UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

CENTRO DE CIÊNCIAS SOCIAIS APLICADAS

DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS

PROGRAMA DE PÓS – GRADUAÇÃO EM ADMINISTRAÇÃO

ALIXANDRE THIAGO F DE SANTANA

ASPECTOS DO GERENCIAMENTO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO NAS EMPRESAS: UM ESTUDO DE CASO MÚLTIPLOS

NATAL

2009

ALIXANDRE THIAGO F. DE SANTANA

ASPECTOS DO GERENCIAMENTO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO NAS EMPRESAS : UM ESTUDO DE CASOS MÚLTIPLOS

Dissertação apresentada ao Programa de Pós-graduação em Administração – PPGA, da Universidade Federal do Rio Grande do Norte, como requisito parcial para a obtenção do título de Mestre em Administração.

Orientador: Prof. Dr.Manoel Veras de Sousa Neto

NATAL
2009

Divisão de Serviços Técnicos

Catalogação da Publicação na Fonte. UFRN / Biblioteca Central Zila Mamede

Santana, Alixandre Thiago F. de.
Aspectos do gerenciamento de riscos de Tecnologia da Informação nas empresas: um estudo de casos múltiplos / Alixandre Thiago F. de Santana. – Natal, RN, 2009.
128 f.

Orientador: Manoel Veras de Sousa Neto.

Dissertação (Mestrado) – Universidade Federal do Rio Grande do Norte. Centro de Ciências Sociais Aplicadas. Departamento de Ciências Administrativas. Programa de Pós-Graduação em Administração.

1. Tecnologia da informação – Dissertação. 2. Gerenciamento de riscos – Estudo de caso – Dissertação. 3. Riscos de TI – Organizações – Pernambuco – Dissertação. I. Sousa Neto, Manoel Veras de. II. Universidade Federal do Rio Grande do Norte. III. Título.

RN/UF/BCZM CDU 65.011.56(043.3)

ALIXANDRE THIAGO F DE SANTANA

ASPECTOS DO GERENCIAMENTO DE RISCOS DE TI NAS EMPRESAS: UM ESTUDO DE CASOS MÚLTIPLOS

Esta dissertação foi julgada adequada à obtenção do título de Mestre em Ciências Administrativas e aprovada em sua forma final pelo Curso de Mestrado em Ciências Administrativas da Universidade Federal do Rio Grande do Norte.

Aprovada em (dia) de (mês) de (ano da defesa).

BANCA EXAMINADORA

_____

Prof. Dr. Manoel Veras de Souza Neto
Universidade Federal do Rio Grande do Norte

_____

Profa. Dra. Anatália Saraiva Martins Ramos

Universidade Federal do Rio Grande do Norte

_____

Prof. Fabio Queda Bueno da Silva, Dr.
Universidade Federal de Pernambuco

A meus pais, Manoel e Marlene, pelo seu exemplo de companheirismo mútuo, pela educação recebida, que moldaram o que sou hoje; e em especial a minha irmã, Andréia, que sempre acreditou no meu potencial, sempre me incentivou a crescer e desenvolver através do estudo, tão valorizado pela família desde a minha infância. A minha professora de matemática da época do ginásio da extinta Escola Cenecista de São José do Campestre/RN, Izabel Ferreira, pelo incentivo.

AGRADECIMENTOS

A Deus, pela dádiva de viver. Ao meu orientador Manoel Veras, pela confiança creditada e pela orientação neste trabalho.

Aos participantes e entrevistados, fundamental para realização desta pesquisa. À Agência Estadual de Tecnologia da Informação de Pernambuco, pelo incentivo através das horas dispensadas a este trabalho.

Aos colegas do mestrado, pelo conhecimento trocado e por compartilharem as mesmas esperanças e angústias, em especial, a José Augusto e Bruno Campelo.

Aos colegas da graduação, pelo estímulo passado através do exemplo.

À professora Anatália Saraiva que, durante o curso de ADI1, apresentou-me parte da disciplina “Gestão da TI”, da qual não sei mais desgostar.

Aos professores do PPGA pelos ensinamentos transmitidos.

Aos amigos do trabalho, pela colaboração e pela amizade. Aos meus amigos, pela compreensão da ausência em alguns momentos durante esses últimos dois anos.

Aos meus amigos pernambucanos.

RESUMO

Os benefícios do uso da Tecnologia da Informação – TI- nas organizações são cada vez mais perceptíveis. Nos últimos anos, os gestores vêm despertando para temas como governança, alinhamento estratégico, segurança da informação, dentre outros. Particularmente este último, vem sendo tratado sob uma abordagem técnica, na qual se privilegia aspectos técnicos como proteção contra invasões, sistemas antivírus, controle de acesso etc. O tema gerenciamento de riscos em TI comumente é tratado sob essa perspectiva, muitas vezes limitando-se a preocupações dos departamentos de TI. Na década de 90, surge uma nova perspectiva para o gerenciamento de riscos, na qual ela é tratada sob uma visão holística dentro da organização. Segundo essa nova abordagem, as estratégias da organização devem levar em conta os riscos de TI em seu processo de elaboração. Com o aumento da dependência das tecnologias para a execução das atividades do negócio, fica latente a necessidade de se compreender melhor o tema. Este trabalho consiste em um estudo de casos múltiplos em três organizações públicas do Estado de Pernambuco que investiga como essas organizações gerenciam os riscos inerentes ao uso da TI. Foram feitas entrevistas semi-estruturadas com os seus gestores de TI, que foram analisadas e comparadas com as categorias retiradas da literatura. Os dados mostram que os conceitos de cultura de riscos e de governança de TI são pouco compreendidos e implementados as organizações e que essas não possuem metodologias de gerenciamento de riscos de TI formalmente definidas, tampouco executadas. No entanto, exercem a maior parte das práticas indicadas pela referência central da pesquisa, sem alinhamento com um processo de gerenciamento de riscos.

Palavras-chave: Riscos, Tecnologia, Informação, Gerenciamento, Segurança, Pernambuco

ABSTRACT

The information technology - IT- benefits have been more perceived during the last decades. Both IT and business managers are dealing with subjects like governance, IT-Business alignment, information security and others on their top priorities. Talking about governance, specifically, managers are facing it with a technical approach, that gives emphasis on protection against invasions, antivirus systems, access controls and others technical issues. The IT risk management, commonly, is faced under this approach, that means, has its importance reduced and delegated to IT Departments. On the last two decades, a new IT risk management perspective raised, bringing an holistic view of IT risk to the organization. According to this new perspective, the strategies formulation process should take into account the IT risks. With the growing of IT dependence on most of organizations, the necessity of a better comprehension about the subject becomes more clear. This work shows a study in three public organizations of the Pernambuco State that investigates how those organizations manage their IT risks. Structured interviews were made with IT managers, and later, analyzed and compared with conceptual categories found in the literature. The results shows that the IT risks culture and IT governance are weakly understood and implemented on those organizations, where there are not such an IT risk methodology formally defined, neither executed. In addition, most of practices suggested in the literature were found, even without an alignment with an IT risks management process.

Keywords: Technology, Risk, Management, Pernambuco, information, security

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIAÇÕES

ATI	Agência Estadual de Tecnologia da Informação de Pernambuco
CIO	Chief Information Officer
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Managemen
SLA	Service Level Agreement
SLM	Service Level Management
TI	Tecnologia da Informação
ITGI	Information Technology Governance Institute

SUMÁRIO

1 INTRODUÇÃO

A organização depende de vários tipos de recursos para manter sua sobrevivência. Todos esses recursos necessitam ser gerenciados e nos últimos anos, houve uma crescente preocupação com a forma como são tomadas as decisões dos gestores sobre os referidos recursos. A busca pela melhor forma de gerência ganhou notoriedade no momento em que o mercado global passou a requisitar maior acurácia, transparência e credibilidade em seus processos de negócio. Surge nesse contexto o conceito de governança corporativa. A governança corporativa, na visão de Weill e Ross (2004),

> *prescinde de um conjunto de ativos organizacionais que devem ser monitorados, quais sejam: ativos humanos, financeiros, físicos, intelectuais e de relacionamento. Nessa visão, tais ativos atuam unidos para a consecução dos objetivos organizacionais. Dentro desse contexto, encontra-se a governança de TI, cujo papel é gerir, particularmente, os ativos de TI.*

A tecnologia da Informação –TI- como provedora de serviços participa cada vez mais nos processos organizacionais, com uma atuação que pode variar, em termos de complexidade, desde o suporte até a habilitação, podendo até contribuir para o redesenho dos processos de negócio. Essa importância crescente da TI nas organizações é discutida e enfatizada em diversos trabalhos (LUFTMAN, 2000; HENDERSON e VENKATRAMAN, 1993*).*

Gerenciar TI tem se tornado uma tarefa crítica para CIOs (do inglês, Chief of Information Officer) e envolvidos, que passaram a ter maiores responsabilidades e administrar orçamentos elevados. Essas transformações descambaram no desenvolvimento de processos específicos de governança e por si só merecem ser estudados e entendidos.

