UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
ESPECIALIZAÇÃO EM GESTÃO PÚBLICA

DECIO DE ABREU MALTA

GERENCIAMENTO DE RISCOS PARA A ÁREA DE TECNOLOGIA DA INFORMAÇÃO DE UMA EMPRESA PÚBLICA DE ECONOMIA MISTA

MONOGRAFIA DE ESPECIALIZAÇÃO

PATO BRANCO
2013

DECIO DE ABREU MALTA

GERENCIAMENTO DE RISCOS PARA A ÁREA DE TECNOLOGIA DA INFORMAÇÃO DE UMA EMPRESA PÚBLICA DE ECONOMIA MISTA

Monografia apresentada como requisito parcial à obtenção do título de Especialista na Pós Graduação em Gestão Pública, Modalidade de Ensino a Distância, da Universidade Tecnológica Federal do Paraná – UTFPR – *Câmpus* Pato Branco.

Orientador(a): Prof. Dr Paulo Cezar Dondoni

PATO BRANCO

2013

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Pesquisa e Pós-Graduação
Especialização em Gestão Pública

TERMO DE APROVAÇÃO

Titulo da Monografia

Por

Décio de Abreu Malta

Esta monografia foi apresentada como requisito parcial para a obtenção do título de Especialista no Curso de Especialização em Gestão Pública, Modalidade de Ensino a Distância, da Universidade Tecnológica Federal do Paraná, *Câmpus* Pato Branco. O candidato foi argüido pela Banca Examinadora composta pelos professores abaixo assinados.

_____

Professor Dr. Paulo Cezar Dondoni
UTFPR – *Câmpus* Pato Branco
(orientador)

_____

_____

Dedico este trabalho aos meus pais,

Nicodemos de Abreu Malta e Cleuza Luiza Malta.

AGRADECIMENTOS

À Deus pelo dom da vida, pela fé e perseverança para vencer os obstáculos.

Aos meus pais, pela orientação, dedicação e incentivo nessa fase do curso de pós-graduação e durante toda minha vida, como também, como exemplos vivos de perseverança, companheirismo e dedicação à família.

Ao meu orientador Professor Dr. Paulo Cezar Dondoni, que me orientou, pela sua disponibilidade, interesse e receptividade com que me recebeu e pela prestabilidade com que me ajudou. Ressaltando que mesmo que de última hora acatou meu projeto e contribuiu para o desenvolvimento deste trabalho

Agradeço aos pesquisadores e professores do curso de Especialização em Gestão Pública, professores da UTFPR, *Campu*s Pato Branco.

Agradeço aos tutores presenciais e a distância que nos auxiliaram no decorrer da pós-graduação.

Agradeço também á minha esposa Paula Cyrillo Lloret e minha Filha Livia Lloret Malta que são o meu objetivo maior e minha grande alegria ao acordar.

Enfim, sou grato a todos que contribuíram de forma direta ou indireta para realização desta monografia.

“Penso, Logo Existo!”.

(René Descartes)

RESUMO

MALTA, Décio de Abreu. Gerenciamento de Riscos para a área de tecnologia da informação de uma empresa de economia mista. 2013. 51 páginas. Monografia (Especialização Gestão Pública). Universidade Tecnológica Federal do Paraná, Pato Branco, ano 2014.

Este trabalho tem como objetivo demonstrar o mapeamento e desenho dos riscos para o ambiente de Tecnologia da informação de uma empresa de economia mista do Estado de São Paulo. O trabalho foi desenvolvido com base em metodologias de mercado utilizadas para identificação, mensuração e controles para reduzir o nível de exposição ao risco, sendo:

- ERM-IF (*Enterprise Risk Management Integrated Framework*;
- COBIT (*Control Objectives for Information and related Technology)*;
- Normas ABNT (Associação Brasileira de Normas Técnicas);

Buscou-se identificar os riscos, mensurar sua exposição com base na probabilidade e impacto quando da possível materialização do contexto do risco. Qualquer evento que impeça ou impacte um objetivo da empresa deve ser considerado um risco a ser mensurado e tratado.

Os resultados demonstraram que os riscos estão parcialmente mitigados e com nível satisfatório, porém, dentre os processos mapeados, identificou-se a necessidade de melhorar os controles voltados ao gerenciamento de informações críticas da empresa, Os controles devem ser implementados visando o gerenciamento do processo de segurança da Informação.

Assim, destacamos a atividade de gerenciamento de riscos como uma forma cíclica para garantir que a tecnologia seja parte do negócio, mudando seu status de despesa para investimento.

Palavras-chave: TECNOLOGIA, COSO, COBIT, ERM, RISCO.

ABSTRACT

MALTA, Décio de Abreu. Risk Management in the area of information technology a public company of mixed economy. 2013. 51 pages. Monograph (Specialization in Public Management). Universidade Técnica Federal do Paraná, Pato Branco, 2014.

This paper demonstrates the design and mapping of risks to the environment of Information Technology for a company of mixed economy of São Paulo. The work was developed based on market methodologies used for identification, measurement and controls to reduce the level of risk exposure, as follows:

- ERM-IF (*Enterprise Risk Management Integrated Framework*;
- COBIT (*Control Objectives for Information and related Technology)*;
- Normas ABNT (Associação Brasileira de Normas Técnicas);

The search to identify risks, measure their exposure based on probability and impact upon the possible materialization of the risk context. Any event that prevents a goal or impact of the company should be considered a risk to be measured and treated.

The results showed that the risks are partially mitigated and satisfactory level, however, among the mapped processes, we identified the need to improve controls aimed at managing critical business information, the controls must be implemented aiming at managing the process safety Information.

Include the activity of risk management as a cyclical basis to ensure that technology is part of the deal, changing their status to investment spending.

Keywords: TECHNOLOGY, COSO, COBIT, ERM, RISK.

LISTA DE FIGURAS

SUMÁRIO

1 – INTRODUÇÃO

Qualquer atividade do cotidiano ao ser executada é dotada de riscos. Desde o início dos tempos, o ser humano é exposto a situações em que os riscos devem ser avaliados, mesmo que não seja de forma premeditada a análise dos riscos é efetuada visando a sua sobrevivência. Assim, correr riscos é inevitável.

Neste contexto o ser humano reconhece os riscos através de um processo de avaliação sistemática, representando um contínuo meio de aprendizagem no gerenciamento dos riscos.

Há algum tempo, algumas empresas públicas do Brasil, buscam como fonte para seus investimentos a abertura de seu capital, sendo fracionada em forma de ações que são negociadas nas bolsas de valores do mercado nacional e internacional, caracterizando assim como uma empresa pública de economia mista.

Ao abrir sua estrutura ao mercado para negociação das ações, a empresa é obrigada a seguir legislações específicas que visam assegurar a adoção de controles e boas práticas de gestão dos seus processos, garantindo a segurança dos investidores que aderiram ao seu capital no mercado de ações.

A empresa ao qual se destina o presente estudo é uma empresa do estado de São Paulo que está vinculada à modalidade de economia mista, sendo que seu capital está dividido entre ações negociadas no novo mercado da bolsa de valores de São Paulo e ações negociadas na bolsa de valores de Nova York.

Quando negociada na bolsa de Nova York a empresa deve se adequar a este setor e para isso seguir a lei americana Sarbanes Oxley, sendo que em sua seção 404, é definido que a empresa deve possuir controles para mitigar os riscos do processo, garantindo a segurança e confiabilidade das ações executadas.

Assim, para garantir a melhoria de seus processos, as empresas adotaram modelos de gerenciamento que propiciem o gerenciamento de riscos, sendo:

- ERM-IF (*Enterprise Risk Management Integrated Framework*), como padrão para gerenciamento de riscos contemplando as avaliações e mensuração.

- COBIT (*Control Objectives for Information and related Technology),* como padrão para identificação de pontos de controle para o ambiente de Tecnologia da Informação.

- Normas ABNT (Associação Brasileira de Normas Técnicas) são normas elaboradas por comitês formados por profissionais que contribuem para elaborar e regulamentos os métodos que são destaque de excelência e qualidade.

O ERM-IF é um modelo elaborado pelo COSO (*Committee of Sponsoring Organizations*) desde 1992 contemplando os procedimentos a serem adotados para gerenciamento dos riscos.

A gestão de riscos contribui para assegurar comunicação eficaz e o cumprimento de leis e regulamentos, bem como evitar danos à reputação da organização e suas consequências. Assim, a gestão de riscos ajuda a organização a atingir seus objetivos e evitar os perigos e surpresas em seu percurso.

Segundo o CobIT, a adoção dos controles envolvidos em seus processos é fundamental para garantir que a empresa esteja com processos seguros.

O processo de tecnologia da informação assegura os demais processos da empresa, sendo considerado um processo chave, pois uma falha em seus controles pode gerar impacto em todo o escopo dos sistemas corporativos e suas funcionalidades.

Assim, a adoção destas metodologias visam garantir que a empresa conheça os riscos envolvidos no processo, os valores envolvidos quando da materialização e a probabilidade de ocorrência, monitorando e avaliando os controles que mitigam os riscos.

