadas. **Parecer:** ***Sugere-se a adoção de um processo de governança de riscos a fim de garantir o alinhamento e a continuidade dos negócios como citado por Fernandes; Abreu (2008, p. 14) na seção 1.1 deste trabalho (p. 15).***
10	**Pergunta:** Quais os principais ***ativos*** que são monitorados ou que sugerem que fossem monitorados pela ***gestão de riscos***? **Análise:** A maioria dos entrevistados mostra-se preocupado em monitorar: telecomunicações (*link de dados*), *servidores e backup* (*salva-guarda de dados*); **RT:** Ativo é tudo aquilo que tenha valor e que necessita de algum tipo de proteção ou cuidado por conta disso (RAMOS et al, 2006, p. 44). **Parecer:** ***Recomenda-se que os ativos citados sejam monitorados e controlados pela gestão de riscos de TI. Pois, os elementos citados pelos entrevistados, fazem parte do modelo sugerido por Mansur na seção 1.1.1 (figura 1.2) deste estudo (p.16).***
11	**Pergunta:** Durante o processo de ***análise e avaliação de risco*** é que serão feitos todos os levantamentos em relação às ameaças, vulnerabilidades, probabilidades e impacto aos quais os ativos estão sujeitos (RAMOS et al, 2006, p. 50). Você considera importante que a empresa conheça os riscos associados a seus ativos? **Análise:** De acordo com as respostas fornecidas, verificou-se que é de extrema importância que a organização conheça as ameaças e as vulnerabilidades de seu ambiente, levando em consideração a probabilidade e o possível impacto que são decorrentes dos mesmos (*100% dos entrevistados concordam com o que foi questionado*). **RT:** Riscos são incertezas. Quanto mais se souber de antemão os riscos e seus impactos, mais preparado se está para lidar com eles caso ocorram (HELDMAN, 2009, p. 232). **Parecer:** ***Percebe-se que há relação entre as repostas inferidas e o referencial teórico.***

13	**Pergunta:** ***Análise qualitativa de riscos*** visa à detecção do impacto dos riscos e sua probabilidade de ocorrência. A ***análise quantitativa*** avalia os impactos e quantifica a exposição aos riscos por meio da atribuição de probabilidades numéricas (HELDMAN, 2009, p. 249). Qual ou quais das técnicas acima você utilizaria no processo de avaliação de riscos? Justifique. **Análise:** Considerou-se válido a escolha de ambas as técnicas. Desta forma, está evidenciado que os riscos precisam ser analisados tanto qualitativos quanto quantitativamente. Utilizando quando possível os dois métodos (*análise qualitativa (2), analise quantitativa (1), as duas (4)*). **RT:** A Análise de riscos com técnicas qualitativas visa à detecção do impacto dos riscos identificados e sua probabilidade de ocorrência. Já a análise quantitativa avalia os impactos e quantifica a exposição aos riscos por meio da atribuição de probabilidades numéricas (HELDMAN, 2009, p. 249-257). **Parecer:** ***Sugere-se a utilização inicial das técnicas qualitativas, pois a mesma traz uma abordagem mais simples e é de fácil interpretação. Como complementação, quando necessário, recomenda-se também a utilização da técnica quantitativa a fim de ter uma visão mais minunciosa.***
15	**Pergunta:** ***Pessoas*** são movidas pelo conhecimento, pela falta dele e também pela emoção e pelo sentimento (RAMOS et al, 2006). Sob esta ótica, você considera que pessoas podem representar riscos para a TI? **Análise:** Fica bastante claro que "Pessoas" estão diretamente ligadas a "Informação". E o mau uso destas informações pode acarretar muitos danos à organização. **RT:** Conforme mencionado por IBM na seção 1.3.1, para ser realmente eficaz, o gerenciamento de riscos deve estar profundamente integrado a mentalidade corporativa da força de trabalho. **Parecer:** ***As pessoas é o que podem diferenciar uma empresa de outra, entre o sucesso e o fracasso nos negócios. Sob esta ótica, recomenda-se a adoção de um processo de gestão de riscos sobre as pessoas que possuem acesso aos ativos sensíveis da organização.***
16	**Pergunta:** ***"Informação"*** pode ser entendida como todo patrimônio que se refere à cultura da empresa ou ao seu negócio, podendo tais informações ser de caráter comercial, técnico, financeiro, legal, de recursos humanos, ou de qualquer outra natureza, que tenham valor para a organização e que se encontrem armazenadas em recursos computacionais da empresa, com tráfego dentro da sua infraestrutura tecnológica (RAMOS et al, 2006, p. 291). As perdas destas informações podem representar prejuízos significativos para a organização. Como você classificaria este risco? **Análise:** Nesta questão, notou-se que há uma interpretação diferente entre os "gerentes; CIO" (5) e os "analistas" de TI (3). O CIO e os gerentes entrevistados apontaram que este é um risco organizacional. Para os analistas, esté é um risco de gerenciamento da informação. **RT:** Segundo Heldman (2009, p. 239)**,** riscos de gerenciamento engloba o planejamento inadequado dos recursos, projetos mal planejados e metodologias de gerenciamento inadequada. Já os riscos organizacionais, envolvem tempo e custos pouco realistas. **Parecer:** ***Percebe-se que há diferentes pontos de vistas, considerando o nível hirárquico dentro das organizações. De qualquer forma, o mais importante é que em ambas as opiniões, a informação precisa ser gerenciada para evitar prejuízos à organização.***
18	**Pergunta:** A ***mitigação de risco*** é outra estratégia utilizada pra riscos negativos que tem por finalidade diminuir a probabilidade de ocorrência e o impacto do risco até um nível aceitável (HELDMAN apud PMBOK, 2009, p. 266). Alguns exemplos de mitigação de riscos incluem utilização de processos menos complexos, criação de protótipos e seleção de fornecedores mais confiáveis. Você adotaria esta estratégia em seu planejamento de resposta aos riscos? **Análise:** Todos os entrevistados responderam que utilizariam a mitigação de riscos com estratégia. O CIO mencionou ainda que: **"Esta é a opção padrão para manipular riscos = redução do impacto/ocorrência".** **RT:** Esta estratégia é sugerida pelos autores pesquisados no presente trabalho (conforme exposto no quadro 1.2 – comparativo sobre estratégias para tratar riscos identificados). **Parecer:** ***Sendo assim, é sugerida a utilização desta estratégia para tratamento de riscos.***

19	**Pergunta:** De acordo com Baraldi (2005, p. 29), os riscos são elementos incertos e as expectativas, que agem constantemente sobre os meios estratégicos (pessoas, processos, informação, e comunicação). Por consequência, se adequadamente gerenciados, forçam a criatividade e fazem nascerem as oportunidades. Heldman (2009, p. 266) sugere que para tratar as oportunidades ou os riscos positivos poderiam-se utilizar algumas ***estratégias*** que são: • **Exploração –** é utilizada quando forem identificados riscos positivos que se queira garantir que ocorram. Ex: risco na redução do tempo total necessário para conclusão do projeto; • **Compartilhamento –** é a transfêrencia do risco para um grupo que esteja mais bem preparado para lidar com a oportunidade que ele representa; • **Melhoria –** é a que observa a probabilidade ou impacto do evento de risco para garantir que a organização perceba os benefícios. Na infraestrutura de TI podem ocorrer riscos positivos que podem ser explorados, compartilhadados ou melhorados. Diante desta afirmação, cite 2 (dois) ou mais riscos positivos ocorridos em sua organização e qual (is) da(s) estratégia(s) foi utilizada. Se nenhuma comente. **Análise:** As repostas ficaram dividas entre as três estratégias sugeridas (*compartilhamento (3), exploração (2) e melhoria (3)*). **RT:** Assim sendo, ficou transparente a relação entre as respostas apuradas com o que foi mencionado por Heldman e Baraldi. **Parecer:** ***Portanto, fica evidente que todas elas podem, em algum momento, serem utilizadas a favor da organização.***
20	**Pergunta:** ***Planejamento de contingência***, na opinião de Heldman (2009, p. 268), consiste na elaboração de alternativas para lidar com os riscos caso eles se concretizem. É diferente de mitigação que visa à "redução" da probabilidade e seu impacto. Significa que caso o risco venha ocorrer, a organização estará preparada para tratá-lo. As reservas ou provisões para contingências é uma opção usada com frequência. Sua empresa possui plano de contingência a riscos? **Análise:** No entendimento dos entrevistados, é necessário que a organização tenha um plano de contingência para garantir a continuidade dos negócios. (*Das 6 (seis) repostas "SIM", 4 foram atribuídas a "link de dados" e 3 para "Backup"*). **RT:** De acordo com Heldman (2009, p. 268), quando não é possível adotar nenhuma das estratégias de tratamento do risco, a contingência entra em jogo quando o evento de risco acontece. Isso significa que os planos devem ser preparados muito antes da ameaça. **Parecer:** ***Sugere-se que os ativos com maior probabilidade e alto impacto, identificados na etapa de "análise de riscos" possuam um plano de contingência definido.***
21	**Pergunta:** A complementação da gestão de riscos para Ramos et al (2006, p. 82), se dá através do uso de mecanismos para monitorar a eficácia de seus componentes. Sua empresa possui um ***sistema de gestão de riscos***? **Análise:** Entre a maioria dos entrevistados, constatou-se que as empresas não possuem um sistema de gestão de riscos implementado e que a gestão dos riscos é feita de forma manual e não estruturada *(3 disseram que "SIM" e que utilizam sistemas próprios e 5 disseram que "NÃO" - é feito manualmente").* **RT:** Ramos et al (2006, p. 82) complementa ainda que o monitoramento é imprescindível e que a manutenção do mesmo servirá – entre outras coisas – para a avaliação da eficácia das proteções e comparar os resultados efetivos com os estimados. **Parecer:** ***Pode-se concluir que para obter uma gestão de riscos eficaz é necessária a adoção de um sistema de gestão que compreenda o processo por completo.***

22	**Pergunta:** Westerman; Hunter (2008; p. 184), alertam que não se tem como provar que alguma coisa não ocorreu graças a seus esforços de risco de TI, contudo, é possível mensurar o esforço que dedica a seu programa, a frequencia e o impacto comercial de incidentes de riscos, níveis de consciência gerais e específicos de cada papel e a agilidade que a empresa adquire ao melhorar seu perfil de risco de TI. Os autores acrescentam ainda: "adote medidas para guiar a consciência, os processos e a simplificação". Diante do exposto, você concorda que um ***sistema de gestão de riscos*** poderia complementar e melhorar o processo de gestão de riscos de sua organização? **Análise:** Observou-se nas respostas do questionário que para esta questão há um consenso de que um sistema de gestão de riscos pode sim complementar e melhorar o processo de gestão de riscos da organização *(100% dos entrevistados responderam "SIM")*. **RT:** Esta é uma das "Dez maneiras de os Executivos melhorarem a Gestão de risco de TI", relatam Westerman; Hunter (2008, p. 179), classificando o sistema de gestão de riscos como sendo a maneira de número 8 (oito). **Parecer:** ***O sisema é recomendável para que a organização tenha o processo formalizado, com ferramentas apropriadas e padronizadas para buscar a melhoria contínua de seus processos por meio de controles e monitoramentos adequados.***

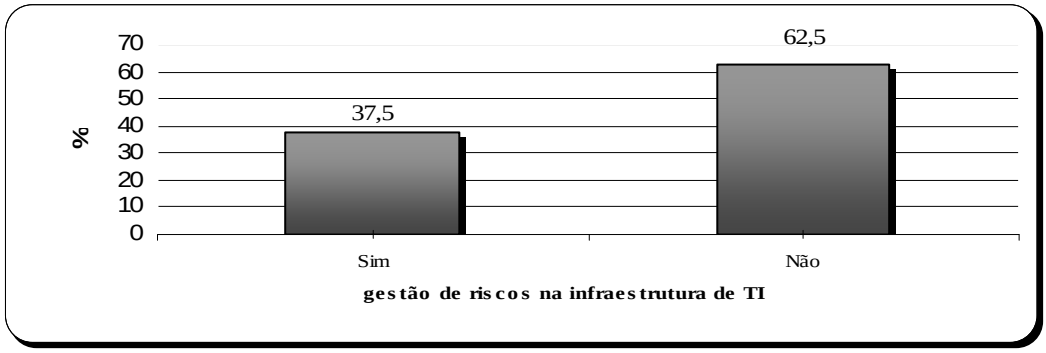
Fonte: Autoria própria (2011).

5.2 Tabulação quantitativa

A seguir, estão dispostas as perguntas qualitativas e algumas quantitativas que foram consideradas mais interessantes pelo autor deste trabalho que fossem analisadas na forma de gráfico. O questionário foi respondido por 8 (oito) pessoas de diferentes empresas e de diferentes níveis hierárquicos. A interpretação sucinta do resultado está feita após cada uma das questões.

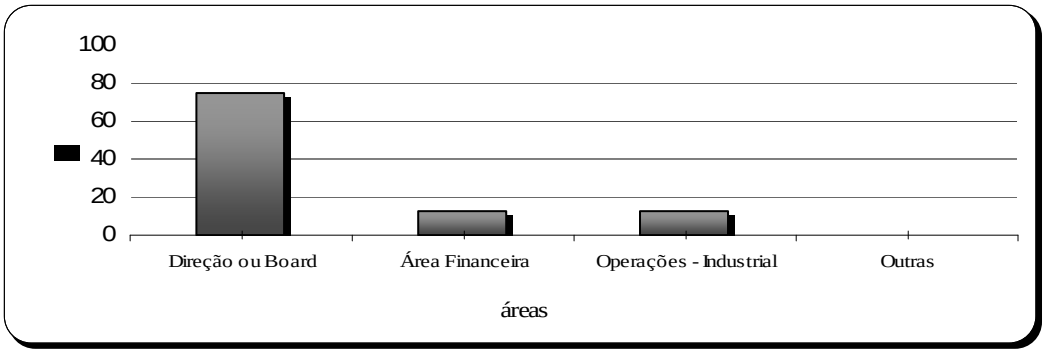
5.2.1 Questões da categoria "Governança de TI"

- ***Pergunta 2*** – Atualmente, sua empresa possui uma gestão de riscos em sua infraestrutura de TI implementada?



37,5% dos entrevistados disseram que já possuem um processo de gestão de riscos implementado com um período maior que 06 meses.

- ***Pergunta 4*** – A área de TI de sua empresa responde hierarquicamente a quem?