A governança de TI, parte integrante do processo de governança (corporativa), consiste de estruturas organizacionais e de liderança, bem como de processos, que assegurem que a organização de TI sustenta e facilita as estratégias e objetivos da organização (WEILL e ROSS, 2004).

Estudos direcionados a essas questões têm sido realizados pelo ITGI (do inglês, *Information Technology Governance Institute*), um dos principais institutos de pesquisa sobre Governança de TI no mundo. O ITGI definiu cinco áreas de concentração de esforços para as atividades de governança de TI, igualmente estudadas pela comunidade cientifica: Alinhamento Estratégico (HENDERSON e VENKATRAMAN 1992; HENDERSON e VENKATRAMAN 1993, 1999; LUFTMAN, 2000; SILVIUS, 2007), Gerenciamento de Recursos de TI (ITIL, do inglês, *Information Technology Infrastrucuture Library*), Gerenciamento de Riscos (HALLIDAY et al., 1996; BANDYOPADHYAY et al., 1999; WESTERMAN, 2005; MCFADZEAN et al., 2007); Retorno de investimento (JURISON, 1996; PESLAK, 2008) e Mensuração de performance (KANG e BRADLEY, 2002; ABRAB e BUGLIONE, 2003).

O gerenciamento dos riscos de TI, tema deste trabalho, ganha importância à medida que os gastos nessa área crescem e as organizações se tornam tecnologicamente dependentes (HALLIDAY et al., 1996; BANDYOPADHYAY ET AL., 1999; WEILL e ROSS, 2004). “Conseqüentemente, tornam-se também vulneráveis aos riscos de falhas da TI, um dos mais importantes desafios enfrentados pelos executivos de TI.” (BANDYOPADHYAY et al., 1999).

> *Dentro desse contexto, o gerenciamento de riscos de TI surge com a função de proteger seus ativos tais como dados, hardware, software, pessoas e recursos de todas as ameaças externas (exemplo: desastres naturais) e internas (como falhas técnicas, acesso não-autorizado, mau planejamento do negócio) de forma que os custos das perdas resultantes da realização de tais ameaças sejam minimizados quando não evitados (GOTTFRIED, 1989).*

“As formas e fontes de ameaça aos ativos mudaram e cresceram substancialmente com o desenvolvimento dos sistemas de computadores, redes eletrônicas, armazenamento de dados e troca de informações” (SOLMS, 2001 apud ANDERSON e CHOOBINEH**,** 2008), o que provocou a necessidade de uma maior responsabilidade a ser assumida pelos gestores, no que diz respeito à segurança da informação.

De fato, uma vez que as organizações se tornam cada vez mais dependentes de seus sistemas baseados em computador, que desempenham um

papel vital nos seus processos de negócio, há a necessidade de uma maior conscientização e preocupação com relação às questões de segurança desses sistemas (HALLIDAY et al., 1996).

Vários esforços vêm sendo envidados por institutos de pesquisa em forma de frameworks, metodologias e processos, a citar alguns, ITIL, COBIT (do inglês, *Control Objectives for Information and related Technology*), CMMi (do inglês, *Control Objectives for Information and related Technology*) etc, sempre com alguma preocupação com os aspectos de riscos de TI. No entanto, afirmam Bandyopadhyay et al. (1999) que o gerenciamento de riscos de TI convencional não é suficiente para a sua complexidade.

O termo convencional foi aqui usado para se referir a muitas das metodologias de gerenciamento e analise de riscos que existem atualmente, cujo foco é dado a questões técnicas de segurança da informação. Um fato comum entre essas metodologias é que elas são baseadas num modelo no qual o foco esta voltado principalmente para o departamento de TI, tornando o modelo direcionado pela perspectiva dos seus ativos, sem levar em consideração questões relativas ao negócio (BANDYOPADHYAY et. al.,1999).

Os riscos de TI existem e é capital para as organizações e, mais especificamente, para seus gestores de TI e de negócio diretamente envolvidos na definição dos objetivos, a conscientização sobre a existência dos mesmos, bem como da importância do seu gerenciamento. Para a Cooperação e Desenvolvimento Econômico –OECD (2004), em seu relatório “Princípios de Governança Corporativa”, sugere que a organização deve ter a responsabilidade de desenvolver uma política de riscos e garantir a integridade de sistemas para esse fim.

O propósito do gerenciamento de riscos de TI é evitar ou diminuir as perdas, selecionando a melhor combinação de medidas de segurança (Bandyopadhyay et al. 1999), provendo para a organização os meios de identificar, avaliar e controlar os seus riscos.

Bandyopadhyay et al. (1999) afirmam ser necessário adotar uma visão holística e avaliar as potenciais ameaças da TI, considerando o inteiro espectro do seu ambiente, já que isso reflete na organização como um todo. Em outras palavras, essa temática passaria de uma preocupação ou responsabilidade departamental para ser uma decisão organizacional, influenciando na sua

estratégia. Mas qual o estado atual dessas práticas de gerenciamento de riscos nas organizações brasileiras? Prevalece a ênfase no tratamento de ameaças técnicas de segurança sustentada por Bandyopadhyay et al. (1999) ? Os gestores estão cientes dos riscos de TI inerentes ao seu uso?

Essas perguntas em aberto caracterizam a necessidade existente de maior conhecimento sobre o problema, visando a uma melhor compreensão de como ele ocorre nas organizações brasileiras. Verificar se os gestores conhecem riscos de TI que afetam o negócio das organizações e como essas os gerenciam, é o primeiro passo para que seja feito um diagnóstico mais preciso do problema, o que representará o ponto de partida para que o problema seja estudado com mais propriedade, conseqüentemente, permitindo que as organizações possam gerenciar efetivamente seus riscos de TI, evitando ou diminuindo os impactos negativos de eventos indesejáveis ou de oportunidades não aproveitadas. O presente trabalho emerge desse contexto, como uma pesquisa de campo na qual serão estudadas algumas organizações através de seus gestores de TI.

1.1 QUESTÃO-PROBLEMA

Como é realizado o gerenciamento dos riscos de TI nas organizações estudadas?

1.2 OBJETIVO GERAL

Investigar como as organizações estudadas gerenciam os riscos inerentes ao uso da TI.

1.3 OBJETIVOS ESPECÍFICOS

- Conhecer as práticas de governança de TI implementadas;
- Descrever a cultura de riscos existente nas organizações do sujeito da pesquisa;
- Conhecer as práticas de gerenciamento de riscos de TI em uso.

1.4 JUSTIFICATIVAS

A justificativa do trabalho pode ser descrita sob duas óticas:

1.4.1 Justificativa teórica

O trabalho procura ver a temática dos riscos de TI sob uma nova perspectiva, abordando os riscos como uma questão de importância estratégica para a organização. Tal pensamento é corroborado por diversos autores como será mostrado adiante.

Desconhecem-se também como as organizações lidam com o gerenciamento de riscos, até o momento. Pouco se sabe como se encontra difundido este conceito nas organizações brasileiras, no que tange as práticas de gerenciamento adotadas, justificando então o estudo específico para essa questão.

