FUNDAÇÃO PEDRO LEOPOLDO

MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO

Gilberto Barbosa Mota

CONTRIBUIÇÃO DA GESTÃO DO CONHECIMENTO PARA OS PROCESSOS DE ANÁLISE E GESTÃO DE RISCOS APLICADOS À GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO:

ESTUDO DE CASO EM UMA ORGANIZAÇÃO DO SETOR DE SAÚDE

Pedro Leopoldo

2012

Gilberto Barbosa Mota

CONTRIBUIÇÃO DA GESTÃO DO CONHECIMENTO PARA OS PROCESSOS DE ANÁLISE E GESTÃO DE RISCOS APLICADOS À GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO:

ESTUDO DE CASO EM ORGANIZAÇÃO DO SETOR DE SAÚDE

Dissertação apresentada ao Programa de Mestrado Profissional em Administração das Faculdades Integradas de Pedro Leopoldo como requisito parcial para a obtenção do grau de Mestre em Administração.

Área de Concentração: Gestão da Inovação e Competitividade.

Linha de Pesquisa: Inovação e Organizações

Orientador: Prof. Dr. Jorge Tadeu de Ramos Neves

Pedro Leopoldo

2012

DEDICO ESTE TRABALHO

Aos meus Pais, Antônio e Lêda, exemplos de luta constante, que não esmorecem diante das dificuldades e que são verdadeiros guias de meus passos terrenos em busca de evolução, dedico este trabalho pela preocupação em relação a uma educação de qualidade e pelo carinho e apoio incondicional, constante e ininterrupto;

À minha esposa, Renata, pela compreensão em minhas inúmeras ausências, e por ter sido Mãe e Pai de nosso filho durante este período;

Especialmente dedico este trabalho ao meu querido e amado filho, Arthur, este pequeno ser de luz, paz e amor, que apesar da pouca idade, e mesmo sem saber, é o maior incentivador deste e de outros tantos trabalhos desenvolvidos neste período. Muito obrigado por ter escolhido a mim para guiar seus passos e assim evoluirmos juntos.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por mais esta oportunidade de evolução.

Ao meu orientador Professor Dr. Jorge Tadeu de Ramos Neves, pela dedicação nas disciplinas lecionadas e por sua orientação e transferência contínua de conhecimento;

Agradeço à Professora Dra. M. Celeste R. L. Vasconcelos, pela paciência e dedicação ao lecionar a Disciplina “Seminários de Dissertação”, pois a disciplina foi crucial para que esta pesquisa tomasse um rumo adequado.

Agradeço ao amigo Professor Dr. Max do Val Machado, pelo incentivo pela conclusão desta pesquisa e aos projetos acadêmicos, além das constantes indicações e acompanhamentos na PUC MINAS;

Agradeço ao Professor Dr. Bernardo Jeunon de Alencar pela confiança depositada em mim ao me permitir lecionar disciplinas cruciais para o bom andamento do Curso de Sistemas de Informação da PUC MINAS e por me incentivar a concluir esta etapa.

Também, agradeço à organização pesquisada, que abriu suas portas para o desenvolvimento desta pesquisa.

“Ninguém pode voltar atrás e fazer um novo começo. Mas qualquer um pode recomeçar e fazer um novo fim"

(Chico Xavier)

RESUMO

Esta pesquisa apresenta as contribuições da gestão do conhecimento para a governança de tecnologia da informação, com foco nos processos de análise e gerenciamento de risco de tecnologia da informação em uma organização do setor de saúde. Nesta organização, a gestão do conhecimento e análise e gestão de risco são praticadas com o objetivo de estabelecer melhorias dos processos de tecnologia da informação, contribuindo para que a organização apresente-se com diferencial competitivo neste segmento, na cidade de Belo Horizonte. A base teórica desta pesquisa está direcionada para as abordagens de gestão do conhecimento e governança de tecnologia da informação, com foco no processo de analisar e gerenciar riscos de tecnologia da informação. A pesquisa, desenvolvida através de estudo de caso, no qual profissionais da Diretoria de Tecnologia da Informação da organização foram entrevistados, conclui que as ações de gestão do conhecimento contribuem para os processos de analisar e gerenciar riscos de tecnologia da informação, apresentando as ações praticadas e os resultados obtidos. Destacam-se, como resultados obtidos, o uso das ações de gestão do conhecimento para planejar as ações de análise de risco, considerando os processos de negócio, os sistemas que suportam estes processos de negócio e os ativos de tecnologia da informação que suportam estes sistemas.

ABSTRACT

This research presents the contributions of knowledge management for information technology governance, focusing on the analysis and risk management of information technology in an organization of the health sector. In this organization, knowledge management and analysis and risk management are practiced in order to establish process improvement of information technology, contributing to the organization forward with competitive advantage in this segment in the city of Belo Horizonte. The theoretical basis of this research is directed to the approaches of knowledge management and governance of information technology, focusing on the process of analyzing and managing risks of information technology. The research, developed through a case study, in which professionals from the Information Technology Board of the organization were interviewed, concludes that the actions of knowledge management contribute to the processes of analyzing and managing risks of information technology, presenting the actions taken and the results obtained. Remarkable, as the results obtained, the use of knowledge management activities to plan the actions of risk assessment, considering business processes, systems that support these business processes and information technology assets that support these systems .

LISTA DE QUADROS

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Esta pesquisa tem como objetivo apresentar quais são as ações de gestão do conhecimento implementadas em uma empresa de planos de saúde do Estado de Minas Gerais, bem como as contribuições dessas ações no processo de governança de tecnologia da informação. Essas ações foram definidas pelo *Control Objectives for Information and Related Technology* (COBIT), considerando-se o processo de avaliar e gerenciar os riscos de tecnologia da informação, processo este integrante do modelo de governança de tecnologia da informação implementado na organização estudada.

Conforme Davenport e Prusak (1998), gestão do conhecimento é um processo estratégico, contínuo e dinâmico que visa gerar o capital intangível da empresa e todos os pontos estratégicos objetivando estimular a conversão do conhecimento, apresentado como o modelo de conversão do conhecimento. A gestão do conhecimento passou a ser vista como inovação nas organizações, conforme apresentado por Alvarenga Neto (2008). O autor afirma que, com as ações de gestão do conhecimento, uma nova forma de olhar e pensar a organização é exigida. Entretanto, em seus estudos, afirma que muitas organizações, de forma contundente, divulgam que exercem internamente um processo de gestão do conhecimento, mas, na realidade, percebe-se que essas organizações aplicam ações de gestão da informação.

Esta pesquisa ainda utiliza como referência, os estudos de Nonaka e Takeuchi (1997), que apresentam os benefícios para as organizações que utilizam os conceitos da gestão do conhecimento, ao apresentarem casos de sucesso de grandes empresas que trabalharam de forma coordenada e não desvinculada destes modelos de conhecimento.

Os estudos de Davenport e Prusak (1999) também são considerados nesta pesquisa, por serem referência para diversos outros estudos. Além disso, os autores apresentam uma correlação para entendimento teórico da formação do conhecimento, extraído dos dados e das informações.

Outros autores, como Nascimento e Neves (1999), são importantes para demonstrar o constante crescimento do tema gestão do conhecimento.

Sobre governança de tecnologia da informação, esta pesquisa apresenta estudos realizados por Sallé (2004) que mostram que os processos de governança de tecnologia da informação são essenciais para ressaltar nas organizações o diferencial competitivo, tendo em vista que a tecnologia da informação é fator essencial para os processos organizacionais. Além disso, Alvarenga Neto (2008) acrescenta que a informação e o conhecimento são os únicos fatores capazes de fortalecer as competências essenciais das organizações e contribuir para a consolidação da vantagem competitiva.

Rezende (2008) afirma que um processo de governança de tecnologia da informação é fator primordial para alavancar qualidade na prestação de serviços de tecnologia da informação, objetivando atender com excelência as necessidades das áreas de negócio das organizações. Tecnologia da informação é a atividade fundamental para sustentar os processos de qualquer organização. Os departamentos que coordenam essas ações, nas organizações, seguem critérios de qualidade e eficiência, aplicando os melhores e mais modernos recursos, normas e padrões de mercado, além de buscarem, incansavelmente, por inovações tecnológicas, objetivando atender seus clientes de maneira exemplar, conforme apresentado nos estudos de Rezende (2008).

Sallé (2004) relata que a tecnologia da informação tem adotado modelos administrativos de estruturação que implicam, necessariamente, na modificação da forma de atuar dos profissionais dessa área, que devem dominar a incorporar novos conhecimentos sobre processos de gestão de tecnologia da informação a fim de adaptarem os novos processos à realidade das organizações.

Outros estudos, a exemplo dos de Sallé (2004), mostram que as organizações estão cada vez mais inclinadas a estabelecer um processo de governança de tecnologia da informação como forma de melhoria da gestão de suas atividades, além de estarem comungando com as definições de planejamento estratégico das organizações.

Portanto, ações de gestão do conhecimento e governança de tecnologia da informação são, para as organizações, fatores primordiais de sucesso e de vantagem competitiva. Em seus relatos, Rodriguez (2002) que afirma que a tecnologia da informação, considerada na década de 1970 e 1980 como um mal necessário, passou a ser, no final do século XX uma ferramenta fundamental em qualquer organização que busca diferencial competitivo.

Esta pesquisa conta, ainda, com análises em documentos internos da organização pesquisada, abordando as ações de gestão do conhecimento, com foco nas ações de criação, disseminação, compartilhamento e criação do conhecimento, além de ações de criação de condições para que este conhecimento seja criado, disseminado e compartilhado. Esta pesquisa ainda conta com análise dos processos de analisar e gerenciar riscos tecnologia da informação. Espera-se, com essa ação, obter-se uma visão clara e reflexões sobre os temas gestão do conhecimento e governança de tecnologia da informação na organização pesquisada.

Considerando-se que as contribuições para o modelo de governança de tecnologia da informação, pela adoção de práticas de gestão do conhecimento na organização pesquisada, não são conhecidas, acredita-se que a compreensão dessas contribuições pode ser valiosa para ações efetivas no processo de governança de tecnologia da informação.

Assim, a questão norteadora deste estudo situa-se, basicamente na seguinte pergunta:

Quais são as contribuições da gestão do conhecimento para a governança de tecnologia da informação, com foco na análise e gerenciamento de risco de tecnologia da informação em uma empresa do setor de saúde?

1.1. Objetivos

A partir desta indagação e visando o desenvolvimento desta dissertação, foram estabelecidos e assumidos os seguintes objetivos:

Objetivo Geral:

Identificar as contribuições da gestão do conhecimento para o processo avaliar e gerenciar os riscos de tecnologia da informação, parte integrante do modelo de governança de tecnologia da informação na organização pesquisada, a partir da adoção de práticas efetivas de gestão do conhecimento.

Objetivos Específicos:

a) Analisar, através da literatura, a teoria de gestão do conhecimento, governança de tecnologia da informação e o COBIT;

b) Apresentar as práticas de gestão do conhecimento adotadas na organização pesquisada;

c) Apresentar e analisar as características do modelo de governança de tecnologia da informação, considerando-se o processo de análise e gestão de risco de tecnologia da informação, da organização pesquisada;

d) Identificar as possíveis contribuições da gestão do conhecimento para o processo avaliar e gerenciar os riscos de tecnologia da informação, parte integrante do modelo de governança de tecnologia da informação da organização pesquisada.

1.2. Justificativas

Conforme Rezende (2008), a governança de tecnologia da informação é fator de qualidade na prestação de serviços de tecnologia da informação. Considerando-se os estudos de Nonaka e Takeuchi (1997), que afirmam que as ações de gestão do conhecimento são primordiais para o sucesso de qualquer organização - inclusive apresentando estudos de casos de sucesso de grandes empresas - e que ações de gestão do conhecimento nas organizações são combustíveis para a inovação e gestão estratégica, esta pesquisa justifica-se, para a organização pesquisada, pois proporcionará `a mesma conhecer as contribuições da gestão do

conhecimento para o modelos de governança de tecnologia da informação, impactando em suas ações de gestão estratégica.

Este estudo justifica-se, ainda, para o pesquisador, por ser profissional atuante na área de tecnologia da informação, por aproximados 17 anos, com ações diretas em governança de tecnologia da informação, atuando diretamente como gestor de tecnologia da informação e segurança da informação.

Justifica-se, finalmente, para a academia, por ser um tema que pode despertar novos interesses e, assim, motivar novos estudos relacionados à gestão do conhecimento e à governança de tecnologia da informação.

2. REFERENCIAL TEÓRICO

O referencial teórico, objetiva apresentar e discutir os principais conceitos que envolvem esta pesquisa e desenvolver um esquema completo e suficiente para a análise dos resultados obtidos. Este referencial teórico aborda conceitos sobre Gestão do Conhecimento, Governança de Tecnologia da Informação, COBIT, Processo de Avaliar e Gerenciar Riscos de Tecnologia da Informação e por fim apresenta a contribuição deste referencial teórico para a pesquisa.

2.1. Gestão do Conhecimento

Parece ser algo simples definir gestão do conhecimento. No entanto, há uma grande diversidade de conceitos, sobretudo devido ao fato de que o assunto ainda é recente. Além disso, verifica-se significativa variedade de ferramentas de tecnologia da informação veiculadas com o apelo de embutirem soluções de gestão do conhecimento entre suas oferecidas funcionalidades.

Para se ter uma idéia da abrangência ou das diversas interpretações acerca do termo gestão do conhecimento, em pesquisa apresentada por Nascimento e Neves (1999), foram identificados os principais *sites* da World Wide Web que discutem o tema gestão do conhecimento, através dos quais obteve-se, como resultado, diversas referências sobre o assunto.

Os estudos de Wilson (2002) apresentam grande e constante crescimento das publicações com a expressão “gestão do conhecimento” em *sites* de empresas de consultoria, análise da literatura e apresentações institucionais de escolas de negócio, sendo possível se identificar diversas interpretações sobre gestão do conhecimento nesses estudos.

Choo (2002) afirma que o objetivo geral da gestão do conhecimento é a concepção da estratégia organizacional, sua estrutura, processos e sistemas para

que a organização possa usar o que ela sabe para criar valor para seus clientes e para a sociedade.

A gestão do conhecimento pode ser entendida, conforme os estudos apresentados por Sveiby (2000), como a arte de criar valor a partir da alavancagem dos ativos intangíveis de uma organização, considerando que os ativos intangíveis são constituídos, basicamente, de competências, relacionamentos e informações.

De acordo com Davenport e Prusak (1998), a gestão do conhecimento leva as organizações a mensurar, com mais segurança, a sua eficiência, a tomar decisões acertadas com relação à melhor estratégia a ser adotada em relação aos seus clientes, concorrentes, canais de distribuição e ciclos de vida de produtos e serviços, a saber identificar as fontes de informação, a saber administrar dados e informações e a saber gerenciar seus conhecimentos. Trata-se da prática de agregar valor à informação e de distribuí-la.

Para Nonaka e Takeuchi (1997), a gestão do conhecimento pode ser entendida como o processo sistemático de identificação, criação, renovação e aplicação dos conhecimentos que são estratégicos na vida de uma organização. Os autores apresentam ainda, em suas pesquisas, resultados obtidos por empresas como a IBM, CANON, HONDA entre outras, que obtiveram sucesso em seus processos de negócio aplicando os conceitos da gestão do conhecimento. Afirmam que as empresas orientais, como a HONDA e CANON, exploram e acreditam fortemente no conhecimento tácito, enquanto empresas ocidentais como a IBM valorizam o conhecimento explícito. Indiferentemente das valorizações em torno da tipificação dos conhecimentos, os sucessos são experimentados constantemente.

Contrapondo os estudos apresentados por Nonaka e Takeuchi (1997) e Davenport e Prusak (1998), Senge (1990) afirma que as empresas são incapazes de funcionar como organizações baseadas no conhecimento. Seguindo esta linha, Stewart (2002), afirma que as organizações apresentam gasto excessivo em programas de gestão do conhecimento e que falham por não descobrirem qual é o conhecimento de que necessitam e como administrá-lo.

Os resultados da pesquisa de Alvarenga Neto (2008) levaram-no a concluir que as organizações praticavam, na verdade, a gestão estratégica da informação,

afirmando desenvolverem programas de gestão do conhecimento. Afirma ainda que, apesar de toda a polêmica e controvérsia a respeito do termo gestão do conhecimento, os resultados de sua pesquisa demonstram que a área conhecida como gestão do conhecimento tem surpreendido aqueles que apostaram em um modismo e tem se estabelecido como um consistente paradigma gerencial nas organizações.

Contudo, Alvarenga Neto (2008) relata que a gestão do conhecimento vai além dos conceitos de gestão da informação, tendo em vista que, grande parte do que se convenciona chamar gestão do conhecimento é, na verdade, gestão da informação.

Diversos outros autores apresentam estudos sobre gestão do conhecimento, porém os conceitos são similares e seguem mesma linha de pensamento.

Autores como Malhotra (1998), Ovum (1998) e Senge (1990) foram pesquisados no intuito de enriquecer este estudo e apresentar as diversas linhas seguidas sobre o assunto.

Malhotra (1998, p. 1) apresenta o seguinte conceito para gestão do conhecimento:

> "A gestão do conhecimento supre os aspectos críticos da adaptação, sobrevivência e competência das organizações diante da mudança ambiental crescente e descontínua. Essencialmente, ela incorpora processos organizacionais que buscam a combinação sinérgica da capacidade de processamento de dados e de informações dos seres humanos."

Ovum (1998) confirma que a gestão do conhecimento é a tarefa de desenvolver e explorar os recursos de conhecimento tangíveis e intangíveis da organização e considera que a gestão do conhecimento cobre questões organizacionais e tecnológicas, apoiando-se em tecnologias da informação e em ações de gestão da informação.

Para Choo (2002), a gestão da informação nasce nas organizações através das necessidades de informação, estabelecendo-se, assim, um processo de aquisição, organização e distribuição da informação. O autor conclui que a

informação deve ser distribuída para a pessoa certa, sendo este o fator primário de atenção nas ações de gestão da informação.

Conforme Marchand e Davenport (2004), a gestão da informação tem como objetivo melhorar o acesso à distribuição de informação e permite dar suporte às operações existentes, nas organizações, voltadas para a disseminação e compartilhamento de informação. Ainda afirmam que gestão da informação tem foco altamente tecnológico e considera que a coleta, tratamento e disseminação da informação devem ser automatizados, necessitando irrestritamente de ferramentas de tecnologia da informação.

Conforme Nonaka e Takeuchi (1997, p.56) “informação é um meio necessário e material para extrair e construir o conhecimento”. Contudo, compreende-se que gerir a informação é um processo de gerir a extração e construção do conhecimento. Afirmam que a informação pode ser encarada sob duas perspectivas:

a) **Informação Sintática:** relacionada com o volume das informações;

b) **Informação Semântica:** relacionada com o significado das informações.

Esses autores consideram que o aspecto semântico é mais importante para a criação do conhecimento, pois dá foco ao significado transmitido pela informação. Contudo, ao se considerar apenas o aspecto sintático, corre-se o risco de não conseguir captar a importância real da informação no processo de criação do conhecimento.

Contudo, Nonaka e Takeuchi (1997) consideram que o conhecimento é criado através de fluxos de informação que, por sua vez, são criados por fluxos de mensagens, cujo conhecimento ancora-se nas crenças e no compromisso de seu portador. Reitera, ainda, que a criação do conhecimento utiliza como insumo a informação que, por sua vez, ancora-se em tecnologia para sua gestão.

A tecnologia da informação é recurso fundamental para a agilidade, efetividade, sucesso ou êxito da organização, conforme relatado por Rezende (2008). Independentemente do tamanho das organizações, a tecnologia da informação se apresenta como fator indispensável, tendo em vista a necessidade de relação com o meio externo ao da organização. O autor conceitua tecnologia da

informação como sendo recursos tecnológicos e computacionais objetivando a guarda, geração e uso da informação e do conhecimento.

2.2. Organizações baseadas no conhecimento

Davenport e Prusak (1998) relatam, em seus estudos, que a única vantagem sustentável que as organizações possuem é aquilo que elas, de forma coletiva, sabem e a eficiência com que elas usam o que sabem, bem como a prontidão com que elas adquirem e usam novos conhecimentos.

Para Stewart (1998), a vantagem obtida com o conhecimento abre possibilidades para a organização sustentar-se diante de suas necessidades de competitividade. Essa vantagem se torna sustentável, de acordo com Davenport e Prusak (1998), que sugerem métodos úteis para que a informação seja transformada em conhecimento, objetivando ações para vantagens competitivas, tais como:

a) **Comparação:** de que maneiras as informações relativas a essa situação se comparam a outras situações conhecidas?

b) **Conseqüências:** que implicações essas informações trazem para as decisões e tomadas de ação?

c) **Conexões:** quais as relações desse novo conhecimento com o conhecimento já acumulado?

d) **Conversação:** o que as outras pessoas pensam dessa informação?

Como estratégias para melhor realizar a transferência do conhecimento, Davenport e Prusak (1999) sugerem as reuniões face a face, o rodízio de executivos e o estímulo a bate-papos informais.

Fleury e Oliveira Jr. (2010) relatam que os gerentes atuais estão conscientes de que a extensão, a profundidade e o escopo do conhecimento e das habilidades da empresa impulsionam, crescentemente, suas chances competitivas. Os autores afirmam, ainda, que lidar com incertezas, apresentadas pela competição, baseadas no conhecimento, exige que as empresas desenvolvam:

a) um sentido claro sobre si mesmas, suas forças e fraquezas;

b) habilidade de enfrentar e de gerenciar os riscos de maior dependência de outros.

Um dos ativos organizacionais intangíveis mais importantes, sob diversos pontos de vista, conforme relatos de Fleury e Oliveira Jr (2010), é o conhecimento organizacional. Os autores afirmam e complementam que, no enfoque organizacional, os conhecimentos de cada um dos colaboradores de uma empresa bem como o que está presente nas cadeias de relacionamento internas e externas à organização influenciam a maneira de se realizar negócios, estruturar ou remodelar os processos inerentes ao funcionamento das estruturas organizacionais vigentes e tomar decisões. Nessa linha, Davenport e Prusak (1998) confirmam a importância do conhecimento como fonte primária para as ações de tomada de decisão nas organizações.

Davenport e Prusak (1998) complementam que as decisões organizacionais não devem ser tomadas apenas considerando dados ou informações. Os autores afirmam isso, considerando-se que os dados são informações não estruturadas, com uma visão simplista dos estados do mundo e que informações são esses dados, porém com relevância e propósito identificados e definidos e que o conhecimento é a relação processada dessas informações na mente humana.

Em suas pesquisas, Choo (2002) contribui para se compreender as distinções entre dado, informação e conhecimento, considerando que devam ser definidos como, processamento, gestão, ação, resultado, aprendizagem. Ressalta que o resultado do gerenciamento desse processo é a capacitação organizacional para ações que possam gerar os resultados desejados para a organização.

Para Nonaka e Takeuchi (1997, p. 56), conhecimento e informação têm diferenças e semelhanças, e afirmam:

> “O conhecimento, ao contrário da informação, é sobre crenças e compromissos... O conhecimento, ao contrário da informação, é sobre ação... O conhecimento como a informação, é sobre significado. É específico ao contexto e relacional.”

Sveiby (1998) relata que o conhecimento é a informação mais valiosa, visto que exige análise, síntese, reflexão e contextualização e define o conhecimento como a capacidade de agir. Infere-se, imediatamente, que o conhecimento é extremamente valioso, além de ser fator determinante para as definições estratégicas organizacionais para se obter vantagens competitivas, desde que a gestão do conhecimento seja feita de forma adequada dentro das organizações.

2.3. Criando Conhecimento nas Organizações

Alvarenga Neto (2008) afirma que a criação do conhecimento nas organizações é feita através de crenças verdadeiras e justificadas, portanto, o conhecimento, ao ser criado, está carregado de crenças pessoais.