1.1 – Objetivo

Gerenciar os riscos envolvidos para os processos contemplados na área de tecnologia da informação de uma empresa de economia mista, determinando os respectivos atributos de cada risco:

1.2 – Objetivo Específico

As análises terão como objetivo específico propiciar um modelo gerencial para avaliação de riscos, possibilitando através de poucos itens avaliar a situação do ambiente geral de tecnologia da informação em seu escopo estratégico, onde serão avaliados os seguintes fatores:

- Risco Inerente: Identificar o risco em sua forma original, sem nenhuma ação para seu controle;
- Impacto: Mensurar o impacto do risco quando da sua ocorrência;
- Probabilidade: Identificar qual é a probabilidade de ocorrência do risco;
- Controles: Identificar os controles que estão vinculados ao risco e que atuam para reduzir a probabilidade de ocorrência ou minimizar o impacto.
- Risco Residual: Identificar o resultado do risco após a vinculação dos controles;
- Tratamento ao Risco: Após a definição do risco residual, definir a ação que se dará ao risco perante seu resultado:
  - Manter: O risco será mantido em seu nível atual;
  - Transferir: O risco será transferido para outro responsável;
  - Reduzir: Serão definidos planos de ações para reduzir o impacto ou probabilidade do risco.

1.3 – Justificativa

O ambiente de Tecnologia da Informação é responsável pelo desenvolvimento e continuidade das aplicações, assim, uma falha em seu processo pode comprometer o negócio da empresa, como também, possibilitar falhas ou fraudes pelas vulnerabilidades envolvidas.

Este estudo possibilitará que seja definido um modelo para avaliação geral dos riscos estratégicos de Tecnologia da informação, podendo ser utilizado por empresas que prestam serviços de utilidade pública (*utilities*) e que possuem uma área de tecnologia da informação.

2 – FUNDAMENTAÇÃO TEÓRICA

Para avaliação dos riscos referente ao ambiente de tecnologia da informação, faz-se necessário a utilização de modelos para avaliação e definição de controles, nesta avaliação foram utilizados três modelos, sendo:

- ERM-IF (*Enterprise Risk Management Integrated Framework*): Utilizado como balizador para desenho do modelo para avaliação dos riscos, a empresa utiliza o modelo do COSO para mapeado e desenho dos controles, assim, utilizar o modelo da mesma organização garante melhor aderência ao método;

- COBIT (*Control Objectives for Information and related Technology)*: Utilizado como balizador para os assuntos de tecnologia da Informação, este modelo é recomendo pelo COSO como melhor referência para mapeamento dos processos de tecnologia da informação.

- Normas ABNT (Associação Brasileira de Normas Técnicas): Utilizado como balizador de controles no cenário Brasileiro e as melhores práticas aqui aplicadas.

Com bases nos modelos, deve ser estabelecida a abrangência de avaliação, para definir o contexto de análise, deve ser avaliada a missão e visão de onde estão contemplados os riscos, assim, a missão e visão que devem estar conectadas às estratégias da **empresa**:

- **Missão:** A missão de uma organização dever definida para satisfazer alguma necessidade do ambiente externo e não simplesmente em oferecer um serviço ou produto, assim a definição da missão deve responder às perguntas: Qual é o nosso negócio?; Quem é o nosso cliente?; Qual a expectativa de satisfação dele? (ANDRADE,1999, p 27).

- **Visão:** A visão de uma organização dever ser a situação futura desejada, dever ser uma meta ambiciosa, e servir como um guia para a definição dos objetivos e a realização da missão. (ANDRADE,1999, p 27).

2.1 - *Enterprise Risk Management Integrated Framework* – ERM – IF

Para caracterização de um risco o COSO avalia a relação dele com a empresa e os impactos que pode gerar frente aos objetivos da empresa, assim, o risco é definido como:

> ""*Risco é um conceito utilizado para expressar preocupações sobre os prováveis efeitos de um ambiente incerto. Uma vez que o futuro é incerto, qualquer conjunto de eventos poderia ter um impacto significativo sobre as metas e objetivos de uma organização. As organizações esforçam-se para cumprir metas através de oportunidades que constituem as possibilidades positivas. Há também o potencial para possibilidades negativas associadas a busca das metas, o que é conhecido como riscos.*"" (COSO, 2009, p10)

No contexto corporativo, a atividade de gerenciamento de riscos está relacionada à forma como a empresa lida com os fatores que influenciam seu valor, assim, o COSO define esta atividade da seguinte forma:

> "*O gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.*" (COSO, 2009, p13)

No modelo COSO, conforme figura 01, os riscos são destacados conforme sua classificação. Conforme o cubo abaixo, destacamos os três eixos:

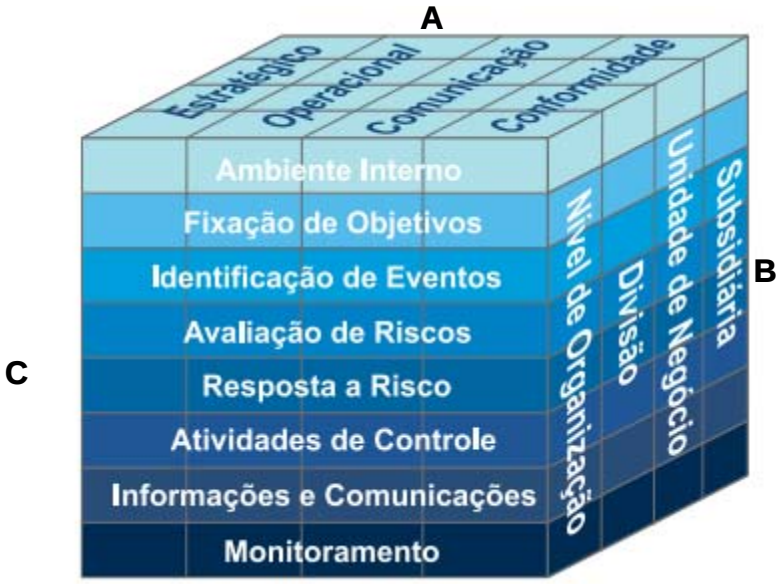

Figura 01 – Cubo COSO (COSO, 2009, p13)

A figura acima foi obtida do modelo COSO, contextualizando como seus eixos interagem, conforme detalhamento abaixo:

A - Objetivos: A classificação do risco demonstra a forma como o risco é avaliado. Seu tratamento pode ocorrer dentro das seguintes categorias:

- Estratégicos: Define metas gerais, alinhadas com o planejamento estratégico e as necessidades da empresa;
- Operações: Define a execução de processos e atividades corporativos;
- Comunicação: Define a confiabilidade de relatórios e divulgações efetuadas.
- Conformidade: Define a aderência da empresa frente às leis e regulamentos aplicáveis.

B - Abrangência: Define a amplitude que contempla o risco, definindo em quais áreas da empresa está contemplada, tal visão é fundamental para a análise do impacto quando da análise do risco.

C - Componentes: Os componentes são responsáveis por classificar o risco e direcionar o seu tratamento. O risco pode permear vários componentes e sua somatória junto a outros fatores, será responsável pela avaliação do risco:

- Ambiente Interno: Define as características da empresa, seus valores e forma de avaliação do risco;
- Fixação de Objetivos: Define o processo responsável por estabelecer os objetivos que propiciem suporte e que alinhe o risco ao plano estratégico da empresa;
- Identificação de Eventos: Define os eventos internos e/ou externos que poderão materializar o Risco.
- Avaliação dos Riscos: Define a avaliação conforme matriz de impacto x probabilidade, considerando sua classificação em inerente e residual.
- Resposta ao Risco: Define a ação da empresa frente ao risco, possibilitando que seja evitado, mantido, reduzido ou compartilhado.
- Atividades de Controle: Define os fatores que possibilitam a avaliação e redução do nível de exposição ao risco.
- Informações e Comunicação: Define quais são as informações relevantes e qual o prazo para sua publicação para que sejam cumpridos os prazos regulamentados.
- Monitoramento: Define a forma que os riscos serão monitoradas, garantindo a avaliação periódica.

Após a análise dos riscos, e definição das matrizes Inerentes e residuais, os riscos são avaliados para que seja definido se está aderente e dentro do apetite ao risco da empresa, segue a definição de apetite ao risco definido pelo COSO:

> "*Apetite a Riscos é a quantidade total de riscos que uma companhia ou outra organização está disposta a aceitar na busca de sua missão (ou visão).*" (COSO, 2009, p26)

2.2 – ABNT NBR ISO 31000 – Gerenciamento de Riscos

A Norma 31000 tem como foco o processo de gerenciamento de Riscos, navegando entre o processo de implantação e suas etapas no âmbito das organizações.