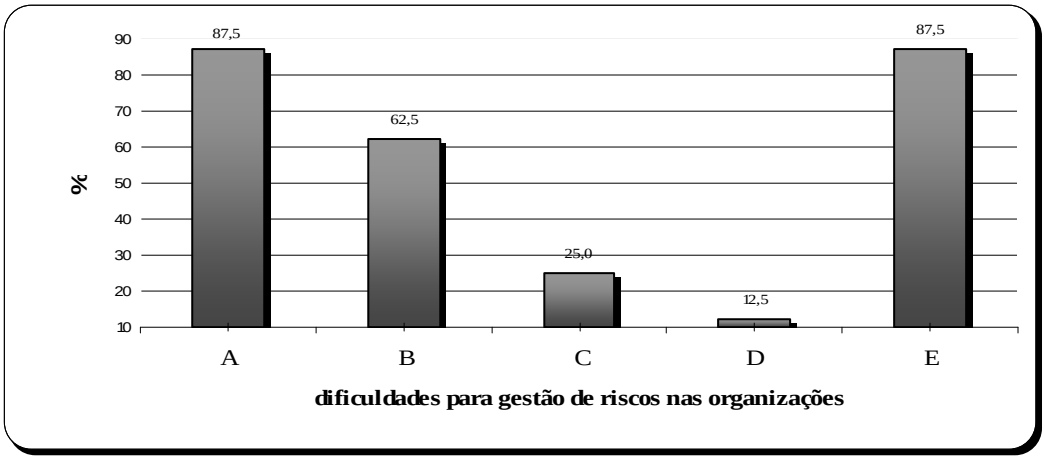


É possível perceber a importância da área de TI nas organizações, uma vez que a maioria dos entrevistados respondeu que esta área responde diretamente à Direção ou "Board".

5.2.2 Questões da categoria "Planejamento da gestão de riscos"

- ***Pergunta 8*** – A gestão de riscos é um processo complexo e trabalhoso que muitas vezes demanda o uso de ferramentas adequadas para identificar e tratar os riscos de forma sistemática e contínua (RAMOS et al, 2006, p. 43). Dos fatores a seguir, selecione 3 (três) que você considera como aqueles que dificultam o processo de gestão de riscos nas organizações?

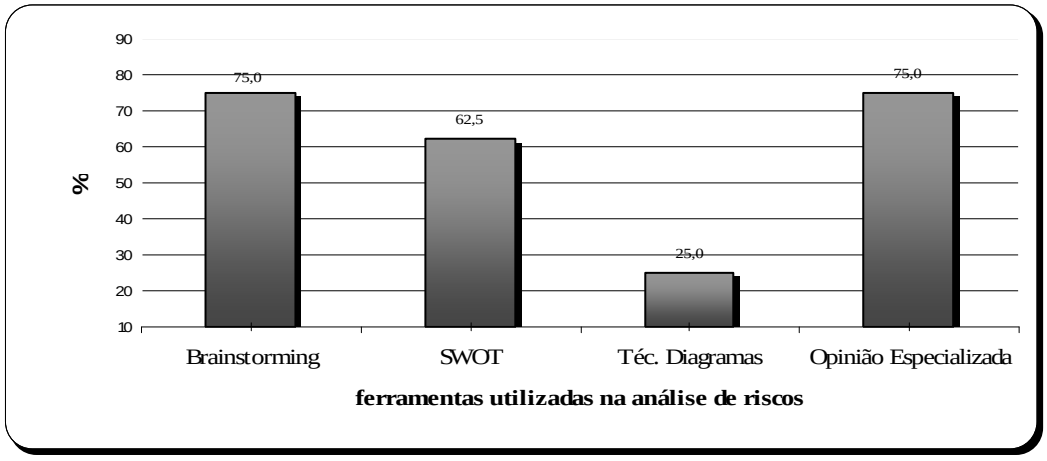
A. ( ) Falta de conhecimento sobre o assunto.
B. ( ) Falta de apoio da alta direção.
C. ( ) Custo de implementação
D. ( ) Infraestrutura deficiente.
E. ( ) Falta de padronização dos processos organizacionais.
F. ( ) Outro(s). Qual (is)?



Nota-se que, a falta de conhecimento sobre gestão de riscos; a falta de apoio da alta direção e a falta de padronização dos processos organizacionais são os principais fatores que dificultam o processo de gestão de riscos nas organizações.

5.2.3 Questões da categoria "Análise de riscos"

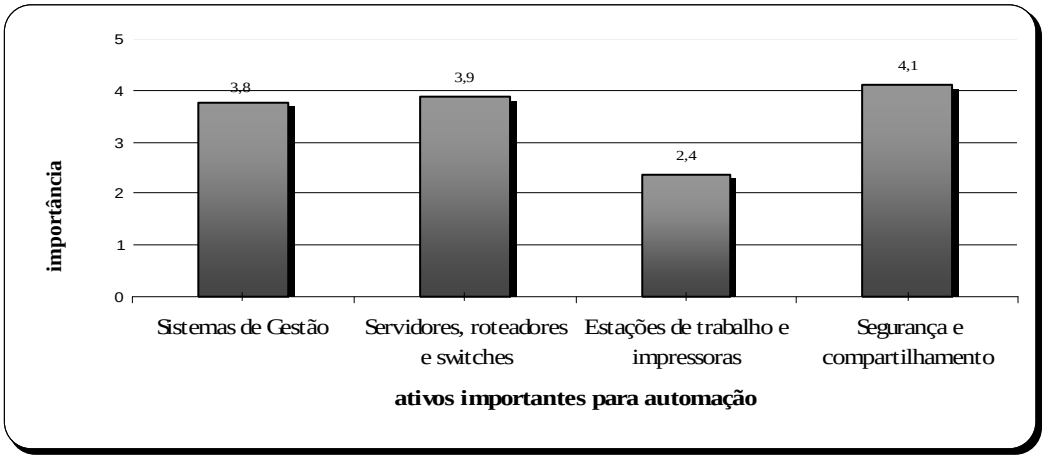
- ***Pergunta 12*** – A tolerância a riscos é o resultado do quanto às empresas estão dispostas em correr o risco, pois sabem que os benefícios decorrentes superam as possíveis perdas – ou o contrário (HELDMAN, 2009, p. 234). Qual (is) ferramenta(s) /técnica(s) listadas você utilizaria para identificar os riscos de um projeto?



Estas citações revelam 3 (três) ferramentas preferidas entre os profissionais pesquisados conforme pode ser visualizado no gráfico acima.

- ***Pergunta 14*** – A automação pode facilitar o gerenciamento dos riscos de TI de duas formas: 1) aliviando a complexidade associada à análise de relatórios de

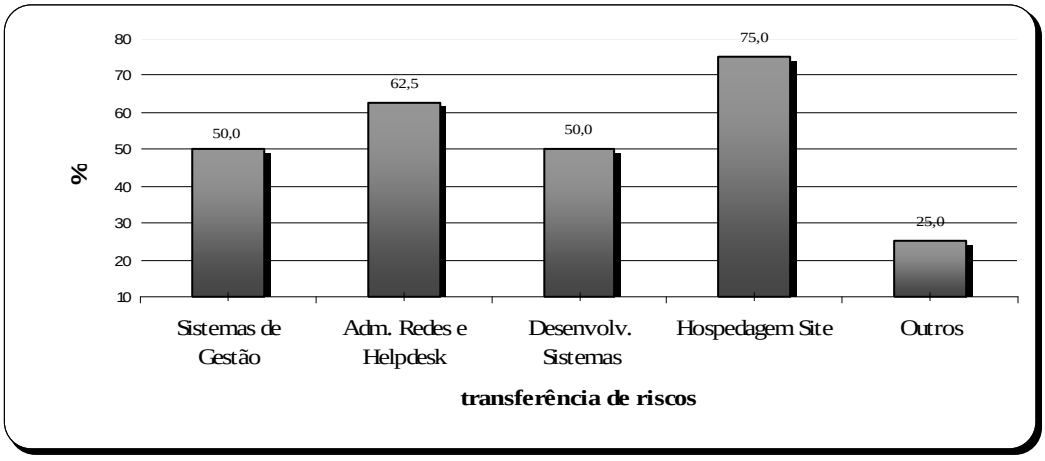
riscos cruciais e 2) facilitando a avaliação e a redução dos riscos reais para operações reais (IBM, 2008, p. 9). Considerando esta definição, pontue os ativos que você considera mais prioritários de automação, colocando 1 para menos importante e 5 para muito importante.



As ponderações dos entrevistados reforçam que a segurança da informação é mais prioritárias até mesmo que os servidores, roteadores e switches.

5.2.4 Questões da categoria "Plano de resposta aos riscos"

- ***Pergunta 17*** – No plano de resposta a riscos, uma das estratégias utilizadas para riscos negativos é a transferência do risco, que consiste em deslocar o risco e suas consequências para terceiros (HELDMAN, 2009, p. 264-265). A área de Tecnologia da Informação pode possuir diversos riscos associados à seus serviços. Para quais serviços de TI você recomendaria a transferência de riscos?



Nesta pergunta, percebe-se que a tranferência de riscos é recomendada para hospedagem de site e para administração de redes e helpdesk. Na opção "outros", merece destaque, pois 2 (dois) entrevistados apontaram a preocupação com a segurança da informação, o que reafirma a importancia da mesma para as organizações.

CONCLUSÃO

A gestão de riscos tornou-se um processo de significativa relevância nas organizações, uma vez que está diretamente ligada aos objetivos estratégicos e operacionais. Nota-se que as empresas estão percebendo que a Tecnologia da Informação tornou-se indispensável para atingirem seus resultados. Em um mundo cada vez mais globalizado, é de extrema importância saber quais são as suas reais ameaças e vulnerabilidades de modo que sejam tomadas medidas que atenuem o máximo possível impacto dessas ao seu negócio.

A gestão de riscos em infraestrutura de TI pode ser uma tarefa complexa, dado que muitas ameaças e vulnerabilidades nem sempre estão visíveis e/ou se fazem mensuráveis de forma clara. Adotando uma gestão de riscos pró-ativa, torna-se viável identificar e classificar os riscos, permitindo – assim – que o empresariado benefecie-se destas análises para investir, ou não, em determinado projeto, com a segurança e o conhecimento dos riscos e oportunidades relacionados ao mesmo.

Este trabalho de conclusão iniciou pelo estudo da bibliografia a respeito de gestão de riscos. Verificou-se no decorrer do estudo que a governança de TI, está diretamente relacionada à gestão de riscos de TI. Desta forma, foi necessário buscar o referencial teórico sobre o tema – mesmo que de forma não muito aprofundada – para que houvesse a correta interpretação de ambos assuntos. As fontes pesquisadas foram, além de livros, revistas e materiais disponíveis na internet.

A partir da bibliografia estudada, propôs-se um modelo de gestão de riscos orientado à Tecnologia da Informação. A principal contribuição do trabalho é o modelo elaborado, que oportuniza a gestão de riscos de TI através dos processo sugerido pelos autores pesquisados. O modelo contempla ainda a geração de planos de ações oriundos das técnicas de análise e avaliação de riscos, a fim de proporcionar um melhor monitoramento e controle sobre os eventos de riscos que serão armazenados e gerenciados pelo sistema.

O objetivo geral, que consistia na proposição de um modelo de gestão de riscos orientado à infraestrutra de TI, teve como resultado o modelo apresentado através do diagrama de classes (p. 40). Neste diagrama, está contemplado a estrutura do sistema (como

se relacionam as ferramentas de identificação, avaliação e tratamento dos riscos) e, por conseguinte, como os riscos serão monitorados e controlados de maneira que se possa obter um processo de melhoria contínua.

Atendendo há um dos objetivos específicos, o Benchmarking foi efetuado para permitir o uso das “melhores práticas”. Verificou-se que uma das soluções disponível no mercado é aquela descrita no capítulo 3 do presente trabalho. Qual seja: o software da Soft Expert. Contudo, esta alternativa requer investimento. Sendo assim, cabe a cada empresa fazer sua avaliação em relação ao custo-benefício do software analisado.

Quanto as empresas que são foco do estudo de caso deste trabalho (indústria calçadista; clínica médica; “software house”; governamental e indústria de alimentos) salienta-se que:

- O modelo transcrito em forma questionário estabeleceu coerência com as respostas fornecidas pelas empresas;
- Há percepção de que gerenciar riscos de TI é uma necessidade das corporações; e
- A informação é um dos “ativos” mais importantes das organizações e que precisam ser monitoradas e controladas.

Por sua vez, no que se refere a indústria química (elemento alvo da pesquisa-ação) faz-se as seguintes ponderações:

- A matriz situada na Holanda, não possui gerenciamento de riscos de TI. O mesmo é feito de forma manual e pontual nos projetos;
- A solução oferecida pela Soft Expert poderia ser utilizada como solução de gestão de riscos na companhia. Este software apresentou características similares ao modelo proposto que atenderia às necessidades da empresa.
- Percebe-se que não há uma política de gestão de riscos dentro do grupo. Apenas algumas unidades da empresa gerenciam seus riscos, mas de forma isolada.

Considerando que esta é uma empresa multinacional e que a TI cumpre um papel importantíssimo dentro da organização, conclui-se que a adoção de uma solução de gestão de riscos torna-se altamente recomendada. Neste sentido, propõe-se 2 (duas) opções: 1) elaborar o protótipo de todas as telas do modelo, a fim de validar visualmente o modelo sugerido; e 2)

criar um projeto para implementação da solução apresentada no capítulo do Benchmarking do presente estudo (Soft Expert) que contemple primeiramente as necessidades da unidade Brasil. Posteriormente que possa também ser adotada como solução de gestão de riscos por todas as outras unidades do grupo. A partir deste contexto, pode-se avaliar o custo-benefício de cada uma das alternativas e, então, submetê-las à matriz a fim de verificar qual das opções seria mais apropriada.

As limitações encontradas no estudo foram:

- A pesquisa foi efetuada em apenas 5 (cinco) empresas. O que não torna possível a generalização das conclusões das mesmas para outras empresas;
- Somente 1 (um) software foi analisado em “maior profundidade”.

Sugere-se para trabalhos futuros:

- Criar um modelo de gestão de riscos focada à infraestrura de TI. Este modelo buscaria evidenciar a importância dos ativos de TI em relação aos objetivos estratégicos da empresa, a fim de identificar quais ativos-chave demandam maior atenção da organização.
- Desenvolver o modelo sugerido e aplicá-lo na empresa estudada;
- Ampliar o número de empresas pesquisadas e, ao mesmo tempo, verificar se os perfis dos sujeitos da pesquisa (nível hierárquico; grau de instrução; experiência profissional etc.) interferem no resultado na pesquisa;
- Através de Benchmark, aprofundar o estudo de softwares disponíveis para realizar a gestão de riscos, associado ao nível de investimento necessário para sua implementação.