Davenport e Prusak (1999, p. 110) relatam que *"*na economia regida pelo conhecimento, conversar é trabalhar". Os autores tecem críticas às ações organizacionais que evitam o encontro das pessoas presencialmente, relatando, como exemplo, os escritórios virtuais, reiterando que os encontros entre os profissionais, fora da organização, devem ser amplamente estimulados. Afirmam que a presença dos profissionais em congressos, feiras e fóruns devem, também, ser estimulados como forma de aumentar a relação de aprendizado e parceria entre profissionais e organizações. Neste sentido, Nonaka e Takeuchi (1997, p.12) consideram a gestão do conhecimento como um processo interativo de criação do conhecimento organizacional, definindo-a como "a capacidade que uma empresa tem de criar conhecimento, disseminá-lo na organização e incorporá-lo a produtos, serviços e sistemas"

Considerando-se a dinâmica nos processos de gestão das organizações, criar conhecimento passa a ser fator fundamental e crucial para o crescimento e posicionamento das organizações perante a sociedade. Nonaka e Takeuchi (1997) afirmam que a organização processa a informação do ambiente externo, transformando-a em conhecimento, para se adaptar a novas circunstâncias.

Os autores afirmam, ainda, que se espera que o processo de criação do conhecimento e o processo de administração da criação desse conhecimento tenham atenção especial, no ambiente organizacional, considerando a importância

desses processos e concluem afirmando que o processo de criação do conhecimento, nas organizações, passa por duas dimensões:

a) Dimensão Ontológica

O conhecimento é criado apenas pelo indivíduo. Uma organização não pode criar conhecimento sem o indivíduo. O processo de criação do conhecimento deve ser entendido como um processo amplificador de conhecimento já criado pelo indivíduo e os cristaliza como parte da rede de conhecimento da organização.

b) Dimensão Epistemológica

Nesta dimensão, Nonaka e Takeuchi (1997) definem o conhecimento tácito e o conhecimento explícito. O conhecimento tácito é pessoal e específico ao contexto, por isso, difícil de formalizar e comunicar; o conhecimento explícito, ou codificado, refere-se ao conhecimento que é transmissível na linguagem formal e sistemática.

Seguindo esta linha, Davenport & Prusak (1998) conceituam conhecimento explícito e tácito como:

- **Explícito:** É o conhecimento que está registrado de alguma forma e assim disponível para as demais pessoas.
- **Tácito:** É o conhecimento que as pessoas possuem, mas não está descrito em nenhum lugar, residindo apenas em suas “cabeças”.

Nonaka e Takeuchi (1997, p. 19) afirmam que o conhecimento explícito pode ser expresso em palavras, números ou sons, podendo ser compartilhado e facilmente transferido entre os indivíduos. Sobre o conhecimento tácito, afirmam que não é facilmente visível ou explicável, é altamente pessoal e difícil de visualizar.

> O conhecimento tácito está profundamente enraizado nas ações e na experiência corporal do indivíduo, assim como nos ideais, valores ou emoções que ele incorpora.

Conforme relatado por Nonaka e Takeuchi (1997), o conhecimento tácito ainda se divide em duas dimensões:

- **Técnica:** Engloba as habilidades informais e de difícil detecção, muitas vezes captadas no termo Know-how

- **Cognitiva:** Consiste em crenças, percepções, idéias, valores, emoções e modelos mentais tão inseridos em nós que os consideramos naturais.

Para Nonaka e Takeuchi (1997) o conhecimento tácito e subjetivo é um processo inerente à experiência do indivíduo, adquirido ao longo do tempo pelo acúmulo de informações referentes ao contexto vivido. O conhecimento explícito, ou objetivo, é o conhecimento da racionalidade, conhecimento que está ao alcance do indivíduo, dentro de um determinado contexto vivenciado, bastando ser resgatado. Além disso, os autores partem do pressuposto de que o conhecimento é criado através da interação entre o conhecimento tácito e o explícito e apresentam quatro modos para conversão do conhecimento, conforme FIGURA 1.

FIGURA 1 – Modelo de conversão do conhecimento

Fonte: Nonaka e Takeuchi, 1997, p. 60.

a) Socialização: de tácito para tácito

É um processo de compartilhamento de experiências, gerando a criação de conhecimento tácito, através de reuniões com visões detalhadas, objetivando solução de determinado problema, interação com clientes e fornecedores, além da interação entre colaboradores da organização. A chave para aquisição do conhecimento tácito é a experiência compartilhada.

b) Externalização: de tácito para explícito

É um processo de articulação do conhecimento tácito em conceitos explícitos. Basicamente, é visto como um processo de criação de conceitos que é desencadeado pelo diálogo e pela reflexão coletiva, que freqüentemente é usado para criar um conceito e combinar a dedução e a indução. Consiste, ainda, na utilização seqüencial da metáfora, analogia e modelos, possibilitando a criação de conceitos explícitos.

c) Combinação: de explícito para explícito

É um processo de sistematização de conceitos em um sistema de conhecimento. Envolve a combinação de diferentes corpos de conhecimento explícito, tais como a troca de conhecimento através de documentos, reuniões, conversas telefônicas ou redes de comunicação.

d) Internalização: de explícito para tácito

É um processo de incorporação do conhecimento explícito em conhecimento tácito, intimamente ligado ao “aprender fazendo”. O processo de verbalização ou diagramação em documentos, manuais ou relatos orais, ajuda na internalização do conhecimento.

Nonaka e Takeuchi (1997) relatam que quando o conhecimento tácito e o explícito interagem, tem-se um processo emergente de inovação e que o processo de criação do conhecimento organizacional é uma interação contínua e dinâmica entre o conhecimento tácito e o explícito. Contudo, Nonaka e Takeuchi (1997) concluem que o conhecimento não é tácito ou explícito. O conhecimento exibe forma paradoxal, pois o tácito se apresenta como oposto do explícito e vice versa. O conhecimento é tanto tácito quanto explícito. Concluem, ainda, não ser possível afirmar que o conhecimento seja formado de uma forma ou de outra, mas pode-se afirmar que o conhecimento é formado através de uma comunhão entre os conhecimentos tácitos ou explícitos existentes em uma organização. Concluem, também, que o conhecimento é produto de informação, que são geradas através dos processos de negócio das organizações.

Por fim, os autores afirmam que o processo de criação do conhecimento de uma organização deve considerar o preparo do ambiente para que o conhecimento possa ser criado, compartilhado e disseminado. Em primeira instância, a organização precisa mostrar intenção em promover a criação do conhecimento e que esta intenção deve ser considerada no planejamento estratégico da organização.

> "Para criar conhecimento, as organizações de negócios devem favorecer o comprometimento de seus empregados, formulando uma intenção organizacional e a propondo a eles." (NONAKA & TAKEUCHI, 1997, p.72)

Para Nonaka e Takeuchi (1997), a organização deve permitir que os indivíduos possam agir de forma autônoma, até onde as circunstâncias permitirem, objetivando a criação de novos conhecimentos, visto que a autonomia aumenta a possibilidade de motivação dos indivíduos para a criação de novos conhecimentos.

Ainda no âmbito da promoção do conhecimento nas organizações, espera-se que a organização estabeleça como condição dessa promoção, a interação entre a organização e o ambiente externo. No entender de Nonaka e Takeuchi (1997), esse é o processo de "decomposição" de rotinas, hábitos ou estruturas cognitivas.

Outra exigência para a promoção do conhecimento é a redundância, que não deve ser entendida como duplicação desnecessária da informação, mas, sim, como a existência de informação que vai além das exigências operacionais imediatas dos membros da organização.

> Compartilhar informações extras também auxilia os indivíduos a entenderem sua posição dentro da organização, o que por sua vez, funciona para controlar a direção tanto do raciocínio quanto das ações individuais. (NONAKA & TAKEUCHI, 1997, p.79)

O requisito de variedade é outra exigência para promover conhecimento na organização, conforme relato de Nonaka e Takeuchi (1997), citando Ashby (1956),

> A diversidade interna de uma organização precisa combinar com a complexidade do ambiente a fim de lidar com os desafios apresentados pelo mesmo... Os membros de uma organização podem enfrentar muitas contingências se possuírem os requisitos variedade, que pode ser realçado pela combinação de informações de maneira diferente, flexível e rápida, além de oferecer também igual acesso a informação em toda organização. (ASHBY (1956) apud NONAKA & TAKEUCHI, 1997, p.80)

2.4. Governança de Tecnologia da Informação

Para se entender o que vem a ser governança de tecnologia da informação é preciso apresentar o conceito de governança corporativa do Instituto Brasileiro de Governança Corporativa (IBGC). O conceito mostra que é o sistema através do qual as sociedades são dirigidas e monitoradas, envolvendo os relacionamentos entre acionistas/cotistas, conselho de administração, diretoria, auditoria independente e conselho fiscal. As boas práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para a sua perenidade.

Rezende (2008) confirma que a governança permite uma maior agilidade operacional além de resposta eficiente e rápida em relação às demandas. Obtêm-se um modelo eficiente de gestão, através dos controles propostos. Esse modelo de gestão causa impactos para as áreas de negócio e de tecnologia da informação.

Ainda seguindo Rezende (2008), a governança está ligada diretamente às responsabilidades dos gestores das organizações, considerando ainda que está fundamentada em pessoas, processos e tecnologia assegurando a sustentação das estratégias da organização e seus objetivos pela tecnologia da informação. Afirma ainda que os recursos de governança de tecnologia da informação não garantem o sucesso das ações de tecnologia da informação, considerando ainda que adaptações para a realidade de cada organização devem ser feitas, de acordo com as respectivas capacidades tecnológica, financeira e humana.

Conforme Weill e Ross (2006, p. 8), governança de tecnologia da informação significa estabelecer quem pode tomar decisões e como essas decisões podem ser tomadas.

> Governança de tecnologia da informação: É a especificação dos direitos decisórios e do framework de responsabilidades para estimular comportamentos desejáveis na utilização.

A complexidade e dificuldade de explicar a governança de tecnologia da informação é uma das mais sérias barreiras ao seu aprimoramento, relatam Weill & Ross (2006). Em seus estudos, apresentam que o melhor indicador de desempenho para a governança de tecnologia da informação é a porcentagem de administradores em cargos de liderança capazes de descrevê-la.

Um grande número de iniciativas de tecnologia da informação experimenta fracassos em proporcionar resultados essenciais esperados pelas organizações, conforme estudos apresentados por Weill e Ross (2006). Os autores afirmam que o valor de negócios de tecnologia da informação resulta diretamente de uma governança de tecnologia da informação eficaz.

As pesquisas de Weill e Ross (2006) revelam que empresas com governança de tecnologia da informação madura apresentam lucros, no mínimo, 20% maiores que as empresas com má governança, considerando os mesmos objetos estratégicos. Afirmam, ainda, que somente 38% da alta gerência consegue descrever, com precisão, sua governança de tecnologia da informação.

Nessa definição de governança de tecnologia da informação, os mesmos autores afirmam que o objetivo principal é capturar sua simplicidade, em direitos e responsabilidades, e capturar sua complexidade, em comportamentos desejáveis que são específicos de empresa para empresa.

Contudo, pode-se entender governança de tecnologia da informação como um braço da governança corporativa, conforme relato do IT Governance Institute (2002). A governança de tecnologia da informação é responsabilidade da alta administração e consiste de uma estrutura organizacional, processos e lideranças para garantir que a tecnologia da informação sustente e auxilie as estratégias e os objetivos da organização.

> Governança de tecnologia da informação é uma parte integral da Governança Corporativa e é formada pela liderança, estruturas organizacionais e processos que garantem que a tecnologia da informação sustenta e melhora a estratégia e objetivos da organização (IT GOVERNANCE INSTITUTE, 2002, p. 78)

Rezende (2008) afirma que governança de tecnologia da informação não deve ser entendida como ações de definições de indicadores. Essa afirmação é

confirmada pelo IBGC ao afirmar que, um dos grandes equívocos é conceituar governança de tecnologia da informação como um conjunto de indicadores, ou como um processo de gestão de portfólio dos projetos estratégicos.

Para Vieira (2004), a governança de tecnologia da informação é um conjunto de processos e estruturas objetivando garantir que a tecnologia da informação dê suporte e maximize adequadamente os objetivos e estratégias do negócio da organização, adicionando valores aos serviços entregues, balanceando os riscos e obtendo o retorno sobre os investimentos. Ainda afirma que a governança de tecnologia da informação está relacionada a dois focos: o valor dos serviços de tecnologia da informação para o negócio e a mitigação dos riscos de tecnologia da informação.

O valor dos serviços tem seu embasamento no alinhamento estratégico entre tecnologia da informação e o negócio; a mitigação dos riscos tem suporte em como as responsabilidades estão divididas dentro das empresas e como deveremos nos antever aos riscos de cada tarefa, completa Vieira (2004).

2.4.1. Áreas de Foco na Governança de Tecnologia da Informação

O modelo de governança de tecnologia da informação tem como focos os processos de alinhamento estratégico organizacional e os processos de gestão de risco, permitindo entendimento sobre gestão de recursos, grandes impactantes e impactados por ações de tecnologia da informação.

Conforme estudos apresentados por Gama e Martinello (2006), é foco fundamental da governança de tecnologia da informação a mensuração de desempenho, possibilitando tratar as entregas determinadas. A figura 2 ilustra as áreas de foco na governança de tecnologia da informação com os respectivos detalhamentos.

FIGURA 2 – Áreas de foco da governança de tecnologia da informação
Fonte: Adaptado de Weill & Ross (2004)

a) **Alinhamento estratégico:** foca em garantir a ligação entre os planos de negócios e de tecnologia da informação, definindo, mantendo e validando a proposta de valor de tecnologia da informação, alinhando as operações de tecnologia da informação com as operações da organização.

b) **Entrega de valor:** é a execução da proposta de valor de tecnologia da informação através do ciclo de entrega, garantindo que tecnologia da informação entrega os prometidos benefícios previstos na estratégia da organização, concentrado-se em otimizar custos e provendo o valor intrínseco de tecnologia da informação.

c) **Gestão de recursos:** refere-se à melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de tecnologia da informação: aplicativos, informações, infraestrutura e pessoas. Questões relevantes referem-se à otimização do conhecimento e da infraestrutura.

d) **Mensuração de desempenho:** acompanha e monitora a implementação da estratégia, término do projeto, uso dos recursos, processo de *performance* e entrega dos serviços, usando-se, por exemplo, *balanced scorecards* que traduzem as estratégias em ações para atingir os objetivos, medidos através de processos contábeis convencionais.

e) Gestão de risco: requer a preocupação com riscos pelos funcionários mais experientes da corporação, um entendimento claro do apetite de risco da empresa e dos requerimentos de conformidade, transparência sobre os riscos significantes para a organização e inserção do gerenciamento de riscos nas atividades da companhia.

Weill e Ross (2004) propõem que a governança de tecnologia da informação eficaz para as estratégias corporativas deve focar três questões básicas:

a) Quais decisões devem ser tomadas para garantir a gestão e o uso eficazes de TI?

b) Quem deve tomar essas decisões?

c) Como essas decisões serão tomadas e monitoradas?

A governança de tecnologia da informação eficaz deixa explícito o aprendizado e difunde, por toda a empresa, as práticas definidas. Tais práticas, conforme relato de Weill e Ross (2006), podem ser entendidas como *framework* de melhores práticas, permitindo que cada organização defina suas práticas, conforme suas estratégias e necessidades.

De acordo como IBGC, os *frameworks* são um conjunto de boas práticas que visam auxiliar na solução de problemas, principalmente ligados à governança de tecnologia da informação. Um dos mais abrangentes e bem aceitos *frameworks* para governança de tecnologia da informação é o *Control Objectives for Information and Related Technology* (COBIT).

2.4.2. Control Objectives for Information and Related Technology - COBIT

Weill e Ross (2006) relatam que o COBIT foi desenvolvido na década de 1990 pela Information System Audit and Control Association (ISACA), e pode ser traduzido como objetivos de controle para a informação e tecnologia. Essa metodologia é composta por três modelos: Modelo de Processos, Modelo de Governança de TI e Modelo de Maturidade.

Os autores afirmam ainda que o objetivo do COBIT é sugerir boas práticas através de um *framework* de domínios e processos e apresentar atividade em uma estrutura lógica gerenciável. Essas práticas visam ajudar a aperfeiçoar a tecnologia da informação, habilitando investimentos, garantindo a entrega de serviços, além de prover sua mensuração. Os autores concluem que o COBIT tenta garantir a governança de tecnologia da informação, provendo um *framework* que garanta quatro aspectos principais:

a) Tecnologia da informação esteja alinhada com o negócio;

b) Tecnologia da informação torne o negócio possível e maximize seus benefícios;

c) Os recursos de TI sejam utilizados com responsabilidade;

d) Os riscos associados a tecnologia da informação sejam gerenciados de maneira apropriada.

O IBGC conceitua o COBIT como relato de melhores práticas para o gerenciamento da tecnologia da informação e seus ativos, seus processos e suas necessidades. Relata ainda que essas atividades são de responsabilidade dos gestores de tecnologia da informação.

> COBIT pode ser entendido como um guia para a gestão e controle dos objetivos das atividades relacionadas com unidade tecnológica da informação nas organizações. O referido guia sugere o compartilhamento de boas práticas por meio de uma estrutura de framework lógica e flexível (REZENDE, 2008. p.136).

Rezende (2008) enfatiza que as boas práticas sugeridas no COBIT podem contribuir para o direcionamento dos investimentos em tecnologia da informação, assegurar a entrega de produtos e mensurar ações corretivas de erros e métricas para avaliação dos resultados. Apresenta, ainda, o objetivo principal do COBIT que é tratar a necessidade de mensurar e avaliar os domínios de gestão de uma organização.

O IBGC complementa que o objetivo inicial do COBIT foi estabelecido para processos de auditoria e, posteriormente, tornou-se, também, uma ferramenta de gestão da área de tecnologia da informação e de alinhamento estratégico para

ajudar a entender e a gerenciar os riscos e benefícios associados à tecnologia da informação.

Conforme COBIT (2006), o *framework* foi projetado para a utilização de três públicos distintos:

a) **Administradores ou gestores de tecnologia da informação:** auxiliando na avaliação e mensuração entre os riscos e investimentos nos controles aplicáveis ao ambiente de tecnologia da informação;

b) **Usuários:** auxilia na garantia de segurança e nos controles dos serviços de tecnologia da informação, fornecidos pela equipe interna ou por prestadores de serviços;

c) **Auditores:** auxilia no subsídio de informações e opiniões e também aconselham os administradores sobre os controles internos e seus objetivos.

2.4.3. Estrutura do COBIT

O COBIT (2006) apresenta a estrutura do *framework*, composto por quatro domínios, 34 objetivos e 215 objetivos de controle detalhados. No nível mais elevado, estão os quatro domínios, que são agrupamentos de processos conforme sua natureza. Os domínios do COBIT são:

a) **Planejamento e Organização:** abrange estratégias e táticas, apontando os caminhos para que a tecnologia da informação possa dar maior contribuição para a obtenção dos objetivos de negócio.

b) **Aquisição e Implementação:** visa realizar a estratégia de tecnologia da informação através da identificação de soluções necessárias, utilizando o desenvolvimento ou aquisição para implementá-las e integrá-las aos processos do negócio.

c) **Entrega e Suporte:** foca os produtos reais dos serviços requeridos, desde operações tradicionais de segurança e aspectos de continuidade, até o suporte efetivo.

d) Monitoração: controla os processos de tecnologia da informação que devem ser avaliados, regularmente, nos aspectos de qualidade e conformidade às necessidades de controle.

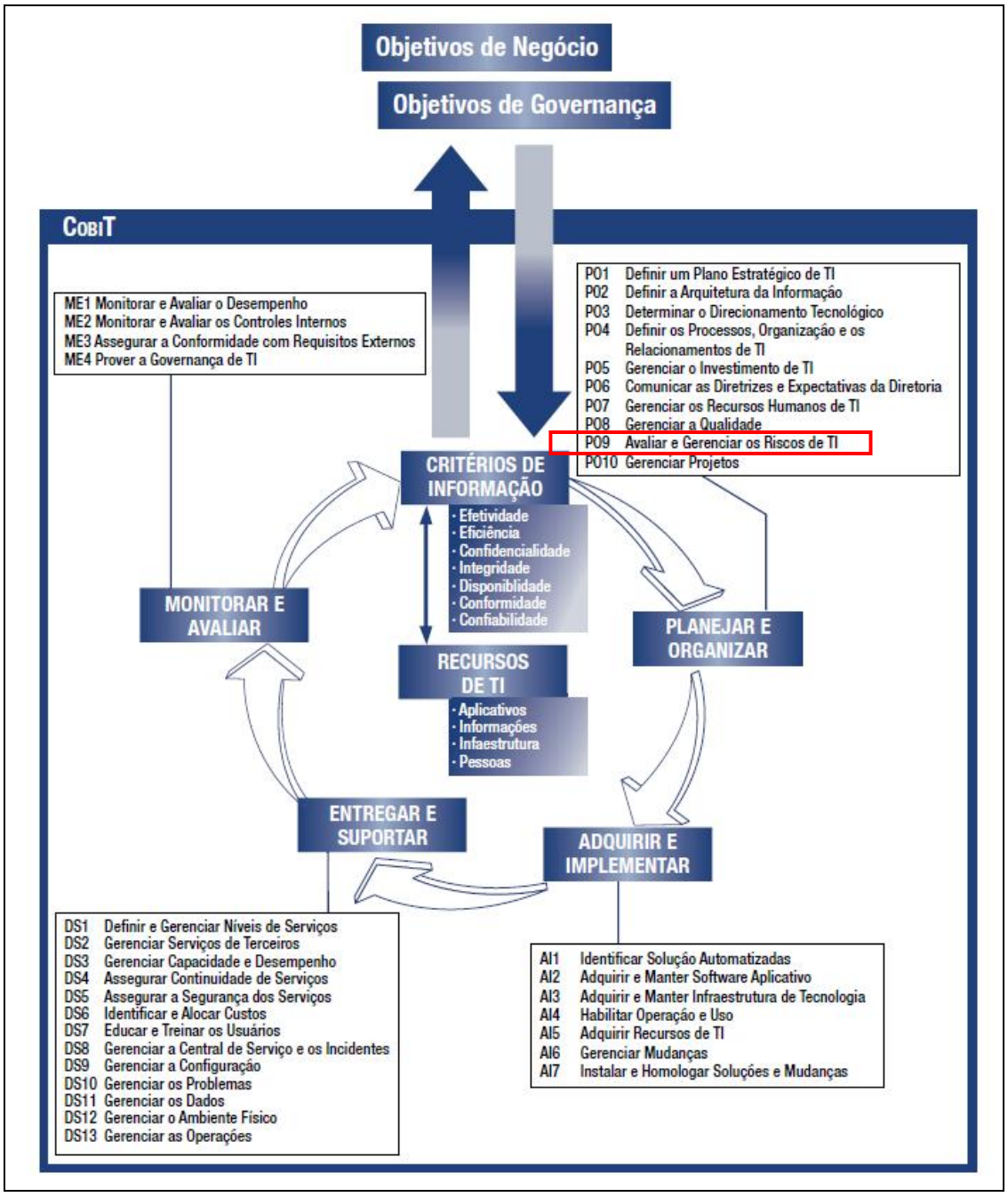
> A estrutura do Cobit com os quatro domínios reitera a necessidade de planejamento, alinhamento e integração com o negócio das organizações (REZENDE, 2008, p. 137)

Em um nível mais abaixo dos quatro domínios, o COBIT estabelece 34 objetivos de controle geral visando garantir a gestão da tecnologia da informação. Os objetivos de controle contêm as declarações dos resultados desejados ou metas a serem alcançadas na implementação dos objetivos de controles específicos dentro de uma atividade de tecnologia da informação, fornecendo uma política para o controle de tecnologia da informação na empresa.

No último nível, dependentes dos 34 objetivos de controle geral, os 215 objetivos de controle específico são apresentados e entendidos como indicadores de controle, a partir dos quais se analisa se os objetivos gerais foram alcançados.