O processo de gestão de Riscos é compreendido pela prática de definir o contexto que será avaliado e posteriormente a aplicação das etapas para mensuração dos riscos, conforme informações do diagrama abaixo:

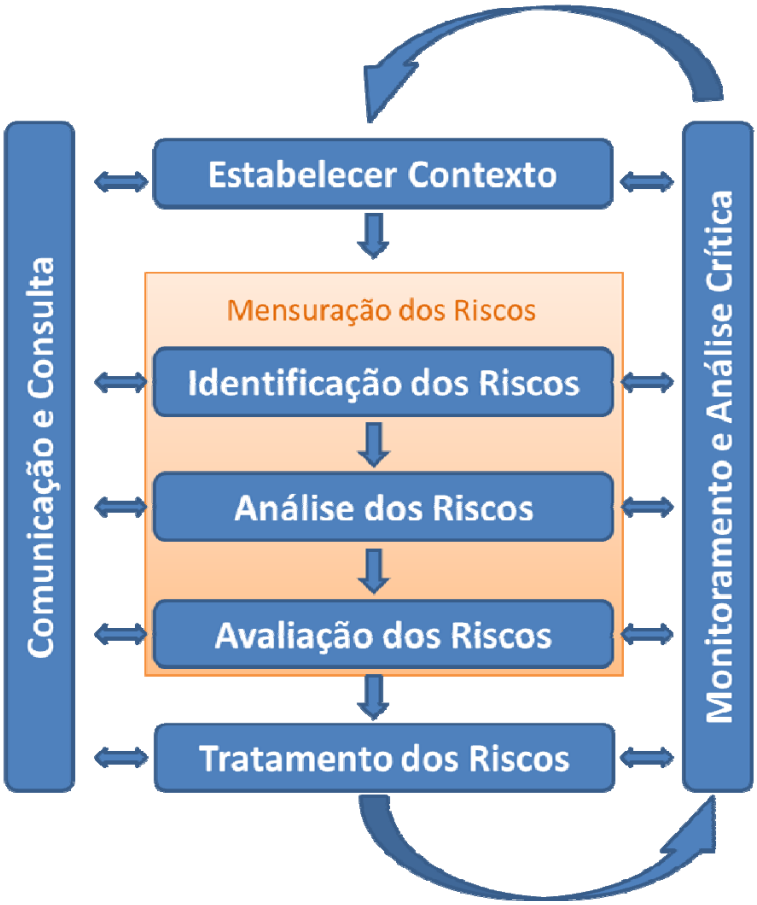

Figura 02 – Gerenciamento de Riscos (ABNT NBR ISO 31000, 2009, p22)

Estabelecer Contexto: Atividade de definição do que será avaliado, tem como característica a definição do processo e seu respectivo responsável;

Mensuração dos Riscos: A mensuração dos riscos compreende as etapas focadas em detalhar as informações dos riscos, sendo:

- Identificação dos Riscos: Atividade que tem como finalidade identificar todos os riscos do processo em avaliação, independente de suas características;
- Análise dos Riscos: Atividade que tem como finalidade identificar os fatores do Risco (causas e consequências), indicando os itens que podem fazer com que o risco se concretize e os impactos gerados;
- Avaliação dos Riscos: Atividade focada em medir os valores derivados da probabilidade e impacto, tendo como referência fatores como histórico, controles, fatores de risco e impacto decorrente de sua materialização.

Tratamento do Risco: Atividade focada na decisão referente ao que se deve fazer após a mensuração do risco, com base nas avaliações de impacto e probabilidade, deve ser avaliado se mantém, mitiga ou transfere o risco;

Monitoramento: Atividade focada na observação, verificação e supervisão que deve ser efetuada de forma contínua, buscando identificar possíveis mudanças em fatores de risco e/ou controles do processo. Para o controle podem ser utilizados indicadores para medição e alarmes;

Análise crítica: Atividade que tem como objetivo determinar a forma de adequar os controles do risco visando atingir os objetivos estabelecidos;

Comunicação e Consulta: Atividade que deve ser executada de forma contínua e interativa entre os envolvidos diretamente com o processo, para compartilhar ou obter informações detalhadas que possibilitem a análise com maior segurança.

2.3 – COBIT – *Control Objectives for Information and related Technology*

O Frame Work de gerenciamento de riscos proposto pelo COSO define em sua essência como deve ser desenvolvida a identificação, gestão e monitoramento dos riscos, porém, visando analisar os riscos envolvidos para o ambiente de desenvolvimento de Sistemas de uma área de Tecnologia da Informação, é necessária a busca de um modelo que possibilite tratar tal assunto de forma mais específica.

Neste cenário, o COBIT (*Control Objectives for Information and related Technology)* é responsável por demonstrar sua abrangência onde se define da seguinte forma:

> "*A orientação para negócios é o principal tema do CobIT, o qual foi desenvolvido não somente para ser utilizado por provedores de serviços, usuários e auditores, mas também, e mais importante, para fornecer um guia abrangente para os executivos e donos de processos de negócios.*
>
> *O modelo CobIT é baseado nos princípios de Prover a informação de que a organização precisa para atingir os seus objetivos, as necessidades para investir, gerenciar e controlar os recursos de TI usando um conjunto estruturado de processos para prover os serviços que disponibilizam as informações necessárias para a organização.*
>
> *O gerenciamento e o controle da informação estão presentes em toda a metodologia e ajudam a assegurar o alinhamento com os requisitos de negócios.*"

Assim a principal contribuição para identificação e desenho dos controles para os respectivos riscos específicos para o processo de Desenvolvimento de TI, virá do CobIT, como também, a categorização dos riscos.

O CobIT está organizado entre domínios, sendo que cada domínio possui uma funcionalidade e característica, o cubo baixo demonstra as características e divisões utilizados pelo CobIT para conversar com a organização, inter-relacionando as partes e destacando sua visão.

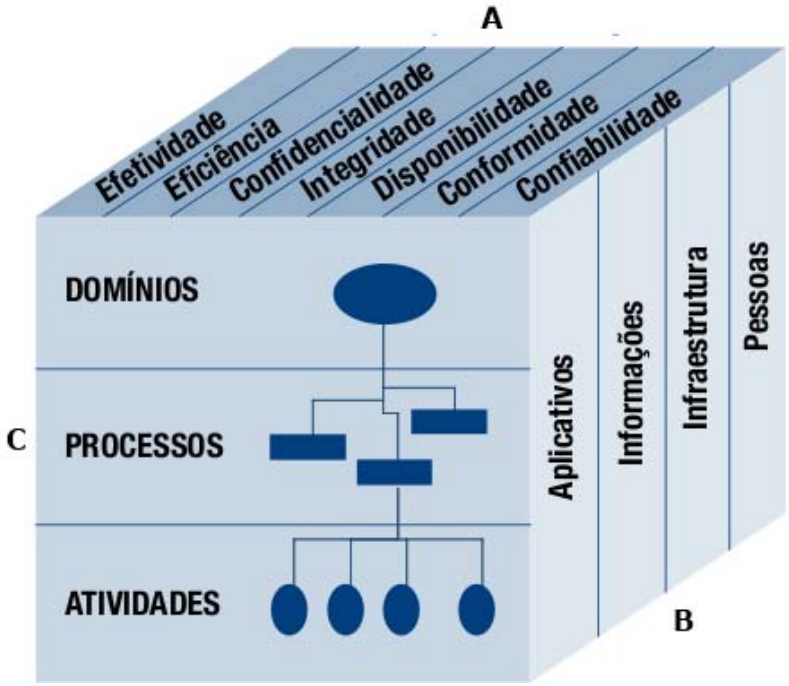

Figura 03 – Cubo do CobIT (COBIT 4.1, 2011,p27)

A – Requisitos de Negócios: Definem quais são os requisitos de negócio a atingir, esta avaliação demanda aos controles a serem avaliados conforme categorias abaixo:

- Efetividade: Define que a informação de ser relevante ao negócio considerando sua tempestividade e consistência;
- Eficiência: Define que os recursos sejam utilizados no melhor método visando à equação entre ser produtivo e econômico;
- Confidencialidade: Define que a informação esteja protegida para quem é seu custodiante e/ou responsável;
- Integridade: Define a disponibilização da informação de forma a garantir sua totalidade e fidelidade quanto aos critérios e expectativas das regras de negócio;
- Disponibilidade: Define que a informação deve estar disponível quando exigida pelo processo de negócio;
- Conformidade: Define a aderência às leis, regulamentos e obrigações;

- Confiabilidade: Define a entrega da informação de forma confiável aos executivos para tomada de decisões.

B – Recursos de TI: Definem quais serão os recursos necessários para atender às expectativas e requisitos de negócios, classificando-os em:

- Aplicativos: Sistemas e procedimentos que processam as informações;
- Informações: Dados em todas as formas considerando para isso sua utilização pelas áreas de negócio;
- Infraestrutura: Todo o suporte para processamento e armazenamento que possibilitam o processamento dos aplicativos.
- Pessoas: Recursos Humanos requeridos para executar todo o ciclo dos sistemas de informação e serviços.

C – Processos de TI: Define os processos a serem avaliados conforme seu domínio, processos e respectivas atividades que darão origem aos controles, vide domínios:

- PO | Planejar e Organizar: Trata-se da visão mais estratégica do framework, onde é avaliada como deve ser propiciada a solução;
- AI | Adquirir e Implementar: Trata do processo de desenvolvimento ou aquisição de soluções para atender as demandas de negócio.
- DS | Entregar e Suportar: Propicia o uso por parte dos usuários finais das soluções implementadas;
- ME | Monitorar e Avaliar: Monitora os processos garantindo sua execução conforme desenho efetuado.

Assim, com base nestes conceitos serão avaliados os riscos inerentes, causas, consequências, controles e riscos residuais para o ambiente tecnológico.