REFERÊNCIAS BIBLIOGRÁFICAS

BARDIN, Laurence. Análise de conteúdo. Lisboa: Edições 70, 2004.

BARALDI, Paulo. **Gerenciamento de riscos empresariais**. Rio de Janeiro: Campus, 2005. 268p.

BECHTOLD, Richard. Managing Risks With Metrics. **Baz.com**, 1997. Disponível em: http://www.baz.com/kjordan/swse625/htm/tp-pm.htm#References. Acesso em Outubro/2010.

BROWN, John Seely. A cultura do riscos. **HSM Management**, São Paulo: p. 60-64. Mar./abr./2005.

BOEHM, Barry. **Software Risk Management**: principle and Practices, IEEE Software. p. 32-41, 1991.

BUEHLER, Kevin; FREEMANN, Andrew; HULME, Ron. O novo arsenal da gestão de risco. **Harvard Business Review.** São Paulo, p. 51-58, Set/2008.

BOSCH, Grady; RUMBAUGH, James; JACOBSON, Ivar. **UML guia do usuário**: o mais avançado tutorial sobre Unified Modeling Language (UML), elaborado pelos próprios criadores da linguagem. Rio de Janeiro: Campus, 2000. 472p.

CARR, Nicolas G., **Será que TI é tudo?:** repensando o papel da tecnologia da informação. São Paulo: Gente, 2009. 188p.

CHIZZOTTI, A. **Pesquisa em ciências humanas e sociais**. Rio de Janeiro: Cortez, 1991.

CMMI. Gerenciamento de Riscos (RSKM). **Software-quality-assurance.org**, Disponível em: http://www.software-quality-assurance.org/cmmi-risk-management.html Acesso em 25/11/2010. 287-314p.;

COUGHLAN, P.; COGHLAN D. **Action research for operations management.** International Journal of Operations & Production Management, Vol. 22, No. 2, 2002, p. 220 – 240.

DAYCHOUW, Merhi. **40 ferramentas e técnicas de gerenciamento**. São Paulo: Brasport, 2007, 272p. Disponível em http://books.google.com.br/books?id=jQ_JOBtvgBAC&printsecz=frontcover&hl=pt-br&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false. Acesso em 10/12/2010.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz. **Impantando a governança de TI**: da estratégia à gestão dos processos e serviços. Rio de Janeiro: Brasport, 2008. Disponível em http://books.google.com.br/books?id=IvLVUdfv158C&pg=PA163&dq=melhores+praticas+de+TI&hl=pt-BR&ei=Dm3VTa7YIOfm0QGCt52aDA&sa=X&oi=book_result&ct=result&resnum=2&ved=0CDYQ6AEwAQ#v=onepage&q=infra-estrutura&f=false. Acesso em 18/05/2011.

FREITAS, Henrique Mello Rodrigues de; JANISSEK, Raquel. **Análise léxica e análise de conteúdo:** técnicas complementares, seqüências e recorrentes para exploração de dados qualitativos. Porto Alegre: Sagra Luzzatto, 2000.

FURLAN, José Davi. **Modelagem de objetos através da UML**: análise e desenho orientados a objeto. São Paulo: Makron Books, 1998. 329p.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2006.

HELDMAN, Kim. **Gerência de Projetos:** guia para o exame oficial do PMI. Rio de Janeiro: Elsevier, 2009. 632p.

HILLSON, David. Mitigando riscos com múltiplas hierarquias. **Mundo Project Management**, São Paulo, p. 9-14, Out./Nov./2008;

HOLANDA, Victor B.; RICCIO, Edson L. **A utilização da pesquisa ação para perceber e implementar sistemas de informações empresariais**. Disponível em: < http://www.ccsa.ufrn.br/depad/simulacaoempresarial/downloads/textos/Utiliza%E7%E3o%20de%20pesquisa-a%E7%E3o.pdf>. Acesso em: 16 maio 2011.

IBM. Guia do CIO para gerenciamento de riscos de TI: explorando o grande potencial de valor de negócios e crescimento financeiro. **IBM.com**, 2008. Disponível em: ftp://public.dhe.ibm.com/common/ssi/ecm/pt/ciw03045brpt/CIW03045BRPT.PDF Acesso em Outubro/2010.

MALHOTRA, Naresh. K. **Pesquisa de marketing:** uma orientação aplicada. 4. ed. Porto Alegre: Bookman, 2006.

MANSUR, Ricardo. **Governança de TI**: Metodologias, Frameworks e Melhores Práticas. Rio de Janeiro: Brasport, 2007. Disponível em http://books.google.com.br/books?id=MkAchF17jmkC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false. Acesso em 16/05/2011.

MARCONI, Marina de A.; LAKATOS, Eva M. **Técnicas de pesquisa**. São Paulo:Atlas, 1999.

POZZEBON, Marlei; FREITAS, Henrique M. R. de. **Pela aplicabilidade – com um maior rigor científico dos estudos de caso em sistemas de informação.** Disponível em <http://www.scielo.br/pdf/rac/v2n2/v2n2a09.pdf>. Acessado em 21 de junho de 2010. P. 143 – 170.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico**. Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. Novo Hamburgo: Feevale, 2009. 288p.

RAMOS, Anderson et al. **Security Officer 1**: guia oficial para formação de gestores em Segurança da Informação. Porto Alegre: Modulo Security Solution, 2006. 460p.

ROESCH, Sylvia M. A. **Projetos de estágio e de pesquisa em administração.** 3ª edição. São Paulo: Atlas, 2006.

SAUVÉ, Jacques P.; SPOHR, Elizabet M. Spohr de, **Avaliação do impacto de tecnologias da informação emergentes nas empresas**. Rio de Janeiro: QualityMark, 2003. 178p.

SCHMITZ, Alencar. **Análise de investimento em projetos de tecnologia da informação**. Rio de Janeiro: Expert Books, 2005. 330p.

SCHNEIER, Robert; MICCOLIS, Jerry. Gerenciamento holístico do risco. **HSM Management**, São Paulo, v.10, p. 125-130, Set./Out./1998;

SEI (Software Engeniering Institute). CMMI for development, version 1.2: Improving processes for better products. **SEI.** Disponível em http://cc.ee.ntu.edu.tw/~farn/courses/SE/CMMI_DEV_V12.pdf, August/2006. Acesso em Novembro/2010.

SLYWOTZKY, Adrian; DRZIK, John. Contra-atacando o maior de todos os riscos, **Harward Business Review**, São Paulo, p. 56-66, Abr./2005;

STONEBURNER, Gary; GOGUEN, Alice; FERINGA, Alexis in National Institute of Standards and Technology (NIST). Risk Management Guide for Information Technology Systems. **Special Publication 800-30**, United Statets, 2002. 55p.

WESTERMAN, George; HUNTER Richard. **O risco de TI**: convertendo ameaças aos negócios em vantagem competitiva. São Paulo: M. Books, 2008. 210p.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em Administração**. 6. ed. São Paulo: Atlas, 2005.

VERGUEIRO, Waldomiro. **Qualidade em serviços de informação**. São Paulo: Arte & Ciência, 2002. 124p. Disponível em http://books.google.com.br/books?id=pOhOtn8HOiUC&printsec=frontcover&hl=pt-br&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false. Acesso em 06/12/2010.

ZAIRI, Mohamed; LEONARD, Paul. **Benchmarking prático**. O guia completo. São Paulo: Atlas, 1995. 326p.

APÊNDICE A – REQUISITOS FUNCIONAIS E NÃO FUNCIONAIS

F1 Cadastro de idiomas			Oculto ( )
Descrição: Este requisito tem o objetivo de fornecer opções de diferentes idiomas que estará relacionado ao País e ao usuário.			
Requisitos Não Funcionais			
Nome	**Restrição**	**Categoria**	**Formato**
NF 1.1 – Cadastro de Idiomas	O sistema deve possibilitar a inclusão, alteração e exclusão de diferentes idiomas para ser utilizado nos Países estrangeiros.	Segurança	Permanente
NF 1.2 – Busca arquivo de tradução	O administrador do sistema deverá indicar o nome do arquivo com o dicionário de palavras de tradução.	Confiabilidade	Permanente

F2 Cadastro de unidade de negócio			Oculto ( )
Descrição: Este requisito visa disponibilizar ao administrador do sistema a inclusão e alteração de Unidades de negócio. A unidade de negócio possui um usuário responsável pela gestão de riscos.			
Requisitos Não Funcionais			
Nome	**Restrição**	**Categoria**	**Formato**
NF 2.1 - Cadastro de unidade de negócio	A unidade de negócio deve estar identificada para que os demais processos sejam relacionadas a mesma.	Confiabilidade	Permanente
NF 2.2 – Idioma unidade de negócio	Obrigatoriamente deverá ser informado o idioma utilizado na unidade de negócio a fim de permitir a validação das pessoas que irão se relacionar com a mesma.	Confiabilidade	Permanente

F3 Cadastro de usuários			Oculto ( )
Descrição: Este requisito visa disponibilizar ao gestor de riscos a inclusão e alteração de usuários.			
Requisitos Não Funcionais			
Nome	**Restrição**	**Categoria**	**Formato**
NF 3.1 – Identificação do usuário	O usuário deverá ser identificado para poder acessar o sistema.	Segurança	Permanente
NF 3.2 – Valida usuário e email	O sistema deve validar se o usuário/email já existe no sistema antes de incluí-lo no banco de dados	Confiabilidade	Permanente
NF 3.3 - Seleção de idioma do usuário	O administrador deverá incluir os idiomas que o usuário domina.	Confiabilidade	Permanente
NF 3.4 – Valida idioma do usuário	O sistema deve validar se o usuário possui habilitação no idioma que foi informado na unidade de negócio.	Confiabilidade	Permanente

F4 Cadastro de times de trabalho			Oculto ( )
Descrição: Este requisito visa disponibilizar ao administrador do sistema a inclusão e alteração de times de trabalho que irão identificar avaliar, tratar, comunicar e controlar os riscos. Também deverá ser ajustados os parâmetros de email para que os usuários participantes deste time sejam informados ou não, dos eventos que serão criados, alterados e/ou controlados no processo de gestão de riscos.			
Requisitos Não Funcionais			
Nome	**Restrição**	**Categoria**	**Formato**

NF 4.1 – Manutenção de times	O sistema deverá permitir a inclusão, alteração e exclusão de times de trabalho.	Confiabilidade	Permanente
NF 4.2 – Envio de e-mails	O sistema deve permitir a parametrização de emails. O endereço de email será consultado o que estiver no cadastro de usuários.	Confiabilidae	Permanente
NF 4.2.1 – Email ao registrar ocorrência	Quando assinalado, o sistema deverá enviar um email informando ao usuário (s) relacionado na inclusão de novos eventos de riscos.	Confiabilidade	Permanente
NF 4.2.2 – Email ao finalizar ocorrência	Quando assinalado, o sistema deverá enviar email ao (s) envolvido (s) do evento de risco no momento em que o evento for encerrado.	Confiabilidade	Permanente
NF 4.2.3 – Email ao vencer o prazo de uma atividade no sistema.	Quando assinalado, o sistema deverá enviar email ao (s) envolvido (s) da atividade que estiver com seu prazo vencido.	Confiabilidade	Permanente
NF 4.2.4 – Email mensal com as estatísticas do sistema.	Quando assinalado, o sistema deverá enviar as estatíticas referente à performance do sistema e dos usuários participantes do respectivo time.	Confiabilidade	Premanente
NF 4.3 – Relacionamento de usuários ao time de trabalho	O sistema deverá permitir o relacionamento dos usuários ao time de trabalho.	Segurança	Permanente
NF 4.3.1 – Inclusão de usuário	Um ou mais usuários poderão ser incluídos no time de trabalho. O Sistema verificará se o usuario que está sendo incluído já não está no corrente time de trabalho.	Segurança	Permanente
NF 4.3.2 – Usuário líder	Deverá obrigatóriamente ter um usuário líder para cada time de trabalho. Ao incluir o primeiro usuário o sistema sempre irá marcar este como líder, mas deve permitir a alteração do mesmo.	Segurança	Permanente
NF 4.3.3 – Exclusão de usuário	Deverá permitir a exclusão de usuários do time de trabalho. Caso o usuário que está sendo excluído seja o usuário líder, o sistema deverá ignorar a operação e emitir uma mensagem de alerta para que seja trocado de líder ou incluído outro usuário líder antes da inclusão.	Segurança	Permanente

F5 Riscos preliminares			Oculto ( )
Descrição: Este requisito visa disponibilizar a inclusão de riscos preliminares que serão relacionados aos processos que poderão estar relacionados aos riscos evidenciados posteriormente			
Requisitos Não Funcionais			
Nome	**Restrição**	**Categoria**	**Formato**
NF 5.1 – Manutenção de riscos preliminares	O sistema deverá permitir a inclusão, alteração e exclusão de riscos preliminares informando qual é o nível do risco e qual o possível nível de impacto.	Confiabilidade	Permanente

F6 Cadastro de processos			Oculto ( )
Descrição: Este requisito visa disponibilizar aos times de trabalho a inclusão de processos e sub-processos em que estão expostos aos riscos.			
Requisitos Não Funcionais			
Nome	**Restrição**	**Categoria**	**Formato**

NF 6.1 – Cadastro de processos	O sistema deverá permitir a inclusão, alteração e exclusão de processos que estão expostos direta ou indiretamente aos riscos. Deverá ser informada a descrição, revisão, data de validade da revisão e o tipo de processo.	Confiabilidade	Permanente
NF 6.2 – Cadastro de sub-processos	O sistema deverá permitir a inclusão, alteração e exclusão de subprocessos oriundos do processo cadastrado.	Confiabilidade	Permanente
NF 6.3 – Riscos preliminares	O sistema deve permitir o relacionamento de riscos preliminares aos processos previamente cadastrados.	Confiabilidade	Permanente