O QUADRO 1 retrata a visão geral do modelo do COBIT, apresentando os domínios, os processos, os requisitos de negócios e requisitos de tecnologia da informação.

QUADRO 1 – Visão geral do modelo do COBIT



Fonte: (COBIT, 2006, p.28)

2.4.4. Aplicabilidade do COBIT

O COBIT é aplicado em todo o conjunto de atividades de tecnologia da informação, tendo como foco o resultado esperado, ou o que deve ser atingido, e não como as ações devem ser feitas para alcançar o resultado, ou seja, como atingir o resultado. Essa abordagem deve ser compreendida a partir do alinhamento com os requisitos do negócio. (COBIT, 2006)

Segundo Rezende (2008), existem várias oportunidades de aplicações do COBIT em organizações, por ser de grande abrangência e, considerando suas padronizações, sua utilização é utilizada como um *checklist* para avaliar os pontos fortes e fracos dos seus processos, dando, assim, subsídios para novas propostas de melhorias.

Aplica-se, ainda, em processo de auditoria dos riscos operacionais de tecnologia da informação, além de ter aplicabilidade direta em implementação modular da governança de tecnologia da informação, considerando que a governança de tecnologia da informação pode ser implementada nas organizações para atender às necessidades básicas, dando maior foco em áreas critica.

Conforme estudos apresentados por Rezende (2008), o *benchmarking* é estruturado utilizando-se o COBIT, considerando-se que a existência de modelos de maturidade para cada processo de tecnologia da informação permite que uma organização possa montar uma estratégia baseada em sua situação atual, utilizando, como parâmetros, a comparação de dados de outras organizações e estabelecendo suas próprias metas e estratégias de melhorias.

O COBIT ainda tem aplicabilidade, segundo Rezende (2008), em processo de qualificação de fornecedores de tecnologia da informação. O COBIT pode promover a qualificação no processo de contratação de fornecedores para execução de serviços de tecnologia da informação, ou mesmo no processo de estabelecer níveis de serviços dentro da organização.

De acordo com o COBIT (2006), a governança de tecnologia da informação pode ser aplicada em pequenas e grandes empresas, considerando-se, como premissa básica, que a aplicação do COBIT esteja consistente com os objetivos do negócio e as estratégias de tecnologia da informação.

Como exposto anteriormente, sobre governança de tecnologia da informação, esta pesquisa dará foco às melhores práticas do COBIT, considerando o processo de analisar e gerenciar os riscos de tecnologia da informação. Este processo será relacionado às ações de governança de tecnologia da informação definidas pela organização pesquisada, conforme QUADRO 2.

QUADRO 2 – Focos para análise de governança de tecnologia da informação por processo do COBIT

Processos do Cobit	Ações de Governança de TI da Organização
Analisar e gerenciar os riscos de tecnologia da informação	Gestão dos riscos de tecnologia da informação

Fonte: Elaborado pelo autor

As ações de gestão dos riscos de tecnologia da informação são parte importante do modelo de governança de tecnologia da informação implementado na organização pesquisada, considerando-se as melhores práticas apresentadas no COBIT, com foco no processo de Avaliar e Gerenciar os Riscos de Tecnologia da Informação (P09).

2.5. Avaliar e Gerenciar os Riscos de Tecnologia da Informação

Os processos de negócio de qualquer organização são suportados por informação independentemente de tecnologia, conforme os estudos apresentados por Campos (2007). Este autor ainda afirma que estes processos de negócio são suportados por serviços ou sistemas de informação que por sua vez são suportados por ativos de tecnologia tais como servidores, equipamentos de conexão entre tantos outros e conclui que estes ativos podem apresentar vulnerabilidades, que quando exploradas geram riscos para os sistemas causando impactos diretos nos processos de negócio das organizações, gerando possíveis prejuízos.

O estudo de gestão de risco de tecnologia da informação, conforme relato de Sêmola (2003), é considerado dentro dos processos de gestão de segurança da informação, que por sua vez compartilha uma percepção abrangente dos desafios e soluções de segurança da informação.

Para Campos (2007), analisar os riscos é uma atividade essencial, da máxima importância para a gestão de segurança da informação. O autor destaca que em um primeiro momento é necessário estabelecer qual será a maneira pela qual os riscos serão avaliados e quais critérios serão utilizados para considerar um risco aceitável ou não. Para tanto, o autor apresenta, em seus estudos, estratégias para avaliação de riscos, que são baseados em estudos qualitativos e quantitativos, permitindo uma análise mais abrangente.

> "Risco é a probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios." (SÊMOLA, 2003, p.50)

A falta de uma estratégia para avaliar os riscos de uma organização traz possíveis impactos aos negócios, além de permitir que os esforços sejam concentrados em pontos de menor risco com menos impacto organizacional.

Sêmola (2003) define impacto como a abrangência dos danos causados por um incidente de segurança, sobre um ou mais processos de negócio. Neste caso, incidente é fato decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando-se à perda dos princípios da segurança da informação, que são: confidencialidade, integridade e disponibilidade.

> "Vulnerabilidades é fragilidade presente ou associada a ativos que manipulam e ou processam informações que, ao serem exploradas por ameaças, permite a ocorrência de um incidente de segurança da informação para a organização". (SÊMOLA, 2003, p.48)

Sêmola (2003) afirma que um incidente gera impacto aos processos de negócio da organização e, enfatiza, que um incidente deve ser evitado. Além disso, independentemente do negócio da organização, variáveis de risco são observadas e essas devem ser alvo primário de atenção no modelo de governança de tecnologia da informação.

O impacto nos processos de negócio deve ser medido através de indicadores, conforme afirmação de Campos (2007), objetivando estimar o prejuízo causado por um incidente de segurança da informação envolvendo um determinado ativo que suporte um determinado processo de negócio. O autor também afirma que é preciso estabelecer uma estratégia de avaliação e gestão dos impactos para definir os possíveis prejuízos.

O QUADRO 3 apresenta os requisitos de negócio e recursos necessários a prover uma gestão de risco efetiva, conforme apresentado por Sêmola (2003), ao afirmar que os requisitos de negócio que devem ser observados para um processo de gestão de risco são: a efetividade do negócio, confidencialidade do negócio, integridade do negócio e disponibilidade do negócio, além de conformidade e confiabilidade. Observando pelo ângulo de recursos necessários para prover uma gestão de risco, o autor ainda apresenta as pessoas, as aplicações tecnológicas e as facilidades em prover o negócio como outros fatores que devem ser observados.

QUADRO 3: Requisitos e recursos para gestão de risco

	Gestão de Risco
Requisitos de Negócio	Primário: Efetividade, confidencialidade, integridade, disponibilidade. Secundário: Conformidade, confiabilidade,
Recursos necessários	Pessoas, aplicações, tecnologia, facilidades

Fonte: Adaptado de Sêmola (2003)

Campos (2007) afirma que alguns serviços de informação, tais como compartilhamento de arquivos, correio eletrônico, acessos a Internet e sistemas acessados pela Internet, devem ser considerados nas estratégias de análise e gestão de risco, pois são pontos fundamentais para as organizações e podem conter o maior número de vulnerabilidades e facilidades de exploração.

Um fator importante deve ser considerado em qualquer processo de análise e gestão de riscos, é a necessidade constante de reavaliação dos riscos organizacionais. Este ponto é apresentado de forma similar por Sêmola (2003) e por Campos (2007) em seus estudos. Esses autores consideram que o risco é baseado em dois pilares: a probabilidade de ocorrência do incidente e o impacto que este incidente causaria para a organização, onde a probabilidade é o produto entre grau de ameaça e grau de vulnerabilidade.

Contudo, os autores esclarecem que se mudanças estratégicas da organização ocorrem com freqüência, o processo de reavaliar os riscos também deve ocorrer na mesma proporção, principalmente se mudanças em processos de negócio ou ativos que suportam esses processos são implementadas.

Sêmola (2003) ressalta que um patamar mínimo de risco aceitável deve ser estabelecido, pois compreende que não é possível atingir um nível zero de risco em qualquer organização. Campos (2007) complementa essa afirmação ao considerar que o valor dos investimentos para a mitigação de risco é muito alto, justificando este patamar aceitável.

Campos (2007) acrescenta, ainda, que somente com um processo bem definido de análise de risco será possível estabelecer um patamar mínimo e aceitável pela organização em relação aos riscos. Além disso, afirma que as pessoas que compõem a equipe de análise de risco passam a ter conhecimento de todos os pontos fracos da organização e reitera a necessidade de contar com pessoas de total confiança para esse processo, por considerar que as informações analisadas podem ser restritas ou confidenciais.

O mesmo autor ainda apresenta, em seus estudos, que muitas organizações não consideram esta questão e deixam as estratégias e definições de análise e gestão de riscos sob a responsabilidade de uma empresa externa, que presta serviços desta natureza e aloca profissionais nas dependências das organizações. Campos (2007) considera essa atitude de grande risco para as organizações e conclui que a análise de risco deve iniciar com as definições estratégicas para o processo de analisar e gerenciar riscos.

Sêmola (2003), através de seus estudos, completa o que foi mencionado por Campos (2007), quando afirma que organizações brasileiras deixam seus processos de análise e gestão de riscos nas mãos de empresas despreparadas, aumentando assim o risco organizacional, ao invés de mitigá-los. Acrescenta que existe um risco neste processo de terceirização, mas reitera que existem empresas sérias no mercado brasileiro e que esta afirmação deve ser considerada e estas empresas devem ser analisadas em momento de contratação.

Este autor ainda afirma que o processo de análise e gestão de riscos é um processo árduo e que necessita de grande conhecimento técnico e do negócio. Assim, a formação de uma equipe adequada para essas atividades é necessária, ressaltando que, diante das necessidades e complexidades exigidas por este processo, uma boa equipe deve ser formada de colaboradores diretos das organizações, ou seja, empregados efetivos e colaboradores indiretos, ou seja, colaboradores alocados na organização. Conclui que os colaboradores alocados devem conhecer tecnicamente a infraestrutura da organização e o colaborador direto deve ser profundo conhecer do negócio.

2.6. Contribuição do referencial teórico para a pesquisa

Considerando o exposto até este ponto, sobretudo no referencial teórico sobre gestão do conhecimento e governança de tecnologia da informação, é possível concluir que as práticas de gestão do conhecimento podem contribuir para as definições dos modelos de governança de tecnologia da informação, tendo em vista que ambos buscam, em suas abordagens, vantagens competitivas e inovação para as organizações.

Para Neef (2005), a ampliação das ações de gestão do conhecimento nas organizações, como contribuição para as ações de análise e gestão de riscos, justifica-se de forma simples, pois sentir e responder a riscos em uma organização é muito dependente do capital intelectual da empresa, ou seja, o conhecimento e julgamento de funcionários em todos os níveis permitem a antecipação de acidentes potenciais.

Este autor ainda ressalta que, para atingir este objetivo é necessário mobilizar esses funcionários, sobre a importância do conhecimento para as ações de análise e gestão de riscos e que estas ações são essenciais para o sucesso organizacional.

Para Nonaka e Takeuchi (1997), o sucesso organizacional é também resultado de ações de gestão do conhecimento que são essenciais para prover inovação, competitividade e garantir a gestão estratégica.

Para Vieira (2004), a governança de tecnologia da informação, objetiva garantir adequação entre as ações de tecnologia da informação com os objetivos estratégicos da organização com objetivo final de prover competitividade, para tanto, apresenta o COBIT como *framework* fundamental para que esta adequação seja de sucesso.

O COBIT (2006) tem como objetivo garantir que a governança de tecnologia da informação esteja alinhada com as estratégias corporativas, apresentando melhores práticas para os processos de governança de tecnologia da informação, tornando o negócio da organização possível e com benefícios maximizados. Para Rezende (2008), este *framework* reafirma que o negócio da organização necessita de planejamento, alinhamento e integração com as ações de tecnologia da informação.

Um dos objetivos específicos deste estudo é apresentar, como resultado da pesquisa, as contribuições da gestão do conhecimento para os modelos de governança de tecnologia da informação em uma organização de saúde do Estado de Minas Gerais.

Contudo, este estudo terá foco nas ações de gestão do conhecimento, considerando-se os estudos de Nonaka e Takeuchi (1997), focando nas ações necessárias para a criação, disseminação e compartilhamento do conhecimento, além das ações que possam contribuir para alinhar a tecnologia da informação à inovação e à competitividade organizacionais. No que se refere a governança de tecnologia da informação, o foco será nos processos de análise e gestão de risco, que é um dos processos do COBIT.

COBIT (2006) afirma que o processo Avaliar e Gerenciar os Riscos de Tecnologia da Informação (PO9) deve estar alinhado com o negócio organizacional,

ou seja, estabelecer uma estrutura de gestão de risco de tecnologia da informação alinhada com a estrutura de gestão de risco da organização, prevendo-se, ainda, o estabelecimento do contexto de risco da organização, ao qual a estrutura de avaliação de risco é aplicada para assegurar resultados esperados, incluindo a definição dos contextos internos e externos de cada avaliação de risco, o objetivo da avaliação e os critérios pelos quais os riscos são avaliados, e conclui que o processo de analisar e gerenciar risco de tecnologia da informação deve acontecer de forma proativa.

Para Neef (2005), o processo proativo de gestão de risco reside na capacidade da empresa mobilizar o conhecimento e a experiência de seus funcionários garantindo que a organização obtenha informações precisas e oportunas sobre potenciais incidentes e conclui afirmando que uma organização não pode gerir o seu risco sem conseguir gerir seu conhecimento e conclui afirmando que, desta maneira, o processo de identificar as ameaças nas organizações passa ser tarefa menos árdua.

O COBIT (2006) recomenda identificar os eventos mais importantes e as ameaças reais que exploram as vulnerabilidades, apresentando os impactos potenciais e negativos nos negócios da organização. Recomenda, ainda, manter um histórico dos riscos relevantes para a organização, possibilitando conhecimentos futuros. O COBIT (2006) recomenda, também, que a avaliação dos riscos seja feita com freqüência e de forma regular, avaliando os impactos e probabilidades de todos os riscos identificados, considerando ainda que a probabilidade e o impacto associado ao risco inerente e residual devem ser determinados individualmente, por categoria e com base no portfólio da organização. Além disso, o COBIT (2006) recomenda que resposta ao risco seja desenvolvida, mantendo um processo sistemático de respostas para assegurar que controles possam mitigar a exposição da organização aos riscos. Por fim, o COBIT (2006) recomenda priorizar e estabelecer plano de ação para mitigar os riscos da organização e reitera a necessidade de monitoramento dos riscos, considerando a necessidade de reportar, para a alta direção da organização, todas as informações relevantes sobre risco organizacional.

Em suma, esta pesquisa considera os autores Nonaka e Takeuchi (1997) para estudos sobre gestão do conhecimento. Sobre o assunto analisar e gerenciar riscos de tecnologia da informação, esta pesquisa considera o COBIT (2006) e os estudos de Sêmola (2003).

3. APRESENTAÇÃO DA ORGANIZAÇÃO PESQUISADA

A organização estudada iniciou as suas atividades, no Estado de Minas Gerais, no ano de 1971, com o propósito de suprimir as necessidades da população que estava sendo submetida à intermediação de grupos privados para os serviços médicos. É uma organização sem finalidade lucrativa e de propriedade coletiva. O seu principal objetivo é a defesa econômica e social dos médicos cooperados, ao gerar oportunidades de trabalho e renda para seus associados.

No final do ano de 1990, essa organização se torna líder no setor de saúde na cidade de Belo Horizonte, contando com mais de 3,7 mil médicos, 300 mil clientes e um faturamento anual da ordem de R$ 300 milhões, valor medido em 2010.

No ano de 2010, a organização atingiu a marca de 1 milhão de clientes, consolidando-se como a maior operadora de saúde do estado e, no Brasil, como a terceira maior operadora de saúde.

A organização chegou, em 2006, com um cenário tecnológico avançado e qualificado. A contribuição da tecnologia da informação na capacidade de automatizar as informações, consolidar visões gerenciais e criar indicadores para um acompanhamento regular do desempenho era (e ainda é) fator de sustentação da posição de liderança da Cooperativa no setor de saúde suplementar na sua área de atuação.

Entretanto, no início do ano de 2011, a Cooperativa reconheceu que apesar de toda a tecnologia utilizada em seus processos, não possuía um ambiente corporativo (Intranet) estruturado, capaz de gerar uma cadeia de valor composta por dado-informação-conhecimento. A intranet que estava no ar era pouco utilizada, não integrava bancos de dados, não possuía busca de informação avançada e, ainda, não era pautado pela navegabilidade e usabilidade.

A gestão atual, eleita em 2010 para gestão até 2014, é composta por:

- **Diretor Presidente:** Médico do trabalho e especialista em saúde pública, com foco em planejamento e administração de serviços de saúde. Formado em 1989 pela UFMG, cursou o MBA Executivo em Gestão de Saúde pelo Ibmec e o Programa de Gestão da Performance, da Fundação Dom Cabral.

- **Diretor Administrativo-Financeiro:** Médico pediatra, formado em 1979 pela UFMG, onde também cursou a residência e o mestrado em Pediatria. É professor assistente do departamento de pediatria desde 1982 e coordena o setor de nutrição pediátrica e integra o setor de gastroenterologia pediátrica do Hospital das Clínicas.

- **Diretor de Provimento de Saúde:** Médico anestesiologista do Hospital Madre Teresa, formou-se pela UFMG em 1985. Possui também residência em Clínica Médica, especializações em Terapia Intensiva e Medicina do Trabalho e pós-graduação em Gestão de Negócios e Tecnologia da Informação (FGV).

- **Diretor Comercial:** Médico oftalmologista, formado pela Faculdade de Ciências Médicas de Minas Gerais em 1967, com especializações nessa escola, na Clínica de Olhos da Santa Casa de Belo Horizonte e na Baylor University (EUA), onde se concentrou na área de lentes de contato. Cursou o mestrado em Oftalmologia na Rejk Universiteit te Gent (Bélgica). Foi professor assistente da Faculdade de Ciências Médicas.

A organização ainda conta com um Conselho de Administração composta por 11 médicos, conta também com um Conselho Técnico composto por 10 médicos e um Conselho Fiscal composto por 6 médicos.

A organização, voltada para a responsável social, apresenta ações sociais para a cidade de Belo Horizonte como campanhas educativas e disseminação de informações sobre saúde e participa de importantes campanhas de saúde coletiva, organizadas pelo poder público e pelas sociedades médicas. A organização faz intervenções no dia a dia da cidade estimulando hábitos de vida saudáveis, patrocinando eventos que proporcione com este objetivo, tais como caminhadas e

corridas pela cidade, além de cuidar de praças e canteiros na cidade objetivando criar lugares mais agradáveis.

Desde meados de 2010, a organização passa por inúmeros problemas inerentes ao planejamento estratégico organizacional que tem como objetivo principal crescimentos na ordem de 15% anuais. Esse pesado planejamento tem motivado mudanças estruturais e movimentado mudanças processuais. Com tantas mudanças acontecendo, todas com único objetivo, a organização passa por necessidades de reestruturação de sua metodologia de gestão, seja em áreas diretas de seu negócio, seja em áreas de suporte do negócio, como ocorre no Departamento de Tecnologia da Informação.

Vários atrasos em projetos de tecnologia da informação são verificados, vários resultados não esperados são apresentados e esses atrasos e resultados colocam à prova o poder de governança de tecnologia da informação da organização em questão.

Além de atrasos e resultados não esperados nos projetos de tecnologia da informação, a organização passa por um momento delicado, principalmente no Departamento de Tecnologia da Informação, pois muitos funcionários estão pedindo demissão e deixando projetos estratégicos e tarefas inacabadas. Considerando a alta exigência para o atendimento completo ao planejamento estratégico organizacional, a organização acredita que as demissões e atrasos nos projetos são decorrentes deste fato. Contudo, preocupada com essa situação, a organização tem buscado, constantemente, investir em atividades motivacionais, apresentando aos funcionários da organização os benefícios após a completa execução do planejamento estratégico, que tem duração até o ano de 2013.

Atrelada a essa má fase, recentemente, um grande concorrente da organização iniciou suas operações no Estado de Minas Gerais, obrigando-a a efetivar uma revisão do planejamento estratégico organizacional, apertando ainda mais as ações e prazos anteriormente acordados, objetivando preparar a organização para as adversidades, além de movimentar a organização para uma reestruturação nas ações de captação de clientes. Contudo, a organização apresenta crescimentos satisfatórios e as ações de reestruturação dessa organização estão acontecendo conforme planejamento.

A palavra de ordem na organização pesquisada, considerando o planejamento estratégico organizacional, é inovação. Objetiva-se inovar para obter diferencial competitivo, em uma época de inúmeras mudanças e adversidades organizacionais.

O planejamento estratégico organizacional prevê inúmeras mudanças para o Departamento de Tecnologia da Informação. Desde o início dessas atividades, o Núcleo de Gestão do Conhecimento tem sido fator chave e preponderante para que as ações de governança de tecnologia da informação sejam formatadas adequadamente, possibilitando comunhão entre o departamento de tecnologia da informação e as estratégias organizacionais, apresentando-se como apoio necessário as ações de avaliação e gestão dos riscos de tecnologia da informação.

O Departamento de Tecnologia da Informação conta com 79 colaboradores, dos quais 14 são funcionários de empresas prestadoras de serviço e estão alocados diretamente em projetos específicos de infraestrutura de informação e desenvolvimento de sistemas. Os colaboradores do departamento possuem formação em análise de sistemas e engenharia de *software*, e gerência de projetos de tecnologia da informação, além de haver colaboradores de nível médio, atuando com desenvolvimento de sistemas.

O Departamento de Tecnologia da Informação dessa organização está estruturado da seguinte forma:

a) **Coordenação de infra-estrutura e suporte de tecnologia da informação:**

   Unidade responsável pela gestão e rede, telecomunicações, servidores estações de trabalho e atendimento aos usuários, em diversas plataformas tecnológicas.

b) **Coordenação de desenvolvimento de sistemas**:

   Unidade responsável pela manutenção e desenvolvimento de sistemas corporativos, objetivando atender às diversas áreas de negócio da organização.

c) Coordenação de segurança da informação:

Unidade responsável pela confidencialidade, disponibilidade, integridade e autenticidade das informações, além de prover recursos de gestão e infraestrutura de contingência para infraestrutura tecnológica e sistemas de informação.

d) Coordenação de projetos de tecnologia da informação:

Unidade responsável por fazer a gestão de todos os projetos de tecnologia da informação e atividades de projetos corporativos nos quais a tecnologia da informação esteja inserida.

e) Coordenação de governança de tecnologia da informação:

Unidade responsável em desenvolver os modelos de governança de tecnologia da informação da organização, considerando os critérios de qualidade, gestão de dados, arquitetura de software, gestão de contratos, fornecedores de tecnologia da informação e segurança da informação.

f) Núcleo de gestão do conhecimento:

Núcleo responsável pelas ações de gestão do conhecimento na organização, tratando das ações de compartilhamento e disseminação de informação, além de gestão e desenvolvimento de *data warehouse* e gestão dos processos de inteligência de negócio, através de *softwares* específicos.

A organização pesquisada solicitou que sua razão social não fosse divulgada, porém concordou em participar de todos os processos e etapas para que a pesquisa fosse concluída com integridade.

Conclui-se que os estudos apresentados no referencial teórico e a apresentação da organização pesquisada são fundamentais para atender os objetivos deste trabalho. Contudo, justifica-se a necessidade de uma pesquisa de campo, objetivando um abrangente estudo de caso. Os procedimentos metodológicos, para esta pesquisa, serão discutidos no próximo capítulo.

4. METODOLOGIA

A fim de alcançar os objetivos propostos, este capítulo aborda o detalhamento de métodos e técnicas utilizados na pesquisa. Inclui a explicação sobre o tipo de pesquisa, a definição da unidade de análise, os instrumentos para coleta de dados e as estratégias para análise dos dados.