Nos elementos textuais, o número de seções do trabalho monográfico deve ser definido pelo pesquisador e orientador. Nesta segunda seção denominada de

fundamentação teórica que pode ser também denominado de referencial teórico ou ainda embasamento teórico. O número de seções secundárias deverá ser conforme a necessidade da pesquisa. Buscando dar o embasamento teórico ao objeto de estudo proposto.

3 – PROCEDIMENTOS METODOLÓGICOS DA PESQUISA

A pesquisa se deu em uma empresa pública de economia mista do estado de São Paulo que atende grande parte dos municípios do estado, com sede em mais de 360 cidades do estado.

A área responsável pelos assuntos de tecnologia da informação está centralizada na sede principal localizada na cidade de São Paulo, estando vinculada á Diretoria de Gestão Corporativa. Visando ilustrar a estrutura organizacional da empresa, segue abaixo organograma gerencial ao qual a Superintendência de Tecnologia da Informação está vinculada e os seus respectivos departamentos:

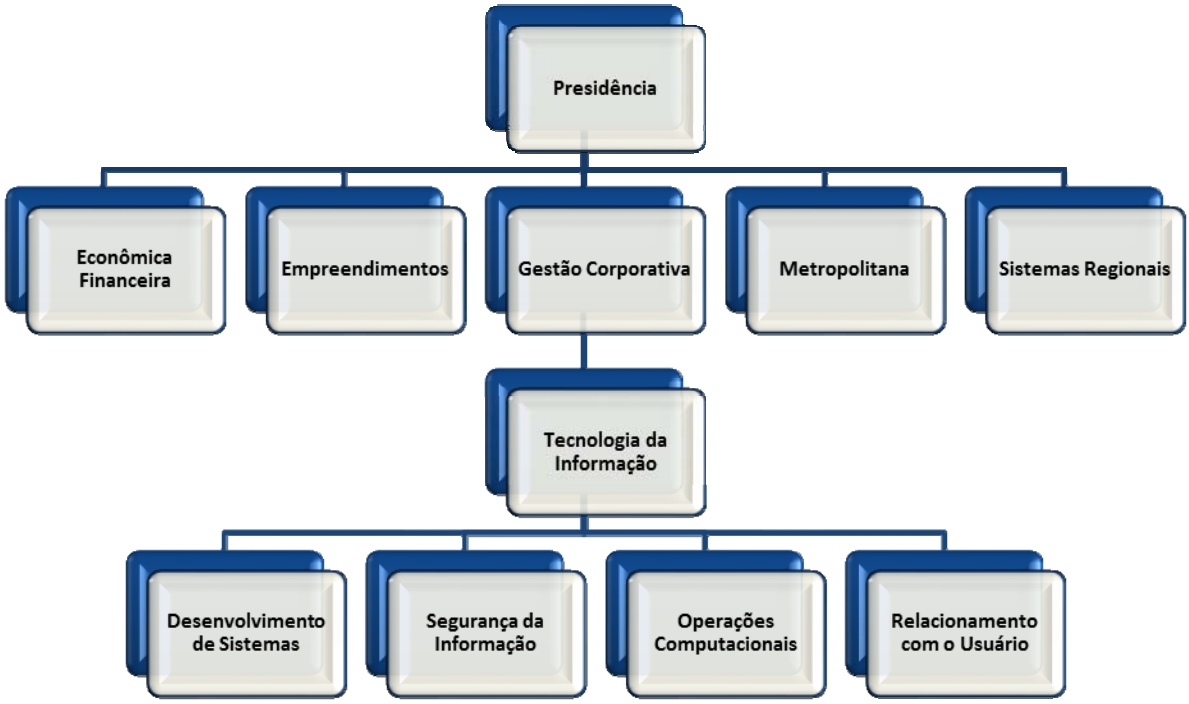

Figura 04 – Organograma da Empresa e Área de Tecnologia da Informação

Para avaliação dos riscos e seus atributos, foram efetuadas reuniões junto ao Superintendente de Tecnologia da Informação e os respectivos gerentes das áreas vinculadas a esta superintendência e as pessoas por eles indicados, totalizando 10 pessoas durante todo o processo.

As reuniões tiveram como objetivo contextualizar o trabalho a ser efetuado e possibilitar a construção conjunta dos riscos e seus atributos, onde todos eram

responsáveis por elencar o risco e definis seus níveis de exposição com base no escopo a ser avaliado para este trabalho.

3.1 – Contextualização

A contextualização do ambiente se dá com base na análise da missão e visão da empresa. Estas informações são utilizadas como norteador para o gerenciamento e identificação dos riscos, utilizando como referência o mapa estratégico da empresa e do ambiente geral de tecnologia da informação.

Segundo as metodologias ERM-IF e a norma ABNT 31000 o primeiro ponto para o gerenciamento de riscos é a contextualização da área de tecnologia da informação tendo como indicador os aspectos estabelecidos pela sua missão e visão

3.2 – Definição dos Objetivos

Após a contextualização da função da área de tecnologia, a próxima etapa é a definição dos objetivos da área de tecnologia. Para isso, utilizamos os domínios do *CobIT* como forma de identificação e organização. O *CobIT* possibilitará estabelecer um padrão de mercado, onde as áreas de tecnologia da informação estão previamente divididas.

O *CobIT* está dividido por domínios, assim, cada domínio representará seus objetivos específicos, e posteriormente o relacionamento com riscos, controles, riscos residuais e planos de ação.

3.3 – Definição dos Riscos

Com base nas informações dos objetivos, os riscos foram definidos de forma a identificar os fatores que poderiam de alguma forma afetar o objetivo do processo, onde segundo Gleim:

A convergência entre o impacto e a probabilidade gera o nível de exposição do risco que define a classificação geral do risco.

Para definição do impacto e probabilidade referente aos riscos, foram utilizadas as definições abaixo como referências para padronização e uniformização dos conceitos quanto a valores envolvidos.

Para que seja efetuada a análise dos impactos quando da materialização dos Riscos, foram aplicadas as seguintes métricas:

- Alto: Comprometerá todo o faturamento da empresa ou com prejuízos similares, inviabilizando a continuidade da empresa;
- Significativo: Comprometerá parcialmente o faturamento da empresa ou com prejuízos similares, colocando a empresa em um processo de restauração demorado;
- Moderado: Comprometerá a empresa no nível médio de seu faturamento ou similar, porém, com fatores rápidos de restauração;
- Baixo: Comprometerá a empresa em valores que não afetam significativamente seus resultados;
- Insignificante: Comprometerá a empresa com necessidade de esforço para recuperação, mas sem impactos financeiros relevante.

Analise das probabilidades para materialização dos Riscos:

- Quase Certo: Certamente ocorrerá na maioria das vezes;
- Provável: Provavelmente ocorrerá na maioria das vezes;
- Possível: Deverá ocorrer alguma vez;
- Remoto: Poderá ocorrer alguma vez;
- Raro: Poderá ocorre somente em circunstâncias excepcionais.

3.4 – Definição das Causas e Consequência dos Riscos

Com base nas análises dos riscos, é necessário avaliar quais as causas que podem fazer com que o risco se materialize, e com sua materialização qual será a consequência envolvida. As causas e consequências serão utilizadas para nortear a definição do impacto e probabilidade do risco envolvido.

3.5 – Definição do Risco Inerente

Para a avaliação destes valores, a equipe de tecnologia da informação foi indagada quanto às incidências e possíveis consequências que envolvem o impacto e a probabilidade de ocorrência.

Para avaliação dos riscos inerentes, é considerado como se o risco não possuísse nenhum controle para redução da probabilidade ou impacto, ficando a critério dos fatos a possibilidade de materialização dos riscos.

3.6 – Definição dos Controles vinculados aos Riscos

Os controles são instrumentos para garantir que as atividades sejam executadas de forma eficaz, possibilitando que os riscos inerentes sejam reduzidos por ter alterado o nível da probabilidade de ocorrência para materialização.

Os controles possibilitam reduzir a probabilidade de ocorrência da materialização do risco, quando o risco ainda encontrar-se em um nível de exposição não aceitável pela organização, novos controles devem ser criados para reduzir ainda mais a probabilidade de ocorrência.

Os controles podem ser categorizados das seguintes formas:

- Preventivos: Atuam de forma a prevenir que o risco seja materializado;
- Detectivos: Atuam de forma a identificar alguma situação que tenha ocorrido e que possa materializar a ocorrência do risco;
- Automáticos: São controles que estão operantes independentes da intervenção de pessoas, sendo basicamente operados por sistemas automatizados;
- Manuais: São controles executados por pessoas, onde o colaborador é responsável por identificar situações que não possuem um comportamento esperado.

3.7 – Definição do Risco Residual

O risco residual é a disposição do risco após a aplicação dos controles. Para a avaliação destes valores, a equipe de tecnologia da informação foi indagada quanto às incidências e possíveis consequências que envolvem o impacto e probabilidade de ocorrência após a aplicação dos controles. Os controles acabam por reduzir a probabilidade de materialização do risco.