F7 Eventos de riscos			Oculto ( )
Descrição: Este requisito visa disponibilizar aos times de trabalho a inclusão de eventos de riscos, os processos relacionados e classificação dos riscos a fim de priorizá-lo posteriormente.			
Requisitos Não Funcionais			
Nome	**Restrição**	**Categoria**	**Formato**
NF 7.1 – Manutenção de eventos de riscos	O sistema deverá permitir a inclusão, alteração e exclusão de eventos de riscos que poderão ser analisados e/ou tratados de acordo com sua classificação, nível, característica e frequencia. Neste evento, será relacionado qual será o time que irá conduzir o processo de gestão de riscos.	Confiabilidade	Permanente
NF 7.2 – Riscos dos processos	O sistema deverá permitir a inclusão, alteração e exclusão de riscos oriundos dos processos previamente cadastrados, contemplando o nível de risco, se o risco deverá ser monitorado/controlado, sua prioridade, característica e frequencia. Estas informações serão utilizadas para análise de riscos.	Confiabilidade	Permanente
NF 7.3 – Análise de riscos	O sistema deverá permitir o uso de das seguintes ferramentas de análises de riscos: geração de probabilidade e impacto; Brainstorming; SWOT; Ishikawa e 5W2H.	Confiabilidade	Permanente
NF 7.3.1 – Matriz de probabilidade e impacto	A partir dos dados informados no NF 6.2, o sistema deverá gerar a matriz de probabilidade e impacto. Para calcular a probabilidade e impacto, deve ser utilizado o cálculo conforme descrito na figura 1.7, seção 1.2.4.1. Os dados para efetuar o cálculo da matriz de probabilidade e impacto devem buscar das classes Threats, Vulnerabilities, Riskprocess.	Confiabilidade	Permanente
NF 7.3.2 – Método de análise Brainstorming	O sistema deverá permitir a inclusão, alteração e exclusão de registros “idéias ou possíveis causas” deste método, juntamente com o nome do usuário e data. Deverá conter um campo para que seja marcada qual a hipótese mais provável apurada. Deverá ainda armazenar o usuário que executou a análise.	Confiabilidade	Permanente
NF 7.3.3 – Método de análise SWOT	O sistema deverá permitir a inclusão, alteração e exclusão da análise SWOT, que deverá prever os campos: forças; fraquezas; oportunidades, ameaças e a causa-e-efeito identificada. Deverá ainda armazenar o usuário que executou a análise.	Confiabilidade	Permanente
NF 7.3.4 – Método de análise Ishikawa	O sistema deverá permitir a inclusão, alteração e exclusão de análise Ishikawa. Os atributos serão utilizados conforme a categoria ou tipo de análise escolhida: 5P ou 5M, conforme descrito	Confiabilidade	Permanente

	na seção 1.2.5.3. A tabela pode unificar os dois métodos.		
N.F. 7.3.5 – Método de análise 5W2H ou 5 Porquês	O sistema deverá permitir a inclusão, alteração e exclusão de análise 5W2H. Os atributos são: Why, Who, Where, When, What, How Much e How Many (Por que, Quem, Onde, Quando, O que, Quanto custa e Quantas vezes). Além disso, deverá armazenar o nome do usuário, data de vencimento do plano de ação e um campo para colocar a implementação da ação.	Confiabilidade	Permanente
N.F 7.3.5.1 – Monitoramento de ações vencidas	O sistema deverá monitorar os planos de ações e emitir email de alertas caso alguma ação esteja vencidada para cada usuário.	Confiabilidade	Permanente
N.F 7.3.5.2 – Implementação do plano de ação	O sistema deverá permitir a adição de informações referente a implementação dos planos de ações.	Confiabilidade	Permanente

F8 Tratamento de riscos			Oculto ( )
Descrição: Este requisito visa disponibilizar ao time de trabalho o registro do tratamento do risco analisado, podendo ser utilizado as estratégias para evitar/eliminar, transferir, aceitar/reter, mitigar. Para qualquer das estratégias, todos os envolvidos no evento de riscos deverão receber email com o tratamento aplicado.			
Requisitos Não Funcionais			
Nome	**Restrição**	**Categoria**	**Formato**
NF 8.1 – Registro do tratamento do risco	O sistema deverá permitir a inclusão e alteração do registro referente ao tratamento adotado do risco analisado.	Confiabilidade	Permanente
NF 8.2 – Aprovação do tratamento	O sistema deverá permitir a inclusão do nome do responsável, data do tratamento e descrição da aprovação da estratégia utilizada no tratamento do risco.	Confiabilidade	Permanente
NF 8.3 – Email aos envolvidos com o evento de risco	O sistema deverá enviar email a todos os envolvidos com o risco para comunicar que após analisado o risco recebeu um tratamento com uma determinada estratégia. Além disso, deve ser comunicado o nome do reponsável e a descrição pela aprovação da estratégia utilizada.	Confiabilidade	Permanente

APÊNDICE B – CASOS DE USO ESSENCIAIS

1 – Registrar eventos de risco (*Register risk events*)

Atores:

Time de trabalho

Pré-condição:

Os usuários e time de trabalho precisam estar cadastrados e parametrizados previamente.

Objetivo:

Registrar os eventos de riscos que será o marco inicial do processo de gestão do risco em questão.

Fluxo de eventos:

16. O ator entra no sistema de gestão de riscos;
17. O sistema solicita usuário e senha do usuário que deve estar cadastrado;
18. O ator informa o nome de usuário e senha e clica em OK para validar os dados;
19. O sistema vefirica se o usuário de senha informado é válido;
20. O sistema exibe o menu principal do sistema;
21. O ator entra no menu Risk Management – IT Risk Module;
22. O ator entra no menu Tasks, Risk events;
23. O sistema deve exibir a tela com os eventos de riscos previamente cadastrados;
24. O ator pode pesquisar eventos de riscos anteriores através do botão pesquisa (lupa);
    24.1. O ator ajusta o filtro de acordo com o que deseja pesquisar;
    24.2. O sistema executa a consulta no banco de dados e exibe o resultado;
    24.3. O ator escolhe o evento de risco que deseja visualizar e clica bo botão OK;
25. O sistema fecha a tela de pesquisa e exibe os dados completos do evento de risco;
26. O ator visualiza o risco consultado;
27. O ator poderá incluir novo evento de risco através do botão New;
28. O sistema limpa os dados dos campos para permitir a inclusão das informações do novo evento de risco;
29. O ator preenche os dados do novo evento de risco e salva os dados através do botão Save;
30. O sistema infere a situação do novo evento de risco como aberto (open);

Fluxo alternativo 1:

1. No item 12, o ator poderá copiar o risco pesquisado para uma nova ocorrência através do botão copiar;
2. O sistema efetua a cópia do evento selecionado para um novo evento de risco e habilita a edição dos dados;
3. O ator poderá alterar os dodos do evento de risco e salvar o registro através do botão Save;
4. O sistema infere a situação do novo evento de risco como aberto (open);

Fluxo alernativo 2:

1. No item 12, o ator poderá modificar o risco pesquisado caso o registro tenha sua situação como aberto (open);
2. O ator poderá alterar os dodos do evento de risco e salvar o registro através do botão Save;
3. O sistema infere a situação do novo evento de risco como aberto (open);

Fluxo alernativo 3:

1. No item 9, o ator poderá ir direto ao evento de risco desejado caso já saiba o código do evento através do botão Ir Para;
2. O ator clica no botão Ir Para;
3. O sistema exibe uma tela para digitação do código do evento de risco;
4. O ator digita o código do evento e clica no botão OK;
5. O sistema exibe os dados completos do evento de risco;

Fluxo alternativo 4:

1. No item 9, o ator poderá navegar nos eventos de riscos já cadastrados através dos botões de navegação que está na parte superior da tela;
2. O sistema exibe os eventos de risco corrente.

Pontos de extensão:

Não se aplica

Casos de uso incluídos:

Register user.

2 – Executar a análise de riscos (*Perform risk assessment*)
Atores: Time de trabalho
Pré-condição: Caso de uso Registrar eventos de risco deve ter sido executado.
Objetivo: Disponibilisar ferramentas de análise de riscos a fim de identificar e avaliar os riscos envolvidos.
Fluxo de eventos: 1. O ator entra no sistema de gestão de riscos; 2. O sistema solicita usuário e senha do usuário que deve estar cadastrado; 3. O ator informa o nome de usuário e senha e clica em OK para validar os dados; 4. O sistema vefirica se o usuário de senha informado é válido; 5. O sistema exibe o menu principal do sistema; 6. O ator entra no menu Risk Management – IT Risk Module; **7.** O ator entra no menu Taks, Risk Assessment; **8.** O sistema irá mostrar uma tela com todos os eventos de riscos pendentes de análise; **9.** O ator escolhe o risco que deseja analisar; **10.** O ator escolhe a(s) ferramenta(s) que deseja utilizar em sua análise e clica no botão correspondente**;** **11.** O ator poderá fazer uma conclusão do evento de risco apartir das análises efetuadas através do botão Conclusion.
Fluxo alternativo 1: Não se aplica
Pontos de extensão: Não se aplica
Casos de uso incluídos: 1. Gerar matriz de probabilidade e impacto (Generate probability x impacts table) 2. Executar Brainstorming (Perform Brainstorming) 3. Executar SWOT (Perform SWOT) 4. Executar Ishikawa (Perform Ishikawa) 5. Executar 5W2H (Perform 5W2H)

3 – Registrar processos expostos aos riscos (*Register process exposed to risks*)
Atores: Time de trabalho
Pré-condição: Os cadastros de processos, ativos, ameaças precisam estar previamente completados e o caso de uso Registrar eventos de riscos terem sido efetuados com sucesso.
Objetivo: Identificar e avaliar os processos que estão expostos a quais riscos.
Fluxo de eventos: 1. O ator entra no sistema de gestão de riscos; 2. O sistema solicita usuário e senha do usuário que deve estar cadastrado; 3. O ator informa o nome de usuário e senha e clica em OK para validar os dados; 4. O sistema vefirica se o usuário de senha informado é válido; 5. O sistema exibe o menu principal do sistema; 6. O ator entra no menu Risk Management – IT Risk Module; 7. O ator entra no menu Tasks, Risk Process; 8. O sistema exibirá a tela com os riscos em situação aberto (open); 9. O ator poderá pesquisar os eventos de riscos ao clicar em pesquisa (lupa); 9.1. O ator ajusta o filtro de acordo com o que deseja pesquisar; 9.2. O sistema executa a consulta no banco de dados e exibe o resultado; 9.3. O ator escolhe o evento de risco que deseja visualizar e clica bo botão OK; 10. O sistema exibe os dados do evento de risco na parte superior da tela e os processos que já tenham sido relacionados anteriormente; 11. O ator seleciona o processo que deseja vincular ao evento de risco; 12. O ator poderá adicionar o processo escolhido ao evento de risco através do botão Add Process (+); 13. O sistema adiciona o processo escolhido à lista de processos selecionados; 14. O ator poderá preencher os dados qualitativos e quantitativos referente ao processo vinculado aos riscos;

15. O ator salva os dados informados através do botão Save;
Fluxo alternativo 1: No item 11, o ator pode clicar no botão Show Assets para exibir os ativos relacionados àquele processo selecionado; **Fluxo alernativo 2:** No item 11, o ator pode clicar no botão Show Threats para exibir as ameaças relacionadas àquele processo selecionado;
Pontos de extensão: Não se aplica
Casos de uso incluídos: 1. Register Process; 2. Register Risk Events; 3. Register Assets; 4. Register Threats;

4 – Executar 5W2H (Perform 5W2H)
Atores: Time de trabalho
Pré-condição: Caso de uso Executar análise de riscos (Perform Risk Assessment)
Objetivo: Identificar as possíveis causas e consequencias dos eventos de risco a fim de fornecer informações para o devido tratamento do risco possibilitando a geração de planos de ações corretivos.
Fluxo de eventos: 1. O ator entra no sistema de gestão de riscos; 2. O sistema solicita usuário e senha do usuário que deve estar cadastrado; 3. O ator informa o nome de usuário e senha e clica em OK para validar os dados; 4. O sistema vefirica se o usuário de senha informado é válido; 5. O sistema exibe o menu principal do sistema; 6. O ator entra no menu Risk Management – IT Risk Module; 7. O ator entra no menu Taks, Risk Assessment; 8. O sistema irá mostrar uma tela com todos os eventos de riscos pendentes de análise; 9. O ator escolhe o risco que deseja analisar; 10. O ator clica no botão do método 5W2H; 11. O sistema exibe na parte superior da tela o risco que está sendo analisado; 12. O ator poderá registar a análise através do botão New; 13. O sistema habilita os campos para inserção dos dados; 14. O ator preenche os dados dos campos do método 5W2H; 15. O ator salva os dados preenchidos através do botão Save; 16. O sistema habilita o botão Action Plan para registra os planos de ações decorrentes da análise efetuada.
Fluxo alternativo 1: No item 12, o ator pode clicar no botão Modify para para habilitar os campos para edição dos dados. Obs: Somente permitir habilitar os campos se o evento de risco estiver em situação aberto (open); **Fluxo alernativo 2:** No item 12, o ator pode excluir a análise anterior através do botão Delete. Obs: somente permitir excluir registro caso o evento de risco esteja com situação aberto (Open) e não possua nenhum plano de ação relacionado à esta análise.
Pontos de extensão: Não se aplica
Casos de uso incluídos: Maintain Action Plan.

APÊNDICE C – QUESTIONÁRIO – PORTUGUÊS

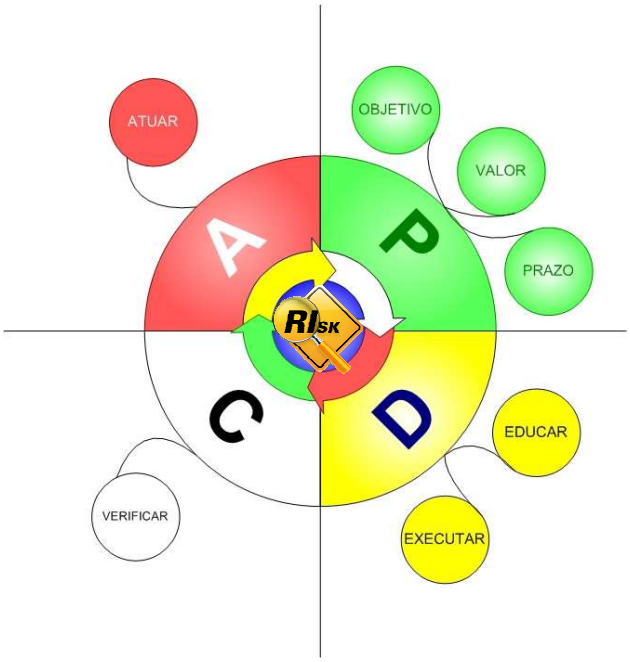
QUESTIONÁRIO DE VERIFICAÇÃO – TRABALHO DE CONCLUSÃO

CLEIBER ANDRÉ MUNIZ DA CUNHA

Universidade Feevale
Instituto de Ciências Exatas e Tecnologia
Curso de Sistemas de Informação
Trabalho de Conclusão de Curso

Professor orientador: Ms Roberto Scheid

Novo Hamburgo, Maio de 2011.