Como evidência desse fato pode ser o número de trabalhos publicados nos anais do ENANPAD – Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração, no ENADI – Encontro de Administração da Informação-, e no CONTECSI – Congresso Internacional de Tecnologia e Sistemas de Informação-, nos últimos cinco anos, nos quais não são encontrados trabalhos voltados a essa temática. Foram também pesquisados os principais periódicos internacionais através dos portais Scopus, Elsevier, ISI Web of Knowledge, sendo as buscas por trabalhos correlatos resumidas aos estudos de Prodromos e Anastasios(2009), Westerman e Hunter(2007), McFadzean et al.(2007), Bandhyopadyay et al.(1999), Chang e Ho (2006), Dhillon e Backhouse (2000) e Von Solms (2004).

Por se tratar de um estudo exploratório, espera-se contribuir corroborando ou não a teoria aqui abordada com a prática, o que contribuirá para consolidação de conhecimentos na área. Espera-se também trazer à tona as primeiras evidências sobre os conceitos em questão, que certamente poderão ser objeto de estudos mais aprofundados. No tocante ao caráter descritivo, o estudo se preocupou em descrever como o fenômeno investigado se apresenta nas organizações em questão.

1.4.2 Justificativa prática

Dada a crescente dependência das organizações em relação a TI, faz-se necessário o uso racional e o controle sobre esta função organizacional. Para tanto, os gerentes de TI e de negócio devem estar cientes dos riscos inerentes ao seu uso da TI, possibilitando um melhor planejamento e minimização dos efeitos de situações adversas. Não é admissível que as organizações ignorem o crescimento da complexidade de seus ambientes de TI e os riscos inerentes ao seu uso. É necessário, então uma utilização consciente dos ativos de TI, seus benefícios, limitações e os riscos inerentes. Espera-se contribuir também para a difusão dessa visão com a realização desta pesquisa, na medida em que a mesma produzirá um diagnóstico de como se encontra o gerenciamento dos riscos de TI em algumas das organizações do estado de Pernambuco.

1.5 ORGANIZAÇÃO DO ESTUDO

O presente trabalho se divide nos seguintes capítulos:

- O Capítulo 1 apresenta o tema e sua relevância e o problema de pesquisa. Também as delimitações do estudo e as limitações da pesquisa serão citados.
- O Capítulo 2 discorre sobre os conceitos teóricos do estudo. Discorre-se sobre temas como estratégia, governança corporativa e de TI, segurança da informação, gerenciamento de riscos e de riscos de TI, modelos de gerenciamento de riscos de TI
- O Capítulo 3 aborda os procedimentos metodológicos utilizados no estudo.
- O Capítulo 4 traz os casos estudados e a descrição dos resultados.
- O Capítulo 5 apresenta a análise e comparação dos resultados.
- O Capítulo 6 faz as considerações finais do estudo.

2 REFERENCIAL TEÓRICO

2.1 ESTRATÉGIA E GOVERNANÇA

> *A palavra estratégia, do grego strategía, adotada inicialmente na área militar, foi definida como a arte de planejar e executar movimentos e operações de recursos militares, visando alcançar ou manter posições relativas e potenciais bélicos favoráveis a futuras ações táticas sobre determinados objetivos (FERREIRA, 1999 apud ARNAUD, 2007, p. 26).*

Nas últimas décadas, essa idéia foi adotada com mais freqüência também nas organizações sem fins militares, como empresas públicas e privadas com os mais diversos modelos de negócio, de modo a definir seus objetivos e assegurar a sobrevivência em seus respectivos meios.

Mais recentemente, com a crescente demanda e dependência das organizações em relação a TI, sendo esta paradoxalmente, algumas vezes submetida a cortes de orçamento em tempos de crise, torna-se indispensável o alinhamento dos objetivos desse setor com os objetivos da estratégia do negócio de forma a garantir que as decisões em TI sigam a orientação da estratégia da organização e que os recursos ou investimentos não sejam desperdiçados, e mais ainda: que sejam otimizados.

É fundamental à TI, portanto, para o planejamento dos sistemas de informação, dos sistemas de conhecimentos e da tecnologia necessária, que o planejamento estratégico empresarial (ou plano de negócios ou *business plan*) tenha sido elaborado (REZENDE, 2003, p. 29, 89).

Weill e Ross (2004) cunham a expressão “comportamentos desejáveis” para a função organizacional da tecnologia da informação. Esses comportamentos desejáveis determinarão como a Gestão de Serviços de TI acontecerá na organização, caracterizando o arranjo de atividades e funções providas pelos recursos de TI em suporte a uma ou mais áreas do negócio. Esse alinhamento é conhecido como alinhamento estratégico (HENDERSON e VENKATRAMAN 1992; HENDERSON e VENKATRAMAN 1993, 1999; LUFTMAN, 2000). O alinhamento estratégico apregoa o planejamento estratégico suportado pela TI (estratégias de TI) para garantir que os recursos ou investimentos da organização sigam as

diretrizes estratégicas. A figura seguinte ilustra o relacionamento ou ponte entre as estratégias do negócio e de TI:

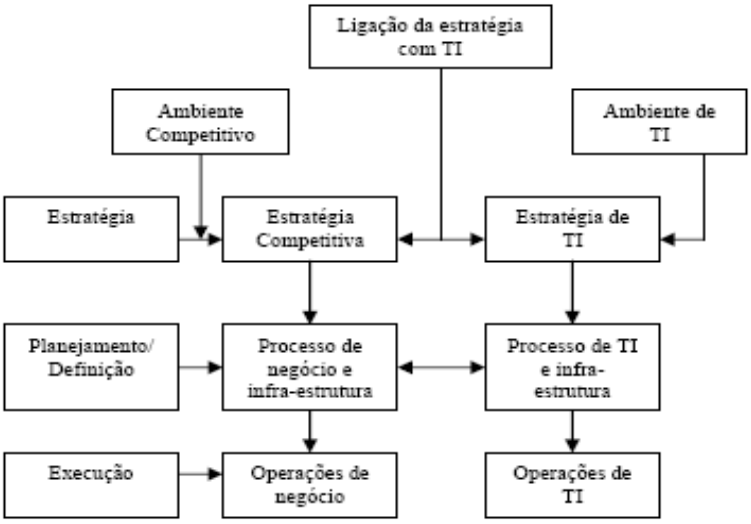

Figura 1 - Alinhamento das estratégias de negócios e de tecnologia da Informação

Fonte: McGEE, James, PRUSAK, Laurence apud BEUREN (2000). “Gerenciamento estratégico da informação:
Aumente a competitividade e a eficiência de sua empresa utilizando a informação”. Rio de Janeiro: Campus,
1994. p.36 apud Rohweder (2007)

A determinação dos comportamentos desejáveis, com suas responsabilidades e direitos decisórios para o alcance do alinhamento estratégico, garantirão uma gestão eficiente e eficaz dos serviços de TI (ARNAUD,2007).

Nesse contexto, frameworks de Governança surgem como resposta a essas necessidades. Alinhamento estratégico, comportamentos desejáveis e mecanismos de controle são preocupações dos recentes frameworks de governança, dentre eles o proposto pelo Instituto de Governança de TI, conforme ver-se - á adiante. A preocupação e o emprego de práticas de governança vêm crescendo nos últimos anos devido a regulamentações governamentais e pressões de mercado recentes, conforme discutido na seção seguinte.

2.2 GOVERNANÇA E GOVERNANÇA DE TI

O termo governança, entendido de maneira simplista como administração, gestão, direção, domínio, controle ou ato de governar, vai muito além da prática de comando de um ambiente formado por tecnologias, pessoas e processos. Define-se como sendo um sistema de estruturas e processos para dirigir e controlar corporações e prestar contas a respeito delas (CAMELO, 2007). Essa definição vem das raízes etimológicas de “Governança” – do verbo latino *gubernare*, que significa “dirigir”.

Transpondo-se para o contexto corporativo, o termo governança vem da expressão inglesa *governance*. Segundo a OECD(1999), a governança é definida como o conjunto de relações entre a administração de uma empresa, seu conselho de administração, seus acionistas e outras partes interessadas, chamada de *stakeholders*.