4.1. Caracterização da Pesquisa

Para entender os objetivos deste estudo, caracterizou-se a pesquisa quanto aos fins como sendo descritiva, devido ao fato de que se pretende apresentar as características das ações de gestão do conhecimento, contribuindo para o modelo de governança de tecnologia da informação, expondo as especificidades do modelo estudado. Para Collis e Hussey (2005), a pesquisa descritiva caracteriza-se por ser aquela que descreve o comportamento dos fenômenos e é usada para identificar e obter informações sobre as características de um determinado problema ou questão.

Para Oliveira (2004), a pesquisa descritiva tem a observação como finalidade, além de registrar e analisar os fenômenos sem, entretanto, entrar no mérito de seu conteúdo.

Quanto aos meios, trata-se de um estudo de caso de natureza qualitativa, pois pretende examinar e refletir sobre as ações de gestão do conhecimento e modelos de governança de tecnologia da informação na empresa pesquisada, obtendo-se, assim, um entendimento global sobre tais assuntos.

Conforme os estudos apresentados por Roesch (2005), o enfoque qualitativo conduz o pesquisador a consolidar os estudos com a coleta de dados, e este tem início com o conhecimento dos conceitos e idéias sobre o fenômeno desejado.

Os estudos de Collis e Hussey (2005) caracterizam uma pesquisa qualitativa como um processo que envolve examinar e refletir sobre as percepções, objetivando entendimento das atividades. Os autores afirmam ainda que um estudo de caso

pode ser feito em uma única unidade de análise e que este estudo é considerado como técnica investigativa, reiterando que o estudo de caso é uma estratégia de pesquisa que busca examinar um fenômeno dentro de seu contexto. Essa estratégia não possui um esquema conceitual rígido e propicia maior flexibilidade na análise dos resultados, possibilitando ainda a consideração de grande número de variáveis e baseia-se no uso de diversas fontes de dados.

Para Thiollent (1987), em uma pesquisa qualitativa, sugere-se a entrevista de um pequeno número de indivíduos que representem a identidade organizacional à qual pertencem. Nesse tipo de pesquisa, o objetivo do pesquisador consiste em aprender sobre o fenômeno extraindo-se, dos indivíduos entrevistados, suas experiências, que se constituem em agentes reveladores da cultura empresarial vivida no dia a dia.

4.2. Unidade de análise e observação e sujeito de pesquisa

Conforme mencionado anteriormente, a unidade de análise escolhida para esta pesquisa foi uma organização do setor de saúde, localizada na cidade de Belo Horizonte, Minas Gerais.

As unidades de observação foram as ações de gestão do conhecimento e os modelos de governança de tecnologia da informação, com foco nos processos de análise e gestão de riscos, estruturados pelo Departamento de Tecnologia da Informação dessa organização.

Os sujeitos de pesquisa foram escolhidos seguindo critérios de acessibilidade e por serem profissionais que lidam com os conceitos e práticas efetivas de gestão do conhecimento e governança de tecnologia da informação. Este grupo é constituído por 7 funcionários. O QUADRO 4 apresenta os sujeitos da pesquisa relacionados com a estrutura organizacional do Departamento de Tecnologia da Informação da organização pesquisada.

QUADRO 4. Estrutura e sujeitos de pesquisa

Estrutura do Departamento de TI	Sujeitos de pesquisa
Gerência de Tecnologia da Informação	1 Gerente de TI
Coordenação de Infra Estrutura e Suporte de TI	1 Coordenador de Infra Estrutura
Coordenação de Desenvolvimento de Sistemas	1 Coordenador de Sistemas
Coordenação de Segurança da Informação	1 Coordenador de Segurança
Coordenação de Projetos de TI	1 Coordenador de Projetos
Coordenação de Governança de TI	1 Coordenador de governança de TI
Núcleo de Gestão do Conhecimento	1 Supervisor de núcleo

Fonte: Elaborado pelo autor.

A escolha deste grupo de respondentes é considerada não-probabilística intencional, conforme apresentado por Mattar (1997), sendo esta categoria caracterizada como subjetiva, sem base estatística, sendo a amostra selecionada através de critérios pessoais decorrentes da experiência profissional e do conhecimento do setor em exame, por parte do pesquisador.

4.3. Técnicas de Coleta de Dados

Neste estudo, informações primárias e secundárias foram utilizadas. As informações primárias foram obtidas através de um roteiro de entrevista semi-estruturada, formado por 11 perguntas, que foram realizadas com os profissionais que atuam diretamente no Departamento de Tecnologia da Informação. (APENDICE 1)

Gil (1999, p. 117) define pesquisa semi-estruturada como “a técnica em que o investigador apresenta frente ao investigado e lhe formulam perguntas, com o objetivo de obtenção de dados que interessam à investigação”.

As informações secundárias foram obtidas através de pesquisa bibliográfica, desenvolvida à luz do material já elaborado, que tem como objetivo a construção do marco teórico da pesquisa, apresentado no capítulo de referencial teórico, além de pesquisa documental em documentos, de propriedade da organização pesquisada, referentes à implementação do projeto de gestão do conhecimento e governança de tecnologia da informação. Ainda foram utilizados os documentos com os modelos de governança de tecnologia da informação e o planejamento e ações de gestão do conhecimento da organização.

4.4. Estratégia de Análise de Dados

O QUADRO 5 apresenta a estratégia que foi usada na análise dos dados. Ela relaciona os objetivos específicos propostos nesta pesquisa com os autores que dão sustentação teórica para os assuntos abordados e os instrumentos de coleta de dados correspondentes .

QUADRO 5 – Estratégia de coleta de dados

Objetivos Específicos	Autores	Instrumento coleta	Fonte de dados
Pesquisar na literatura a teoria de GC, Governança de TI e COBIT	Nonaka e Takeuchi, Davenport e Prusak. Alvarenga Neto, Choo, Malhotra, Rezende, Sallé, Stewart, Fleury e Oliveira Jr, Sveiby, Ovum, Weill e Ross, Vieira, Cobit	Pesquisa bibliográfica	Referencial Teórico
Analisar e apresentar as principais características do modelo de governança de tecnologia da informação da organização pesquisada;	Collis e Hussey, Weill e Ross, Vieira, Rezende, Cobit	Entrevistas e Pesquisa Documental	Questões: 3,4,5 e 6 Documentos do projeto de governança de TI e modelo de governança de TI
Analisar e apresentar as práticas de gestão do conhecimento adotadas na organização pesquisada;	Nonaka e Takeuchi, Davenport e Prusak. Alvarenga Neto, Choo, Malhotra, Rezende, Sallé, Stewart, Fleury e Oliveira Jr, Sveiby, Ovum,	Entrevista e Pesquisa Documental	Questões: 7 e 8 Documentos do projeto GC e Ações de GC
Relacionar, através da pesquisa semi estruturada, as contribuições da gestão do conhecimento para o modelo de governança de tecnologia da informação, considerando o processo de gestão de risco de tecnologia da informação, da organização pesquisada.	Nonaka e Takeuchi. (Criar, disseminar e compartilhar o conhecimento) Cobit	Entrevista e Pesquisa Documental	Questões: 9,10 e 11

Fonte: Elaborado pelo autor.

5. PESQUISA DOCUMENTAL E DE CAMPO

A pesquisa de campo, objetivando responder à pergunta que norteia este trabalho e alcançar seus objetivos, teve duração de 35 dias entre as ações de análise documental e entrevista.

Os sete sujeitos da pesquisa responderam ao roteiro composto por 11 perguntas e cada entrevista teve duração máxima de uma hora. As entrevistas foram gravadas com o consentimento dos entrevistados e todo esse esforço teve duração de 9 dias.

A pesquisa documental foi concluída em 15 dias e contou com uma grande quantidade de documentos de projetos e de ações diárias da organização sobre o tema gestão do conhecimento.

Sobre o tema governança de tecnologia da informação, as pesquisas foram concentradas nos documentos de avaliação e gestão de riscos de tecnologia da informação. Porém, os resultados das análises dos outros documentos são apresentados de forma sucinta, objetivando prover um conhecimento global sobre o assunto. O resultado da pesquisa resultou em um extenso material com a transcrição das respostas dos entrevistados.

Para a elaboração da análise das entrevistas e de documentos, foram necessários 15 dias, totalizando-se 41 dias de pesquisa.

É importante ressaltar que durante as entrevistas novas informações foram surgindo e estas foram consideradas, pois muitas informações não estavam diretamente no contexto das questões, mas foram fundamentais para o entendimento adequado das questões.

Portanto, optou-se pela seguinte estrutura para a apresentação dos resultados:

a) Resultados dos documentos analisados sobre gestão do conhecimento

Os documentos analisados sobre gestão do conhecimento tiveram foco nas ações de planejamento das ações de gestão do conhecimento e nas ações de criação, disseminação e compartilhamento do conhecimento, além das ações praticadas, pela organização pesquisada, com o objetivo de criar condições para o compartilhamento e disseminação do conhecimento.

b) Resultados dos documentos analisados sobre Governança de Tecnologia da Informação com foco na análise e gerenciamento de risco de tecnologia da informação.

Os documentos analisados foram focados nos processos de análise e gestão de riscos de tecnologia da informação, mas os documentos de planejamento da governança de tecnologia da informação foram estudados e apresentados de forma sucinta, objetivando contextualizar e permitir maior entendimento sobre o assunto.

c) Resultados dos dados analisados nas entrevistas

Neste item, as informações estão apresentadas separadamente, iniciando-se pelas ações de gestão do conhecimento, passando pelos processos de analisar e gerenciar riscos de tecnologia da informação e, por fim, apresenta-se o resultado observado pelos entrevistados sobre os benefícios da gestão do conhecimento para os processo de analisar e gerenciar riscos de tecnologia da informação.

5.1. Resultados dos documentos analisados sobre Gestão do Conhecimento

Neste capítulo, apresenta-se de forma sintética o resultado dos documentos analisados sobre o assunto gestão do conhecimento. Tais documentos são utilizados diariamente pela organização pesquisada, objetivando o direcionamento correto das ações relativas a essa atividade.

5.1.1. Planejamento das ações de Gestão do Conhecimento

O planejamento das ações de gestão do conhecimento teve início no final do ano de 2009 e foi fortalecido no ano de 2010, com a reestruturação do planejamento estratégico organizacional. O Departamento de Tecnologia da Informação, como muitos outros departamentos da organização, passou por mudanças significativas e diante as inúmeras metas estabelecidas, mudanças estruturais foram necessárias, contudo, mudanças nas ações de gestão do conhecimento foram definidas neste período.

O planejamento das ações de gestão do conhecimento objetivou a explicitação e registro das ações de gestão do conhecimento necessárias para que a organização pudesse conhecer os processos operacionais e suas integrações entre os processos dos demais departamentos. Objetivou-se, ainda, a definição de ações de gestão do conhecimento que pudesse mudar a forma de pensar dos funcionários e com isso transformar o conhecimento tácito em conhecimento explícito. Em um segundo momento, o planejamento teve foco em ações objetivando transformar conhecimento explícito em tácito, com foco nos treinamento de colaboradores, funcionários e parceiros. Objetivou-se, com essas ações, um maior entendimento por parte do departamento de tecnologia da informação sobre os processos de negócio da organização e a explicitação dos conhecimentos, considerando as constantes trocas de funcionários.

O planejamento teve grande foco em ações para criar condições objetivando a disseminação e compartilhamento do conhecimento no Departamento de Tecnologia da Informação e, posteriormente, essas ações serão estendidas para toda a organização.

5.1.2. Plano de Implantação de Gestão do Conhecimento

O plano de implantação de gestão do conhecimento foi elaborado e passou por reformulações no ano de 2010, considerando as necessidades estabelecidas no planejamento estratégico organizacional. Esse plano apoiou-se, basicamente, nos conceitos de criação, compartilhamento e disseminação do conhecimento e criação de condições para o compartilhamento e disseminação desse conhecimento.

5.1.2.1. Criação, compartilhamento e disseminação do conhecimento

Objetivando a criação, compartilhamento e disseminação do conhecimento na organização pesquisada, algumas ações foram implementadas e outras ações foram reformuladas. Em primeiro momento, estas ações foram implementadas pensando em atender o Departamento de Tecnologia da Informação e, posteriormente, atender os demais departamentos da organização, tornando-as ações corporativas para criação, compartilhamento e disseminação do conhecimento.

Para o plano de implantação de gestão do conhecimento, as ações implementadas ou reformuladas foram:

a) Base de conhecimentos para o time de desenvolvimento de sistemas e infraestrutura - objetivou-se o registro de todos os problemas e soluções encontrados nos sistemas ou no ambiente de infra estrutura tecnológica. Estes problemas podem ser percebidos e assim cadastrados em momento de definição, desenvolvimento, implantação, homologação e produção.

b) Base de conhecimentos com vulnerabilidades conhecidas e ações para eliminação ou mitigação dos riscos - essa base de conhecimento permite que os colaboradores das gerências de desenvolvimento de sistemas e infraestrutura possam buscar o conhecimento obtido através de análises de risco, onde as vulnerabilidades são apresentadas com suas possíveis soluções.

c) Base de conhecimento com lições aprendidas em projetos de tecnologia da informação - essa base permite que os projetos ao terem início possam ser qualificados quando aos problemas e vulnerabilidades conhecidas, permitindo que o novo projeto conte com mais este banco de conhecimento objetivando maior sucesso, com menor atraso e menor custo.

d) Reuniões ampliadas - reuniões com todos os colaboradores da tecnologia da informação, que acontece uma vez a cada mês e objetiva nivelar o conhecimento de todos os colaboradores sobre os projetos em andamento;

e) Reuniões de projetos - reuniões de acompanhamento dos projetos de tecnologia da informação que acontece com a presença dos envolvidos diretamente nos projetos e com a equipe da área de negócio que demandou o projeto.

f) Reuniões de inicio de projetos com *brainstorming* entre a equipe de tecnologia da informação e a área de negócio;

g) Seminários Internos - os seminários são incentivados e acontecem sem datas previstas, mas existem esforços para que aconteçam, no mínimo, três seminários durante um ano.

h) Treinamentos e repasse de treinamentos - os treinamentos são incentivados e fazem parte das estratégias da empresa e fazem parte, também, do orçamento anual do departamento de tecnologia da informação. Os repasses aos demais colaboradores são feitos logo após o término de um treinamento, considerando que nem todos os colaboradores da área de tecnologia da informação participam diretamente de todos os treinamentos. Os repasses objetivam nivelar o conhecimento dos colaboradores à luz de determinados assuntos de caráter essencial para a inovação das atividades do departamento de tecnologia da informação.

i) Documentação de ambiente de infra-estrutura - essa documentação é exigida sempre que alguma alteração é efetuada no ambiente de infraestrutura da organização pesquisada. Por menor que seja a alteração, sendo esta física ou lógica, a documentação deve ser atualizada ou criada. O objetivo principal desta documentação é externalizar o conhecimento sobre a infraestrutura da organização preservando com isso a constante disseminação e compartilhamento de conhecimentos.

j) Documentação funcional e técnica de sistema - esta documentação, a exemplo do que é feito com as documentações de ambiente de infraestrutura, objetiva o constante armazenamento de alterações efetuadas nos sistemas já desenvolvidos, por menor que sejam estas alterações, dando continuidade à necessidade exigida pela organização

de constante externalização dos conhecimentos, preservando sua disseminação e compartilhamento.

k) Portal Interno - o portal interno da organização pesquisada é munido de tecnologia que facilita a criação de áreas para cada departamento objetivando que as informações desses departamentos possam ser compartilhadas com todos os colaboradores da organização, de forma fácil e rápida, além de ser um incentivo para todos os colaboradores para continuidade constante dos processos de disseminação e compartilhamento do conhecimento.

l) Blog de negócio e técnico - essa área está inserida no portal interno e tem como objetivo a troca de conhecimento entre os colaboradores da organização. Permite que qualquer colaborador possa inserir um assunto objetivando-se estabelecer uma discussão entre os interessados. Esse ambiente é controlado por um moderador que tem a função de garantir que os assuntos postados sejam de interesse corporativo. Os assuntos podem ser técnicos e sobre regras de negócio da organização, permitindo que qualquer colaborador possa participar das discussões. A organização pesquisada justifica essa ação por entender que este é um dos canais através dos quais muitas soluções para os problemas técnicos, ou de negócio são encontradas, e as contribuições são ricas de conhecimento tácito, que passam a ser explícitos e ficam armazenados para a organização. Até o momento desta pesquisa, existiam 78 assuntos em discussão.

m) Bate Papo Gerencial - este evento é de extrema importância, conforme justificativa da organização pesquisada. É o momento para a organização no qual todos os gerentes, coordenadores e supervisores da organização encontram-se para discutir assuntos técnicos e de negócio. Tem o objetivo de nivelar o conhecimento desses colaboradores à luz das ações que estão acontecendo em diversos departamentos da organização. Permite que as gerências apresentem seus projetos, dificuldades e soluções. Objetiva, ainda, que outros departamentos possam, através dessas apresentações, mudar o rumo de seus projetos, unir projetos ou participar

de algum projeto gerando, com isso, sinergia entre departamentos e projetos.

n) Portal de segurança da Informação - este portal é acessado através do portal interno da organização pesquisada e objetiva apresentar informações sobre as ações executadas na organização sobre o assunto segurança da informação, apresentando informações e notícias sobre riscos e vulnerabilidades na organização, além de ações mitigadoras, melhores práticas, procedimentos e política, visando nivelar os colaboradores sobre o assunto segurança da informação. Através desse portal, os usuários da organização ainda podem informar para a gestão de segurança da informação os riscos percebidos ou experimentados, as vulnerabilidades descobertas nos ambientes tecnológicos e ações suspeitas que possam causar impactos negativos para a organização.

o) *Chat* interno e externo - objetiva facilitar a comunicação interna entre os colaboradores da organização e externa entre colaboradores com os fornecedores e parceiros. O *chat* externo é controlado e apenas os endereços eleitos como necessários são liberados, objetivando a conversa ágil e direta, sobre assuntos corporativos. Toda a conversa é passível de auditoria, pois essas conversas ficam armazenadas por um período indeterminado.

p) Páginas pessoais - esta opção está liberada no portal interno da organização e tem como objetivo principal permitir que os colaboradores possam explicitar seus conhecimentos permitindo, à empresa conhecer suas características profissionais. Essa ação justificou-se por considerar a constante necessidade de alocação de colaboradores com conhecimentos específicos em projetos da organização.

q) Fale conosco - este é um espaço destinado aos clientes da organização, que tem como objetivo permitir que estes clientes possam registrar suas opiniões, sugestões e reclamações, além de efetuar solicitações. Essa área é de suma importância para a organização, pois permite a ela escutar seus clientes e perceber eventuais erros em suas regras de negócio, ou sistemas, permitindo correções e melhorias nos processos. Essa área

permite, também, que a organização possa considerar o exposto pelos clientes em momento de definição de suas estratégias ou definição de algum projeto que impacte os clientes. A organização pesquisada considera que esta é uma área estratégica para todos os departamentos da organização por permitir análise e agrupamento dos assuntos mencionados.

r) Sistema para registro de incidentes, riscos e vulnerabilidades - este sistema é acessado através do portal de segurança da informação e tem como objetivo principal permitir que os colaboradores do Departamento de Tecnologia da Informação possam efetuar os registros dos incidentes de segurança da informação, as vulnerabilidades e os riscos para a organização. Objetiva, ainda, que ser a base de conhecimento sobre o assunto, possibilitando disseminação e compartilhamento de conhecimentos.

5.1.2.2. Criando condições para o compartilhamento e disseminação do conhecimento

Conforme exposto no referencial teórico, a criação de condições para o compartilhamento e disseminação do conhecimento é fator essencial para o sucesso dessas ações. A organização pesquisada implementou algumas importantes alterações em seu ambiente, no intuito de favorecer o compartilhamento e a disseminação do conhecimento, tais como:

a) Incentivo à participação em seminários, congressos, eventos técnicos e à ampliação da formação acadêmica. A organização pesquisada implementou programas de incentivo à formação acadêmica, proporcionando bolsas de até 40% de desconto para os colaboradores interessados em ampliar sua formação acadêmica, em cursos que possam formar um profissional mais qualificado para execução de suas atividades na organização. Esses programas ainda incentivam e proporcionam pagamentos integrais para os colaboradores para que possam participar

de seminários, congressos e eventos técnicos, cujo conteúdo esteja adequado com as estratégias organizacionais.

b) Criação de ambiente propício para compartilhar informações. O espaço denominado de Pilotis é uma grande área com mesas redondas, cadeiras, poltronas, máquinas de café, bebedouro, revistas e jornais atualizados, possibilitando que os funcionários possam usar deste espaço para reuniões, convívio profissional, possibilitando geração de novas idéias e criação, compartilhamento e disseminação do conhecimento, conforme apresentado na FIGURA 3.

FIGURA 3. Ambiente propício para compartilhamento e disseminação da informação.

Fonte: Elaborado pelo autor

Conforme afirmam Davenport e Prusak (1999, p. 110), “conversar é trabalhar” e, foi pensando nesta afirmação, que esse espaço foi projetado. O espaço ainda conta com uma área externa, cujo objetivo é o encontro informal, após os horários de trabalho, nos quais os colaboradores e parceiros da organização possam compartilhar experiências e conhecimentos.

c) Auditório com equipamentos multimídia - este espaço objetiva incentivar, facilitar e manter o colaborador confortável quando estiver utilizando esse ambiente, para participar de eventos diversos, como palestras, seminários e reuniões.

d) Salas de treinamentos equipadas com equipamentos tecnológicos atualizados - as salas ficam à disposição de qualquer gerência da organização e permite que os treinamentos sejam mais produtivos, em um ambiente que favoreça o compartilhamento e disseminação do conhecimento, possibilitando o uso de recursos tecnológicos atualizados.

e) Estações de trabalho dimensionadas para abrigar o maior número de pessoas, com o maior conforto, privilegiando a facilidade no relacionamento profissional;

f) Incentivos e verbas financeiras para o encontro profissional a cada 3 meses fora o ambiente de trabalho - esta ação é de suma importância para manter o colaborador motivado. Os encontros acontecem, geralmente, no horário do almoço, onde uma palestra é ministrada por um convidado e mesas redondas são formadas para que o assunto possa ser discutido entre os colaboradores e convidados. Essa ação é vista, pela organização pesquisada, como o ponto alto para promover o relacionamento profissional e técnico entre os colaboradores do Departamento de Tecnologia da Informação e colaboradores de outras gerências da organização, além de proporcionar o compartilhamento e disseminação do conhecimento com colaboradores de outras instituições.

g) Encontro gerencial a cada 6 meses fora do ambiente de trabalho objetivando-se revisar as estratégias corporativas e apresentação de novas determinações e projetos, além do encontro anual para a definição das estratégias corporativas para o período seguinte. Esses encontros são ações corporativas e não somente para a área de tecnologia da informação.

5.1.3. Plano de Comunicação de Gestão do Conhecimento

O plano de comunicação de gestão do conhecimento foi encarado pela organização como o fator primordial para o sucesso das ações. Esse plano foi minuciosamente preparado pelas gerências de tecnologia da informação com total apoio da gerencia de marketing da organização.

Basicamente, esse plano teve como objetivo apresentar, a todos os colaboradores do Departamento de Tecnologia da Informação, as características e importância de ações de gestão do conhecimento dentro da organização, os benefícios diretos que essas ações poderiam trazer para o departamento e, por conseqüência para a organização em geral.

O plano de comunicação contou, basicamente, com palestras quinzenais sobre ações de gestão do conhecimento já existentes na organização, apresentação de novas ações necessárias para atender às exigências do planejamento estratégico organizacional e mudanças em algumas ações que, diante das necessidades, necessitavam de modificações.

É parte integrante do plano de comunicação a continuidade das divulgações das ações, eventuais mudanças nas ações e implementações de novas ações, além de apresentação de resultados obtidos pelo Departamento de Tecnologia da Informação com o uso permanente de ações de gestão do conhecimento.