Para avaliação do risco residual os controles exercem forte interferência na navegação do risco entre risco inerente e residual. Para isso, destacamos abaixo, em sequência de efetividade a interferência dos controles no risco:

- Controle Automático e Preventivo: É o melhor tipo de controle, por reduzir de forma significativa e automática a probabilidade de ocorrência;
- Controle Automático e Detectivo: Poderá reduzir a probabilidade de ocorrência, porém, identificar uma situação após sua materialização, dependendo de alguma ação para mitigar o risco;
- Controle Manual e Preventivo: Reduzirá de forma significativa desde que seja executado de forma eficaz, porém, por ser manual, acaba por possibilitar falhas em sua execução;
- Controle Manual e Detectivo: É o controle com menor eficiência, pois, dependerá da execução de forma eficaz, e posteriormente desencadear uma nova ação para mitigar o risco.

3.8 – Tratamento dado ao Risco Residual

O tratamento do risco se dá após a definição dos riscos residuais, neste ponto deve ser avaliado se a empresa está confortável com a situação e exposição a qual seus processos estão incluídos.

A empresa poderá atribuir aos riscos os seguintes tratamentos:

- Reduzir: Para reduzir o risco deverão ser criados novos controles, ou melhorados os existentes, para garantir que a probabilidade de ocorrência seja reduzida;
- Transferir: A transferência do risco se dá quando a empresa não deseja mais conviver com o risco, e para isso, transfere para outra empresa sua administração, tendo como exemplo um seguro que cubra os impactos quando da materialização dos riscos;
- Aceitar: A decisão por aceitar o risco se dá quando a empresa opta por não implementar novos controles, acabando por conviver com o risco com os níveis de impacto e probabilidade vigente.

3.9 – Planos de Ação

Os planos de ação são utilizados quando a situação em que o risco residual está não possibilita que a empresa esteja confortável, desta forma, faz-se necessária a definição de ações que contribuam para reduzir a probabilidade ou impacto da materialização do risco. Os planos de ação estão voltados aos riscos com necessidades de redução ou transferência.

Quando da redução, serão desenhados novos controles ou redesenhados os controles existentes, visando aumentar sua eficiência.

Quando da transferência, a ação será por encontrar um meio de garantir que dada uma ocorrência de materialização do risco, os valores de impactos estejam segurados de alguma forma.

Argumentar nesta seção o que foi realizado no estudo. Por exemplo, Local da pesquisa ou local do estudo (caracterização do local da pesquisa), tipo de pesquisa ou técnicas de pesquisa, variáveis investigadas, instrumentos utilizados na coleta de dados, entre outros. Esta seção deverá ser organizada a critério do pesquisador e do orientador, conforme o tipo de pesquisa.

4 – RESULTADOS E DISCUSSÃO

Com base na metodologia desenhada no capítulo 3, foi aplicado junto aos responsáveis pela área de tecnologia da informação os modelos desenhados, onde foram obtidos os resultados a seguir.

4.1 – Contextualização

Destacamos abaixo as definições para missão e visão, definidos no manual de organização empresarial, considerando que as estratégias de Tecnologia da Informação devem estar conectadas às estratégias da o planejamento:

- **Missão:**

> *"Prover e manter soluções e serviços de tecnologia da informação e comunicação que satisfaçam as necessidades dos clientes e suportem a evolução dos negócios."*

- **Visão:**

> "*Em 2018...Ser reconhecida pela excelência em soluções e serviços de tecnologia da informação e comunicação.*"

4.2 – Definição dos Objetivos

Após a contextualização, foram definidos os objetivos da área de tecnologia, considerando os domínios do *CobIT* como forma de identificação e organização:

Domínio	Objetivo
Planejar e Organizar	Assegurar a aderência das funções de TI às necessidades do Negócio
Adquirir e Implementar	Assegurar que as alterações sejam efetuadas de forma devida com o uso eficiente dos recursos de TI.
Entregar e Suportar	Assegurar o processamento das informações de forma correta e garantindo a integridade
Monitorar e Avaliar	Assegurar a continuidade dos serviços de TI e o sigilo das informações

4.3 – Definição dos Riscos

Os riscos foram avaliados visando possibilitar aos executivos de tecnologia da informação uma visão estratégica e gerencial dos riscos mais relevantes para os processos. A visão possibilita demonstrar de forma simplificada qual processo de tecnologia deve ser atacado considerando seu nível de exposição ao risco. Os riscos foram definidos, com base nas informações dos objetivos identificando os fatores que poderiam expor os processos de tecnologia da informação.

4.3.1 – Planejar e Organizar:

Código	Descrição do Risco
01	Incapacidade ou não adequação da área de Tecnologia da Informação para atender ao plano estratégico, acarretando perdas para o Negócio da Empresa.

4.3.2 – Adquirir e Implementar:

Código	Descrição do Risco
02	Implementações ou mudanças de sistemas efetuadas de forma não autorizada, inconsistente, fraudulenta ou irregular, acarretando perdas para a empresa.

4.3.3 – Entregar e Suportar:

Código	Descrição do Risco
03	Processamento indevido, incompleto, duplicado ou com erros, na execução de programas ou transações, acarretando prejuízo ao negócio da empresa.
04	Indisponibilidade dos recursos tecnológicos ou humanos, acarretando interrupções em atividades de TI com impacto nos negócios.

4.3.4 – Monitorar e Avaliar

Código	Descrição do Risco
05	Extravio ou divulgação indevida ou não autorizada de informações corporativas, acarretando perdas para o Negócio.

4.4 – Definição das Causas e Consequência dos Riscos

Com base nas análises dos riscos, foram avaliadas as causas poderão materializar o risco quando da sua ocorrência, e a respectiva consequência envolvida.

4.4.1 – Risco 01: Incapacidade ou não adequação da área de Tecnologia da Informação para atender ao plano estratégico, acarretando perdas para o Negócio da Empresa.

#	Descrição das Causas
A	1. O Plano diretor de Investimento para a área de tecnologia da informação é criado sem o vínculo com o plano estratégico corporativo; 2. A área de Tecnologia não acompanha a evolução tecnológica.
	Descrição das Consequências
	1. A falta de vínculo entre o plano diretor de investimento e o planejamento estratégico corporativo possibilita que as ações de tecnologia da informação não estejam aderentes às necessidades que serão provisionadas pelo negócio; 2. A falta de evolução acaba por deixar a área de tecnologia da informação com recursos obsoletos.

4.4.2 – Risco 02: Implementações ou mudanças de sistemas efetuadas de forma não autorizada, inconsistente, fraudulenta ou irregular, acarretando perdas para a empresa.

#	Descrição das Causas
B	1. Ausência de metodologia para desenvolvimento e alteração de sistemas com as devidas fases que devem ser seguidas durante o processo de construção e implementação; 2. Ausência de avaliação do código antes da efetivação em produção, garantindo *workflow* de aprovação para documentações obrigatórias e segregação de funções entre desenvolvimento e efetivação em produção; 3. Ausência de controles na aquisição de aplicações suporte para apoio ao negócio.
	Descrição das Consequências
	1. A falta de uma metodologia de desenvolvimento que defina as etapas com suas respectivas entradas e saídas, alçada de aprovação e revisões, acaba por ocasionar que rotinas sejam implementadas de forma indevida, causando erro e gerando indisponibilidade ao negócio; 2. A falta de avaliação do código, de forma segregada, antes da efetivação possibilita que erros não sejam identificados ou que códigos maliciosos sejam inseridos para prejudicar o negócio; 3. A falta de avaliação das aquisições de soluções propicia que sejam agregados ao parque tecnológico serviços e softwares incompatíveis com as plataformas existentes.

4.4.3 – Risco 03: Processamento indevido, incompleto, duplicado ou com erros, na execução de programas ou transações, acarretando perdas ou danos ao negócio da empresa.

#	Causa
C	1. Ausência de procedimentos definindo as rotinas e sua sequência de execução, definindo o acompanhamento e registro do início e Fim; 2. Ausência de controle de acesso para execução de rotinas em ambiente de produção; 3. Ausência de controle de execução de rotinas em duplicidade ou que

	foram interrompidas por iniciativa administrativa ou por falha; 4. Ausência de controles de documentação quando da execução, falha e ações tomadas na execução das rotinas.
	Consequência
	1. A falta de procedimentos que definam a sequência de execução das rotinas e ação a tomar em cada etapa, possibilita o desencadeamento de erros nas rotinas; 2. A falta de controles de acesso possibilita que um usuário não autorizado possa executar indevidamente rotinas em ambiente de produção; 3. A falta de controles de execução possibilita que rotinas sejam executadas de forma incompleta ou em duplicidade; 4. A falta de documentação da execução das rotinas impossibilita a identificação quanto à execução de sua totalidade ou detalhamento das ações tomadas para solucionar o problema.

4.4.4 – Risco 04: Indisponibilidade dos recursos tecnológicos ou humanos, acarretando interrupções em atividades de TI com impacto nos negócios.