A adoção de tecnologia está em ritmo surpreendentemente rápido, tornando o ambiente de TI presente não apenas por toda parte, mas também difusa e complexamente interconectada dentro e fora das empresas. Conforme a dependência e a interdependência da TI pelas empresas foram aumentando, as consequências do risco de TI aumentaram igualmente (WESTERMAN; HUNTER, 2008, p. 40).

Este questionário visa identificar a necessidade de implementação de um processo estruturado de gestão de riscos. Vale dizer também que o mesmo faz parte de uma pesquisa-ação com objetivo de trazer melhoria para o processo de gestão de riscos da Tecnologia da Informação, processo esse que é crucial para a organização. Para melhor entendimento, lista-se os principais conceitos sobre gestão de riscos:

- ***Risco*** – deve ser considerado como a probabilidade de uma ameaça explorar uma – ou várias – vulnerabilidades causando prejuízos. Em termos gerais, risco pode estar associado a algo negativo ou positivo (RAMOS et al, 2006, p. 48-49);

- ***Gestão de riscos*** – é um conjunto de atividades que tem por objetivo, de uma forma economicamente racional, maximizar o efeito dos fatores de riscos positivos e minimizar o efeito dos negativos (SCHMITZ, 2005, p. 63);
- ***Processo de planejamento de riscos*** – O PMBOK Guide afirma que o processo de planejar o gerenciamento de riscos é base para todos os processos de riscos. O plano assegura que a quantidade apropriada de recursos e o tempo apropriado são dedicados ao mesmo (HELDMAN, 2009);
- ***Plano de respostas aos riscos*** – especifica as medidas a serem tomadas para reduzir ameaças e tirar proveito das oportunidades encontradas nos processos de análise de riscos;

  > Quanto mais eficazes os planos de resposta aos riscos, maiores as chances de êxito no projeto (HELDMAN, 2009, p. 266).
- ***Monitoramento e controle*** – são mecanismos para monitorar a eficácia dos componentes da gestão de riscos (RAMOS et al, 2006, p. 67). A partir deste monitoramento, é possivel gerar a base de dados que servirá para realimentar o processo de melhoria contínua de todo o processo;
- ***Ameaça*** – tudo aquilo que tem potencial de causar algum dano a um ativo e, consequentemente, a uma organização (RAMOS et al, 2006, p. 45);
- ***Vulnerabilidade*** – são as circunstâncias que levam um ou mais ativos a ficarem expostos a uma ou mais ameaças.

Muito obrigado pela colaboração!

CATEGORIA 1 - GOVERNANÇA DE TI

1) Considerando que Tecnologia da Informação é o processo de transformação dos conceitos, conhecimentos e equipamentos das áreas de informática e telecomunicações, em aplicações úteis a todas as outras áreas em todo e qualquer contexto, onde ela (a TI) possa ser efetivamente aplicada (SPOHR; SAUVÉ, 2003, p. 240), é necessário que as empresas estejam atentas a importância de sua infraestrutura de TI. De acordo com esta situação, cite 3 (três) fatores que você considera importante na ***gestão da Tecnologia da Informação***.
2) Atualmente, sua empresa possui uma ***gestão de riscos em sua infraestrutura de TI*** implementada?
   ( ) Não.
   ( ) Sim. Há quanto tempo?
      i. ( ) De 0 a 6 meses;
      ii. ( ) Entre 7 meses a 18 meses;
      iii. ( ) Entre 19 meses a 24 meses;
      iv. ( ) Em mais de 24 meses;

3) Em que área ou departamento sua empresa possui ou pretende implementar ***a gestão de riscos.*** Observação: é possível marcar mais de uma opção.
   a. ( ) Tecnologia da Informação.
   b. ( ) Financeiro.
   c. ( ) Atendimento a clientes.
   d. ( ) Departamento de compras.
   e. ( ) Nenhuma.
   f. ( ) Outra(s). Qual(is)?

4) ***A área de TI*** de sua empresa responde hierarquicamente a quem?
   a. ( ) Direção ou "*Board*".
   b. ( ) Área financeira.
   c. ( ) Operações - Industrial.
   d. ( ) Outra. Qual?

CATEGORIA 2 – PLANEJAMENTO DA GESTÃO DE RISCOS

5) De acordo com Spohr; Sauvé (2003, p. 6) é necessário que as empresas conheçam melhor os recursos, as promessas e a realidade das novas tecnologias, avaliando até que ponto elas devem modificar sua forma de trabalho para adotar alguma destas tecnologias. Diante desta afirmação, você acredita que a ***gestão de riscos*** poderia contribuir em qual situação abaixo. Observação: é possível marcar mais de uma opção.
    a. ( ) A gestão de riscos pode contribuir para que as empresas conheçam suas limitações, ou seja, os riscos envolvidos na adoção de novas tecnologias.
    b. ( ) A gestão de riscos quando usada de forma adequada, permitirá que a organização tenha uma visão completa do processo, o que pode transformar a incerteza em uma oportunidade.
    c. ( ) A gestão de riscos não ajudaria neste processo.
    d. ( ) Outra(s). Qual (is)?

6) Segundo Heldman (2009, p. 233), o ***plano de gerenciamento de riscos*** assegura que a quantidade apropriada de recursos e o tempo apropriado são dedicados ao gerenciamento de riscos. Diante desta afirmação, qual sua opinião sobre o ***processo de gestão de riscos***? Observação: marcar apenas uma das opções abaixo.
    a. ( ) Deve ser utilizado somente em empresas financeiras.
    b. ( ) Aumenta a assertividade nos projetos diminuindo a(s) incerteza(s).
    c. ( ) Gera custos adicionais para as empresas.
    d. ( ) É irrelevante sua utilização.
    e. ( ) Outra. Qual?

7) Para Westerman; Hunter (2008, p. 182), a ***governança de riscos de TI*** deveria estar embutida nos mais importantes processos decisórios da organização, onde a empresa evita deixar-se "cegar" e consegue assumir mais riscos, e, portanto, mais oportunidades, com maior confiança. Você concorda com esta afirmação? Por quê?

8) ***A gestão de riscos*** é um processo complexo e trabalhoso que muitas vezes demanda o uso de ferramentas adequadas para identificar e tratar os riscos de forma sistemática e contínua (RAMOS et al, 2006, p. 43). Dos fatores a seguir, selecione 3 (três) que você considera como aqueles que dificultam o ***processo de gestão de riscos*** nas organizações.
    a. ( ) Falta de conhecimento sobre o assunto.
    b. ( ) Falta de apoio da alta direção.
    c. ( ) Custo de implementação
    d. ( ) Infraestrutura deficiente.
    e. ( ) Falta de padronização dos processos organizacionais.
    f. ( ) Outro(s). Qual (is)?

9) Qual sua opinião sobre gestão de riscos de ***infraestrutura de TI***?

10) Quais os principais ***ativos*** que são monitorados ou que sugere que fossem monitorados pela ***gestão de riscos***?

CATEGORIA 3 – ANÁLISE DE RISCOS

11) Durante o processo de ***análise e avaliação de risco*** é que serão feitos todos os levantamentos em relação às ameaças, vulnerabilidades, probabilidades e impacto aos quais os ativos estão sujeitos (RAMOS et al, 2006, p. 50). Você considera importante que a empresa conheça os riscos associados a seus ativos?
    ( ) Sim. De que forma?
    ( ) Não. Por quê?

12) A ***tolerância a riscos*** é o resultado do quanto às empresas estão dispostas em correr o risco, pois sabem que os benefícios decorrentes superam as possíveis perdas – ou o contrário (HELDMAN, 2009, p. 234). Qual (is) ferramenta(s)/técnica(s) listadas você utilizaria para ***identificar os riscos*** de um projeto: Observação: é possível marcar mais de uma opção.
    a. ( ) Brainstorming.
    b. ( ) Análise SWOT.
    c. ( ) Técnicas de diagramas.
    d. ( ) Opinião especializada.
    e. ( ) Outra(s). Qual (is)?

13) ***Análise qualitativa de riscos*** visa à detecção do impacto dos riscos e sua probabilidade de ocorrência. A ***análise quantitativa*** avalia os impactos e quantifica a exposição aos riscos por meio da atribuição de probabilidades numéricas (HELDMAN, 2009, p. 249). Qual ou quais das técnicas acima você utilizaria no processo de avaliação de riscos? Justifique.

14) A ***automação*** pode facilitar o gerenciamento dos riscos de TI de duas formas: 1) aliviando a complexidade associada à análise de relatórios de riscos cruciais e 2) facilitando a avaliação e a redução dos riscos reais para operações reais (IBM, 2008, p. 9). Considerando esta definição, pontue os ativos que você considera mais prioritários de automação, colocando 1 para menos importante e 5 para muito importante:
    a. ( ) Sistemas de gestão.
    b. ( ) Servidores, roteadores e "*switches*".
    c. ( ) Estações de trabalho e impressoras.
    d. ( ) Segurança e compartilhamento de dados.
    e. ( ) Outros. Identifique e pontue.

15) ***Pessoas*** são movidas pelo conhecimento, pela falta dele e também pela emoção e pelo sentimento (RAMOS et al, 2006). Sob esta ótica, você considera que pessoas podem representar riscos para a TI?
    ( ) Não.
    ( ) Sim. Cite 2 (dois) exemplos de riscos de TI relacionado à pessoas.

16) ***"Informação"*** pode ser entendida como todo patrimônio que se refere à cultura da empresa ou ao seu negócio, podendo tais informações ser de caráter comercial, técnico, financeiro, legal, de recursos humanos, ou de qualquer outra natureza, que tenham valor para a organização e que se encontrem armazenadas em recursos computacionais da empresa, com tráfego dentro da sua infraestrutura tecnológica (RAMOS et al, 2006, p. 291). As perdas destas informações podem representar prejuízos significativos para a organização. Como você classificaria este risco: Observação: é possível marcar apenas uma das opções abaixo.
    a. ( ) Risco técnico, de qualidade ou desempenho.
    b. ( ) Risco de gerenciamento da informação.
    c. ( ) Risco organizacional.
    d. ( ) Risco externo.

CATEGORIA 4 – PLANO DE RESPOSTA AOS RISCOS

17) No plano de resposta a riscos, uma das estratégias utilizadas para riscos negativos é a ***transferência do risco***, que consiste em deslocar o risco e suas consequências para terceiros (HELDMAN, 2009, p. 264-265). A área de Tecnologia da Informação pode possuir diversos riscos associados à seus serviços. Para quais serviços de TI você recomendaria a ***transferência de riscos***? Observação: é possível marcar mais de uma opção.
    a. ( ) Sistema de gestão.
    b. ( ) Administração de redes e "*helpdesk*".
    c. ( ) Desenvolvimento de sistemas.
    d. ( ) Hospedagem do site.
    e. ( ) Nenhuma. Por quê?
    f. ( ) Outra(s).Qual (is)?

18) A ***mitigação de risco*** é outra estratégia utilizada pra riscos negativos que tem por finalidade diminuir a probabilidade de ocorrência e o impacto do risco até um nível aceitável (HELDMAN apud PMBOK, 2009, p. 266). Alguns exemplos de mitigação de riscos incluem utilização de processos menos complexos, criação de protótipos e seleção de fornecedores mais confiáveis. Você adotaria esta estratégia em seu planejamento de resposta aos riscos?
    ( ) Sim. Por quê?
    ( ) Não. Por quê?

19) De acordo com Baraldi (2005, p. 29), os riscos são elementos incertos e as expectativas, que agem constantemente sobre os meios estratégicos (pessoas, processos, informação, e comunicação). Por consequência, se adequadamente gerenciados, forçam a criatividade e fazem nascerem as oportunidades. Heldman (2009, p. 266) sugere que para tratar as oportunidades ou os riscos positivos poderia-se utilizar algumas ***estratégias*** que são:
    - ***Exploração –*** é utilizada quando forem identificados riscos positivos que se queira garantir que ocorram. Ex: risco na redução do tempo total necessário para conclusão do projeto;
    - ***Compartilhamento –*** é a transfêrencia do risco para um grupo que esteja mais bem preparado para lidar com a oportunidade que ele representa;
    - ***Melhoria –*** é a que observa a probabilidade ou impacto do evento de risco para garantir que a organização perceba os benefícios.

Na infraestrutura de TI podem ocorrer riscos positivos que podem ser explorados, compartilhadados ou melhorados. Diante desta afirmação, cite 2 (dois) ou mais riscos positivos ocorridos em sua organização e qual(is) da(s) estratégia(s) foi utilizada. Se nenhuma, comente.

20) ***Planejamento de contingência***, na opinião de Heldman (2009, p. 268), consiste na elaboração de alternativas para lidar com os riscos caso eles se concretizem. É diferente de mitigação que visa à "redução" da probabilidade e seu impacto. Significa que caso o risco venha ocorrer, a organização estará preparada para tratá-lo. As reservas ou provisões para contingências são uma opção usada com frequência. Sua empresa possui plano de contingência a riscos?
    ( ) Sim. Cite os principais riscos que possuem planejamento de contingência.
    ( ) Não. Por quê?

CATEGORIA 5 – MONITORAMENTO E CONTROLE

21) A complementação da gestão de riscos para Ramos et al (2006, p. 82), se dá através do uso de mecanismos para monitorar a eficácia de seus componentes. Sua empresa possui um ***sistema de gestão de riscos***?
    ( ) Sim.
        i. ( ) Próprio
        ii. ( ) Terceiro
    ( ) Não. Como é feito o gerenciamento dos registros de identificação, análise e tratamento dos riscos?

22) Westerman; Hunter (2008; p. 184), alertam que não se tem como provar que alguma coisa não ocorreu graças a seus esforços de risco de TI, contudo, é possível mensurar o esforço que dedica a seu programa, a frequencia e o impacto comercial de incidentes de riscos, níveis de consciência gerais e específicos de cada papel e a agilidade que a empresa adquire ao melhorar seu perfil de risco de TI. Os autores acrescentam ainda: "adote medidas para guiar a consciência, os processos e a simplificação". Diante do exposto, você concorda que um ***sistema de gestão de riscos*** poderia complementar e melhorar o processo de gestão de riscos de sua organização?
    ( ) Sim. Como?
    ( ) Não. Por quê?