Em 2012, o plano de comunicação está em fase de reestruturação e contará com ações mais diretas e objetivas com os colaboradores, incentivando a participação nas listas de discussão, nos *blogs* e bancos de conhecimento. Esse plano ainda conta com um novo fator motivador, que é a instituição de uma das ações de meritocracia da organização, ou seja, metas organizacionais a serem atingidas, no que se refere à redução de retrabalho nas ações de implementação de novos sistemas e manutenção de sistemas já existentes, além da mitigação e eliminação de riscos pelo conhecimento e tratamento. O objetivo disso é solucionar as vulnerabilidades no ambiente de tecnologia da informação, entre outras ações voltadas diretamente para o Departamento de Tecnologia da Informação.

5.2. Resultados dos documentos analisados sobre Governança de Tecnologia da Informação com foco na análise e gerenciamento de risco de tecnologia da informação.

Neste capítulo, apresentam-se os resultados dos documentos analisados sobre o assunto governança de tecnologia da informação, com foco no gerenciamento de riscos de tecnologia da informação. Muitos documentos sobre o

assunto gerenciamento de risco são classificados, pela organização pesquisada, como confidenciais ou restritos. Por isso, apenas os documentos classificados como públicos e restritos foram analisados na íntegra. Os documentos tratados como confidenciais foram explorados de forma sintética, com a constante presença do responsável pelas ações de segurança da informação e continuidade de negócio da organização pesquisada.

5.2.1. Planejamento de Governança de Tecnologia da Informação

O planejamento de governança de tecnologia da informação teve início na organização pesquisada em meados do ano de 2008 com a implantação da Coordenação de Governança de Tecnologia da Informação. Basicamente, este plano estava voltado para ações de gestão de projetos de tecnologia da informação e arquitetura de *software*, englobando as ações de gestão de dados.

Ao final do ano de 2008, após estudos detalhados e treinamentos no *framework* COBIT envolvendo os integrantes responsáveis pela coordenação de governança de tecnologia da informação, o planejamento foi estruturado de forma definitiva e, até os dias de hoje, segue a seguinte estrutura:

a) Qualidade das ações de tecnologia da informação;

O objetivo principal da equipe de qualidade das ações de tecnologia da informação é o desenvolvimento de padronizações e métricas para o direcionamento correto das solicitações de serviço que são demandadas diariamente por toda a organização. Objetiva, ainda, a elaboração e apresentação de resultados, para a gerência de tecnologia da informação, em relação as coordenações e núcleos do Departamento de Tecnologia da Informação.

b) Gestão de dados;

Tem como objetivos elaborar, dimensionar e implementar modelagens de dados e qualidade de dados, que são requisitos importantes para a qualidade das informações na organização. Essa equipe está envolvida diretamente nas modelagens de todos os sistemas que são desenvolvidos ou passam por manutenção, na organização.

c) Arquitetura de *software;*

A equipe de arquitetos de *softwares* trabalha diretamente com a equipe de qualidade de dados e sua função principal é determinar a arquitetura necessária e suficiente para os sistemas que são desenvolvidos na organização. Essa equipe apresenta, ainda, relatórios sobre as necessidades de modificações nas arquiteturas, sejam físicas ou lógicas, para a melhoria constante dos ativos tecnológicos da organização.

d) Gestão de contratos e fornecedores de tecnologia da informação;

O objetivo desta equipe é analisar, estruturar e manter os contratos de todos os fornecedores de tecnologia da informação. Controla as demandas de novos contratos e garante que os contratos sigam a estrutura definida pela organização, além de garantir e apresentar as medições mensais sobre os níveis de acordo de serviços pactuados contratualmente, permitindo que essa equipe autorize os pagamentos aos fornecedores.

e) Gestão de projetos de tecnologia da informação;

A gestão de projetos de tecnologia da informação foi absorvida por uma coordenação específica, considerando as recomendações de consultorias que identificaram que a gestão não poderia ficar nas mãos de quem, efetivamente, participa das execuções dos projetos de tecnologia da informação.

f) Segurança da informação;

Esta equipe é responsável pela segurança física e lógica dos ambientes tecnológicos da organização, e visa preservar a confidencialidade, integridade disponibilidade e autenticidade das informações, sejam elas confidenciais,

restritas ou públicas. Essa equipe ainda é responsável pelas ações de continuidade de negócio e definições de políticas, normas e procedimentos de segurança da informação. Outra atribuição dessa equipe são as ações de analisar e gerenciar os riscos de tecnologia da informação, que objetivam mitigar ou eliminar os riscos no ambiente de tecnologia da informação através do constante monitoramento das vulnerabilidades e ações efetivas com foco em eliminar ou tratar as vulnerabilidades conhecidas, proporcionando um ambiente tecnológico mais seguro. Essa estrutura, considerando as proporções adquiridas, foi modificada e, com isso, criou-se uma coordenação de segurança da informação e continuidade de negócios, proporcionando mais força às ações implementadas.

As definições das ações de analisar e gerenciar os riscos de tecnologia da informação tiveram início com o plano de segurança da informação.

5.2.2. Plano de Segurança da Informação

O plano de segurança da informação foi estruturado considerando-se os quatro pilares da segurança da informação, que são: confidencialidade, integridade, disponibilidade e autenticidade.

O objetivo principal desse plano foi direcionar um trabalho efetivo de proteção dos ativos de informação, estabelecendo os procedimentos operacionais, com suas respectivas normas e padrões de segurança, além de apresentar política de segurança da informação, que é o guia principal de todos os processos de segurança. Foi composto ainda, por vários outros sub-planos, que dão direcionamento ao processo de segurança da informação, conforme apresentado na FIGURA 4.

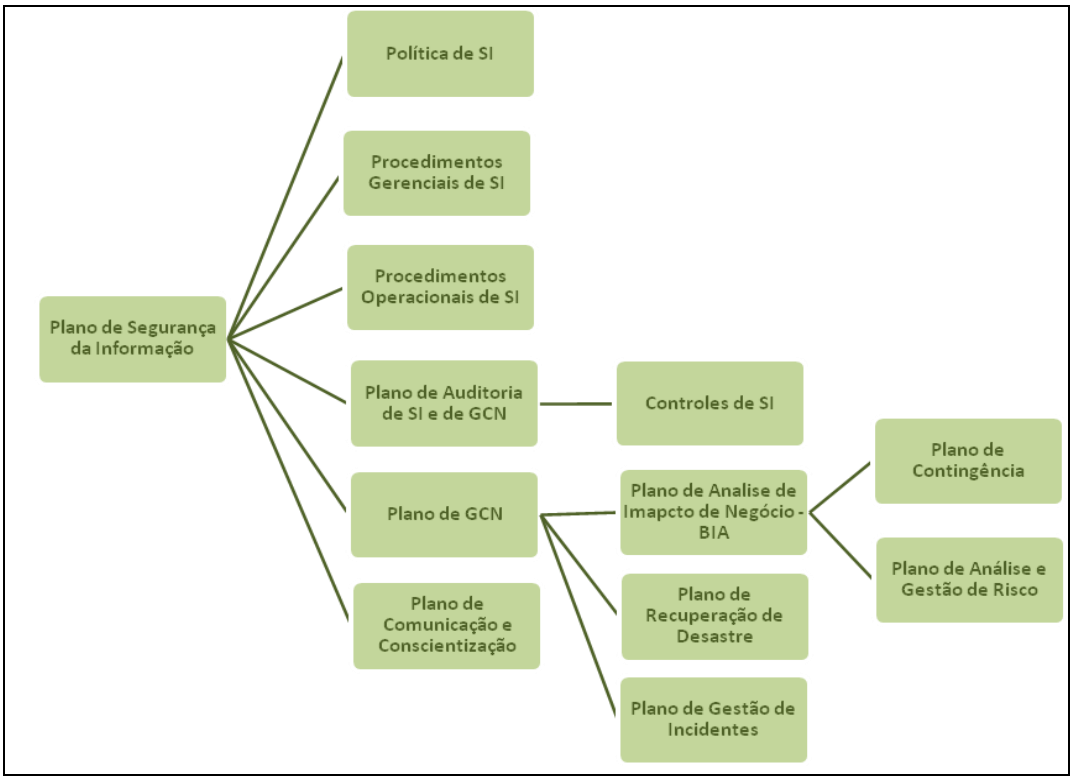


FIGURA 04 – Estrutura do plano de segurança da informação

Fonte: Elaborado pelo autor, com base na pesquisa documental.

Resumidamente, o plano de segurança da informação na organização pesquisa é composto por:

a) Política de Segurança da Informação;

A política de segurança é um documento aprovado pela diretoria da organização pesquisada e foi publicado internamente objetivando fácil acesso e conhecimento por parte de todos os colaboradores. Esse documento objetiva determinar diretrizes a serem seguidas por todos da organização e busca a preservação dos ativos tecnológicos no âmbito da segurança da informação.

b) Procedimentos Gerenciais de Segurança da Informação;

Os Procedimentos Gerenciais foram desenvolvidos levando-se em consideração a ABNT NBR ISO/IEC 27001:2006 que são as melhores práticas para se desenvolver um ambiente seguro e direcionam as atividades para o que deve ser feito para prover segurança da informação. Os procedimentos gerenciais são de conhecimento de todos da organização por estarem publicados internamente em

local de fácil acesso. Em suma, os procedimentos gerenciais direcionam o que deve ser feito para efetivar um processo de segurança da informação em diversas áreas da tecnologia da informação.

Esses procedimentos foram desenvolvidos separados por grupos tecnológicos, tais como: *hardware*, *software* e telecomunicação. Dentro de cada grupo tecnológico, os procedimentos foram desenvolvidos seguindo-se as definições estratégicas da organização e os conhecimentos obtidos através das ações de gestão do conhecimento.

Considerando as ações de gestão do conhecimento e os resultados, os procedimentos gerenciais foram desenvolvidos com mais detalhes, possibilitando real impacto no que é importante e, assim, podendo gerar impacto negativo para a organização.

c) Procedimentos Operacionais de Segurança da Informação;

Os procedimentos operacionais objetivam a efetivação dos procedimentos gerenciais e a política de segurança da informação como um todo. Esses procedimentos relacionam como as ações devem ser executadas para atender a cada item de cada procedimento gerencial.

É de suma importância que os colaboradores estejam engajados no processo da segurança como um todo. Caso contrário, os procedimentos não serão eficazes e os controles revelarão o fracasso do projeto. Essa premissa foi considerada desde o início deste projeto, contudo, a organização pesquisada ressalta a necessidade constante de revisão e avaliação dos procedimentos, bem como os resultados obtidos após suas implementações.

d) Plano de Auditoria de Segurança da Informação e de GCN;

O Plano de Auditoria é uma atividade de avaliação independente, voltada para o exame e avaliação da adequação, eficiência e eficácia dos sistemas de controle, bem como da qualidade do desempenho da política de segurança da informação, planos, metas, objetivos e normas definidas. O Plano de Auditoria contempla, entre as demais atividades, os controles de segurança da informação, possibilitando auditorias nos procedimentos operacionais.

- **Controle de Segurança da Informação.**

Os controles de segurança da informação são atividades de auditoria para garantir que os procedimentos operacionais estejam sendo cumpridos, possibilitando, assim, garantir o cumprimento dos procedimentos gerenciais e política de segurança da informação.

e) Plano de Gestão de Continuidade de Negócio;

O Plano de Gestão de Continuidade de Negócio é dividido em plano de contingência, plano de recuperação de desastre e plano de gestão de incidentes.

- **Plano de Análise de Impacto de Negócio**

O Plano de Análise de Impacto de Negócio objetiva identificar os processos de negócios considerados críticos que mais afetam a receita, ativos e clientes da organização. Esse plano permite priorizar as estratégias de recuperação que poderiam ser necessárias durante uma extensa parada dos processos de negócio na organização pesquisada.

Em suma, esse plano possibilita que a organização levante os impactos negativos para o negócio da organização em momento de crise ou interrupção, trace um plano de contingência mais eficiente. Assim, é possível que a organização também trace e execute um plano de análise e gestão de risco focado nos processos de negócio de maior impacto negativo em momento de crise.

Destacam-se como pontos principais:

a) Identificar processos e ativos da empresa que requerem o nível mais alto de proteção;

b) Incluir recomendações sobre possíveis estratégias e alternativas de recuperação de ativos;

c) Fornecer dados financeiros para ajudar a selecionar os níveis apropriados de investimento para proteção do negócio;

d) Possibilitar traçar planos para execução de análise de risco, com foco em processos de negócio mais críticos.

A análise de impacto nos negócios quantifica e qualifica a exposição aos riscos, identifica a criticidade e interdependência dos processos de negócios e das funções de suporte. A partir disso é possível se determinar os Recovery Time Objective **(**RTO) e Recovery Point Objective (RPO).

a) Recovery Time Objective – RTO: é o tempo no qual o processo de negócio é restaurado a um nível aceitável de capacidade operacional, de forma que o negócio não sofra um prejuízo significativo.

b) Recovery Point Objective – RPO: é o período de tempo máximo desejado antes de uma falha ou desastre durante o qual as alterações feitas aos dados podem ser perdidas como processo de uma recuperação.

Para elaborar a análise de impacto de negócio, foi necessário fazer o levantamento de todos os processos existentes na organização pesquisada, definindo-se o limite para a análise e identificando-se os processos de negócio, os sistemas que suportam estes processos e os ativos que suportam estes sistemas. Após a elaboração da análise de impacto de negócio, foi possível identificar os processos de negócios que, possivelmente, causam maior impacto negativo para a organização, caso alguma falha ou interrupção ocorra, possibilitando-se executar análise de risco para esse processo em específico, além de permitir a elaboração dos planos de contingência, análise e gestão de risco, recuperação de desastre e gestão de incidentes.

- ✓ **Plano de Contingência;**

O Plano de Contingência é um documento que contem os procedimentos e ações que visam à integração dos diversos planos de emergência em tecnologia da informação, bem como a definição dos recursos humanos, materiais, equipamentos e sistemas para garantir que os ativos tecnológicos estejam sempre em operação.

- ✓ **Plano de Análise e Gestão de Risco.**

O objetivo principal deste plano foi estabelecer critérios e ações para análise de risco, possibilitando identificar os pontos de vulnerabilidade do ambiente ou dos

ativos analisados, traçar um plano de ação para mitigação dos riscos, criando-se, assim, ambiente mais estável e seguro, bem como uma gestão eficiente dos riscos.

O processo de gestão de risco foi delimitado a partir das análises de impacto de negócio e dos sistemas e ativos da organização pesquisada, e foi projetado para uma efetiva gestão.

Esse plano é um dos focos principais desta pesquisa e, portanto, será apresentado com detalhamento adequado no item 5.2.3 - Planejamento de análise e gestão de riscos.

- **Plano de Recuperação de Desastre;**

O Plano de Recuperação de Desastres é um documento que contém os procedimentos e ações que visam restabelecer um determinado ativo tecnológico após incidente de desastre.

Para se implementar corretamente esse plano, foi preciso estabelecer o plano de gestão de incidentes.

- **Plano de Gestão de Incidentes.**

Este plano possibilitou traçar ações corretas para execução em momento de incidente. O plano permite cadastros e acompanhamento de incidentes internos e externos a organização, possibilitando informações para elaboração de plano de ação para tratar o incidente e objetiva minimizar os impactos negativos em momento de crise.

f) Plano de Comunicação e Conscientização

O Plano de Comunicação foi elaborado com o objetivo de possibilitar que todos os colaboradores da organização pesquisada conheçam a política de segurança da informação e os procedimentos de segurança da informação.

Esse plano tem periodicidade de revisão anual ou quando um plano de segurança da informação, ou continuidade de negócio, for modificado e suas ações de comunicação são tratadas de forma contínua e ininterruptas.

5.2.2.1 Aprovação da Estrutura de Segurança da Informação

O processo de aprovação da estrutura de segurança da informação foi fator determinante para o sucesso das ações de segurança da informação, dentre estas, as ações de planejar a análise e gerenciamento de riscos de tecnologia da informação. A organização pesquisada considera que as ações de segurança da informação só terão força, na organização, se algumas das aprovações forem feitas pelos níveis, estratégico e tático. Em especial, os processos de análise e gestão de riscos de tecnologia da informação passam por um critério especial de provação, por impactarem em ações tecnológicas e ações de negócio, necessitando alterações em infraestrutura e em regras de negócio. Quando uma dessas necessidades é levantada pelo processo de análise de risco, não há o que discutir, considerando a força previamente fornecida ao processo, por parte das aprovações efetivadas.

As aprovações seguem os seguintes níveis e critérios, conforme apresentado no QUADRO 6.

QUADRO 6 – Níveis de aprovação da estrutura de segurança da informação

	Estratégico	Tático	Operacional	Gestor Auditoria	Jurídico	Recursos Humanos
Política de Segurança da Informação	O				O	O
Procedimentos Gerenciais		O			O	O
Procedimentos Operacionais			O			
Controle Procedimentos Operacionais			O	O		
Auditoria de Segurança				O		
Plano de Segurança da Informação	O					

Fonte: Elaborado pelo autor

a) **Aprovação Estratégica:** Aprovação feita pela Presidência da organização, e Superintendência de Tecnologia da Informação. Apenas os documentos macro, ou seja, aqueles que contem informações consolidadas são aprovados por este nível, considerando que os detalhes não são expostos, porém os resultados são apresentados.

b) **Aprovação Tática:** Aprovação feita pela Gerência de Tecnologia da Informação e Governança de Tecnologia da Informação. Os documentos com detalhes mais específicos são apresentados, analisados, criticados e aprovados.

c) **Aprovação Operacional:** Aprovação pela Coordenação de Sistemas e Infraestrutura. Os detalhes operacionais são apresentados, analisados, criticados e aprovados.

d) **Gestor de Auditoria:** Aprovação feita pela coordenação da auditoria interna da organização pesquisada, objetivando estabelecer critérios para o processo de

auditoria de segurança da informação, além de estabelecer metas para o cumprimento dos procedimentos gerenciais e operacionais.

e) **Gestor Jurídico e Gestor de RH:** Aprovações para concordância de procedimentos gerenciais e políticas, objetivando concordância com a legislação brasileira.

O processo de aprovação tem um ponto de atenção, que é a determinação para que todas as políticas e procedimentos gerenciais sejam criticados e aprovados pelos departamentos de recursos humanos e jurídicos da organização. Essa ação permite maior credibilidade para as ações de segurança da informação e gestão de continuidade de negócio, resguardando o departamento de tecnologia da informação por eventuais desvios, que possa ser contrária a legislação vigente no Brasil.

5.2.3. Plano de análise e gestão de riscos

Na organização pesquisada, este plano foca as ações de análise de risco para identificar os pontos de vulnerabilidade do ambiente ou ativo analisado e traçar um plano de ação para mitigação dos riscos, possibilitando, assim, ambiente mais estável e seguro.

Essa análise de riscos consistiu no mapeamento dos ativos e processos críticos de tecnologia da informação, além da identificação de vulnerabilidades, riscos e ameaças em potencial. Tem como objetivo a elaboração de um detalhado plano de ação com os pontos positivos e focos onde ações corretivas de segurança devem ser implantadas para que sejam eliminadas as ameaças e vulnerabilidades encontradas no ambiente tecnológico.

A organização pesquisada apresentou como premissa para a elaboração das ações de análise de risco, levantar os impactos para o negócio, caso um determinado recurso tecnológico esteja indisponível. Para tanto, elaborou a análise de impacto de negócio, possibilitando identificar, em toda a organização pesquisada, os pontos de maior impacto e, assim, executar as devidas análises de risco no ambiente específico.

Após a análise de impacto de negócio, foi possível estruturar analise de risco nos sistemas e ativos que suportam um determinado processo de negócio. Essa análise de risco permitiu levantar subsídios suficientes para trabalhar na mitigação desses riscos e as informações serviram para a elaboração do plano de continuidade de negócio e plano de recuperação de desastre.

Um ponto de atenção estruturado nesse plano é que a execução de análise de risco em todo o ambiente tecnológico não foi recomendado, pois o ambiente é formado de vários processos, sistemas e ativos, tornando inviável uma análise prática e objetiva. Recomendou-se uma análise focada nos processos de negócio com maior risco atribuído, para que o processo de mitigar riscos fosse concluído com sucesso.

5.2.3.1 Análise de Risco

A análise de risco identificou, para os processos de negócio, as vulnerabilidades existentes possibilitando traçar um plano de ação no sentido de mitigar os riscos. É importante ressaltar que outras vulnerabilidades ainda podem existir, mesmo após as ações de análise de risco, mas não foram identificadas nesse processo de análise.

Ressalta-se, ainda, que a organização pesquisada baseou-se, para o processo de análise de risco, nas melhores práticas da ABNT NBR ISO/IEC 27001, ABNT NBR ISO/IEC 27002, ABNT NBR ISO/IEC 15408.

Essa análise foi implementada nos sistemas e ativos que suportam os processos de negócio e utilizaram ferramentas específicas para esta tarefa. Não é recomendada uma análise manual destas vulnerabilidades, por se tratar de atividade de alta complexidade. Como exemplo, destaca-se a análise de risco implementada em um sistema gerenciador de banco de dados ORACLE 10g. Nesse, processo as seguintes questões foram levantadas:

a) Quais são as vulnerabilidades dos sistemas suportados por um sistema gerencial LINUX FEDORA em um servidor INTEL?

b) Depois de identificadas tais vulnerabilidades, quais critérios devem ser seguidos para corrigi-las?

A análise de risco justifica a utilização de uma ferramenta específica para esta finalidade, excluindo a possibilidade de uma execução manual.

Em suma, a análise de risco foi implementada por processo de negócio, onde são suportados sistemas e ativos que podem apresentam vulnerabilidades, que se exploradas, causando riscos ao negócio, conforme ilustrado na FIGURA 5.

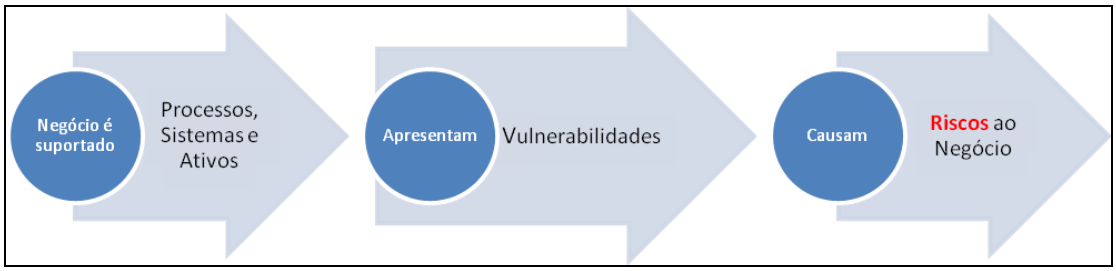


FIGURA 5 – Cadeia geradora de riscos ao negócio da organização

Fonte: Elaborado pelo autor

A análise de risco é fundamental para a mitigação e eliminação dos riscos. Entretanto, a organização pesquisada enfatiza que não é possível conhecer todas as vulnerabilidades do ambiente à tempo de eliminá-las. Apresenta como fundamental o processo de gestão de riscos, que tem como objetivo principal implementar ações para acompanhamento, eliminação ou mitigação dos riscos.

5.2.3.2 Gestão de Riscos

Com a análise de impacto de negócio elaborada, os riscos primordiais identificados e o plano para mitigação elaborado e concluído, foi possível traçar ações de gestão para acompanhamento de vulnerabilidades e falhas, registrando todos os riscos de segurança e criando plano de ação para mitigá-los. Essas ações foram coordenadas pela equipe de segurança da informação e gestão de continuidade de negócio.

O risco, se tratado de maneira superficial, pode resultar em desastre para a organização, justificando a importância de um tratamento eficaz. O processo de gestão de risco da organização pesquisada ainda apresenta pontos de atenção, ressaltando que risco não deve ser enxergado apenas como ameaça ao negócio, que de fato é, mas deve ser tratado, também, como oportunidade para o negócio, conforme ilustrado na FIGURA 6.