Rossi (2004) apud Rohweder (2007) conceitua governança como a criação de princípios capazes de nortear a gestão, cujo principal foco é dar suporte ao planejamento e gerenciamento. Também, define 3 (três) participações diferentes e necessárias da governança para que a missão da organização seja atingida:

• Servindo como *interface* entre *stakeholders*, a governança também objetiva a mensuração do trabalho e ações da organização;

• Gerenciando a ligação entre governança e trabalho, isto é, a organização das atividades, pessoas, relacionamentos e tecnologia para se ter o trabalho realizado;

• Propiciando a execução do trabalho, que nada mais é do que o desenvolvimento das
atividades necessárias para o alcance da missão.

A Governança Corporativa surge num contexto de segregação da propriedade e da gestão empresarial, para agregar maior transparência e controle à tomada de decisão na organização. Nesse modelo, o titular da propriedade, delega a um "agente" o poder de decisão sobre essa propriedade (recursos), surgindo a

partir daí, o que se pode chamar de conflitos de agência, já que os interesses daquele que administra nem sempre estão alinhados com os de seu titular.

A Teoria da Agência (JENSEN e MECKLING, 1976)

> *sustenta que os gestores não agirão para maximizar o retorno para os acionistas a não ser que mecanismos de Governança estejam implementados largamente na organização. Considera-se então, que a preocupação maior é criar mecanismos eficientes (sistema de monitoramento e incentivos) para garantir que o comportamento executivo esteja alinhado com o interesse dos acionistas. O propósito dos mecanismos de governança é lidar com essas questões.*

As práticas de governança ganharam ainda mais respaldo nas organizações após diversos escândalos envolvendo grandes corporações americanas na última década. A governança sobre os diversos ativos veio para agregar proteção, transparência e controle a essas organizações. Ainda como conseqüência dos escândalos, como o da empresa norte-americana *Enron*, que acabou por afetar drasticamente a empresa de auditoria *Arthur Andersen*) alguns marcos regula tórios foram criados como a Lei Sarbanes-Oxley (ESTADOS UNIDOS, 2002).

Mais conhecida como Sarbox ou ainda de SOX, a lei Sarbanes-Oxley, promulgada no dia 30 de maio de 2002, proposta pelos Senadores Paul Sarbanes e Michael Oxley, visa a garantir a criação de mecanismos de auditoria e segurança confiáveis nas empresas que possuem capital aberto e ações na Bolsa de Nova York e *Nasdaq (v*árias organizações brasileiras, multinacionais, estão nesse grupo*)*, incluindo ainda regras para a criação de comitês encarregados de supervisionar suas atividades e operações, de modo a mitigar riscos aos negócio; a evitar a ocorrência de fraudes ou assegurar que haja meios de identificá-las quando ocorrem, garantindo a transparência na gestão das empresas; e a evitar o esvaziamento dos investimentos financeiros e a fuga dos investidores causada pela aparente insegurança a respeito da governança adequada das empresas (ARNAUD, 2007).

A Sarbox forçou a adequação das organizações às suas exigências e à adoção de práticas de governança. E o reflexo disso no mercado começa a ser percebido como nas situações abaixo (ARNAUD, 2007):

- O International Finance Corporate (IFC), braço financeiro do Banco Mundial, vai incorporar aos seus critérios de análise para concessão de financiamentos uma avaliação das práticas de governança corporativa;
- O grupo das nações mais ricas do mundo (G7) considera a governança corporativa o mais novo pilar da arquitetura econômica global.
- A Bovespa criou o Itag, índice que acompanha o desempenho das ações de empresas que concedem o *tag along* (proteção a minoritários no caso de venda do controle da empresa), e esse índice busca demonstrar que essas ações têm o melhor desempenho no mercado;
- O BNDES e a Bovespa estão montando diversos mecanismos de apoio a empresas, independentemente do porte, para modernização e capitalização, com elevadas exigências no campo da governança.

A ação do setor de TI se torna então de fundamental importância nesse processo, por ser essa a área responsável pelo controle, segurança da informação e sistemas. Portanto, deverá estar inteirada a adequação desta Lei para garantir a aplicabilidade das regras de transparência fiscal e financeira (ARNAUD, 2007).

Motivada ou não por essas regulamentações externas, ocorre que a função TI passa por uma evolução no que se refere ao uso das aplicações organizacionais da tecnologia da informação, passando de aplicações operacionais e baseadas em acontecimentos passados, a aplicações para apoio à tomada de decisão da alta administração sobre problemas complexos e incertos (OLIVEIRA, 2004, p.102-103). A TI passa de um paradigma operacional, caracterizado pela subtilização dos recursos no qual ela é como vista como um centro de custos, para o paradigma estratégico, sendo parceira estratégica e vista como centro de investimentos. A evolução da TI pode ser acompanhada na figura a seguir:

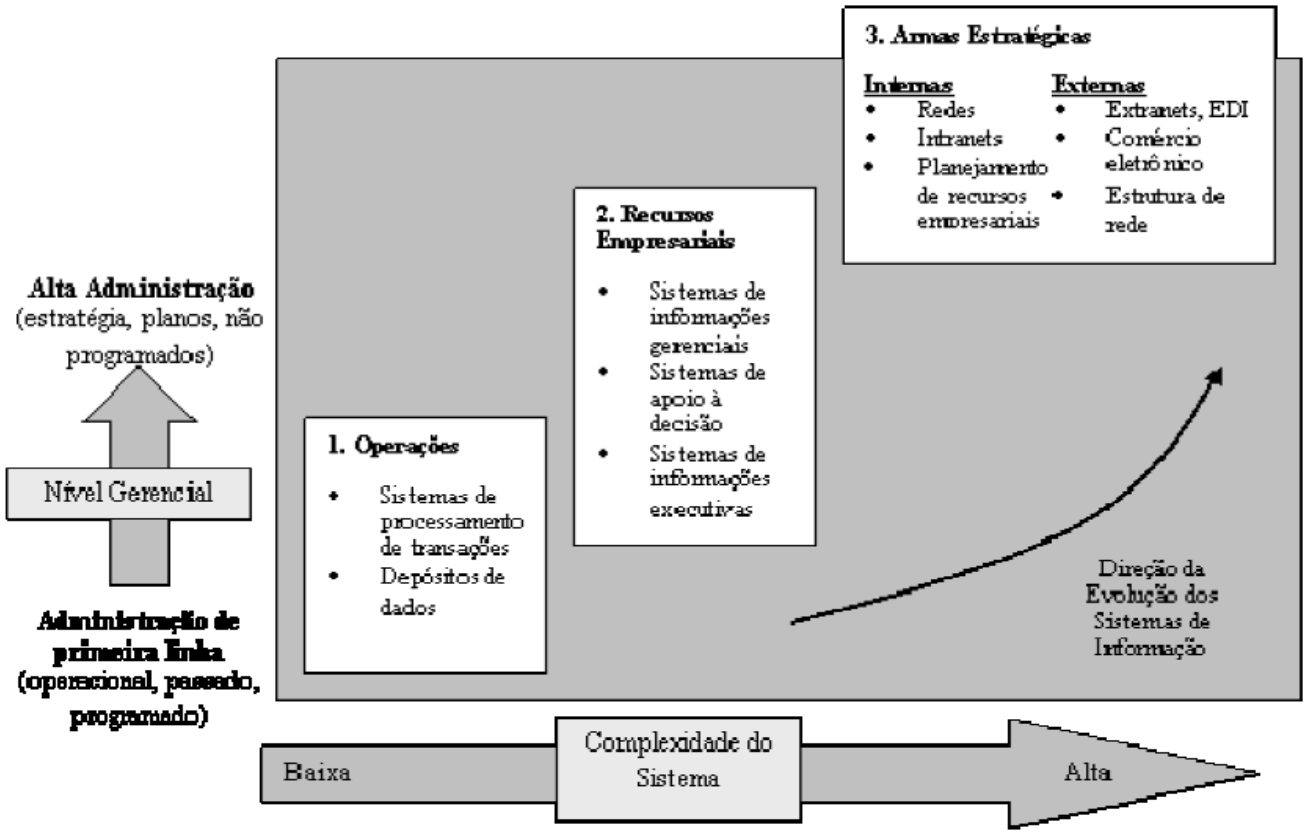

Figura 2 - Evolução da TI nas organizações

Fonte: Oliveira (2004, p.103) apud Rohweder (2007)