APÊNDICE D – QUESTIONÁRIO – INGLÊS

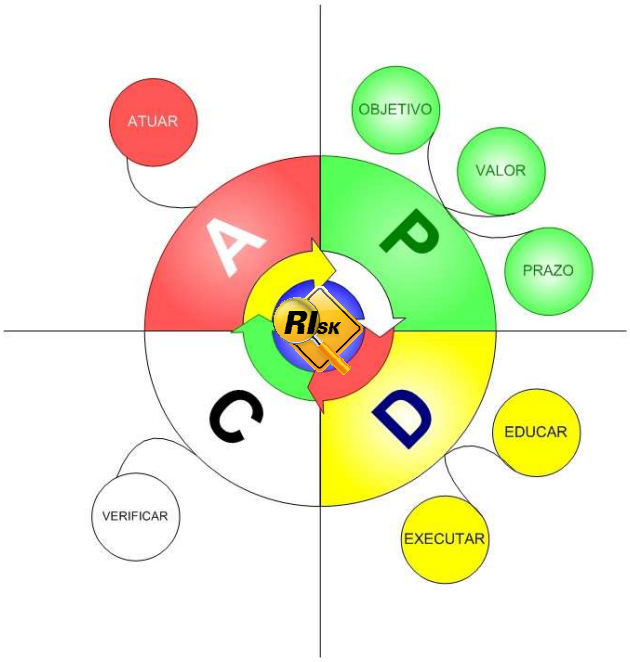
VERIFICATION QUESTIONNARE (SURVEY) – FINAL PAPER

CLEIBER ANDRÉ MUNIZ DA CUNHA

Feevale University
Institute of Science and Technology
Information Systems Graduation
Final Paper

Teacher Advisor: Ms Roberto Scheid

Novo Hamburgo, May 2011.



The adoption of technology is in a surprisingly quick pace, making the IT environment in mind, not only everywhere, but also diffuse and complexly interconnected inside and outside enterprises. As IT's dependence and interdependence from the companies have been increasing, the IT risk consequences also increased (WESTERMAN; HUNTER, 2008, p. 40).

This questionnaire (survey) aims to identify the need to implement of a risk management structured process. It is also worth saying that it is part of an action-research in order to bring improvement to risk management on IT infrastructure, a process that is crucial for the organization. For context, we list the main concepts of risk management:

- ***Risk*** – should be considered as the probability of a threat exploiting one - or several – vulnerabilities, causing damage. In general, risk can be associated with something negative or positive (RAMOS et al, 2006, p. 48-49);
- ***Risk management*** – is a set of activities that aims, in an economically rational way, maximize the effect of positive risk factors and minimize the effect of negatives (SCHMITZ, 2005, p. 63).

- ***Process of risks planning –*** The PMBOK *Guide* states that the process of planning the risks management is the basis for all risk processes. The plan ensures that the appropriate resources and the appropriate time are dedicated to this process (HELDMAN, 2009);
- ***Risk response plan*** – specifies the measures to be taken to mitigate threats and take advantage of opportunities found in the processes of risk analysis;

  The more effective are the risk response plans; greater are the chances of success in the project (HELDMAN, 2009, p. 266);
- ***Control and monitoring*** – are mechanisms to monitor the effectiveness of the risk management components (RAMOS et al., 2006, p. 67). From this monitoring, it is possible to generate a database that will serve to fully reload the continuous improvement process;
- ***Threat*** – everything that has the potential to cause harm to an asset and, consequently, to an organization (RAMOS et al, 2006, p. 45);
- ***Vulnerability*** – are the circumstances that lead one or more assets to be exposed to one or more threats.

Thank you in advance for your collaboration!

CATEGORY 1 – IT GOVERNANCE

1) Considering that Information Technology is the transformation process of concepts, knowledge and equipment of IT and Telecommunications areas in useful applications to all other areas, in any context where IT can be effectively applied (SPOHR; SAUVÉ, 2003, p. 240), it is necessary that companies are aware of the importance of their IT infrastructure. Under this situation, write three (3) factors that you consider important in ***Information Technology Management***.

2) Actually, does your company have implemented a **risk management in their IT infrastructure**?
   ( ) No.
   ( ) Yes. When?
      a. ( ) From 0 to 6 months;
      b. ( ) From 7 to 18 months;
      c. ( ) From 19 to 24 months;
      d. ( ) After than 24 months.

3) In which area or department, does your company has or intends to implement ***risk management***? Note: You can select more than one option.
   a. ( ) Information Technology.
   b. ( ) Finance
   c. ( ) Customer service
   d. ( ) Purchasing department.
   e. ( ) None.
   f. ( ) Other. What?

4) ***The IT department*** of your company in the hierarchy responds to whom?
   a. ( ) To the board.
   b. ( ) Finances department.
   c. ( ) Operations.
   d. ( ) Other. What?

CATEGORY 2 – RISKS MANAGEMENT PLANNING

5) According to Spohr; Sauvé (2003, p. 6) there is necessary that the companies know better their resources, the promises and the reality of new technologies, assessing how far they should change their way of working to adopt some of these technologies. Given this statement, do you believe that ***risk management*** could help in which situation below? Note: You can select more than one option.
    a. ( ) Risk management can help companies to know their limitations, or the risks involved in adopting new technologies;
    b. ( ) Risk management when used appropriately, will allow the organization to have a complete overview of the process, which can transform uncertainty into an opportunity;
    c. ( ) Risk management would not help in this process;
    d. ( ) Other(s). What?

6) According to Heldman (2009, p. 264), the ***risk management plan*** ensures that the appropriate amount of resources and the appropriate time are dedicated to risk management. Given this statement, what is your opinion about the ***risk management process***? Note: Choose only one of the options below.
    a. ( ) Should be used only in financial companies.
    b. ( ) Increases assertiveness in reducing the project (s) uncertainty (s)
    c. ( ) Generates additional costs to the companies.
    d. ( ) Its use is irrelevant.
    e. ( ) Other. What?

7) To Westerman, Hunter (2008, p. 42), ***IT risks governance*** should be embedded in the most important decision-making processes of the organization, where the company avoids to be "blind" and can take more risks, therefore more opportunities, with more confidence. Do you agree with this statement? Why?

8) ***Risk mnagement*** is a complex and laborious process that often requires the use of appropriate tools to identify and mitigate risks in a systematic and continuous way (Ramos et al, 2006, p. 65). Among the factors below, select 3 (three) that you consider as those that difficult the process of ***risk management*** in the organization.
    a. ( ) Lack of knowledge on the subject.
    b. ( ) Lack of support from top management.
    c. ( ) Implementation cost.
    d. ( ) Poor infrastructure.
    e. ( ) Lack of standardization of business processes.
    f. ( ) Other(s). What?

9) What is your opinion on ***risk management of IT infrastructure***?

10) What are the main assets that are monitored or that you suggest to be monitored by ***risk management***?

CATEGORY 3 – RISKS ANALYSIS

11) During the process of ***risk analysis and assessment*** is when all survey will be made in relation to threats, vulnerabilities, probabilities and impact to which assets are exposed (Ramos et al, 2006, p. 67). Do you consider important that the company know the risks associated with their assets?
    ( ) Yes. In which way?
    ( ) No. Why?

12) The ***risk tolerance*** is the result of how much the companies are willing to take the risk because they know that the benefits overcome the possible losses - or vice versa (Heldman, 2009). Which tool (s) / technique (s) listed below would you use to ***identify the risks*** of a project? Note: You can select more than one option.
    a. ( ) Brainstorming.
    b. ( ) SWOT.
    c. ( ) Technical diagrams.
    d. ( ) Expert judgments.
    e. ( ) Other(s). What?

13) The ***risk quantitative analysis*** aims to detect the risks impacts and their possibility of occurrence. The quantitative analysis assesses the impacts and quantifies the exposure to risks by assigning numeric probabilities (Heldman, 2009, p. 238). Which of the above techniques you would use in the process of ***risk assessment***? Justify.

14) ***Automation*** can facilitate the IT risks management in two ways: 1) alleviating the complexity associated with analysis of key-risks reports and 2) facilitating the assessment and mitigation of real risks for real operations (IBM, 2008, p. 9). Given this definition, score the assets that you consider most priority in automation, making for 1 to less important and 5 to very important:
    a. ( ) Management system (ERP).
    b. ( ) Servers, routers and switches.
    c. ( ) Workstation and printers.
    d. ( ) Security and sharing of data.
    e. ( ) Others. Identify and score.

15) ***People*** are moved by the knowledge, by the lack of it and also by the emotion and feeling (Ramos et al, 2006). Under this view, do you consider that people may represent risks for IT?
    ( ) No.
    ( ) Yes. Give 2 (two) examples of IT risks related to people.

16) ***"Information"*** can be understood as every asset that relates to the company's culture or to its business, such information may be of a commercial, technical, financial, legal, human resources nature, or any other nature, that have value for the organization and that are stored on computing resources of the company, with traffic inside your technology infrastructure (Ramos et al, 2006, p. 291). The loss of these may represent significant losses to the organization. How would you rate this risk? Note: You can select only one of the options below.
    a. ( ) Technical, quality or performance risk
    b. ( ) Information management risk
    c. ( ) Organizational risk.
    d. ( ) External risk.

CATEGORY 4 – PLAN RESPONSE TO RISK

17) In the response plan to risks, one of the strategies used for negative risks is the ***transfer of risk***, which is to shift the risk and its consequences to others (Heldman, 2009, p. 264). The Information Technology area may have different risks associated with their services. For which IT services do you recommend the ***transfer of risk***? Note: You can select more than one option.
    a. ( ) Management System (ERP).
    b. ( ) Network administration and helpdesk.
    c. ( ) Systems development.
    d. ( ) Web hosting.
    e. ( ) None. Why?
    f. ( ) Other(s).Which?

18) The ***risk mitigation*** is another strategy used for negative risks which aims to reduce the probability of occurrence and the risk impact up to an acceptable level (PMBOK apud Heldman, 2009, p. 266). Some examples of risk mitigation include the use of less complex processes, prototyping and selection of more reliable suppliers. Would you adopt this strategy in your risk response plan?
    ( ) Yes. Why?
    ( ) No. Why?

19) According to Baraldi (2005, p. 73), the risks are uncertain elements and expectations, which constantly act on the strategic means (people, processes, information and communication). Consequently, if properly managed, force the creativity and bring the opportunities. Heldman (2009, p. 264) suggests that to address the opportunities or positive risks could be used some ***strategies*** that are:
    - **Exploration** - is used when positive risks are identified and you want to ensure that occur. E.g.: risk in the reduction of total time needed to conclude a project;
    - **Sharing -** is the transfer of risk to a group that is better prepared to deal with the opportunity that it represents;
    - **Improvement -** is the one which considers the probability or impact of the risk event to ensure that the organization realizes the benefits.

    In IT infrastructure can occur positive risks that can be exploited, shared or improved. Given this statement, mention 2 (two) or more positive risks occurring in your organization and which strategy was used to. If no, comment.

20) ***Contingency planning,*** according to Heldman (2009, p. 269) is the development of alternatives to deal with the risks in case of they materialize. It's different from mitigation that aims to "reduce" the probability and impact. Means that in case the risk will occur, the organization will be prepared to treat it. The budget or provisions for contingencies are an option used frequently in this case. Does your company have a contingency plan to risks?
    ( ) Yes. Mention the main risks that have a contingency plan.
    ( ) No. Why?

CATEGORY 5 – CONTROL AND MONITORING

21) The completion of risk management to Ramos et al (2006, p. 75), happens through the use of mechanisms to monitor the effectiveness of its components. Does your company have a ***risk management system***?
    ( ) Yes.
        i. ( ) Own.
        ii. ( ) Outsourcing.
    ( ) No. How is it made the management of records of identification, analysis and treatment of risks?

22) Westerman; Hunter (2008, p. 212) warn that there is no way to prove if something did not happen due to your efforts to keep IT risk controlled, however, it is possible to measure the effort you devote to your program, the frequency and business impact of incidents, risk levels and general awareness of each specific role and agility that the company assume to improve their IT risk profile. The authors further add: "adopt measures to guide the behavior, processes and the simplification". Given the above, do you agree that a ***risk management system*** could complement and improve the process of risk management in your organization?
    ( ) Yes. How?
    ( ) No.Why?

APÊNDICE E – ANÁLISE DE CONTEÚDO DA CATEGORIA GOVERNANÇA DE TI

Categoria Inicial (Perguntas [4])	Alternativas possíveis (Questionário)	Categoria Intermediária (Respostas)	Categoria Final (Categ Inferidas)
1) Considerando que Tecnologia da Informação é o processo de transformação dos conceitos, conhecimentos e equipamentos das áreas de informática e Telecomunicações, em aplicações úteis a todas as outras áreas em todo e qualquer contexto, onde ela (a TI) possa ser efetivamente aplicada (SPOHR; SAUVÉ, 2003, p. 240), é necessário que as empresas estejam atentas a importância de sua		***Diretor de TI (CIO):*** Não respondeu. ***Gerentes de TI:*** 1) a) Understanding and commitment from top level management; b) Knowledgeable IT staff and IT infrastructure that moves along with the business and technology; c) Proper business continuity plan that protects IT infrastructure and the business; 2) Considero de extrema relevância a acuracidade dos dados inseridos em um sistema de gestão, para o mesmo tenha a condição de gerar informações consistentes e, assim, favorecer de uma forma segura, a tomada de decisões do corpo diretivo de uma organização. Para que esta acuracidade se faça presente, a cultura organizacional dos colaboradores deve estar voltada a excelência na qualidade dos micro e macroprocessos adotados pela mesma. Por isso, mesmo conjectura, a gestão de TI juntamente com o departamento de controladoria da organização, atuam como sinalizadores da saúde processual vigente em todos os departamentos da empresa, podendo assim, adotar a melhoria contínua dos processos. Neste nível de maturidade de uma organização, visando alicerçar a infraestrutura de TI para comportar a performance dos processos organizacionais, também é de extrema importância a adoção de tecnologia de ponta, a fim de garantir a segurança das informações, agilidade na comunicação interna e externa e hardwares/softwares envolvidos na cadeia produtiva, visando a excelência na qualidade do produto ou serviço oferecido pela empresa. 3) a) Immediacy to Information; b) Production and Manipulation of Sensitive Information, Comprehensive and flexible report generation e c) Streamlining of business processes and timely upgradation; 4) Planejamento estratégico, mensuração de impacto e desempenho, relacionamento com clientes. ***Analistas de TI:*** 1) Usabilidade, balanceamento entre o custo benefício das	- Segurança da Informação; - Plano de Continuidade; - Melhoria contínua;

infraestrutura 2) 3) de TI. De acordo com esta situação, cite 3 (três) fatores que você considera importante na ***gestão da Tecnologia da Informação***.		tecnologias, melhoria de processos; 2) Não respondeu; 3) Políticas de segurança a acessos as informações; Contingência que garanta a continuidade da empresa em caso de um desaster; Não centrar o conhecimento somente em uma única pessoa, em caso de ausência/perda ser possível a sua continuidade.	
4) A área de TI de sua empresa responde hierarquicamente a quem?	A. ( ) Direção ou "Board". B. ( ) Área financeira. C. ( ) Operações - Industrial. D. ( ) Outra. Qual?	***Diretor de TI (CIO):*** A. ***Gerentes de TI:*** 1) C; 2) A; 3) B; 4) A. ***Analistas de TI:*** 1) A; 2) A; 3) A.	- Nível estratégico;