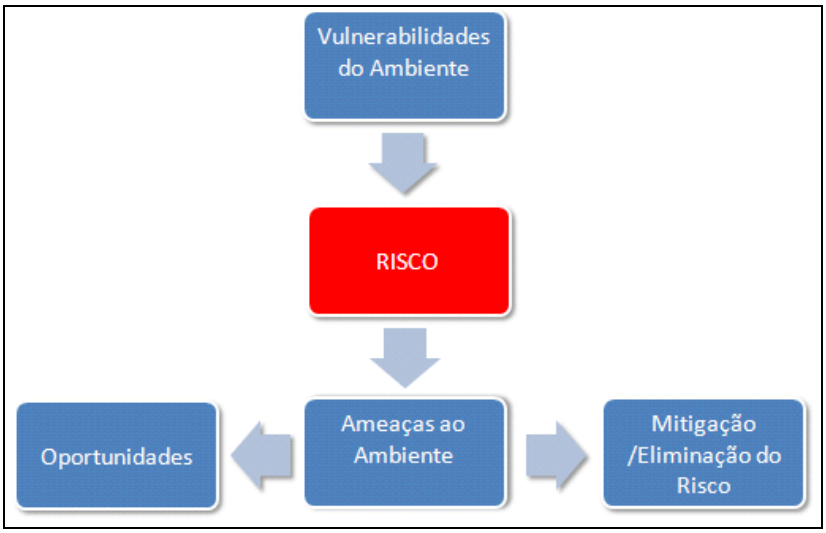


FIGURA 6 - Vulnerabilidades, riscos, mitigação e oportunidade

Fonte: Elaborado pelo autor

A organização pesquisada enxerga o processo de análise e gestão de risco também como fator de oportunidade para melhorar a estrutura tecnológica, as metodologias de trabalho e o conhecimento dos profissionais, propondo treinamentos e reciclagens de conhecimentos entre tantas outras ações possíveis e oportunas diante de um risco identificado.

Após os processos de análise e gestão de riscos, os seguintes produtos e benefícios foram apresentados à organização, tais como:

a) Relatório completo dos resultados obtidos na análise de risco, separados por processo de negócio, sistemas e ativos;

b) Conhecimento da real situação do ambiente tecnológico da organização

pesquisada;

c) Identificação das medidas de segurança apropriadas;

d) Orientação para a manutenção dos procedimentos de segurança;

e) Conhecimento das potencias ameaças ao ambiente de negócios;

f) Aderência a padrões internacionais de Segurança;

g) Vantagem competitiva, tendo em vista a melhora dos processos e sua confiabilidade.

Percebe-se, através da análise dos documentos, que pouco adianta um processo de análise e gestão de risco bem estruturado se não existe um plano de mitigação desses riscos e das vulnerabilidades do ambiente tecnológico. A organização pesquisada entende que os procedimentos adotados para mitigar ou eliminar os riscos, passa pela necessidade de conhecimento das vulnerabilidades do ambiente, além do conhecimento dos processos de negócio. Contudo, estruturaram o plano de mitigação de riscos e vulnerabilidades.

5.2.4. Plano de Mitigação de Riscos e Vulnerabilidades

Conforme afirmação de Sêmola (2003), apenas conhecer as vulnerabilidades do ambiente não é suficiente para que o plano de mitigação de riscos e vulnerabilidades nas organizações seja executado. É necessário conhecer os processos de negócio. Muitos ambientes tecnológicos estão vulneráveis devido à estrutura tecnológica necessária para atender determinado processo de negócio. Neste caso, o risco é iminente e a única ação a ser feita é de acompanhar os processos de negócio e suas execuções, permitindo subsídios para execução de ações mitigadoras, afirma Campos (2007).

Esse plano, elaborado pela organização pesquisada, tem como objetivo principal apresentar as ações necessárias objetivando a mitigação ou eliminação dos riscos e das vulnerabilidades do ambiente tecnológico.

Outra possibilidade apresentada pela organização é o desenvolvimento de um parecer técnico, sobre as vulnerabilidades e riscos encontrados em determinado processo de negócio, onde o risco é proveniente da execução e formato do referido processo de negócio. Este parecer técnico visa apresentar uma proposta de mudança para a execução do processo de negócio, para obter mais segurança.

Apenas quem conhece bem os processos de negócio da organização pode propor alguma mudança em algum desses processos, considerando, ainda, que muitos processos são relacionados, o que se justificam as ações constantes de gestão do conhecimento na organização.

Essa é uma premissa do Plano de Mitigação de Riscos e Vulnerabilidades, ou seja, conhecer o processo de negócio cujos ativos e sistemas estão passando por processo de análise de risco. Esse Plano está estruturado em etapas, que devem ser consideradas para que o resultado seja satisfatório

Primeira Etapa: Analise do processo de negócio.

Essa etapa é premissa básica para que o plano seja executado com sucesso.

Segunda Etapa: Executar as ações de análise de risco.

A análise é feita considerando-se que, se um processo de negócio pode ser suportado por mais de um sistema ou ativo de tecnologia da informação, a análise de risco poderá ser efetuada em vários sistemas e ativos, além de outros processos de negócio relacionados.

Terceira Etapa: **Estudo dos resultados da análise de risco efetuada.**

Essa é uma das etapas mais desafiadoras desse processo. É preciso determinar, dentre os resultados obtidos com o processo de análise, os riscos e as vulnerabilidades que causam esses riscos, além de identificar os impactos para a organização.

A organização pesquisada efetua as ações da segunda e da terceira etapas deste plano, utilizando um sistema específico para análise de riscos. O sistema, de nome *Risk Manager*, foi adquirido da empresa Módulo *Security* S/A, uma empresa brasileira líder mundial no segmento de análise e gestão de riscos.

Esse sistema apresenta vários modelos para análise de risco em ambientes de infraestrutura e sistemas, além de disponibilizar outros modelos para análise de risco organizacional, tais como: processos financeiros, administrativos entre outros. Além disso, o sistema, após a análise implementada, apresenta os resultados e o nível de risco do ambiente analisado, restando à organização definir se esse nível é passível de alguma ação mitigadora, conforme pode ser visto na FIGURA 7,

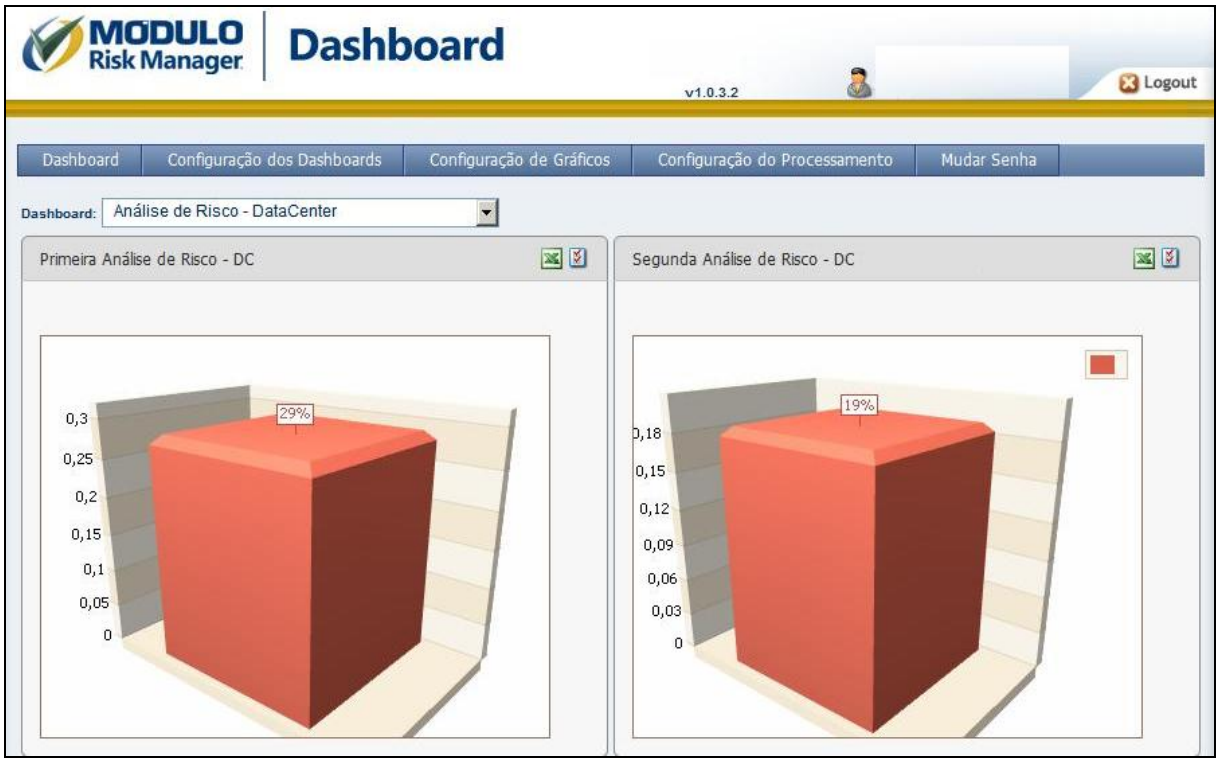


FIGURA 7 – *Dashboard* – Relatório de análise de risco

Fonte: Sistema *Risk Manager* versão 7 implantado na organização pesquisada

O sistema *Risk Manager* apresenta diversas formas de relatórios que facilitam a visualização dos ambientes ou objetos que passaram por análise de risco, além de apresentar os ambientes onde apresentam maiores riscos e os ambientes que estão em conformidade e o grau de conformidade com as recomendações do sistema em relação a riscos. Esse sistema ainda apresenta, para alguns ambientes tecnológicos, principalmente para os sistemas operacionais, tais como Windows, Unix e Linux, as ações necessárias a serem tomadas para mitigar ou eliminar os riscos encontrados.

Em suma, o sistema *Risk Manager* busca, no ambiente desejado, as vulnerabilidades, apresenta os riscos para a organização, considerando a possibilidade de alguma destas vulnerabilidades a serem exploradas, relata o nível crítico desses riscos e apresenta as possíveis medidas mitigadoras.

Quarta Etapa: Busca de conhecimento.

Essa etapa objetiva a buscar, nas bases de conhecimento da organização, possíveis ações mitigadoras para os riscos apontados. A organização considera que esta é uma importante etapa do processo, pois o sistema *Risk Manager* não apresenta as possíveis ações mitigadoras para os sistemas proprietários da organização, ou seja, para os sistemas desenvolvidos internamente, e as ações que o sistema *Risk Manager* apresenta, são frutos da base de conhecimento disponibilizada para atualização neste sistema pela empresa Módulo *Security*.

Em suma, esta etapa deve ser considerada, conforme o plano apresentado pela organização pesquisada, pois nem todas as vulnerabilidades do ambiente são conhecidas pelo sistema *Risk Manager*, além de considerar que a base de conhecimento da organização reflete a realidade do ambiente organizacional.

Quinta etapa: Elaboração e execução de plano de ação para mitigar riscos.

Essa etapa é a preparação dos planos de ação para mitigar ou eliminar os riscos observados pelas etapas anteriores e, em seguida, executar esses planos. É uma etapa técnica e deve ser executada pelos analistas que gerenciam os ambientes tecnológicos, com a finalidade de manter o ambiente íntegro após intervenções.

Portanto, é de suma importância que a elaboração e execução desse plano considere as bases de conhecimento da organização, como fonte de informação e conhecimento para a boa elaboração e execução do plano de mitigação de riscos.

Sexta etapa – Análise de relacionamento:

Esta etapa visa identificar se existem outros processos que são suportados pelos mesmos ativos ou sistemas que o processo em questão. Objetiva-se garantir que outros processos de negócio não sejam afetados pelas mudanças ocorridas objetivando a mitigação dos riscos e das vulnerabilidades.

Relatos apresentados no relatório final deste plano apontam que as ações implementadas para mitigar um risco, tratando as vulnerabilidades de um determinado ativo ou sistema, afetaram outros processos de negócio e, assim, impactos negativos para a organização foram experimentados.

Sétima Etapa – Registro de riscos e vulnerabilidades.

O processo de registrar os riscos conhecidos tem como objetivo, principalmente, criar um banco de conhecimentos na organização, permitindo que os colaboradores possam, através dessa explicitação, solucionar problemas similares em menor tempo e com maior qualidade. Essa base de conhecimento serve de subsídios para este plano, em especial para a terceira etapa deste plano.

5.3. Apresentação dos Dados Coletados nas Entrevistas

Neste capítulo, são apresentados os resultados coletados nas entrevistas efetuadas com os sete colaboradores da organização pesquisada.

A entrevista foi dividida em etapas, iniciando-se com questões sobre gestão do conhecimento, questões sobre análise e gestão de riscos de tecnologia da informação e, finalmente, passando pelas questões sobre a contribuição da gestão do conhecimento para os processos de análise e gestão de riscos de tecnologia da informação.

5.3.1. Sobre gestão do conhecimento

O resultado foi apurado com a aplicação das questões de três a seis, no sentido de se identificar quais ações foram implementadas, na organização, voltadas para a criação, coleta, organização, transferência e compartilhamento do conhecimento.

Durante as entrevistas, os entrevistados mostraram-se interessados pela pesquisa e afirmaram que o esforço da organização tem sido muito grande para empreender as ações de gestão do conhecimento e ressaltaram que os benefícios com a implementação dessas ações são visualizados imediatamente.

As ações mais mencionadas foram: a) alteração feita no portal interno da organização, possibilitando uma área específica para cada departamento da organização. Os entrevistados consideram que esta ação foi de grande importância para estabelecer um único local para disseminar conhecimento sobre diversos processos de negócio da organização, permitindo que todos os departamentos possam conhecer todos os processos da empresa. b) criação das bases de conhecimento como fatores primordiais para a gestão do conhecimento. Os entrevistados estão convictos de que essa ação permita que o conhecimento fique na organização, mesmo após a saída de algum colaborador, fato ainda comum no Departamento de Tecnologia da Informação.

Os entrevistados ressaltaram, ainda, a criação do Espaço Pilotis como a forma de integrar pessoas de diversas gerências da organização, possibilitando a criação, disseminação e compartilhamento do conhecimento.

O Gerente de Tecnologia da Informação ressalta, dentre as ações de gestão do conhecimento, as reuniões ampliadas, que acontecem uma vez por mês com a presença de todos os colaboradores do Departamento de Tecnologia da Informação objetivando nivelar o conhecimento de todos sobre os projetos em andamento.

> "Esta é uma ação primordial para que os colaboradores possam criar e compartilhar conhecimento gerando resultado imediato para a organização. Percebe-se que colaboradores que não estão diretamente inseridos em determinados projetos, colaboram com boas idéias que mudam para melhor a estrutura, seja de um sistema ou de uma infraestrutura tecnológica." **Gerente de Tecnologia da Informação.**

Esse entrevistado ainda ressalta que as bases de conhecimento são de suma importância para a explicitação do conhecimento na organização e faz com que o Departamento de Tecnologia da Informação se fortaleça, com o registro do conhecimento. Ressalta, ainda, a importância dos treinamentos tecnológicos e sobre as regras de negócio da organização e, em especial, menciona o processo de repasse dos treinamentos, pois não é possível enviar todos os colaboradores para um treinamento externo, mas acredita que estão conseguindo treinar em novas tecnologias grande parte dos colaboradores através dos repasses.

O Coordenador de Infraestrutura e Suporte, no momento da entrevista, apresentou idéias semelhantes às apresentadas pelo Gerente de Tecnologia da Informação, mostrando que há sintonia, no Departamento de Tecnologia da Informação, além de descrever os benefícios com os treinamentos e repasses, reiterando a importância das reuniões ampliadas, onde os ganhos são imediatos.

> "Funcionários treinados e motivados dão resultado imediato para a organização, pois colocam em prática o conhecimento adquirido nos treinamentos ou nos repasses, permitindo melhoras nos processos da tecnologia da informação." **Coordenador de Infraestrutura e Suporte.**

Esse coordenador ainda ressaltou a importância dos treinamentos e seminários dos quais a equipe participa, sendo essas atividades maneiras

essenciais de compartilhar conhecimento entre colaboradores da organização e profissionais de outras instituições. Ressalta, ainda, o quando são produtivos os encontros profissionais que acontecem a cada três meses.

> "Os encontros profissionais permitem que os colaboradores do Departamento de Tecnologia da Informação possam participar de uma mesa redonda com profissionais de outras gerências e até de outras empresas, possibilitando o surgimento de novos projetos, ou novas ideias, para solução, ou melhorias, de sistemas ou infraestrutura." **Coordenador de Infraestrutura e Suporte**.

Já no final da entrevista, esse coordenador ainda declarou que o processo de documentação do ambiente de infraestrutura é uma ação essencial para a retenção do conhecimento na organização, pois considera que muitos registros nesta documentação são conhecimentos criados através de experiências profissionais, permitindo que a organização tenha, de forma explícita, as experiências dos colaboradores. Reitera que não é tarefa fácil, pois alguns analistas ainda são relapsos quanto à exigência da documentação. Conclui afirmando que existe um esforço muito grande por parte de todo o Departamento de Tecnologia da Informação para que a documentação dos ambientes tecnológicos seja desenvolvida e concluída junto com os projetos ou ações de manutenção do ambiente.

A entrevista feita com o Coordenador do Departamento de Sistemas e com dois analistas de sistemas aponta, como fator primordial para a organização e para as atividades executadas por eles, as bases de conhecimentos e as reuniões de início de projetos. Em especial, esses entrevistados apresentaram-se com total sintonia, pois suas respostas foram similares e levaram a compreender que o conhecimento armazenado nas bases de conhecimento e o conhecimento compartilhado nas reuniões de início de projeto fazem a diferença em suas atividades diárias, possibilitando que os processos de desenvolvimento de sistemas tenham cada vez mais acertos.

O Coordenador do Departamento de Sistemas ainda esclareceu que a base de conhecimento para armazenar as vulnerabilidades e suas possíveis tentativas para eliminar ou mitigar riscos, é fator primordial para o início de qualquer desenvolvimento de especificação funcional e técnica para o desenvolvimento dos sistemas na organização. Conclui que a organização precisa dar mais foco ao

registro dessas informações para que possam ser tratadas como conhecimentos, pela Coordenação de Sistemas e, assim, melhorar seus processos.

Esse entrevistado ainda ressaltou a importância da documentação do ambiente de infraestrutura para o processo de compartilhamento e disseminação do conhecimento, além de considerar de suma importância a documentação funcional e técnica dos sistemas.

> "Documentar é a tarefa mais difícil em um Departamento de Desenvolvimento de Sistemas, pois são muitas atividades com tempo determinado para conclusão, porém estamos determinados a ter o maior numero de documentações com a maior qualidade possível. Acredito temos muito a ganhar, principalmente com a troca de colaboradores, fato ainda constante na organização." **Coordenador de Departamento de Sistemas.**

A entrevista feita com o Coordenador de Segurança da Informação foi uma das mais longas entrevistas e teve duração de duas horas e dez minutos. Esse profissional apresentou-se como profundo conhecedor do assunto segurança da informação, em especial sobre análise e gestão de riscos de tecnologia da informação e mostrou-se como conhecedor da teoria sobre gestão do conhecimento. Nessa entrevista, esse colaborador falou várias vezes sobre os ganhos obtidos pela organização com a implementação do portal de segurança da informação, como fonte de armazenamento de conhecimento, que pode ser acessado por todos os colaboradores da organização através da intranet. Salienta que o acesso é medido semanalmente e constatam uma média de 150 acessos semanais neste portal, o que o deixa particularmente satisfeito, considerando que o assunto segurança da informação é crítico em qualquer organização.

Esse colaborador aponta a base de vulnerabilidades - que é o sistema de registro de incidentes, riscos e vulnerabilidades - como essencial para o desenvolvimento de qualquer projeto que necessite de tecnologia da informação e informou que existiam, até o momento da entrevista, 2.414 registros nesta base de conhecimentos e que estes registros permitem análise apurada do histórico de vulnerabilidades e riscos iminentes na organização. Aponta, ainda, a possibilidade de busca por aplicativo, ou por processo de negócio, onde é possível focar em um objeto e apurar os possíveis riscos, através das conhecidas vulnerabilidades e a sua forma de tratamento, salientando que a organização como um todo deveria acessar

essa base de conhecimento e não somente o Departamento de Tecnologia da Informação.

O Coordenador de Segurança da Informação, objetivando ressaltar a importância das bases de vulnerabilidades para a organização pesquisada, afirmou que, recentemente, o Departamento Jurídico solicitou a liberação para que pudessem analisar as bases de vulnerabilidades. Justificou a necessidade disso diante de uma auditoria que acontecia na organização, cujo objetivo foi identificar os riscos no sistema de gestão de planos de saúde.

A base de conhecimento de vulnerabilidades foi o ponto de partida para as análises executadas por esta empresa de auditoria. Contudo, outros documentos foram analisados e concluíram que essa base de conhecimento, se bem explorada, possibilitará que a organização possa apresentar, rapidamente, os resultados das analises de risco por processos da organização com as ações mitigadoras ou corretivas para as vulnerabilidades e assim para a eliminação dos riscos.

A Coordenação de Projetos de Tecnologia da Informação também ressalta o portal de segurança da informação como inovação na organização, pois através de um único local é possível mapear todas as ações de segurança da informação, tão importantes para o desenvolvimento de qualquer projeto.

Salienta que a gestão dos projetos está sendo mais ágil e com mais qualidade, possibilitando prever problemas e riscos em diversos projetos. Essa Coordenação ainda destaca os *blogs* técnicos e de negócio da organização como uma fonte de acompanhamento de projetos. Afirma que muitos projetos de tecnologia da informação, ao serem iniciados, provocam quase que em momento imediato, conversas nos *blogs*, permitindo que o traçado inicial do projeto seja, inclusive, alterado, conforme as conversas evoluem. Afirma, ainda, que a qualidade das especificações tem aumentado gradativamente e os resultados são cada vez melhores, além de reduzir os prazos. Conclui que a base de conhecimento que contém lições aprendidas em projetos de tecnologia da informação está sendo constantemente acessada por colaboradores da organização e os acertos e os erros experimentados em cada projeto servem de conhecimento inicial para a determinação de novos projetos.

A entrevista com a Coordenação de Governança de Tecnologia da Informação apontou os *blogs* e as listas de discussão como fatores essenciais para disseminar e compartilhar o conhecimento na organização. Ressaltou que os colaboradores gostam de deixar explícitos seus conhecimentos sobre assuntos da organização, pois acreditam que esta é a porta de entrada para alcançar maiores colocações na organização além de serem convidados a participar de projetos essenciais para a organização e serem escolhidos para os treinamentos e seminários. Ressaltou ainda que, para a organização, essa ação é lucrativa, pois o conhecimento fica armazenado.

Esse entrevistado ainda chamou a atenção para os *sites* pessoais, em que cada colaborador tem uma área determinada e, com isso, pode inserir seus conhecimentos técnicos e sobre o negócio da organização.

A entrevista com a Supervisão do Núcleo de Gestão do Conhecimento foi especialmente abrangente, permeando todas as ações executadas e apresentando alguns resultados. Destacou o papel dos seminários internos, que são constantemente promovidos, nos quais os debates sobre assuntos técnicos e processos de negócios são estimulados, gerando, com isso, uma base de conhecimento de grande valor, além de inúmeros planos de ação para melhorias contínuas, além de novos sistemas ou processos de negócio.

Todos os entrevistados percebem o esforço da gestão da organização para promover as ações de gestão do conhecimento e, em especial, percebem o esforço do Núcleo de Gestão do Conhecimento para promover essas ações. Acreditam ainda que, a médio prazo, esse núcleo será promovido, com a criação da Gerência de Gestão do Conhecimento, onde esse assunto será tratado com força por toda a organização e não somente pelo Departamento de Tecnologia da Informação.