Seja para atender à adequação dos controles que a Sarbox demanda, ou impulsionada por forças internas como a mudança de paradigma ilustrada na figura acima, traduzidas principalmente pelo aumento da complexidade da gerência de TI, a Governança Corporativa tende a ganhar espaço e importância nas organizações de diversas natureza. Dados da evolução do número de associações ao IBGC - demonstram o interesse pelo tema, conforme se pode observar na Figura a seguir:

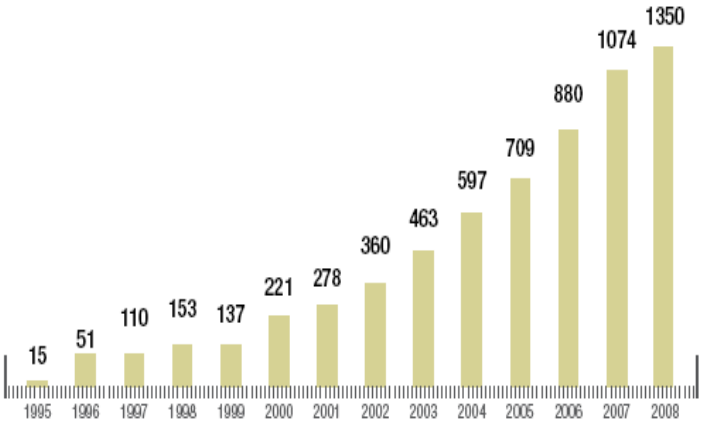

Figura 3 - Evolução do número do quadro de associados pessoas físicas desde a fundação do IBGC

Fonte: IBGC (2008)

Para Weill e Ross (2004), governança é o processo de especificar os direitos de decisão e um framework de controle de como ocorrem essas, encorajando comportamentos desejados que possibilitem a consolidação das estratégias do negócio. Ainda para esses autores, a governança corporativa compreende a governança de seis ativos, dentre eles, os de TI, interesse da chamada governança de TI. A figura abaixo representa o framework de Governança Corporativa apontado por Weill e Ross (2004):

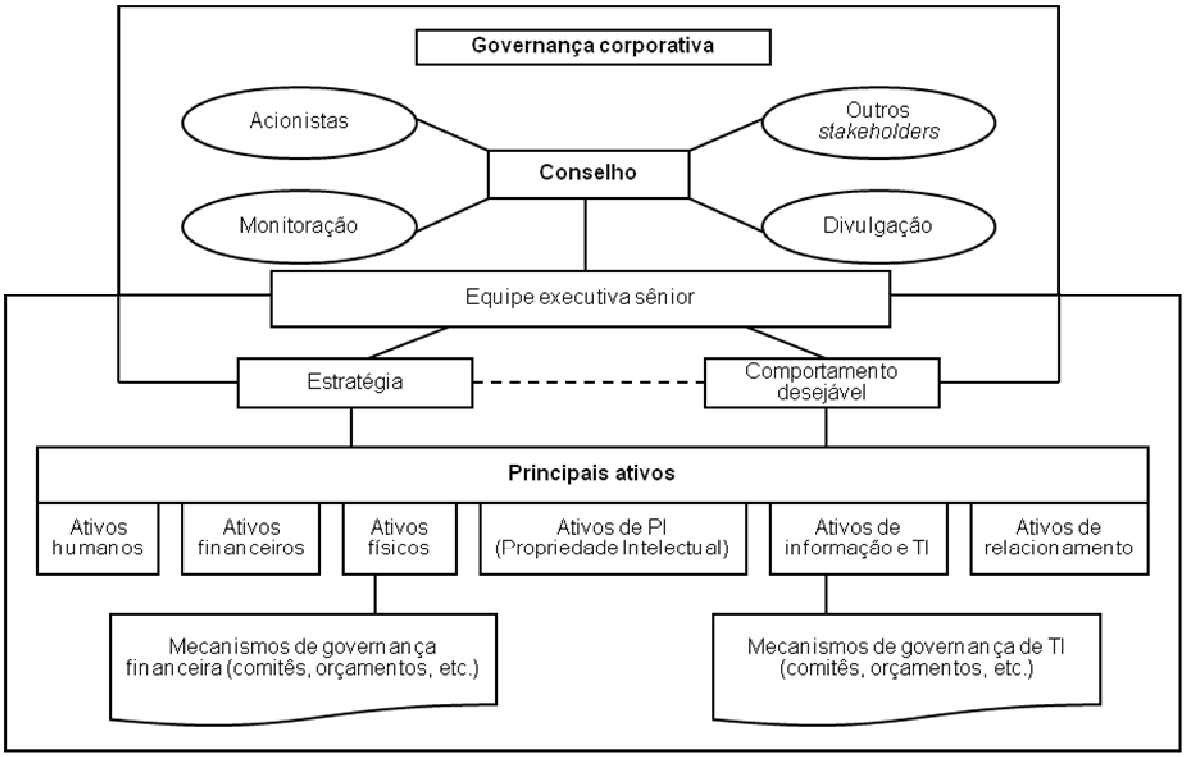

Figura 4 - Framework de Governança corporativa

Fonte:Weill e Ross (2004)

Na seqüência, será abordado o tema governança de TI em maior profundidade.

2.2.1 Governança de TI

Segundo Oliva (2005) apud Arruda (2006), “as áreas de TI são muito requisitadas para auxiliar na implantação e na viabilização de ações que tornem possível a realização dos objetivos da organização.”

Porém, no processo decisório, diariamente os gestores confrontam-se com questões dos tipos: Como sincronizar as estratégias de negócio e de TI? Como gerar resultados à organização por meio de investimentos em TI? Como lidar com a crescente dependência do negócio em relação à TI? Como mensurar e monitorar o desempenho de TI? Como controlar os processos de TI? Como melhorar os processos de análise e risco e decisório?

Para responder aos quesitos anteriores, Oliva (2005)

> *"considera necessário um processo estruturado para gerenciar e controlar as iniciativas de TI nas organizações, para garantir o retorno de investimentos e adição de melhorias nos processos empresariais." Esse processo seria a governança de TI"*

Van Grembergen (2003) define governança de TI como sendo a capacidade organizacional exercida pelo conselho diretor, gerente executivo e o gerente de TIC de controlar o planejamento e implementação das estratégias de TIC e dessa forma, permitir a fusão de TIC ao negócio. Hardy (2006)

> *[....] conclui que o objetivo principal para comitês e executivos deveria ser entender os problemas e a importância estratégica da TI, de tal forma que as organizações pudessem suportar suas operações e expandir suas atividades assim como elas se movem em direção ao futuro.*

A governança de TI então deveria focar em garantir que as expectativas fossem atendidas e os riscos devidamente mapeados.

Dada a variedade de definições, para Arruda (2006), não é possível discutir e explicar o termo *Governança de TI* por meio de um único conceito, havendo na literatura várias representações e entendimentos sobre o assunto. Keyes-Pearce (2002) apud Arruda (2006) coletaram vários conceitos sobre o tema variando desde a ênfase na estrutura da TI até o foco no processo.

Keyes-Pearce (2002) apud Arruda(2006) classificaram em cinco categorias as diferentes visões sobre Governança em TI:

- Governança de TI como estrutura
- Governança de TI como estrutura com ênfase no controle
- Governança de TI como estrutura com ênfase na coordenação
- Governança de TI como um processo centrado na sustentabilidade
- Governança de TI como processo contínuo

Na tentativa de sintetizar um conceito para Governança de TI, Webb et al.(2006) realizaram uma revisão da literatura sobre o tema e analisaram qualitativamente os conceitos encontrados, procurando elaborar uma definição comum que servisse da base para as pesquisas na área. Os autores chegaram a seguinte definição:

> *Governança de TI é o alinhamento estratégico da TI com o negócio de tal maneira que o valor máximo do negócio é obtido, através do desenvolvimento e manutenção de controles efetivos de TI , gerenciamento de performance, gerenciamento de riscos e prestação de contas.*

Diversidades conceituais à parte, com a adoção de um modelo de Governança de TI, espera-se que as estruturas e processos venham a garantir que a TI suporte e maximize os objetivos e estratégias da organização, possibilitando controlar a medição, a auditagem, a execução e a qualidade dos serviços.