APÊNDICE F – ANÁLISE DE CONTEÚDO DA CATEGORIA PLANO GESTÃO DE RISCOS

Categoria Inicial (Perguntas [6])	Alternativas possíveis (Questionário)	Categoria Intermediária (Respostas)	Categoria Final (Categorias Inferidas)
5) De acordo com Spohr; Sauvé (2003, p. 6) é necessário que as empresas conheçam melhor os recursos, as promessas e a realidade das novas tecnologias, avaliando até que ponto elas devem modificar sua forma de trabalho para adotar alguma destas tecnologias. Diante desta afirmação, você acredita que a gestão de riscos poderia contribuir em qual situação abaixo. Observação: é possível marcar mais de uma opção.	1) ( ) A gestão de riscos pode contribuir para que as empresas conheçam suas limitações, ou seja, os riscos envolvidos na adoção de novas tecnologias. 2) ( ) A gestão de riscos quando usada de forma adequada, permitirá que a organização tenha uma visão completa do processo, o que pode transformar a incerteza em uma oportunidade. 3) ( ) A gestão de riscos não ajudaria neste processo. 4) ( ) Outra(s). Qual (is)?	***Diretor de TI (CIO):*** A e B. **Gerentes de TI:** 1) A e B; 2) A e B; 3) A e B; 4) B. **Analistas de TI:** 1) A e B; 2) A e B; 3) A.	- Limitações; - Visão completa do processo;
6) Segundo Heldman (2009, p. 233), o plano de gerenciamento de riscos assegura que a quantidade apropriada de recursos e o tempo apropriado são dedicados ao gerenciamento de riscos. Diante desta afirmação, qual sua opinião sobre o processo de gestão de riscos? Observação: marcar apenas uma das opções abaixo.	A. ( ) Deve ser utilizado somente em empresas financeiras. B. ( ) Aumenta a assertividade nos projetos diminuindo a(s) incerteza(s). C. ( ) Gera custos adicionais para as empresas. D. ( ) É irrelevante sua utilização. E. ( ) Outra. Qual?	***Diretor de TI (CIO):*** B. ***Gerentes de TI:*** 1) B, C e E (Helps to the business sustainability); 2) B; 3) B; 4) B. ***Analistas de TI:*** 1) B; 2) B; 3) B.	- Redução da incerteza;
7) Para Westerman; Hunter (2008, p. 182), a governança de riscos de TI deveria estar embutida nos mais importantes processos decisórios da organização,		***Diretor de TI (CIO):*** I do agree wit this statement. If one does not know the risks and it's possible impact, chances are that one is either to careful or not careful enough. Knowing and understanding helps to take the correct decisions. ***Gerentes de TI:***	- Saber os impactos aos negócios; - Tomar decisões mais acertivas; - TI faz parte do negócio;

onde a empresa evita deixar-se "cegar" e consegue assumir mais riscos, e, portanto, mais oportunidades, com maior confiança. Você concorda com esta afirmação? Por quê?		1) Yes, IT is an integral part of the business and hence for the sake of business continuity, it should be part of the organizational decision making process; 2) Sim, concordo. Acredito que a gestão de riscos trabalha em conjunto com a gestão estratégica de uma organização, pois as duas alicerçam, através de uma visão sistêmica, os pontos fortes e os pontos fracos da mesma, gerando assim, maior acertividade em um norte mais seguro para o alcance das metas traçadas; 3) No, I don't agree. This would result in business loss more than challenging; 4) Sim, entendo que quando falamos de governança de riscos de TI estamos nos referenciando em deixar de perder. Com esta abordagem de total controle, todas as áreas de negócio deveriam ter uma mensuração de perda e probabilidade deste evento.. ***Analistas de TI:*** 1) Concordo, pois se esse processo está na cultura da empresa, as mudanças poderão ser executadas de forma consciente e minimizando os riscos; 2) Concordo, quando o risco é conhecido é possível através da aplicação de medidas cabíveis evitarem que este ocorra, podendo também através de uma avaliação decidir em correr o risco para atingir determinado objetivo, medindo o custo que a empresa teria em assumir este risco; 3) Sim, porque não é difícil encontrar tecnologias implantadas que apresentam subutilização, ou que causam demandas (principalmente de tempo, financeiras e limitações) que não foram corretamente estimadas.	
8) A gestão de riscos é um processo complexo e trabalhoso que muitas vezes demanda o uso de ferramentas adequadas para identificar e tratar os riscos de forma sistemática e contínua (RAMOS et al, 2006, p. 43). Dos fatores a seguir, selecione 3 (três) que você considera como aqueles que dificultam o processo de gestão de riscos	A. ( ) Falta de conhecimento sobre o assunto. B. ( ) Falta de apoio da alta direção. C. ( ) Custo de implementação D. ( ) Infraestrutura deficiente. E. ( ) Falta de padronização dos processos organizacionais. F. ( ) Outro(s). Qual (is)?	***Diretor de TI (CIO):*** A, B e F (Time). ***Gerentes de TI:*** 1) A, B e E; 2) A, B e E; 3) B, D e E; 4) A, B e E. ***Analistas de TI:*** 1) A, C e E; 2) A, B e E;	- Padronização; - Conhecimento;

nas organizações.		3) A, C e E.	
9) Qual sua opinião sobre gestão de riscos de infraestrutura de TI?		***Diretor de TI (CIO):*** Worthwhile for new technologies and for areas where local meets external, for commodity not very interesting. ***Gerentes de TI:*** 1) It is a critical part. If the IT infrastructure is not perfect, then risks are high. Given the complexity involved in IT, having the right resources (man and machine) is a higher order requirement; 2) Considero de extrema importância a gestão de riscos de infraestrutura de TI, pois esta garante a manutenção das operações e da segurança das informações de uma organização; 3) It is essential for all business not only the IT industries so that the business contingency is achieved; 4) É de suma importância para a estrutura da empresa onde, geralmente, usam-se regras, Acordos de Nível de Serviço, para avaliação dos serviços prestados buscando o alinhamento entre TI e o negócio. ***Analistas de TI:*** 1) É um processo muito importante, pois qualquer parada dos ativos de TI custa muito economicamente para a empresa; 2) Penso que a empresa deve se preocupar com o assunto, fazendo um trabalho no sentido de identificar o que melhor serve para a sua realidade; *3)* Pode ser a diferença entre o sucesso e o fracasso de uma mesma tecnologia em diferentes ambientes/organizações.	- Segurança da Informação; - Continuidade dos negócios; - Excelente para novas tecnologias; - Alinhamento da TI com os negócios;
10) Quais os principais ativos que são monitorados ou que sugerem que fossem monitorados pela gestão de riscos?		***Diretor de TI (CIO):*** Telecom, servers, firewalls, storage cabinets, UPS, Fireprotection (just took IT). ***Gerentes de TI:*** 1) a) In an organization, HR & SHE related activities that keep the morality & safety of the employees; b) Customer focused business strategies; c) Continuous monitoring of the marketing strategies and d) Maintain IT in its perfect condition with adequate data security and backup in order to provide un-interrupted service to the business; 2) Sugiro o monitoramento dos acessos funcionais aos diversos sistemas disponibilizados aos usuários, das condições de hardware e	Telecom; servidores; backup.

		software dos servidores, disponibilidade das informações, dos backups de todas as informações críticas, dentre outros; 3) None response. 4) Serviços prestados pela TI e Criticidade dos serviços. ***Analistas de TI:*** 1) Na área de TI, os servidores são monitorados, a conexão a Internet é monitorada, a atualização dos sistemas operacionais, espaço no storage e servidores, monitoramento do sistema de backup, o antivirus e também o serviço de e-mail. Também as mudanças propostas devem ser avaliadas, pois erros podem gerar impacto negativo ou downtime; 2) Considerando que ativo é tudo o que tem valor para a empresa, penso que para cada empresa podem ser identificados ativos diferentes, vai depender a avaliação da empresa; 3) Segurança e indisponibilidade da informação (ameaças), extração do valor da informação, semelhantemente ao conceito de BI, como oportunidade.	

APÊNDICE G – ANÁLISE DE CONTEÚDO DA CATEGORIA ANÁLISE DE RISCOS

Categoria Inicial (Perguntas [6])	Alternativas possíveis (Questionário)	Categoria Intermediária (Respostas)	Categoria Final (Categorias Inferidas)
11) Durante o processo de ***análise e avaliação de risco*** é que serão feitos todos os levantamentos em relação às ameaças, vulnerabilidades, probabilidades e impacto aos quais os ativos estão sujeitos (RAMOS et al, 2006, p. 50). Você considera importante que a empresa conheça os riscos associados a seus ativos?	A. ( ) Sim. De que forma? B. ( ) Não. Por quê?	***Diretor de TI (CIO):*** A (It provides an insight on the impact of failures hence the provides input on the need to put in place (additional) mitigating controls). **Gerentes de TI:** 1) A (It is important for any company to know the risks associated to their business in order to counter it. If they are ignorant of it, then the threats and vulnerabilities will become reality that will lead to worst case scenario of closing down the business); 2) A (Através de uma abordagem analítica dos ativos considerados relevantes aos processos críticos de uma organização, visando tomar as ações necessárias à manutenção das operações, sendo esta uma análise embasada nos impactos conseqüentes da falta de pró-atividade na segurança); 3) A (To be more proactive and plan and prepared to face situations during disasters); 4) Criando mecanismos para obtenção do consenso na empresa e também possibilitando um maior conhecimento sobre os riscos. **Analistas de TI:** 1) A (Temos que prevenir as falhas antes que as mesmas aconteçam, prevenir o impacto negativo e positivo das mudanças, a perda de dados e sistemas indisponíveis ou downtime); 2) A (Relacionando todos eles e fazendo um estudo sobre cada um); 3) A (Principalmente no tocante a gestão das limitações que determinados ativos e recursos poderão apresentar que em um momento prévio é difícil de visualizar).	- Identificação das ameaças e vulnerabilidades;

12) A tolerância a riscos é o resultado do quanto às empresas estão dispostas em correr o risco, pois sabem que os benefícios decorrentes superam as possíveis perdas – ou o contrário (HELDMAN, 2009, p. 234). Qual (is) ferramenta(s)/técnica(s) listadas você utilizaria para identificar os riscos de um projeto: Observação: é possível marcar mais de uma opção.	A. ( ) Brainstorming. B. ( ) Análise SWOT. C. ( ) Técnicas de diagramas. D. ( ) Opinião especializada. E. ( ) Outra(s). Qual (is)?	***Diretor de TI (CIO):*** A, B e E (Dependance & Vulnerability Analysis). ***Gerentes de TI:*** 1) A, B, C, D, E (Historical data, if available); 2) B e D; 3) C e D; 4) A e D. ***Analistas de TI:*** 1) A e B; 2) A, B e D; 3) A, D e E.	Brainstorming (A = 6); SWOT (B = 5); Opinião especializa (D = 6).
13) Análise qualitativa de riscos visa à detecção do impacto dos riscos e sua probabilidade de ocorrência. A análise quantitativa avalia os impactos e quantifica a exposição aos riscos por meio da atribuição de probabilidades numéricas (HELDMAN, 2009, p. 249). Qual ou quais das técnicas acima você utilizaria no processo de avaliação de riscos? Justifique.		***Diretor de TI (CIO):*** I go for number one which to me is more clear and understandable. Also easier to explain to others.. ***Gerentes de TI:*** 1) I would try to use all. Because, in order to reduce the risk, there is no limit in gathering the information that helps. Also would look forward to any other tool or method that helps in reducing the risks as it is utmost important to have the risk checked to sustain the business; 2) Eu utilizaria as duas técnicas, pois ambas fornecem o real cenário dos riscos envolvidos no projeto em questão; 3) Would go for the risk quantitative analysis as this covers and detect the risk and their impacts; 4) Tanto Brainstorming quanto Testes de hipóteses no projeto mostram-se validas, pois permitem vislumbrar as principais alternativas. ***Analistas de TI:*** 1) O ideal seria usar ambos os processos, tanto qualitativo como quantitativo, porém, priorizamos a análise qualitativa, pois é mais fácil de identificar; 2) Penso que deveriam se utilizar as duas técnicas, pois uma complementa a outra; 3) Os dois, mas em primeiro plano a análise qualitativa, que pode apresentar números mais significativos se considerado o ambiente sistêmico.	- Qualitativa (2); - Quantitativa (1); - Qualitativa e Quantitativa (4);