A Supervisão do Núcleo de Gestão do Conhecimento aponta a criação dos ambientes, como o Espaço Pilotis e as salas de treinamento, como espaços destinados à criação do conhecimento, disseminação e compartilhamento do conhecimento. Chama a atenção para que outros ambientes sejam criados, como, por exemplo, salas de reuniões com possibilidade de executar vídeo conferência, para facilitar e agilizar as reuniões entre colaboradores que estejam em outras unidades da organização. Esse mesmo entrevistado acredita que, ao facilitar a

comunicação entre os colaboradores da organização, o conhecimento poderá ser compartilhado com mais rapidez e, com isso, a organização ganha agilidade nos projetos e melhoria dos processos.

> "Já conseguimos muito, porém ainda necessitamos de mais áreas para promover a disseminação e compartilhamento de conhecimento. Espero no futuro conseguir salas de reuniões com videoconferência e equipamento multimídia, para proporcionar um contato rápido e direto com colaboradores de outras unidades." **Supervisão do Núcleo de Gestão do conhecimento.**

5.3.2. Sobre Governança de Tecnologia da Informação – Analisar e gerenciar riscos de tecnologia da informação

Os resultados foram apurados com a aplicação das questões 7 e 8 com o objetivo de se verificar quais são as ações de analisar e gerenciar os riscos de tecnologia da informação.

As entrevistas foram produtivas e comprovam o conhecimento de todos os entrevistados sobre as ações de análise e gestão de riscos de tecnologia da informação e, sobretudo, que entendem que essa ação é de suma importância para os processos de negócio da organização. Os entrevistados ressaltam que contribuem diretamente para essas ações quando iniciam qualquer projeto, ou solução de problema, pela base de vulnerabilidades, estudando as ações já implementadas para eliminar ou mitigar os riscos.

Para o Gerente de Tecnologia da Informação, analisar e gerenciar riscos de tecnologia da informação é papel fundamental de todos os colaboradores da tecnologia da informação, mas, aponta os colaboradores do desenvolvimento de sistemas e infraestrutura e suporte como os colaboradores que devem ter maior atenção com suas ações. Afirma ainda que com a aquisição do sistema *Risk Manager* essas ações foram facilitadas.

> "Não é admissível um ambiente desatualizado, no qual servidores, sistemas e ativos tecnológicos não estejam com as ultimas atualizações, disponibilizadas pelos fabricantes aplicadas. Muitas destas atualizações são disponibilizadas para eliminar vulnerabilidades e se queremos ter um ambiente livre de riscos, este é o primeiro passo e o mais leve de todos." **Gerente de Tecnologia da Informação.**

Sobre os investimentos feitos no ambiente tecnológico, para permitir ações eficientes de analisar e gerenciar riscos de tecnologia da informação, o Gerente de Tecnologia da Informação afirma que a organização investiu uma quantidade considerável de recursos para adquirir licenças de uso do sistema *Risk Manager*. Todo esse investimento foi feito para que o processo de análise e gestão de risco fosse executado com total transparência, esperando-se um resultado sempre positivo.

Esse gerente ainda ressalta que o sucesso em ações de análise de risco é encontrar problemas. Portanto, quando uma análise de risco é executada e nenhuma vulnerabilidade é encontrada, é preciso refazer ou rever o processo de execução e afirma que sempre existirá vulnerabilidade em qualquer ambiente, por conseqüência, sempre existirão riscos nos ambiente tecnológicos.

O Gerente de Tecnologia da Informação afirma, também, que analisar e gerenciar riscos não são tarefas fáceis para qualquer organização, além de ser um processo caro. Entretanto, permite que a organização trabalhe de forma cada vez mais proativa, deixando a reatividade nas ações de caráter emergenciais cujo risco não tenha sido identificado anteriormente.

Para o Coordenador de Desenvolvimento de Sistemas, as ações de análise e gestão de riscos de tecnologia da informação mudam suas atividades e seus projetos, pois quando uma vulnerabilidade é descoberta e esta gera risco para o ambiente, imediatamente um plano de ação deve ser desenvolvido e sua execução deve ser imediata.

> "Um plano de ação com execução imediata requer paralisação de outras atividades e projetos, desmontando equipes já coesas, para que possam executar este plano. Isso significa em atrasos para os novos projetos. Estes atrasos justificam a análise mais apurada da base de conhecimento de vulnerabilidades antes de iniciar qualquer projeto." **Coordenação de Desenvolvimento de Sistemas.**

O Coordenador de Segurança da Informação ainda aponta a gestão de riscos como fator de atenção. Ressalta que é necessário analisar, diariamente, as atualizações enviadas pelos fabricantes dos sistemas e dos equipamentos

tecnológicos, para identificar necessidades urgentes de atualizações, já que aplicar atualizações é um processo demorado e crítico, exige tempo de parada do ambiente tecnológico e somente poderá ser executado nos finais de semana.

> "Caso tenhamos que paralisar um ambiente para aplicar uma atualização para eliminar ou mitigar um uma vulnerabilidade e conseqüentemente reduzir o risco tecnológico, esta paralisação será feita sem a espera das datas semanais previamente programadas. Por isso, a gestão é de suma importância. O quanto antes identificarmos a necessidade de atualização, menor será o risco da organização." **Coordenador de Segurança da Informação**

A Coordenação de Governança de Tecnologia da Informação salienta que a Coordenação de Segurança da Informação foi criada em detrimento da quantidade de ações necessárias, principalmente para analisar e gerenciar riscos de tecnologia da informação. Além disso, a referida Coordenação enxerga como necessária a criação de uma Gerência de Segurança da Informação para que as ações sejam implementadas de forma corporativa.

Ressalta, ainda, que as ações de análise e gestão de riscos só podem ser bem implementadas se o processo de negócio for bem conhecido. Com isso, o primeiro passo a ser dado deve ser o estudo do processo de negócio, posteriormente o estudo dos sistemas e ativos que suportam esses processos e, por fim, as possíveis vulnerabilidades que se exploradas possam causar riscos para o negócio da organização.

Esse entrevistado complementa que é necessário executar análise de risco para os processos de negócio pensando nas pessoas. Informa que a organização está trabalhando com ações dessa natureza, pois os maiores problemas para a segurança da informação são as pessoas que exploram as vulnerabilidades conhecidas e que essas pessoas podem ser os colaboradores da organização. Com isso, justifica-se um intenso trabalho para identificar se os colaboradores internos estão usando de vulnerabilidades conhecidas para burlar os sistemas e resultados.

> "Já estamos analisando as ações dos colaboradores em cada um dos sistemas da organização, analisando os registros de ações executadas. Acreditamos que esta ação poderá mostrar para a organização as vulnerabilidades ainda não identificadas pelos nossos processos e assim possibilitar ação de mitigação imediata, além de apresentar para a

> organização a conduta dos colaboradores. Este processo ainda está embrionário, mas vai evoluir muito e de forma rápida, pois os demais processos de análise e gestão de riscos já estão maduros.” **Coordenação de Governança de Tecnologia da Informação**

Em geral, todos os entrevistados afirmaram que as ações executadas por eles, relativas ao processo de analisar e gerenciar riscos de tecnologia da informação passam, basicamente, pela execução do plano previamente desenvolvido. Afirmam ainda que, sempre no início de uma análise de risco, eles estão envolvidos, seja para analisar o processo de negócio, seja para prover suporte em relação aos ativos de tecnologia ou sistemas em análise.

Relatam, ainda, que seguem um cronograma de ações de análise de risco e o uso do sistema *Risk Manager* é um facilitador. Entretanto, os entrevistados ressaltam que o sistema *Risk Manager* não permite, de forma nativa, a análise de todos os sistemas ou arquiteturas de infraestrutura presentes na organização, mas é necessária a intervenção dos analistas de segurança da informação para criar as condições e critérios de análise. Reiteram, também, a necessidade de constante atualização desse sistema para que as análises sejam cada vez mais eficientes.

Concluem que, com as atualizações do sistema *Risk Manager*, as análises estão ficando cada vez mais detalhadas e, com isso, os resultados das análises de risco apresentam vulnerabilidades e possíveis impactos no ambientes jamais percebidos ou pensados.

> “Acredito que o sistema *Risk Manager* seja uma das mais importantes aquisições da organização para o processo de analise e gestão de riscos. Com isso, a equipe envolvida neste processo cresce profissionalmente, pois aprendemos diariamente com as indicações de risco e recomendações para mitigá-los ou eliminá-los.” **Coordenador de Segurança da Informação**.

5.3.3. Contribuição da gestão do conhecimento para os processos de análise e gestão de riscos de tecnologia da informação.

O resultado deste item foi apurado com a aplicação das questões 9, 10 e 11, e objetivou conhecer as contribuições da gestão do conhecimento para o processo de analisar e gerenciar riscos de tecnologia da informação.

Todos os entrevistados consideram que as ações de gestão do conhecimento contribuem para os processos de análise e gestão de riscos, e apontam, especialmente, para as ações denominadas de reunião de lições aprendidas em projetos e as bases de conhecimentos como determinantes.

Para o Coordenador de Projetos de Tecnologia da Informação, a reuniões de lições aprendidas contribuem muito para conhecer as dificuldades e facilidades dos projetos, facilitando o início e condução de projetos já em produção. Afirma, ainda, que os registros das lições aprendidas são de extrema importância, pois a rotatividade de funcionários na organização é muito grande e o conhecimento não é perdido com a saída de alguns colaboradores.

Esse Coordenador ainda aponta as bases de conhecimentos como fundamentais para o processo de analisar e gerenciar riscos de tecnologia da informação.

> "Não é possível gerenciar riscos sem conhecer as ocorrências, sejam de sistemas ou infraestrutura, além de ser impossível estruturar novos projetos sem conhecer o que ocorreu com os projetos passados, contudo, as bases de conhecimentos são fatores essenciais para definir por onde começar a análise de risco e como estruturar esta análise." **Coordenador de Projetos de Tecnologia da Informação.**

O Coordenador de Desenvolvimento de Sistemas ressalta que alguns colaboradores ainda resistem sobre as ações de gestão do conhecimento, e acredita que esta resistência ainda persiste, pois estes colaboradores não conhecem ou não perceberam os benefícios destas ações, e que, com isso, atrapalham as ações de análise e gestão de riscos de tecnologia da informação. Afirma que o conhecimento disseminado nas reuniões de lições aprendidas se perde em poucos dias, por isso insiste que este conhecimento tem que ser cadastrado por todos.

Esse mesmo coordenador reconhece que os constantes seminários internos de tecnologia da informação são importantes, pois os processos de análise e gestão de riscos de tecnologia da informação não são papel apenas da equipe de segurança da informação, mas um dever de todos os profissionais do Departamento de Tecnologia da Informação

> "Os seminários internos de TI são importantes, pois para fazer análise e gestão de riscos é preciso conhecer de vários

> assuntos dentro da TI além de ser dever de todos os profissionais do departamento. Para desenvolver sistemas seguros é preciso conhecer os riscos e vulnerabilidades do ambiente da empresa e este assunto várias vezes foram abordadas nestes seminários." **Coordenador de Desenvolvimento de Sistemas**

Para as Coordenações de Segurança da Informação e Governança de Tecnologia da Informação, as ações de gestão do conhecimento contribuem, diretamente, para as definições dos processos de análise gestão dos riscos, pois é impossível tratar vulnerabilidades, mitigar ou eliminar riscos sem conhecer os processos de negócio. Contudo, ações de gestão do conhecimento, como as bases de conhecimentos são de suma importância para que ocorra um acompanhamento desses processos de negócio, além das reuniões gerenciais e reuniões de início de projeto. Essas ações são bases iniciais para qualquer início de análise e gestão de riscos e apresenta um exemplo que ilustra sua fala.

> "Estávamos planejando a análise de risco para o processo de auditoria de controle de medicamentos, pois muitos medicamentos eram utilizados sem a cobrança devida. Este processo é suportado por um módulo do sistema de controle hospitalar. Ao analisar a base de conhecimento, verificamos 6 ocorrências sobre este assunto, onde apontavam para uma falta de integração com o processo de controle de pacientes, onde identificamos que este controle não considerava os medicamentos destinados aos pacientes que estavam sendo atendidos pelo pronto atendimento. Era preciso identificar de forma manual qual paciente usou determinado medicamento. Isso era feito através de análise de relatório. Com isso, implementamos uma análise de risco nos dois processos e apontamos esta falha, que foi corrigida." **Coordenações de Segurança da Informação**

O Coordenador de Segurança da Informação ainda afirmou que constantemente altera a forma de execução da análise de risco, por considerar as ações de gestão do conhecimento.

> "Conhecer os processos de negócio, as dificuldades de implementação de sistemas e até os eventuais erros encontrados pelos usuários, motiva alterações nos processos para a execução das análises de risco. Considero que estas alterações são essenciais para a melhoria das análises. Conseguimos com isso, fazer uma análise focada no problema, não sendo necessário analisar todo o processo, mas sim, a parte onde as ações de gestão do conhecimento já identificaram dificuldades" **Coordenador de Segurança da Informação**

Esse Coordenador ainda ressalta que os resultados das análises e da gestão de riscos de tecnologia da informação são conhecimentos criados que, quando

registrados, passam a ser fontes de informação e conhecimento para a organização e conclui que esses resultados são fundamentais para futuras estratégias de análise e gestão de riscos de tecnologia da informação.

> "É um ciclo. Os resultados das análises, quando registradas, são vistas como informações e conhecimentos para outros processos de análise e para a organização como um todo." **Coordenador de Segurança da Informação**

O Coordenador de Governança de Tecnologia da Informação ressalta que as definições de análise e gestão de riscos podem sofrer alterações a cada resultado obtido. Salienta que essas definições consideram os resultados apresentados de análises já implementadas além de considerar bases de conhecimentos e o exposto nas reuniões e seminários e conclui que nenhuma análise de risco segue a mesma definição da análise anterior.

> "Não é possível usar sempre a mesma definição para analisar o mesmo objeto, pois muitas mudanças acontecem na organização, sejam estas de tecnologia ou de negócio e por isso usar sempre o mesmo critério e encontrar sempre o mesmo risco, se ainda não tiver sido tratado ou não encontrar riscos, caso o tratamento já tenha sido implementado. Trabalhamos com a realidade da organização e as ações de gestão do conhecimento são as matérias primas que necessitamos para nossas definições." **Coordenador de Governança de Tecnologia da Informação**

Para o Coordenador de Infraestrutura e Suporte de Tecnologia da Informação, tanto a base de conhecimento quanto a base de vulnerabilidades são de grande importância no momento de compra de ativos de tecnologia, além de nortear os processos de manutenção evolutiva e corretiva da infraestrutura da organização. Esse Coordenador ressalta que erram menos, pois já conhecem as vulnerabilidades e já sabem como tratá-las, com isso permitem menores impactos negativos nos ambientes, contribuindo para a melhoria nos processo de analisar e gerenciar riscos de tecnologia da informação.

O Núcleo de Gestão do Conhecimento afirma que a empresa se tornou mais segura após as ações de gestão do conhecimento, principalmente para os processos de análise e gestão de riscos, pois as ações de criação, compartilhamento e disseminação do conhecimento são incentivadas, constantemente. Apesar de alguns colaboradores ainda apresentarem resistência,

esse conhecimento é fator determinante para de definições dos processos de análise e gestão de riscos.

> “Como seria possível efetuar processos de gestão de riscos sem saber o que acontece na organização, quais são as mudanças efetivadas ou propostas e quais são os problemas experimentados. Sem as ações de gestão do conhecimento não temos porque fazer gestão de riscos. Poderíamos fazer as análises de riscos, mitigar ou eliminar os riscos e o processo estaria terminado. Fazemos a gestão exatamente porque entendemos que as mudanças são constantes e somente será possível conhecer as mudanças se os processos de gestão do conhecimento forem considerados.” **Supervisor do Núcleo de Gestão do Conhecimento**

O Gerente de Tecnologia da Informação afirma que a base de conhecimento mais acessada é à base de riscos e vulnerabilidades, e que está sendo alvo primário das auditorias externas contratadas pela organização. Informou que os auditores estão traçando o risco organizacional considerando também os relatos apresentados das vulnerabilidades descobertas, dos riscos eminentes e as ações executadas para mitigar ou eliminar esses riscos. Reitera que as bases de conhecimentos estão sendo utilizadas para outras ações que não foram pensadas no início do projeto.

Ressaltou ainda que as coordenações de infraestrutura e suporte e de desenvolvimento de sistemas estão, constantemente, analisando os resultados das análises de risco, e com isso, elaborando melhorias tecnológicas. Afirmou, também, que através da relação da gestão do conhecimento e dos resultados das análises de risco, alterações são propostas para a execução dos processos de negócio, possibilitando aumento de segurança e até redução de tempo nas execuções. Além disso, as ações de gestão do conhecimento contribuem para as definições de análise e gestão de riscos, pois os resultados das análises de riscos não são iguais, considerando um mesmo objeto, apontando que o conhecimento criado e compartilhado está sendo utilizado para as definições dos processos de análise e gestão de riscos.

Um importante ponto foi abordado pelo Coordenador de Desenvolvimento de Sistemas ao relatar que o interesse pelo registro de conhecimento é pequeno, apesar dos esforços da empresa em promover essa necessidade. Afirma, porém, que o processo é importante e poderia ter resultado mais satisfatório se fosse realmente utilizado por todos do Departamento de Tecnologia da Informação.

> “Algumas vezes encontramos problemas na infraestrutura, que já passou por uma análise de risco. Estes problemas impactam diretamente nos sistemas que desenvolvemos, com isso, existem atrasos nas entregas e insatisfações das áreas de negócio. Acredito que nem todas as ações de gestão do conhecimento contribuem para as definições do processo de analisar e gerenciar risco, pois não são exploradas na integra ou não são utilizadas pelos demais colaboradores.” **Coordenador de Desenvolvimento de Sistemas**

O entrevistado conclui relatando que a base de conhecimentos com as vulnerabilidades conhecidas, através do processo de análise e gestão de riscos, é fundamental para as manutenções e desenvolvimento de aplicações. Os resultados das análises de risco, em geral, motivam a criação de um plano de ação para a equipe de manutenção de sistemas. No processo de desenvolvimento de qualquer especificação funcional de um novo sistema, esta base de conhecimento é consultada e considera que já contabilizam ganhos positivos, pois os sistemas estão mais estáveis e as análises de riscos têm apontado cada vez menos vulnerabilidades. Porém afirma que o resultado poderia ser ainda melhor, se todos os colaboradores conscientizassem da importância dos registros de ocorrências nas bases de conhecimentos.

6. ANÁLISE E DISCUSSÃO DOS RESULTADOS

Neste capítulo, apresenta-se a relação dos resultados da pesquisa documental com o resultado das entrevistas. É importante ressaltar que, durante a análise e discussão dos resultados, novas questões foram surgindo e, com isso, foram feitos contatos com os entrevistados, através de e-mail e telefone, no sentido de sanar as dúvidas e efetivar confirmações.

Portanto, optou-se pela seguinte estrutura para a discussão e análise de resultados:

a) Análise e discussão dos resultados sobre gestão do conhecimento;

b) Análise e discussão dos resultados sobre análise e gestão de riscos de tecnologia da informação;

c) Análise e discussão dos resultados sobre as contribuições da gestão do conhecimento para os processos de analisar e gerenciar riscos de tecnologia da informação.

6.1. Análise e discussão dos resultados sobre gestão do conhecimento.

Os resultados das pesquisas apontam que os colaboradores conhecem as ações de gestão do conhecimento implementadas na organização, conforme suas afirmações e respostas dadas às questões. Apontam, também, que esses colaboradores seguem as orientações do Núcleo de Gestão do Conhecimento para a constante execução e utilização dessas ações.

A pesquisa mostra que as bases de conhecimento são as ações mais consideradas pelos colaboradores da organização em momentos de implementação de projetos ou planejamento de manutenções evolutivas ou corretivas nos ambientes de tecnologia da informação e que os colaboradores entrevistados

enxergam as bases de conhecimento como uma ação efetiva de gestão do conhecimento. A pesquisa aponta, ainda, que essas ações fornecem subsídios diretamente os colaboradores que planejam e executam os processos de analise e gestão de riscos de tecnologia da informação.

Durante a pesquisa, os entrevistados, cujas atividades estão diretamente ligadas com as ações de analisar e gerenciar riscos de tecnologia da informação, relatam que as bases de conhecimento são fundamentais para o planejamento de suas atividades e concluíram que, sem conhecer a organização, é impossível planejar processos de analisar e gerenciar riscos. Assim, para eles, a maneira mais adequada para conhecer a organização é a constante utilização das bases de conhecimento, apontadas por eles como ação primordial do Núcleo de Gestão do Conhecimento.

Percebeu-se ainda, com a análise dos resultados, que os colaboradores acreditam nas ações de gestão do conhecimento, apesar de confirmarem que alguns ainda apresentam-se resistentes. Ainda assim, acreditam que o constante amadurecimento dessas ações fará com que a resistência seja superada.

A pesquisa apresentou uma tendência para a disseminação das ações de gestão do conhecimento para toda a organização, tendo em vista os benefícios apresentados pelo Departamento de Tecnologia da Informação.

Os entrevistados apontam os benefícios diretos para a criação, disseminação e compartilhamento do conhecimento com a implantação das salas de treinamentos e reuniões, equipadas com tecnologias multimídia, além de apontarem o espaço Pilotis como um ganho para a gestão do conhecimento.

As reuniões de início de projetos, reuniões ampliadas e bate papo gerencial foram apontadas como a melhor forma de aproximação entre os colaboradores alocados diretamente em projetos e ressaltaram que essa ação permite que todos os colaboradores possam conhecer os projetos em execução, na organização. As pesquisas ainda apontam que soluções e novas definições para os projetos nascem nessas reuniões, permitindo melhoras constantes.

Algumas ações de gestão do conhecimento levantadas através da pesquisa documental pouco, ou nenhuma vez, foram citadas pelos colaboradores, durante as

entrevistas, tais como: *blogs*, portal interno e a documentação de ambientes. Por outro lado, as bases de conhecimento foram amplamente citadas pelos entrevistados, podendo-se considerar isso como um indício indispensável para o planejamento das ações de comunicação ligadas às ações de gestão do conhecimento nas organizações.

6.2. Análise e discussão dos resultados sobre análise e gestão de riscos de tecnologia da informação.

Analisar e gerenciar riscos de tecnologia da informação é um dos processos das ações de governança de tecnologia da informação e, durante a pesquisa, muitos colaboradores ressaltaram a importância dessas ações para a organização, não só como fator de segurança da informação mas, também, como fator necessário para melhorias e inovações nos sistemas e infraestrutura de tecnologia da informação.

Um ponto importante levantado durante a pesquisa, é que o resultado dos processos de analisar e gerenciar os riscos de tecnologia da informação está sendo utilizado pela organização como fonte de informações para as ações das auditorias, tendo em vista que o planejamento dos processos de análise e gestão de riscos considera as ações de gestão do conhecimento.

Portanto, concluem os entrevistados, que o processo de análise e gestão de riscos apresenta resultados de riscos corporativos e não somente de tecnologia da informação, apesar do direcionamento dessas ações estarem diretamente voltado para as ações de tecnologia da informação. Essa conclusão pode ser confirmada analisando-se o planejamento dos processos de análise e gestão de riscos de tecnologia da informação. O planejamento considera os processos de negócio organizacional como fonte principal para a análise de riscos, e não somente os sistemas e ativos que suportam estes processos. As análises de risco consideram, em primeira instância, os processos de negócio e, logo em seguida, os sistemas e ativos de tecnologia da informação que suportam esses processos de negócio.

Os processos de análise de risco foram amplamente discutidos durante as entrevistas e um vasto material sobre o assunto foi analisado na organização. Entretanto, muito pouco foi dito sobre o processo de gestão de riscos de tecnologia

da informação. Os entrevistados ressaltaram, durante as entrevistas - em especial os colaboradores com atividades diretamente voltadas para os processos de analisar e gerenciar riscos de tecnologia da informação - que os resultados das análises são registrados nas bases de conhecimento, mas o processo de gestão desses resultados foi pouco explorado.