Segundo Araújo (2005) apud Arruda (2006), o modelo de governança deve ser capaz de possibilitar o alinhamento das estratégias de negócio com TI, ou seja, a clara percepção de TI do que o negócio "espera" de seu desempenho, e do desenvolvimento de processos e controles efetivos.

Para construir esse alinhamento, as organizações devem implementar instrumentos de governança como estruturas, processos e comunicação (WEILL e ROSS, 2004). Na seqüência, apresenta-se o modelo de governança proposto pelo ITGI.

2.2.2 Domínios ou esforços de governança de TI

O Instituto de Governança de TI - ITGI - definiu o que chama de esforços de base ou domínios que suportam o processo de governança de TI. Para o ITGI, são cinco processos complementares, representados na Figura 5 e que serão discutidos adiante:

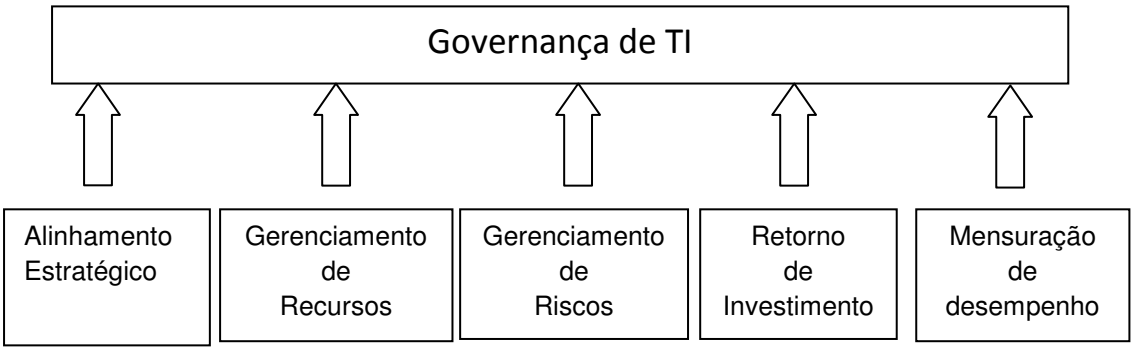

Figura 5 - Esforços da Governança de TI definidos pelo ITGI

Fonte: adaptado de (ITGI, 2004)

2.2.2.1 Alinhamento estratégico

O alinhamento estratégico, já citado anteriormente, tem como objetivo garantir a boa relação entre os planejamentos de negócio e de TI, alinhando as operações de TI com as operações de negócio e estabelecendo soluções colaborativas que garantam (LAINHART, 2008):

- A adição de valor e posicionamento competitivo para os produtos e serviços da organização.
- Redução de custos e melhoria da eficiência e eficácia da administração.

A importância do alinhamento estratégico é conhecida e bem documentada desde a década de 70 e com o passar dos anos, o tema persiste entre as maiores preocupações dos executivos de TI (LUFTMAN, 2000).

2.2.2.2 Gerenciamento de recursos

O gerenciamento de recursos compreende a otimização de investimentos, uso e alocação de recursos de TI (pessoas, aplicações, tecnologias, dados) na satisfação das necessidades do negócio, maximizando a eficiência e custos, decidindo quando e onde terceirizar processos (LAINHART, 2008). Por meio do gerenciamento de recursos, é possível tratar questões como *outsourcing*, seleção de fornecedores, treinamento, desenvolvimento de profissionais e retenção de talentos, buscando sempre a melhor relação custo/benefício.

2.2.2.3 Retorno de investimento

O objetivo dos processos de retorno de investimento é garantir que a TI entregue os benefícios prometidos e alinhados com a estratégia, concentrando-se na otimização dos custos e no provimento de valor da TI, bem como no controle de projetos e processos operacionais com práticas que aumentem a probabilidade de sucesso (risco, tempo, custos, orçamento etc.) (LAINHART, 2008).

O princípio básico desse valor está relacionado à entrega de serviços com qualidade, que ofereçam os benefícios prometidos, dentro do prazo e conforme foram orçados para auxiliar a organização a obter vantagem competitiva, redução do tempo dos ciclos de processos de negócios, maior satisfação de clientes, redução de tempo de espera de clientes e maiores produtividade e lucratividade por empregado (ARRUDA, 2006).

2.2.2.4 Mensuração de performance

Os processos de mensuração de desempenho têm como objetivo o monitoramento de serviços e de processos com base em alguns princípios: foco no cliente, eficiência dos processos, e na habilidade de aprender e crescer (LAINHART, 2008).

2.2.2.5 Gerenciamento de riscos

O gerenciamento de riscos lida com as ameaças decorrentes do uso da TI na organização. É tratado mais adiante com detalhes.

2.2.3 Práticas de Governança de TI

As práticas de governança são instrumentos que operacionalizam os conceitos de governança já discutidos. No presente trabalho, procura-se investigar quais as práticas utilizadas pelas organizações do estudo. Para tanto, serão investigadas quinze das práticas de Governança de TI mais comuns, pesquisadas em 256 organizações em um conjunto de 23 países. Apontadas por Weill e Ross (2004). Tas práticas são classificadas em 3 (três) categorias.

a) Estruturas de tomada de decisão

Unidades organizacionais, papéis e responsabilidades no processo de tomada de decisão são definidos. São os instrumentos mais notórios de governança de TI e que geram naturalmente comprometimento mútuo entre negócio e TI. Algumas práticas elencadas por aqueles autores são:

- Comitê, ou estrutura semelhante, dedicado a tomar decisões de TI, na totalidade ou subconjunto delas, com ou sem participação de membros da TI (monarquia, duopólio, federalismo), de acordo com o modelo decisório sobre TI.

- Existe um comitê ou estrutura semelhante que cuida da arquitetura de TI (padronização, normas, diretrizes para os projetos etc) da organização.

- Preocupação com o relacionamento entre as decisões do Negócio e da TI. Um ou mais profissionais são responsáveis por esse relacionamento (CIO, geralmente).

- Existe equipe que cuida dos processos da Organização juntamente com membros da TI.

b) Processos de alinhamento

Processos de alinhamento asseguram o envolvimento de toda a organização no efetivo gerenciamento e uso da TI. Não basta definir as estruturas de tomada de decisão. É preciso monitorar como esse processo ocorre e os instrumentos abaixo apontados auxiliam o referido monitoramento:

- Comitê de aprovação de investimento

Podendo ser composto por integrantes da TI, negócio ou ambos, o objetivo desse comitê é garantir que os investimentos de TI geram retornos significativos para a organização quando comparados com outras alternativas de investimento.

- Acordos de nível de serviço

A organização trabalha comumente com Acordos de Nível de Serviço definindo tempo máximo de interrupção de um sistema, tempo máximo para resolução de problemas de TI, dentre outros indicadores de qualidade de TI para o negócio. As negociações para a construção desses acordos tornam claros os requisitos do negócio em termos das necessidades de infra-estrutura, arquitetura e de aplicações de TI (JANDER et al., 2000).

- Monitoramento do andamento dos projetos e dos recursos (pessoas, dinheiro etc.) consumidos.

Passo importante para a garantia da implementação da governança de TI e que tem impacto na entrega de valor de TI ao Negócio.

- Monitoramento do valor da TI nos projetos

Um dos grandes desafios da função TI nas organizações é a garantia da entrega de valor ao Negócio. Definir um processo formal para tanto, estimula o alinhamento estratégico (ARRUDA, 2005).

c) Processos de comunicação

Com o intuito de difundir os comportamentos desejáveis, decisões sobre governança e processos de TI, alguns processos de comunicação são evocados:

- Comunicações da alta diretoria

A alta diretoria tem como prática a comunicação para os todos os níveis hierárquicos das decisões que afetam a organização, visando à transparência do processo e demonstrando comprometimento para com toda a organização.

- Escritório de Governança Corporativa

Existe a presença de um gestor encarregado de difundir as idéias e responder pela Governança de TI corporativa.