#	Causas
D	1. Indisponibilidades dos serviços gerados pelas seguintes ocorrências: i. Desastres naturais ou de terrorismo no ambiente tecnológico; ii. Falta de energia elétrica para provimento dos serviços; iii. Ataques por vírus ou hackers no ambiente corporativo; 2. Ausência de capital humano adequado para prover os serviços de tecnologia; 3. Falha técnica nos equipamentos de Tecnologia da Informação e comunicação.
	Consequência

	1. A ausência de controles focados na detecção e tratamento de incidentes (desastres, terrorismo, falta de energia, vírus ou hackers) pode causar a parada na execução dos serviços com prejuízo ao negócio; 2. A ausência de capital humano qualificado poderá gerar instabilidade por não possuir os conhecimentos adequados para manter o ambiente tecnológico; 3. A falha nos equipamentos poderá impactar na recuperação e restauração do ambiente para suporte ao ambiente de negócios

4.4.5 – Risco 05: Extravio ou divulgação indevida ou não autorizada de informações corporativas, acarretando perdas para o Negócio.

#	**Causa**
E	1. Ausência de política formal de segurança da informação e procedimentos que determinem as regras referentes à segurança da informação; 2. Ausência de controle de acesso eficaz ao ambiente com as informações críticas; 3. Ausência de classificação dos ativos de informação e métodos de controle quanto à disseminação de informações dentro e fora do ambiente corporativo; 4. Ausência de controles de tráfego de informações (firewall / DLP - Data Lost Prevention) para controlar o acesso e trânsito de dados no âmbito corporativo.
	Consequência

	1. A falta de política e procedimentos formais para segurança da informação possibilita que não exista convergência nas tratativas que devem ser dadas às informações corporativas; 2. A falta de controles de acesso eficazes possibilita que usuários não autorizados tenham acesso a dados críticos da empresa; 3. A falta de classificação dos ativos da informação possibilita que as informações sejam divulgadas sem a devida restrição quanto ao público que deve tomar ações ou apenas conhecimento; 4. A falta de controles de tráfego de informações (firewall / DLP - Data Lost Prevention) possibilita que as informações críticas sejam divulgadas ou extraviadas sem a autorização devida ou rastreabilidade da forma em que foi divulgada.

4.5 – Definição do Risco Inerente

O risco inerente é à disposição do risco sem a existência de controles, para esta avaliação foi solicitado aos responsáveis por tecnologia da informação um grande esforço para avaliar o risco sem a existência dos controles existentes, e assim dimensionar qual será o nível de exposição ao risco com base na probabilidade e impacto.

4.5.1 – Risco 01: Incapacidade ou não adequação da área de Tecnologia da Informação para atender ao plano estratégico, acarretando perdas para o Negócio da Empresa.

Classificação do Risco Inerente		
Grau	**Probabilidade**	**Impacto**
	Quase Certo	**Significativo**
Classificação	**Alto**	
Justificativa	Caso não exista uma forte atuação da área de tecnologia da informação para integrar suas ações ao planejamento corporativo, há grande probabilidade de desvios dos investimentos. Dada à dependência da empresa nos recursos de TIC o alinhamento com o negócio deve estar pronto para atender as demandas e não impactar no crescimento.	

4.5.2 – Risco 02: Implementações ou mudanças de sistemas efetuadas de forma não autorizada, inconsistente, fraudulenta ou irregular, acarretando perdas para a empresa.

Classificação do Risco Inerente		
Grau	**Probabilidade**	**Impacto**
	Provável	**Significativo**
Classificação	**Alto**	
Justificativa	O processo de desenvolvimento é crítico por tratar todos os processos da empresa, considerando que podem ocorrer falhas neste processo que poderão desestabilizar ou prejudicar o ambiente. A ausência de controles neste risco possibilita que rotinas sejam implementadas de forma indevida, podendo gerar grandes impactos financeiros para os negócios, considerando que os sistemas corporativos são responsáveis por pagamentos, serviços, faturamento, contabilidade, tributação etc., caso existam erros, poderá haver impactos significativos, além de ser um ambiente suscetível a fraudes dada a possibilidade de intervenção de forma sigilosa em dados corporativos.	

4.5.3 – Risco 03: Processamento indevido, incompleto, duplicado ou com erros, na execução de programas ou transações, acarretando perdas ou danos ao negócio da empresa.

.Classificação do Risco Inerente		
Grau	**Probabilidade**	**Impacto**
	Provável	**Significativo**
Classificação	**Alto**	
Justificativa	O processamento sem controles pode ocasionar na duplicidade de processamento ou que seja executado de forma parcial, gerando falhas no processo e informações errôneas. A Execução em duplicidade pode gerar desembolsos financeiros indevidos atribuindo impacto significativo às falhas no processo.	

4.5.4 – Risco 04: Indisponibilidade dos recursos tecnológicos ou humanos, acarretando interrupções em atividades de TI com impacto nos negócios.

.Classificação do Risco Inerente		
Grau	**Probabilidade**	**Impacto**

	Provável	**Alto**
Classificação	**Alto**	
Justificativa	Em virtude da quantidade de variáveis que pode ocasionar a interrupção dos serviços é provável que o risco se materialize e devido à dependência da empresa nos serviços de TI para faturamento, pagamentos e demais serviços corporativos.	

4.5.5 – Risco 05: Extravio ou divulgação indevida ou não autorizada de informações corporativas, acarretando perdas para o Negócio.

.Classificação do Risco Inerente		
Grau	**Probabilidade**	**Impacto**
	Possível	**Alto**
Classificação	**Alto**	
Justificativa	O ativo de informação é considerado como grande valor, tanto na tomada de decisões quanto no sigilo de dados críticos para o mercado acionário.	

4.5.6 – Matriz de exposição dos Riscos: A matriz abaixo demonstra a disposição dos riscos na matriz de riscos inerentes:

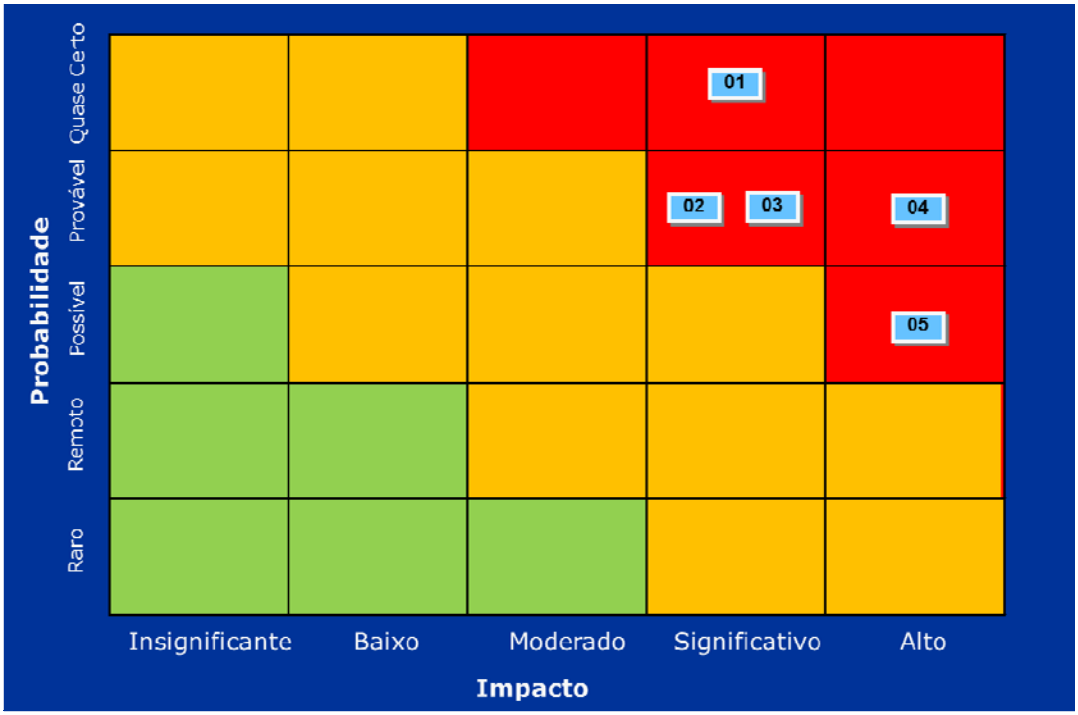

Figura 05 – Matriz de Riscos Inerentes

4.6 – Definição dos Controles vinculados aos Riscos

Os controles são instrumentos para garantir que as atividades sejam executadas de forma eficaz, possibilitando que os riscos inerentes sejam reduzidos por ter alterado o nível da probabilidade de ocorrência para materialização.

4.6.1 – Risco 01: Incapacidade ou não adequação da área de Tecnologia da Informação para atender ao plano estratégico, acarretando perdas para o Negócio da Empresa.

Código	Descrição do Controle	Redução Probabilidade %
A01	Quando da criação do Plano Diretor de Tecnologia da Informação (PDTI) é efetuado o vínculo com o Planejamento Estratégico.	20
A02	Os projetos de Tecnologia devem estar vinculados ao Plano Diretor de Tecnologia da Informação.	20
A03	Toda demanda de projeto de Tecnologia é aprovado pelo Grupo de Gestão de Mudanças, onde é avaliada sua aderência à estratégia da empresa.	50

4.6.2 – Risco 02: Implementações ou mudanças de sistemas efetuadas de forma não autorizada, inconsistente, fraudulenta ou irregular, acarretando perdas para a empresa.