14) A automação pode facilitar o gerenciamento dos riscos de TI de duas formas: 1) aliviando a complexidade associada à análise de relatórios de riscos cruciais e 2) facilitando a avaliação e a redução dos riscos reais para operações reais (IBM, 2008, p. 9). Considerando esta definição, pontue os ativos que você considera mais prioritários de automação, colocando 1 para menos importante e 5 para muito importante:	A. ( ) Sistemas de gestão. B. ( ) Servidores, roteadores e "*switches*". C. ( ) Estações de trabalho e impressoras. D. ( ) Segurança e compartilhamento de dados. E. ( ) Outros. Identifique e pontue.	***Diretor de TI (CIO):*** 5, 5, 1, 4, ( ). ***Gerentes de TI:*** 1) 5, 5, 4, 5, ( ); 2) 3, 5, 2, 4, ( ); 3) 1, 2, 4, 3, ( ); 4) 5, 3, 2, 4, ( ). ***Analistas de TI:*** 1) 4, 5, 2, 5, 5 (Sistema de Backup); 2) 3, 4, 2, 5, ( ); 3) 4, 2, 1, 3 ,5 (Pensamento sistêmico e conhecimentos sobre os significados diversos impactos de cada indicador).	Sistema de gestão **MEDIA**(A = 5 + 5 + 3 + 1 + 5 + 4 + 3 + 4 = **3,75**); Servidores, roteadores e switches **MEDIA**(B = 5 + 5 + 5 + 2 + 3 + 5 + 4 + 2 = **3,875**); Estações de trabalho e impressoras MEDIA(C = 1 + 4 + 2 + 4 + 2 + 2 + 2 + 1 = **2,375**) Segurança e compartilhamento de dados MEDIA(D = 4 + 5 + 4 + 3 + 4 + 5 + 5 + 3 = **4,125**).
15) Pessoas são movidas pelo conhecimento, pela falta dele e também pela emoção e pelo sentimento (RAMOS et al, 2006). Sob esta ótica, você considera que pessoas podem representar riscos para a TI?	A. ( ) Não. B. ( ) Sim. Cite 2 (dois) exemplos de riscos de TI relacionado às pessoas.	***Diretor de TI (CIO):*** B (Molest of equipment, Steeling data/information). ***Gerentes de TI:*** 1) B (a) IT is a fast developing arena. IT staff who are not moving along with the technology will not be able to provide right technical solutions to the company; b) Frequent staff replacement in IT will result in delays in IT activities. This will escalate the cost and ultimately may lead to loss of business etc. Hence stability in the IT side is an important factor);. *2)* B (a) Quando o conhecimento encontra-se localizado nas mãos das pessoas e não devidamente documentado como patrimônio da empresa, o risco centra-se na dependência funcional do processo. Por isso, neste âmbito, o ideal é a adoção de uma metodologia de mapeamento, redesenho e melhoria contínua dos processos, viabilizando assim, a disseminação do conhecimento entre processos multifuncionais, funcionais e atividades devidamente documentadas e b) A política de motivação de recursos humanos de uma organização é de extrema importância para a redução de riscos em TI, pois o básico é ter confiança no capital humano, ou a empresa desce a níveis exagerados de controle e perde eficiência, além do descontentamento de ambas as partes com os resultados apresentados mediante as metas estabelecidas);	- Segurança da Informação; - Demotivação e mau uso da informação;

		3) A; 4) B (Motivação e fatores externos relacionados a sentimentos e emoção). ***Analistas de TI:*** 1) a) A ((Funcionário insatisfeito com desejo de vingança pode causar graves problemas desde dentro da empresa; b) Falta de conhecimento pode causar prejuízo para o bom funcionamento dos ativos da empresa); 2) B (a) Mau uso do seu conhecimento nos processos da empresa e b) Descaso com situações de riscos que venham a tornar realidade); 3) B (a) Desmotivação em utilizar a informação e o que ela representa e b) Não capacitação..	
16) "Informação" pode ser entendida como todo patrimônio que se refere à cultura da empresa ou ao seu negócio, podendo tais informações ser de caráter comercial, técnico, financeiro, legal, de recursos humanos, ou de qualquer outra natureza, que tenham valor para a organização e que se encontrem armazenadas em recursos computacionais da empresa, com tráfego dentro da sua infraestrutura tecnológica (RAMOS et al, 2006, p. 291). As perdas destas informações podem representar prejuízos significativos para a organização. Como você classificaria este risco: Observação: é possível marcar apenas uma das opções abaixo.	A. ( ) Risco técnico, de qualidade ou desempenho. B. ( ) Risco de gerenciamento da informação. C. ( ) Risco organizacional. D. ( ) Risco externo.	***Diretor de TI (CIO):*** C. ***Gerentes de TI:*** 1) C; 2) C; 3) C; 4) C. ***Analistas de TI:*** 1) B; 2) B; 3) B.	Gerentes de TI (C = 4); CIO (C = 1); Analistas de TI (B = 3);

APÊNDICE H – ANÁLISE DE CONTEÚDO DA CATEGORIA PLANO DE REPOSTAS AOS RISCOS

Categoria Inicial (Perguntas [4])	Alternativas possíveis (Questionário)	Categoria Intermediária (Respostas)	Categoria Final (Categorias Inferidas)
17) No plano de resposta a riscos, uma das estratégias utilizadas para riscos negativos é a transferência do risco, que consiste em deslocar o risco e suas consequências para terceiros (HELDMAN, 2009, p. 264-265). A área de Tecnologia da Informação pode possuir diversos riscos associados à seus serviços. Para quais serviços de TI você recomendaria a transferência de riscos? Observação: é possível marcar mais de uma opção.	A. ( ) Sistema de gestão. B. ( ) Administração de redes e "*helpdesk*". C. ( ) Desenvolvimento de sistemas. D. ( ) Hospedagem do site. E. ( ) Nenhuma. Por quê? F. ( ) Outra(s).Qual (is)?	***Diretor de TI (CIO):*** A, B, C e D. **Gerentes de TI:** 1) A, B, C e D; 2) A e F (Administração da confiabilidade e da segurança das informações); 3) C; 4) B e D. **Analistas de TI:** 1) B, C e D; 2) B e D; 3) A, D e F (Backup).	Sistema de Gestão (A = 4); Adm. Redes e helpdesk (B = 5); Desenv. Sistemas (C = 4); Hospedagem de Sites (D = 6);
18) A mitigação de risco é outra estratégia utilizada pra riscos negativos que tem por finalidade diminuir a probabilidade de ocorrência e o impacto do risco até um nível aceitável (HELDMAN apud PMBOK, 2009, p. 266). Alguns exemplos de mitigação de riscos incluem utilização de processos menos complexos, criação de protótipos e seleção de fornecedores mais confiáveis. Você adotaria esta estratégia em seu planejamento de resposta aos riscos?	A. ( ) Sim. Por quê? B. ( ) Não. Por quê?	***Diretor de TI (CIO):*** A (Is standard option for handling risk, mitigation = reduction of impact/occurrence). ***Gerentes de TI:*** 1) A (Lack of IT man power forces us to look for outsourcing. Outsourcing now is a common phenomenon among IT and is reliable too with adequate Service Level Agreement (SLA) that reduces the risk); 2) A (Acredito que na geração de uma realidade pré-concebida à planejada agregará na visualização dos resultados e dos riscos envolvidos no projeto em questão); 3) A (To save Time and Cost);	Mitigação (A = Todos) - Redução de Impactos; - Prevenção

		4) A (Principalmente nas áreas vitais da empresa é necessário a mitigação de riscos. Na empresa em questão adotamos uma parceria com um fornecedor que deve repor eventuais peças de equipamentos vitais em um determinado prazo, fazendo assim com que diminuamos o risco de ficarmos inoperantes alem do prazo máximo previsto. ***Analistas de TI:*** 1) A (Evitar qualquer trastorno ao funcionamento da empresa e prevenir o impacto); 2) A (Acredito que dentre todos os riscos, alguns são viáveis de gerenciar, diminuindo a probabilidade de sua ocorrência a até um nível aceitável); 3) A (Os protótipos antecipam os resultados, e fornecedores mais confiáveis fazem parte do valor do seu próprio produto.).	
19) De acordo com Baraldi (2005, p. 29), os riscos são elementos incertos e as expectativas, que agem constantemente sobre os meios estratégicos (pessoas, processos, informação, e comunicação). Por consequência, se adequadamente gerenciados, forçam a criatividade e fazem nascerem as oportunidades. Heldman (2009, p. 266) sugere que para tratar as oportunidades ou os riscos positivos poderia-se utilizar algumas estratégias que são: ● Exploração – é utilizada quando forem identificados riscos positivos que se queira garantir que ocorram. Ex: risco na redução do tempo total necessário para conclusão do projeto; ● Compartilhamento – é a transfêrencia do risco		***Diretor de TI (CIO):*** Outsourcing of hosting ERP system, less risk while using state of the art equipment (sharing). ***Gerentes de TI:*** 1) A (a) Exploration: As mentioned earlier, looking for developers outside the organization with proper SLA covered; b) Sharing: Given the expansion of Internet, allowing customers and vendors accessing company's IT infrastructure in a controlled and secured manner that helps reducing data entries, speeding up the process and eventually giving more customer satisfaction (Currently we are doing this at inter-company level); 2) Projeto de Implantação do ERP: foi utilizada a estratégia de exploração para planejamento e implantação da infraestrutura de servidores e de banco de dados, onde empresas parceiras foram contatadas, visando troca de conhecimentos e experiências sobre base já instalada, contemplando prazos de implantação, performance e segurança das operações; 3) No, we have not experienced it so far; 4) Tive dificuldades de interpretar a realidade da empresa com as possibilidades, talvez não tenha entendido bem a questão =/ sorry. ***Analistas de TI:*** 1) a) Compartilhamento.- No caso de mudanças na infraestrutura, são realizadas reuniões de avaliação e encaminhado para os especialistas realizarem a tarefa; b) Melhoria.- Toda possível melhora no funcionamento é avaliada para ser aplicada, trazendo um melhor	- Compartilhamento (3); - Exploração (2); - Melhoria (3).

para um grupo que esteja mais bem preparado para lidar com a oportunidade que ele representa; • Melhoria – é a que observa a probabilidade ou impacto do evento de risco para garantir que a organização perceba os benefícios. Na infraestrutura de TI podem ocorrer riscos positivos que podem ser explorados, compartilhadados ou melhorados. Diante desta afirmação, cite 2 (dois) ou mais riscos positivos ocorridos em sua organização e qual(is) da(s) estratégia(s) foi utilizada.		desempenho para a empresa; 2) Não respondeu; 3) Treinamento e capacitação, que proporcionam mais qualidade, menor rotatividade dos funcionários e aumentam as chances de agregação de valor.;	
20) Planejamento de contingência, na opinião de Heldman (2009, p. 268), consiste na elaboração de alternativas para lidar com os riscos caso eles se concretizem. É diferente de mitigação que visa à "redução" da probabilidade e seu impacto. Significa que caso o risco venha ocorrer, a organização estará preparada para tratá-lo. As reservas ou provisões para contingências são uma opção usada com frequência. Sua empresa possui plano de contingência a riscos?	A. ( ) Sim. Cite os principais riscos que possuem planejamento de contingência. B. ( ) Não. Por quê?	***Diretor de TI (CIO):*** A (Backup lines for telecom, backup of data, Halon equipment). ***Gerentes de TI:*** 1) A (a) IT Hardware and software failures; b) Loss of data (back up process) and c) Protection of IT room from Fire and other environmental hazards); 2) B (A organização não possui sistema de gestão de riscos devidamente implementada em nenhuma área da empresa); 3) A (a) Communication / Connectivity down and b) Proper systems are put in place and backup link is established); 4) A (Criação de um Site backup e redundância nos links). ***Analistas de TI:*** 1) A (Quando são realizadas mudanças, está previsto um "rollback", caso exista algum problema, o ambiente pode ser restaurado para a situação prévia. No caso da Internet, não tem plano de contingência e depende-se de um único provedor, que as vezes, falha); 2) B (Está sendo trabalhado o assunto e em vias de desenvolvimento); 3) A Se o link de sistema cai, as recepcionistas prestam atendimentos por guias de autorizações em papéis.	- Contingência (6) - Link (4); - Backup (3);

APÊNDICE I – ANÁLISE DE CONTEÚDO DA CATEGORIA MONITORAMENTO E CONTROLE

Categoria Inicial (Perguntas [2])	Alternativas possíveis (Questionário)	Categoria Intermediária (Respostas)	Categoria Final (Categorias Inferidas)
21) A complementação da gestão de riscos para Ramos et al (2006, p. 82), se dá através do uso de mecanismos para monitorar a eficácia de seus componentes. Sua empresa possui um sistema de gestão de riscos?	A. **( ) Sim.** a. ( ) Próprio b. ( ) Terceiro B. **( ) Não.** Como é feito o gerenciamento dos registros de identificação, análise e tratamento dos riscos?	***Diretor de TI (CIO):*** B (Manual within each project by the project team). **Gerentes de TI:** 1) A (Own); 2) B (O gerenciamento dos registros de identificação, análise e tratamento dos riscos dentro da organização é efetuado conforme a expertise dos profissionais de nível gerencial e estratégico da empresa, baseado na experiência, formação e própria metodologia de trabalho); 3) A (Own); 4) B (Manualmente, quando necessário). **Analistas de TI:** 1) A (Próprio); 2) B (Conforme comentado anteriormente está em fase de elaboração, no momento é de acordo com a oportunidade, não tem rotina definida); 3) B (Existem alguns mecanismos, mas não podem ser chamados de "Gestão de Riscos". No restante é o popular "apagar incêndio").	- Gerenciamento Manual; - Sistemas próprios;
22) Westerman; Hunter (2008; p. 184), alertam que não se tem como provar que alguma coisa não ocorreu graças a seus esforços de risco de TI, contudo, é possível mensurar o esforço que dedica a seu programa, a frequencia e o impacto comercial de incidentes de riscos, níveis de consciência gerais e específicos de cada papel e a agilidade que a empresa adquire ao melhorar seu perfil de risco de TI. Os autores	A. ( ) Sim. Como? B. ( ) Não. Por quê?	***Diretor de TI (CIO):*** A (At least to standardize the approach and ability to benchmark over time/projects). ***Gerentes de TI:*** 1) A (Risk Management System helps to identify the risks involved. Even if you can't afford to mitigate the identified risks now, it prepares you to be ready to resolve the problem later when it happens); 2) A (Concordo, desde que a empresa já possua em sua maturidade uma gestão estratégica voltada a organização e melhoria contínua dos processos, à preparação das pessoas, objetivando que as mesmas colaborem para o atingimento das metas traçadas, e políticas pré-estabelecidas de âmbito organizacional, visando direcionar as equipes a um norte alicerçado pela convicção dos objetivos definidos pelo	- Software de gestão.

acrescentam ainda: “adote medidas para guiar a consciência, os processos e a simplificação”. Diante do exposto, você concorda que um sistema de gestão de riscos poderia complementar e melhorar o processo de gestão de riscos de sua organização?		corpo diretivo da organização. Acredito que tais prerrogativas sejam essenciais para que um sistema de gestão de riscos retorne resultados positivos, efetivos e confiáveis à gestores de riscos); 3) A (Prepare ourselves for the risks in advance and plans are made in advance to cover the risks); 4) A (). ***Analistas de TI:*** 1) A (Automatizando, simplificando e organizando o processo já existente); 2) A (Acredito que através de um sistema simplificaria o processo de identificação, trazendo agilidade); 3) A (Não mostrando apenas o que deu certo, mas mostrando também o que deixou de dar errado).	