- Portais baseados na Web e intranets para a TI.

Essas ferramentas se tornam aliados no processo de comunicação da Governança, dos investimentos, dos acordos de nível de serviço a toda organização.

O Quadro 1 apresenta as principais práticas investigadas retiradas de Weill e Ross (2004), com seus objetivos e comportamentos desejáveis:

Quadro 1 - Principais práticas de Governança de TI e seus objetivos

Fonte: dados da pesquisa (2009)

Mecanismos	Objetivos	Comportamento desejado	Comportamento indesejado
Comitê de decisões de TI	Envolvimento da alta direção e conscientização do agregação de valor ao negócio junto com a TI	Envolvimento e alinhamento	Abdicação da alta direção
Comitê de arquitetura de TI	Identificar tecnologias estratégicas e padrões	Negócio direcionando as decisões de TI	Atrasos de TI e engessamento
TI na Equipe de processos	Obter uma visão de processos usando a TI efetivamente	Gerenciamento do processo fim a fim	Estagnação das habilidades funcionais e fragmentação da infra-estrutura de TI.
Comitê de aprovação de investimentos	Separação de aprovação e proposta de investimentos	Investimento prudente em TI	Paralisia dos investimentos por falta de conhecimento de TI
Acordos de nível de serviço	Especificar e mensurar o serviço de TI	Demanda e suporte profissional	Gerenciar SLA e não as necessidades do negócio
Monitoramento dos projetos, recursos e investimentos.	Recompensar os custos da TI para o negócio. Gerar valor.	Uso responsável da TI	Disfunção do uso da TI e dos investimentos

A seção seguinte trata com mais aprofundamento o tema riscos de TI, dando continuidade ao tema do presente trabalho.

2.3 RISCOS E RISCOS DE TI

O termo “risco” deriva da palavra italiana “*riscare”*, cujo significado original era navegar entre rochedos perigosos, e que foi incorporada ao vocabulário francês em torno de 1660 (Rosa et al, 1995 apud BRASIL, 2002).

No entanto, o conceito mais contemporâneo origina-se da teoria das probabilidades e implica a consideração de predição de situações ou eventos por meio do conhecimento ou pelo menos possibilidade de conhecimento da potencialidade de perdas e danos e da amplitude de suas conseqüências.

"Do ponto de vista taxonômico, não existe uniformidade na classificação dos tipos de riscos enfrentados pelas organizações." Jorion (2000, 3-4) apud Padoveze e Bertolucci(2005) oferece uma classificação básica dos riscos em riscos operacionais (*business risks*), estratégicos e financeiros. Brito (2003, 16-19) apud Padoveze e Bertolucci (2005) apresenta classificação similar à de Jorion., com três grandes categorias, riscos financeiros e operacionais, riscos de mercado, e outros tipos de riscos.

Barrese e Scordis (2003, 28) apud Padoveze e Bertolucci (2005), por sua vez, entendem que as classes primárias de incertezas são ambiental geral, indústria e incertezas específicas da companhia. Outra classificação cabível aos eventos de risco é dada por Steinberg et. al. (2003, 39) apud Padoveze e Bertolucci (2005). "Segundo tal interpretação, os fatores de risco podem ser classificados como sendo de origem interna ou externa."

Esses autores não mencionam os riscos de TI, ou os tratam indistintamente dos demais. Pode-se inferir de suas pesquisas, que não pensaram mecanismos específicos para o gerenciamento de riscos de TI, cuja natureza difere daquela pertinente aos riscos financeiros, por exemplo. Conhecer as tipologias de riscos visando à elaboração de metodologias específicas para seu gerenciamento deveria ser imprescindível para o gerenciamento da organização e sua sobrevivência.

2.3.1 Gerenciamento de riscos

As organizações têm a responsabilidade de efetuar julgamentos formais e decisões apropriadas que a levarão a um destino de sucesso. Idealmente, tais decisões deveriam ser tomadas em um ambiente determinístico, no qual todas as informações necessárias deveriam estar disponíveis para se tomar a decisão correta de forma que o resultado da decisão poderia ser previsto com alto grau de confiança. Na realidade, o que ocorre é que as decisões são tomadas sem a presença da informação completa.

AUSTRALIA (2004) define o gerenciamento de riscos como sendo “um processo multifacetado, interativo e de constante melhoria, parte integrante do processo de gerenciamento da organização e que contribui para o aprimoramento organizacional daquela. De uma maneira geral, riscos fazem parte das operações rotineiras de uma organização e podem ser gerenciados através de diversas abordagens, usando uma variedade de mecanismos. Pode ser também aplicado nos vários níveis de uma organização, seja ele estratégico ou operacional, ou mesmo em projetos específicos, para auxiliar decisões específicas, e para gerenciar áreas específicas de riscos conhecidos, como é o caso da TI.

Um ciclo de vida do gerenciamento de riscos comumente encontrado pode ser observado na figura abaixo:

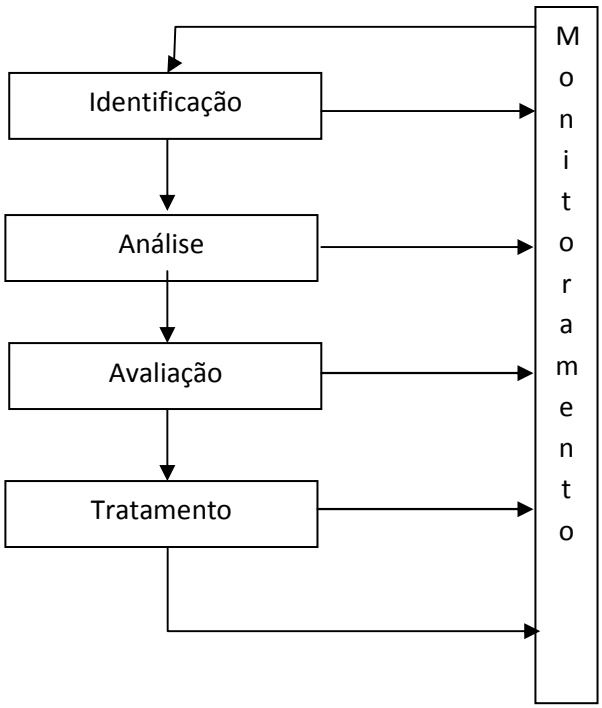

Figura 6 - Processo genérico do gerenciamento de riscos

Fonte: adaptado de (AUSTRALIA, 2004)

No que segue, as fases acima descritas são abordadas em detalhes.

2.3.1.1 Identificação dos riscos

"Essa fase consiste em identificar todas as possíveis ameaças, internas e externas, que podem impactar significativamente no sucesso da organização" (WIDEMAN, 1992).

Um processo de identificação de riscos sistemático e bem estruturado é crítico, uma vez que o risco potencial que não for identificado nessa fase poderá ser excluído de futuras análises. A identificação deve incluir todos os riscos, esses estando ou não sob controle da organização (AUSTRALIA, 2004).

Abordagens utilizadas para identificar riscos incluem *checklists*, julgamentos baseados na experiência e registros, gráficos, *brainstormings,* análise de sistemas e de cenários, dentre outros.

2.3.1.2 Análise dos riscos

Nesta fase, analisam-se os riscos em termos de conseqüência e probabilidade de ocorrência. O objetivo é separar os riscos aceitáveis da maioria dos riscos a serem tratados, bem como, prover dados para auxiliar na avaliação e tratamento dos riscos posterior (AUSTRALIA, 2004).

Conceitualmente, os riscos podem variar numa escala de alto-impacto/ alta-probabilidade, alto-impacto/baixa-probabilidade, baixo-impacto/alta-probabilidade e baixo-impacto/baixa-probabilidade. Dessa forma, conseqüências e probabilidades podem ser combinadas para produzir uma estimativa do nível do risco. Existem algumas metodologias quantitativas, qualitativas ou ainda, combinação das duas utilizadas na análise dos riscos. .