Código	Descrição do Controle	Redução Probabilidade %
B01	O processo de alteração e desenvolvimento de sistemas é definido em metodologia própria que se evidencia em um sistema suporte.	10
B02	O processo de desenvolvimento exige workflow de aprovação nas etapas críticas: • Solicitação; • Desenho dos Requisitos; • Desenvolvimento dos códigos; • Testes Individuais e Integrados; • Homologação; • Treinamento; • Aceitação Formal da unidade solicitante; • Implantação em ambiente de produção após a validação de todas as etapas anteriores; • Monitoramento pós-implantação.	30

B03	O acesso dos analistas de sistemas é restrito ao ambiente de desenvolvimento, não possibilitando que as alterações sejam efetuadas diretamente em produção, garantindo assim a segregação de funções no ambiente.	20
B04	A aquisição de novas aplicações deve estar amparada pelo parecer da área de tecnologia da informação, garantindo sua aderência ao ambiente corporativo e continuidade.	10

4.6.3 – Risco 03: Processamento indevido, incompleto, duplicado ou com erros, na execução de programas ou transações, acarretando perdas ou danos ao negócio da empresa.

Código	Descrição do Controle	Redução Probabilidade %
C01	As rotinas pontuais executadas em produção devem possuir uma solicitação formal onde seja definido o motivo da execução.	10
C02	As rotinas executadas periodicamente em produção possuem controle de data e começo / fim de sua execução. Quando identificadas falhas no processo é aberto chamado para execução da análise.	30
C03	O acesso para execução de rotinas está restrito à equipe de suporte.	10

4.6.4 – Risco 04: Indisponibilidade dos recursos tecnológicos ou humanos, acarretando interrupções em atividades de TI com impacto nos negócios.

Código	Descrição do Controle	Redução Probabilidade %
D01	Caso ocorra desastres naturais ou terrorismo no ambiente tecnológico, há um plano de recuperação de desastres que prevê o restabelecimento das operações a partir de um backup site em até 03 horas.	35
D02	Caso ocorra falta de energia elétrica, o centro de processamento de dados tem condições de operar a partir de geradores que suportam os processos corporativos.	15

D03	O ambiente corporativo está configurado com firewalls que asseguram a rede corporativa e todos os servidores internos.	10
D04	O ambiente corporativo está configurado com antivírus atualizado em todos os servidores e estações de trabalho, assegurando a atualização periódica.	05
D05	A área de tecnologia da informação possui contrato com uma fábrica de software para suportar os picos de demanda para desenvolvimento ou falta de capital humano.	15
D06	A manutenção, preventiva ou por falha, e executada por empresa contratada com níveis de atendimento de serviço, além de possuir redundância para as atividades mais críticas, como: • Servidores de Aplicação • Servidores de banco de dados críticos; • Conexões com Redes Públicas;	10

4.6.5 – Risco 05: Extravio ou divulgação indevida ou não autorizada de informações corporativas, acarretando perdas para o Negócio.

Código	Descrição do Controle	Redução Probabilidade %
E01	O acesso aos dados é controlado através de formalização de concessão e revisão de acesso periódica.	10
E02	O uso de e-mail pessoal é restrito ao corpo gerencial da empresa	05
E03	O ambiente corporativo está configurando com firewalls que asseguram o acesso externo a rede corporativa e todos os servidores possuem antivírus atualizado instalado.	10

4.7 – Definição do Risco Residual

O risco residual é foi avaliado com base nos controles existentes e que estejam em operação, considerando que sua análise tem como princípio testes

periódicos efetuados pela área de Auditoria Interna, assim, um controle poderá ser vinculado à matriz apenas após o teste quanto a sua eficiência, para garantir a característica do controle para reduzir a probabilidade de materialização do risco.

4.7.1 – Risco 01: Incapacidade ou não adequação da área de Tecnologia da Informação para atender ao plano estratégico, acarretando perdas para o Negócio da Empresa.

Classificação do Risco Inerente		
Grau	**Probabilidade**	**Impacto**
	Raro	**Significativo**
Classificação	**Moderado**	
Justificativa	O vínculo entre o Plano Diretor de Tecnologia da Informação ao Planejamento estratégico garante a aderência entre Tecnologia e Negócios.	

4.7.2 – Risco 02: Implementações ou mudanças de sistemas efetuadas de forma não autorizada, inconsistente, fraudulenta ou irregular, acarretando perdas para a empresa.

Classificação do Risco Residual		
Grau	**Probabilidade**	**Impacto**
	Remoto	**Moderado**
Classificação	**Moderado**	
Justificativa	A metodologia de desenvolvimento padroniza e define os documentos obrigatórios, mitigando os projetos com maior materialidade, porém, faz-se necessário o desenho de solução para manutenções corretivas e avaliação de códigos fontes antes da efetivação em ambiente de produção.	

4.7.3 – Risco 03: Processamento indevido, incompleto, duplicado ou com erros, na execução de programas ou transações, acarretando perdas ou danos ao negócio da empresa.

Classificação do Risco Residual		
Grau	**Probabilidade**	**Impacto**
	Possível	**Significativo**
Classificação	**Moderado**	
Justificativa	Os controles de agendamento e execução de rotina garantem sua integridade, porém, é necessário melhorar os controles de monitoramento dos acessos executados por usuários com permissão para iniciar rotinas em ambiente de produção.	

4.7.4 – Risco 04: Indisponibilidade dos recursos tecnológicos ou humanos, acarretando interrupções em atividades de TI com impacto nos negócios.

.Classificação do Risco Residual		
Grau	**Probabilidade**	**Impacto**
	Raro	**Alto**
Classificação	**Moderado**	
Justificativa	Dado os controles de Backup site, segurança e contingências para prover serviços de infraestrutura e capital humano terceirizado.	

4.7.5 – Risco 05: Extravio ou divulgação indevida ou não autorizada de informações corporativas, acarretando perdas para o Negócio.

.Classificação do Risco Residual		
Grau	**Probabilidade**	**Impacto**
	Possível	**Alto**
Classificação	**Alto**	
Justificativa	Os controles existentes não mitigam de forma satisfatória os riscos, devem ser implementados controles para avaliar as informações corporativas.	

4.7.6 – Matriz de exposição dos Riscos Residuais: A matriz abaixo demonstra a disposição gráfica dos riscos na matriz de riscos:

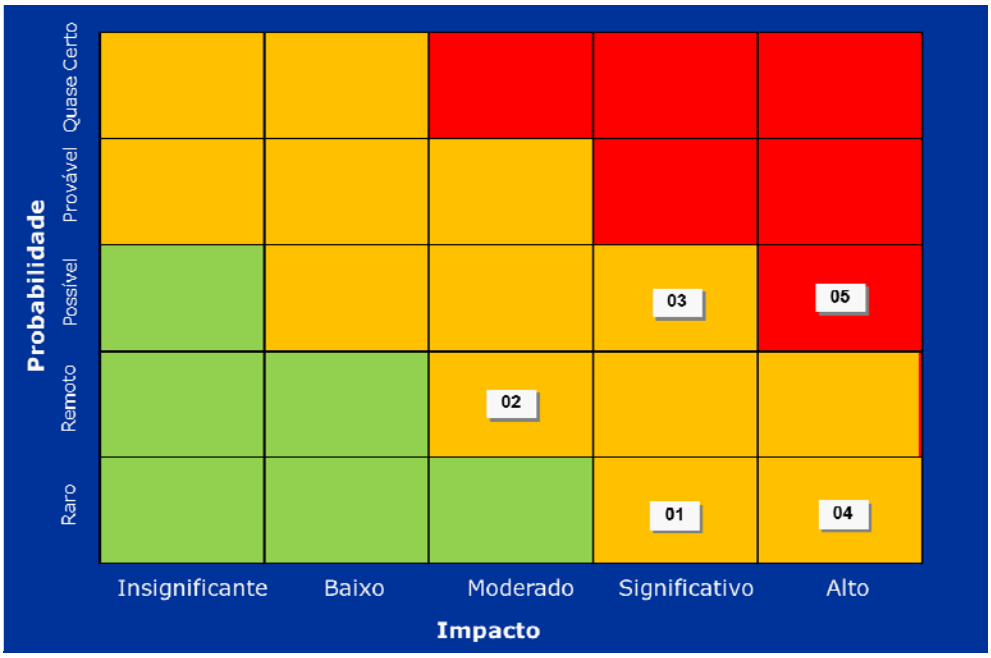

Figura 06 – Matriz de Riscos Residuais

4.7.7 – Matriz de navegação dos Riscos: A matriz de navegação dos riscos demonstra a disposição gráfica dos riscos inerentes e residuais em uma única matriz de riscos, este gráfico possibilita demonstrar qual foi a evolução das tratativas dadas aos riscos, contribuindo claramente para a avaliação das tratativas dos riscos:

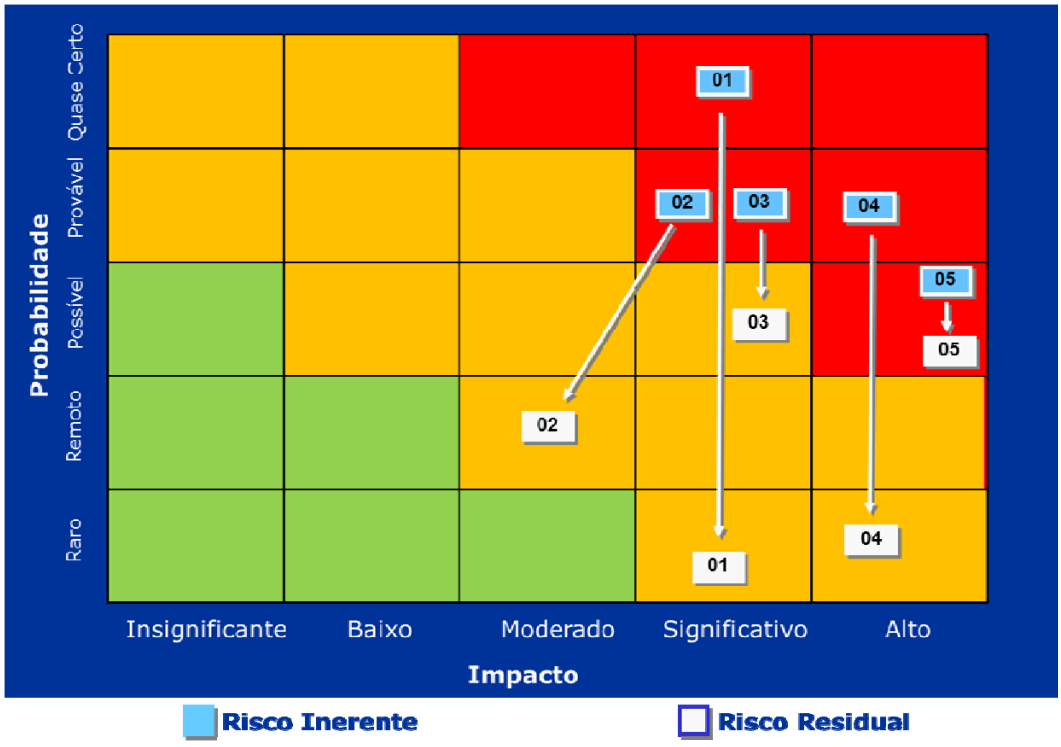

Figura 07 – Matriz de navegação dos Riscos

4.8 – Tratamento dado ao Risco Residual

O tratamento do risco se dá após a definição dos riscos residuais, neste ponto deve ser avaliado se a empresa está confortável com a situação e exposição a qual seus processos estão incluídos.

4.8.1 – Risco 01: Incapacidade ou não adequação da área de Tecnologia da Informação para atender ao plano estratégico, acarretando perdas para o Negócio da Empresa.

Classificação	**Moderado**	**Tratamento**	**Manter**

4.8.2 – Risco 02: Implementações ou mudanças de sistemas efetuadas de forma não autorizada, inconsistente, fraudulenta ou irregular, acarretando perdas para a empresa.

Classificação	**Moderado**	**Tratamento**	**Reduzir**

4.8.3 – Risco 03: Processamento indevido, incompleto, duplicado ou com erros, na execução de programas ou transações, acarretando perdas ou danos ao negócio da empresa.

Classificação	**Moderado**	**Tratamento**	**Reduzir**

4.8.4 – Risco 04: Indisponibilidade dos recursos tecnológicos ou humanos, acarretando interrupções em atividades de TI com impacto nos negócios.

Classificação	**Moderado**	**Tratamento**	**Manter**

4.8.5 – Risco 05: Extravio ou divulgação indevida ou não autorizada de informações corporativas, acarretando perdas para o Negócio.

Classificação	**Alto**	**Tratamento**	**Reduzir**

4.9 – Planos de Ação

Os planos de ação foram definidos pela área de tecnologia da informação com foco em reduzir o risco residual. Estas ações foram necessárias quando a administração entendeu que o nível de exposição ao risco continuou alto após os controles. Na definição do controle houve o cuidado por parte da gestão em não onerar as equipes com atividades que não representassem avanço na mitigação do risco.

4.9.1 – Risco 01: Incapacidade ou não adequação da área de Tecnologia da Informação para atender ao plano estratégico, acarretando perdas para o Negócio da Empresa.

- Para este risco não houve a decisão de reduzir o risco

4.9.2 – Risco 02: Implementações ou mudanças de sistemas efetuadas de forma não autorizada, inconsistente, fraudulenta ou irregular, acarretando perdas para a empresa.

- Apesar de bons controles voltados a metodologia de desenvolvimento e sistema suporte, faz-se necessário desenhar as seguintes ações para reduzir a probabilidade de ocorrência:
    a) Implementar ação para garantir que as manutenções corretivas sejam controladas pelo sistema suporte ao desenvolvimento;
    b) Implementar controle para avaliar os códigos dos sistemas antes da efetivação em produção, buscando identificar códigos maliciosos;

4.9.3 – Risco 03: Processamento indevido, incompleto, duplicado ou com erros, na execução de programas ou transações, acarretando perdas ou danos ao negócio da empresa.

- Apesar de bons controles voltados a agendamento de atividades, faz-se necessário desenhar as seguintes ações para reduzir a probabilidade de ocorrência:
    a) Implementar controle de monitoramento para usuários com perfil para executar rotinas em ambiente de produção;

4.9.4 – Risco 04: Indisponibilidade dos recursos tecnológicos ou humanos, acarretando interrupções em atividades de TI com impacto nos negócios.

- Para este risco não houve a decisão de reduzir o risco

4.9.5 – Risco 05: Extravio ou divulgação indevida ou não autorizada de informações corporativas, acarretando perdas para o Negócio.

- Os controles existentes não mitigam totalmente o risco, sendo necessário implementar as seguintes ações para controle das informações:
    a) Restringir o acesso para armazenar dados em dispositivos de armazenamento portáteis;
    b) Controlar o tráfego de conteúdos na rede através de ferramenta de análise de conteúdo;
    c) Limitar o acesso apenas ao e-mail corporativo para todo o corpo de empregado;
    d) Implementar política de segurança de informação e procedimentos que norteiem o acesso a dados críticos, com foco em:
        i. Classificação e ciclo de vida dos ativos de informação;
        ii. Critérios de concessão e revisão dos acesso;
        iii. Ciclo de vida dos usuários corporativos;
    e) Implementar formulário de responsabilidade a ser assinado por empregados e terceirizados;
    f) Avaliar periodicamente as vulnerabilidades de invasão e acesso a dados críticos;
    g) Implementar processo de treinamento contínuo para conscientização quanto à segurança da informação.

5 – CONSIDERAÇÕES FINAIS E SUGESTÃO

As análises demonstraram que para os principais riscos do ambiente geral de tecnologia da informação há controles que contribuem para mitigar e reduzir o nível de exposição dos riscos, conforme matriz de navegação demonstrada.

Apesar dos controles reduzirem o nível de exposição, alguns riscos ainda necessitam de ações para que novos controles sejam implementados e assim o seu nível de exposição seja aceitável pela administração.

Como sugestão para trabalhos futuros há de se destacar a necessidade de explorar todos os riscos do ambiente geral de tecnologia da informação, mapeando dos riscos estratégicos até os riscos operacionais, identificando as causas, consequências e controles, validando assim as suas correlações.

Outra sugestão de pesquisa é elabora um método para identificar os impactos dos riscos que envolvem serviços de tecnologia da informação, estabelecendo um método para definição de métrica, tendo como base as informações contábeis da empresa.

6 – CONCLUSÃO

O gerenciamento de risco demonstrou ser uma ferramenta eficaz para materializar as preocupações de Tecnologia da Informação e atribuir o gerenciamento para que ações sejam tomadas antes que os riscos se concretizem, ressaltando que atualmente grande parte dos processos estão informatizados e por algumas vezes o comprometimento de um risco de tecnologia da informação pode comprometer um risco de negócio.

Gerenciar os riscos de tecnologia da informação tem como objetivo não só garantir os processos de tecnologia, mas também ser uma ferramenta para demonstrar a importância do ambiente de tecnologia para a organização. Assim, gerenciar riscos não é uma atividade pontual, mas sim contínua e cíclica.

REFERÊNCIAS

ABNT, NBR ISO 27000 – Sistemas de Gerenciamento de Segurança da Informação, Brasil: ABNT, 2012.

ABNT, NBR ISO 31000 – Princípios e Diretrizes do Gerenciamento de Riscos, Brasil: ABNT, 2012.

ANDRADE, Armando – Controles Internos: Eficácia, eficiência e Economicidade: como atingi-las através de adequados sistemas de controles internos. São Paulo: Petrobrás, 1999.

COBIT 4.1, Control Objectives for Information and related Technology, EUA: ISACA, 2011.

COSO, Committee Of Sponsoring Organizations of the Treadway Commission. Internal Control – Integrated Framework. Executive Summary,EUA:COSO, 2009.

GLEIM, CIA I – Certified Internal Auditor part I, EUA: Institute of Internal Auditors - IIA, 2012.

GLEIM, CIA II – Certified Internal Auditor part II, EUA: Institute of Internal Auditors - IIA, 2012.

GLEIM, CIA III – Certified Internal Auditor part III, EUA: Institute of Internal Auditors - IIA, 2012.