Sendo assim, a pesquisa apresenta resultados positivos, considerando-se as ações de análise de riscos de tecnologia da informação, além de apresentar indícios sobre a necessidade de melhorias no processo de gestão destes riscos. A pesquisa ainda aponta que, diante da abordagem estabelecida pela organização pesquisada, ao se analisar riscos, considerando-se os processos de negócio, esses riscos são entendidos como corporativos e não somente como riscos de tecnologia da informação.

6.3. Contribuição da gestão do conhecimento para os processos de analisar e gerenciar riscos de tecnologia da informação.

A pesquisa feita com os colaboradores, após a análise dos resultados, aponta que as ações de gestão do conhecimento contribuem para os processos de analisar e gerenciar riscos de tecnologia da informação, em especial pelos seguintes fatores:

a) O processo de análise e gestão de riscos de tecnologia da informação é planejado conforme os conhecimentos obtidos através das bases de conhecimento que são ações diretas e reconhecidas, pelos colaboradores, como ações de gestão do conhecimento.

b) Os resultados das análises de riscos são armazenados nas bases de conhecimento e são fontes primárias para novas análises. Percebe-se, com a pesquisa, que à medida que os resultados são armazenados e considerados em novas análises, melhor será o nível do conhecimento sobre o assunto análise e gestão de riscos, na organização pesquisada, além de permitir que eventuais erros nos processos de analisar e gerenciar riscos de tecnologia da informação sejam corrigidos.

c) As questões levantadas pelos usuários dos sistemas e pelos colaboradores do Departamento de Tecnologia da Informação a respeito das possíveis vulnerabilidades no ambiente tecnológico, são consideradas no planejamento de análise e gestão de riscos. Apenas através de ações de gestão do conhecimento é possível armazenar essas questões levantadas e permitir que elas sirvam de insumos para o planejamento das ações de analisar e gerenciar riscos de tecnologia da informação.

d) As discussões apresentadas e armazenadas durante as reuniões de início de projeto, reuniões ampliadas e bate papo gerencial são consideradas em situações de planejamento dos processos de analisar e gerenciar riscos de tecnologia da informação. A pesquisa aponta que o conhecimento criado com essas ações de gestão do conhecimento são primordiais para se definir estratégias de análise e gerenciamento dos riscos, além de permitir haja uma melhora substancial nos processos de desenvolvimento e manutenção de sistemas e infra estrutura, reduzindo as vulnerabilidades, aumentando a segurança do ambiente tecnológico pela redução dos riscos e, conseqüentemente, diminuindo os iminentes impactos negativos para a organização.

e) As bases de vulnerabilidades conhecidas são essenciais para o planejamento de qualquer análise de risco na organização pesquisada, pois retratam a realidade do ambiente tecnológico e apresentam medidas mitigadoras ou de eliminação de riscos e, com isso, minimizam os impactos negativos na organização. Essa base de conhecimento é uma eficaz ação de gestão do conhecimento e permite, ainda, que auditorias externas a usem para suas análises corporativas, sobre os riscos da organização.

f) O portal de segurança da informação centraliza as informações sobre vulnerabilidades, riscos e ações mitigadoras e permite que os colaboradores possam interagir e discutir os processos de analisar e gerenciar riscos de tecnologia da informação. Com isso, o

> conhecimento sobre o assunto fica armazenado e novos conhecimentos são criados.

Porém, a relação de contribuição entre gestão do conhecimento e análise e gestão de riscos somente foi apontada, com detalhes, pelos Coordenadores de Segurança da Informação e Governança de Tecnologia da Informação e pelo Gerente de Tecnologia da Informação. A pesquisa aponta uma necessidade de expandir o conhecimento da possível relação entre gestão do conhecimento e análise e gestão de riscos ou, pelo menos, apresenta uma real necessidade de criar condições para que essa análise crítica seja feita para identificar mais relações entre a gestão do conhecimento e a análise e gestão de riscos.

Os demais coordenadores apontam a importância e contribuição da gestão do conhecimento para analisar e gerenciar riscos de tecnologia da informação, mas ficaram presos ao afirmar o uso das bases de conhecimento como fonte primária de conhecimento para definir as ações de analisar e gerenciar riscos de tecnologia da informação. Muito pouco, ou quase nada, foi dito sobre as outras ações implementadas e suas relações de contribuição entre gestão do conhecimento e análise e gestão de riscos de tecnologia da informação.

7. CONSIDERAÇÕES FINAIS – CONCLUSÃO

Este trabalho de pesquisa investigou a temática denominada gestão do conhecimento e governança de tecnologia da informação em uma organização do setor de saúde.

Objetivou-se investigar e analisar na literatura o assunto gestão do conhecimento e governança de tecnologia da informação com foco no processo de análise e gestão de riscos de tecnologia da informação.

Através da pesquisa de campo, objetivou-se apresentar as práticas de gestão do conhecimento e, apresentar e analisar as características do modelo de governança de tecnologia da informação, considerando-se o processo de análise e gestão de risco de tecnologia da informação na organização pesquisada.

Buscou-se também responder quais as possíveis contribuições da gestão do conhecimento para o processo de avaliar e gerenciar os riscos de tecnologia da informação, que é parte integrante do modelo de governança de tecnologia da informação nesta organização.

Como marco teórico, esta pesquisa considerou os autores Nonaka e Takeuchi (1997), referência no assunto gestão do conhecimento. Estes autores apresentam em seus estudos, os benefícios para as organizações que utilizam os conceitos da gestão do conhecimento e que estes conceitos são primordiais para o sucesso de qualquer organização.

Nonaka e Takeuchi (1997) concluem em seus estudos que as organizações que praticam as ações de gestão do conhecimento são mais inovadoras, e que este resultado só é possível com implementação de processos de criação do conhecimento organizacional. Estes autores ainda ressaltam que as organizações devem incentivar e dar condições a seus colaboradores para exercerem ações de criação de novos conhecimentos.

Ações de gestão do conhecimento na organização devem estar alinhadas com as metas organizacionais, conforme afirmação de Nonaka e Takeuchi (1997), a exemplo do que o COBIT (2006), marco teórico para o assunto governança de tecnologia da informação, apresenta.

Para o COBIT (2006), um dos aspectos que a governança de tecnologia da informação tenta garantir é que a tecnologia da informação esteja alinhada com o negócio da organização e o torne possível e maximize seus benefícios. Outro importante aspecto relatado pelo COBIT (2006) é que os riscos associados à tecnologia da informação devem ser gerenciados de maneira apropriada.

Sêmola (2003) afirma que as vulnerabilidades encontradas nos processos de negócio das organizações, se exploradas, geram riscos diretos para esta organização, e que os impactos destes riscos devem ser gerenciados e medidos, possibilitando definir ações para mitigá-los, e afirma que o processo de analisar e gerenciar riscos de tecnologia da informação deve ser constante e ininterrupto

Após identificar as práticas de gestão do conhecimento adotadas na organização pesquisada e analisar as características do modelo de governança de tecnologia da informação, considerando-se o processo de análise e gestão de risco de tecnologia da informação, concluiu-se que, na organização pesquisada, existem indícios de pró-atividade nos processos de análise e gestão de riscos de tecnologia da informação, tendo em vista que as definições desses processos consideram as ações de gestão do conhecimento. A pesquisa ainda permite concluir que essas ações são praticadas por todos os colaboradores do Departamento de Tecnologia da Informação além de serem praticadas por alguns colaboradores de outros departamentos.

Concluiu-se também, que esses colaboradores estão obtendo resultados positivos com as práticas das ações de gestão do conhecimento, comprovando a teoria apresentada por Nonaka e Takeuchi (1997), e que essas práticas beneficiam os processos de análise e gestão de riscos de tecnologia da informação, corroborando com os estudos apresentados por Neef (2005).

Estas comprovações podem ser visualizadas tendo em vista a melhora nas definições dos processos de analisar e gerenciar riscos de tecnologia da informação.

Por considerar as ações de gestão do conhecimento, essas definições são focadas nos processos de negócio, cujas vulnerabilidades são apontadas pelos colaboradores, sejam através das bases de conhecimento, sejam através das reuniões ou documentação dos sistemas.

Conclui-se ainda que o processo de analisar e gerenciar riscos de tecnologia da informação, definido na organização pesquisada, apresenta as vulnerabilidades e possíveis tratativas para mitigar, ou eliminar, os riscos inerentes a essas vulnerabilidades, apontando os riscos e impactos para a organização.

Considerando que os riscos de tecnologia da informação são analisados por processos de negócio, que são suportados por sistemas que por sua vez são suportados por ativos de tecnologia da informação, mitigando ou eliminando as vulnerabilidades desses ativos tecnológicos e dos sistemas, os processos de negócio também terão suas vulnerabilidades mitigadas ou eliminadas.

Durante a pesquisa não foi mencionado qualquer dado sobre indicadores que possibilitassem medir a contribuição das ações de gestão do conhecimento para o processo de analisar e gerenciar riscos de tecnologia da informação; porém, a organização pesquisada apresentou o sistema *Risk Manager*, que possibilita fazer a gestão de riscos corporativos; contudo, maiores detalhes sobre o funcionamento desse sistema não foram apresentados por não fazer parte dos objetivos desta pesquisa.

É importante salientar que a pesquisa aponta fragilidades no processo de gestão de riscos de tecnologia da informação, pois pouco foi mencionado sobre esse assunto; porém, o processo de análise de riscos foi detalhado com profundidade.

Um fator importante mencionado durante a pesquisa é que as auditorias implementadas na organização estão considerando as análises de riscos de tecnologia da informação, como forma de análise dos riscos corporativos na organização, tendo em vista que a organização considera as ações de gestão do conhecimento para as definições dos processos de analisar e gerenciar riscos.

Os responsáveis pelas auditorias na organização pesquisada consideram que as ações de gestão do conhecimento contribuem, diretamente, para o processo de

análise e gestão de riscos de tecnologia da informação, por considerarem os resultados dessa análise como insumos para as auditorias corporativas.

Outra conclusão importante é que o resultado de uma análise de risco de tecnologia da informação, ao ser armazenado em base de conhecimento, serve de insumos diretos para o planejamento de outras análises. Esse fator relaciona, diretamente, os benefícios das ações de gestão do conhecimento com os processos de analisar e gerenciar riscos de tecnologia da informação. A organização considera o conhecimento adquirido nas análises anteriores para as definições das futuras análises. Com isso, os erros experimentados em uma análise podem ser corrigidos para as demais, refinando-se o processo e objetivando-se a excelência.

Não ficou claro, durante a pesquisa, se os colaboradores da organização sabem distinguir quais ações de gestão do conhecimento são promovidas para compartilhar, disseminar ou criar conhecimento. As respostas deixaram essa dúvida principalmente porque os colaboradores ficaram muito presos em falar sobre as bases de conhecimento. Conclui-se que este é um indício de que o Núcleo de Gestão do Conhecimento deve trabalhar mais essa questão, promovendo as ações de gestão do conhecimento, apresentando seus objetivos e ganhos diretos para a organização e para as tarefas diárias de cada colaborador.

Durante a pesquisa, pouco foi mencionado sobre projetos futuros com objetivos de ampliar as ações de gestão do conhecimento na organização. O Núcleo de Gestão do Conhecimento apresentou um incipiente plano para ampliar as ações de gestão do conhecimento para toda a organização, permitindo que essas ações sejam corporativas e não, apenas, ações do Departamento de Tecnologia da Informação.

Esta pesquisa permite que algumas reflexões sejam feitas. Existem muitas ações de gestão do conhecimento, porém existem poucos resultados medidos com a aplicação destas ações. Diversas reuniões e encontros profissionais foram mencionados, porém, nenhum resultado esperado e efetivo sobre estas ações foi apresentado. Os sujeitos de pesquisa ficaram presos às bases de conhecimento, ao responderem os questionários, e não exploraram os resultados positivos das demais ações, o que permite refletir que não conhecem estes resultados, comprovando a fragilidade do processo.

Esta pesquisa ainda permite refletir sobre a efetividade dos gestores desta organização. Ações desvinculadas de resultados e de objetivos específicos, não são eficientes, pois, representam pouco no montante de resultados da organização. Pode-se inferir, através dos resultados apresentados que os gestores necessitam de um olhar mais direto e crítico sobre as ações de gestão do conhecimento e para os processos de analisar e gerenciar riscos de tecnologia da informação.

Por outro lado, conhecer as fragilidades permite que a organização melhore seus processos. O resultado desta pesquisa auxilia a organização pesquisada a enxergar suas fragilidades, objetivando reformulações dos processos e melhoria na condução dos resultados.

Por fim, conclui-se, através desta pesquisa, que as ações de gestão do conhecimento, implementadas pela organização pesquisada, contribuem para as definições dos processos de análise e gestão de riscos. Contudo, essa contribuição ainda é muito superficial, restringindo-se a usar o conhecimento obtido nas análises anteriores para o planejamento de análises futuras, além de usar das informações explicitadas nas bases de conhecimento para esta definição.

Considerando a amplitude do assunto gestão do conhecimento e análise e gestão de riscos de tecnologia da informação, acredita-se que a organização pesquisada poderá, no futuro, apresentar novos benefícios para os processos de analisar e gerenciar riscos de tecnologia da informação, considerando as ações de gestão do conhecimento.

7.1. Dificuldades e limitações da pesquisa

Para a conclusão desta pesquisa, algumas dificuldades e limitações surgiram; porém foram contornadas permitindo obter o resultado esperado.

As dificuldades encontradas para a execução deste trabalho foram, em um primeiro momento, determinar os sujeitos de pesquisa, considerando-se a grande quantidade de colaboradores no Departamento de Tecnologia da Informação, da organização pesquisada. A preocupação foi determinar sujeitos de pesquisa que pudessem realmente contribuir para o resultado deste trabalho.

Durante a apresentação dos resultados da pesquisa, outra dificuldade foi encontrada. Algumas respostas tiveram que ser ouvidas várias vezes, objetivando uma compreensão adequada e correta, além da dificuldade de se generalizar os resultados obtidos para a apresentação.

Outra dificuldade a ser relatada, foi determinar o roteiro da entrevista, pois houve uma preocupação em determinar um roteiro que, de fato, respondesse à questão norteadora deste trabalho e que atendesse aos seus objetivos,

Sobre as limitações, pode-se relatar que o resultado desta pesquisa não pode ser generalizado, considerando-se que este resultado é referente à realidade desta organização do setor de saúde e de seu Departamento de Tecnologia da Informação. Inclusive, não é possível atribuir que o resultado observado neste departamento poderá ser observado em outros departamentos desta organização.

7.2. Sugestões para novos estudos

A partir das respostas obtidas com este estudo, acredita-se que algumas questões merecem novas análises, pois um estudo de caso constitui-se tarefa fundamental para gerar pesquisas futuras. Contudo, sugere-se que novos estudos de caso possam apresentar modelos e implementações de ações de gestão do conhecimento que contribuam para outros processos de governança de tecnologia da informação, esperando-se obter, com a relação existente entre esses resultados, um modelo adequado para ações de gestão do conhecimento, que possam contribuir para todos os processos de governança de tecnologia da informação ou que, pelo menos, atendam à maioria dos processos relacionados no COBIT (2006).

Estudos desta natureza podem melhorar as ações de governança de tecnologia da informação nas organizações, contribuindo ainda para o aumento das ações de gestão do conhecimento. Para as academias, estes estudos poderão dar uma nova conotação às pesquisas sobre gestão do conhecimento e governança de tecnologia da informação, fortalecendo os assuntos no âmbito acadêmico.

REFERÊNCIAS

ALVARENGA NETO, R. C. D. **Gestão do conhecimento em organizações**: proposta de mapeamento conceitual integrativo. São Paulo: Saraiva, 2008.

ALVARENGA NETO, R. C. D.; NEVES, J. T. R. Gestão da informação e do conhecimento nas organizações: resultados de análise de casos relatados em organizações públicas e privadas. **Revista de Economia e Administração do IBMEC Educacional**, v.2, n.3, p.43-62, jul./set. 2003.

BARDIN, L. **Análise de conteúdo**. Lisboa: Edições 70, 1995

CAMPOS, André. **Sistema de segurança da informação**: Controlando os Riscos. 2. Ed. Florianópolis: Visual Books, 2007

CHOO, Chun Wei. **Knowing organization**: how organizations use information to construct meaning, create knowledge and make decisions. New York: Oxford University Press, 2002.

COBIT (Control Objectives for Information and Related Technology) - Controls, Objetives, Management Guidelines and Maturity Models. Rolling Meadows, IL, USA: IT Governanace Institute, 2006

COLLIS, Jill; HUSSEY, Roger. **Pesquisa em administração**: um guia prático para alunos de graduação e pós graduação. 2 ed. Porto Alegre: Bookman, 2005.

DAVENPORT, Thomas H. **Ecologia da Informação**: porque só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura. 1998.

DAVENPORT, Thomas H; PRUSAK, Laurence. **Conhecimento empresarial**. Rio de Janeiro: Campus, 1999.

DAVENPORT, T. **Reengenharia de processos**: como inovar a empresa através da tecnologia da informação. Rio de Janeiro: Campus, 1994.

DE LONG, D.; DAVENPORT, T.; BEERS, M. **What is a knowledge management project ?** Research note. Disponível em: <http://www.businessinovation.ey.com/mko> Acesso em fev. 2010.

FLEURY, MARIA T. L. E OLIVEIRA JR., MOACIR M. (org) **Gestão estratégica do conhecimento:** integrando aprendizagem, conhecimento e competência. São Paulo: Atlas, 2001.

GAMA, F. A. ; MARTINELLO, M. . Análise do impacto do nível da governança de tecnologia da informação em indicadores de performance de TI: estudo de caso no setor siderúrgico. In: ENCONTRO NACIONAL DE PESQUISA EM ADMINISTRAÇÃO. Salvador: ANPAD, 2006.

GIL, Antônio C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2002. Disponível em: http://isaca.org/cobit. Acesso em: 02 de Março de 2011.

GIL, Antônio Carlos. Métodos e Técnicas de Pesquisa Social. São Paulo: Atlas, 1991.

HUBER, George P. A theory of the effects of advanced information technology on organization design, intelligence, and decision making. **Academy of Management Review,** v. 15., n.1, p. 47-71, 1990.

IT Governance http://www.itgovernance.org - Executive IT Governance Summary

KAPLAN, S. R., NORTON, P.D. **The strategy-focused organization**: how balanced scorecard companies thrive in the new business environment. Harvard Business School, 2001

MALHOTRA, Yogesh. **Knowledge management for the new world of business**. 1998. Online. Documento recuperado em 13/10/2000. Disponível na Internet via WWW. URL: http://www.brint.com/km/whatis.htm.

MARCHAND, Donald A.; DAVENPORT, Thomas H. (Orgs.). **Dominando a gestão da informação**. Porto Alegre: Bookman, 2004.

MATTAR, F. N. **Pesquisa de marketing**: metodologia, planejamento. São Paulo: Atlas, 1997.

NASCIMENTO, Niraldo José; NEVES, Jorge Tadeu de Ramos. A gestão do conhecimento na World Wide Web: reflexões sobre a pesquisa de informações na rede. **Perspectivas em Ciência da Informação**, v.4, n.1, p.29-48, jan./jun. 1999.

NEEF, Dale. Managing corporate risk through better knowledge management. **The Learning Organization,** v. 12, n.2, p.112-124. 2005.

NONAKA, Ikujiro; TAKEUCHI, Hirotaka. **Criação de conhecimento na empresa**: como as empresas japonesas geram a dinâmica da inovação. Rio de Janeiro: Campus, 1997.

OLIVEIRA, Sílvio Luiz. **Tratado de metodologia científica**: projetos de pesquisa TGI, TCC, monografias, dissertações e teses. São Paulo: Pioneira Thomson Learning, 2004.

OVUM. KM: applications, markets and technologies. 1998. Online. Documento extraído em 13/12/2010. Disponível na Internet via WWW. URL: http://www.keele.ac.uk/depts/is/af/kmnag1/sld013.htm.

REZENDE, Denis Alcides. **Planejamento de sistemas de informação e informática**: guia prático para planejar a tecnologia da informação integrada ao planejamento estratégico das organizações. 3 ed. São Paulo: Atlas, 2008.

RODRIGUEZ, M. V. R. **Gestão empresarial**: organizações que aprendem. Rio de Janeiro: Qualitymark, 2002.

ROESCH, Sylvia Maria. **Projetos de estágio e de pesquisa em administração**. 3 ed. São Paulo: Atlas, 2005.

SALLÉ, M. **IT service management and IT governance**: review, comparative analysis their Impact on utility computing. trusted systems laboratory: Palo Alto: HP Laboratories, 2004 http://www.hpl.hp.com/techreports/2004/HPL-2004-98.pdf

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva.** Rio de Janeiro: Campus Elsevier, 2003.

SENGE, Peter. As cinco disciplinas. **HSM Management**, v.2, n.9, p.82- 87, jul./ago. 1998.

STEWART, Thomas. **Capital intelectual**: a nova vantagem competitiva das empresas. Rio de Janeiro: Campus, 1998.

SVEIBY, K. E. **A nova riqueza das organizações**. Rio de Janeiro: Campus, 1997.

TOWETT, Paul, ROTHWELL, Margaret. The Economics of Information Technology. McMillan Press, 1986

WEILL, Peter; ROSS, Jeanne. **Governança de TI**. São Paulo: M. Books do Brasil, 2006.

APÊNDICES

APENDICE 1 - Informação sobre a pesquisa

Você está participando de uma pesquisa acadêmica, através de um questionário semi estruturado, cujo resultado constará em uma dissertação de mestrado do Programa de Mestrado Profissional em Administração das Faculdades Integradas de Pedro Leopoldo.

Esta pesquisa objetiva Identificar as contribuições da gestão do conhecimento para o processo de avaliar e gerenciar os riscos de tecnologia da informação, parte integrante do modelo de governança de tecnologia da informação da organização pesquisada, com a adoção de práticas efetivas de gestão do conhecimento.

Ressalta-se que as informações prestadas por você destinam-se exclusivamente a esta pesquisa, não sendo divulgada ou cedida para outra finalidade, reiterando a seriedade deste estudo, sobre tudo no âmbito ético.

Considerando sua atenção e cordialidade em receber esta pesquisa, agradeço pela atenção e o tempo dispensado e informo que o resultado final desta pesquisa será enviado a você tão logo todos os processos acadêmicos sejam concluídos com aprovação.

Atenciosamente,

Gilberto Barbosa Mota.

APENDICE 2 - Roteiro da entrevista semi-estruturada

Seção 1 - Informações Pessoais.

1. Que cargo ocupa na organização?
2. Há quando tempo trabalha na organização?

Seção 2 - Sobre Gestão do Conhecimento.

3. Você conhece as ações de gestão do conhecimento implementadas pelo Núcleo de Gestão do Conhecimento?

Se você respondeu sim na pergunta 3, responda às questões seguintes:

4. Quais são os processos destinados à criação, coleta, organização, transferência e compartilhamento do conhecimento na organização?
5. Você considera que a organização cria condições para o processo de criação, transferência e compartilhamento do conhecimento?

Se você respondeu sim na pergunta 5, responda às questões seguintes:

6. Quais são as ações executadas pela organização objetivando criar condições para criação, transferência e compartilhamento do conhecimento?

Seção 3 - Sobre Governança de Tecnologia da Informação.

7. Você conhece o processo de avaliar e gerenciar os riscos de tecnologia da informação, processo integrante do modelo de governança de tecnologia da informação da organização?

Se você respondeu sim na pergunta 7, responda às questões seguintes:

8. Quais são as ações que conhece ou executa, cujo objetivo é de analisar e gerenciar os riscos de tecnologia da informação.

Seção 4 - Gestão do Conhecimento e Governança de Tecnologia da Informação.

9. Você considera que as ações de gestão do conhecimento contribuíram para o processo de avaliar e gerenciar os riscos de tecnologia da informação?

Se você respondeu sim na pergunta 9, responda às questões seguintes:

10. Quais foram às contribuições para o processo de avaliar e gerenciar os riscos de tecnologia da informação considerando as ações de gestão do conhecimento?
11. Quais foram os principais ganhos para a organização?