2.3.1.3 Avaliação dos riscos

Avaliação de riscos envolve comparar o nível do risco encontrado durante o processo de análise com um critério pré-estabelecido de riscos. Se o risco atender ao critério de baixo ou aceitável, ele passará por um tratamento mínimo. Riscos baixos e aceitáveis devem ser monitorados e periodicamente revisados para

garantir que eles continuem aceitáveis. Caso contrário, o risco seguira para a fase discutida na seqüência.

A saída do processo de avaliação é uma lista priorizada dos riscos para posterior tratamento.

2.3.1.4 Tratamento

O tratamento de riscos envolve identificar as possibilidades de se tratar o risco, avaliar essas opções, preparar o plano de tratamento e implementá-lo. A seguir, têm-se algumas possibilidades para o tratamento dos riscos;

a) Transferência de responsabilidade

Uma organização ou unidade pode transferir a responsabilidade de um evento adverso para uma outra parte de duas formas: Por renúncia ou por acordo. A organização renuncia a responsabilidade quando ela se encarrega de uma atividade com o entendimento explícito de que ela não será responsável pelas conseqüências de eventuais adversidades. No entanto, não se especifica quem será o responsável por essas conseqüências. A organização transfere responsabilidade quando formalmente em acordo com uma terceira parte, define que essa será responsável pelas conseqüências das adversidades. Mecanismos utilizados para tanto podem ser contratos, acordos de seguro ou estruturas organizacionais como parcerias e *joint ventures* (AUSTRALIA, 1999).

Uma desvantagem dessa abordagem é que, uma vez transferido o risco para uma terceira parte, a organização acaba de criar um novo risco, qual seja: que a organização que reteve o risco transferido, não tenha capacidade de efetivamente gerenciá-lo.

b) Compensação ou indenização

A organização pode indenizar a si própria contra as conseqüências de um evento adverso. Duas estratégias comuns utilizadas nesse caso são a fila de indenização e a indenização por aposta.

Na abordagem de filas de indenização, várias unidades da organização compartilham o custo de determinados riscos. Se um evento adverso é improvável de acontecer simultaneamente com todos os participantes da fila, o custo do risco assumido por cada participante. Já na abordagem de compensação por apostas, uma unidade da organização realiza uma aposta considerando que um evento adverso ocorrerá. Se o evento é improvável, outras organizações ou indivíduos assumem a aposta, caso a probabilidade seja alta de o risco não se materializar. Caso o evento adverso não ocorra, a organização que criou a aposta pagará a aposta.Se o evento ocorrer, os apostadores arcarão com os custos ou conseqüências do risco. O fator crítico de sucesso para a organização é calcular as probabilidades de modo a realizar uma boa aposta.

c) Mitigação

A organização pode tentar reduzir o custo de um risco, reduzindo a probabilidade de ocorrência da adversidade, ou reduzindo as conseqüências caso o risco se materialize. A probabilidade de uma adversidade ocorrer pode ser reduzida a partir do redesenho dos sistemas e/ou processos de forma a evitar eventos desconhecidos ou causas suspeitas. A probabilidade de a adversidade ocorrer pode ser reduzida a zero, quando se evita completamente a ação causadora dos eventos, o que nem sempre é a melhor escolha.

As conseqüências de materialização de um risco podem ser reduzidas evitando que os prejuízos se proliferem pela organização, ou diminuindo o tempo de vida do evento adverso, acelerando a sua detecção e recuperação, com planos de contingência por exemplo.

d) Retenção

Se um evento adverso não é tão caro ou improvável de ocorrer, ou seus benefícios conquistados assumindo o risco são grandes, a organização pode optar por reter o risco e suas conseqüências. Adicionalmente, algumas organizações se previnem financeiramente de tempos em tempos, de forma a ser possível reter riscos decorrentes de ações consideradas estratégicas, criando uma espécie de seguro próprio.

A figura abaixo ilustra os principais tipos de decisão quanto ao tratamento dos riscos identificados:

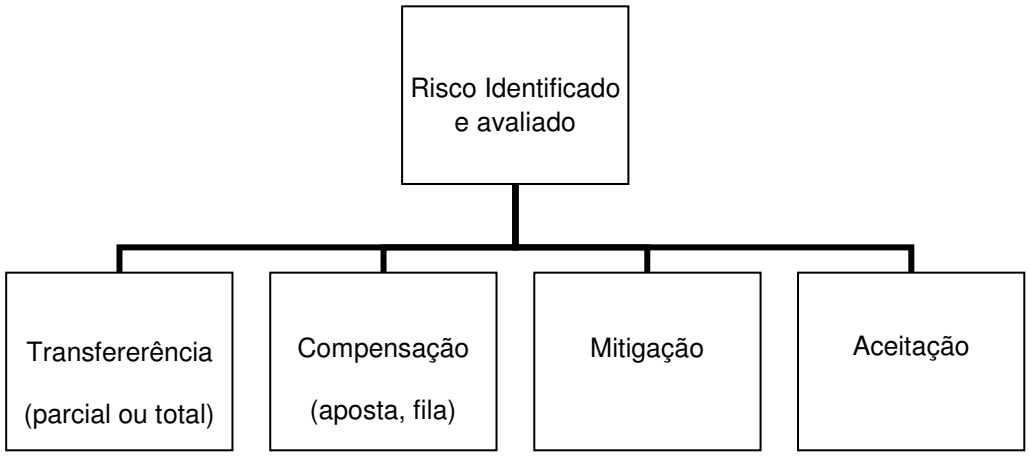

Figura 7 - Abordagens para tratamento dos riscos identificados

Fonte: o autor

2.3.1.5 Monitoramento

É necessário o monitoramento dos riscos, da efetividade do plano de tratamento escolhido, estratégias e o sistema de gerenciamento preparado para controlar a implementação do tratamento. Os riscos e a efetividade das medidas de controle precisam ser monitorados para garantir que as circunstancias não alteram as prioridades de riscos definidas (AUSTRALIA, 1999).

Poucos riscos se mantém estáticos, necessitando portanto de revisão e de constante monitoramento. Uma vez apresentado o conceito geral de gerenciamento de riscos, falar-se-á a partir de então sobre os riscos de TI, especificamente.

2.3.2 Riscos de TI

Toda organização enfrenta vários riscos como fato natural da execução de seu negócio. Alguns riscos, como a perda de um executivo chave, não estão relacionados com a TI. Outros têm um componente de TI importante em sua composição. Outros afetam a organização de forma mais direta, como a parada de um sistema. (WESTERMAN, 2004).

Um risco de TI pode ser definido como o potencial de um evento não planejado envolvendo a falha ou mau uso que causa prejuízos ao negócio e envolvidos (WESTERMAN e HUNTER, 2007).

A partir da criação de novas ameaças, vulnerabilidades e riscos organizacionais, o crescimento dos ativos de TI introduziu vários problemas de gerenciamento, requerendo políticas, tecnologias e competências organizacionais para gerenciá-los (KARYDA et al., 2005 apud Anderson e Choobineh, 2008).

Por exemplo, a proteção dos ativos de informação, ou melhor, de suas partes físicas, criou novos e indesejáveis custos, que respondem pelas despesas com ferramentas que detectam e previnem brechas de segurança (ANDERSON e CHOOBINEH, 2008).

> *Westerman e Hunter (2007) afirmam que a maioria dos riscos advém não de questões técnicas de usuário, mas sim de falhas da visão organizacional e do processo de governança de TI. Estas falhas produzem um conjunto de decisões pobres e má estruturação dos ativos de TI que se manifestam através da inefetiva governança, complexidade incontrolada e desatenção ao risco. Em suma, para esses autores, o risco de TI não surge da tecnologia por si própria, mas do processo de decisão que conscientemente ou não, ignora as potenciais conseqüências dos riscos de TI para o negócio e que ao longo do tempo se acumulam e constituem as condições para incidentes de risco e desastres para o negócio.*

2.3.3 Gerenciamento de Riscos de TI

Conforme visto na seção 2.2.2., dentro do contexto da Governança de TI, o gerenciamento de riscos de TI surge com a função de proteger os ativos de TI tais como dados, hardware, software, pessoas e recursos de todas as ameaças externas (exemplo: desastres naturais) e internas (como falhas técnicas, acesso não-autorizado, mau planejamento do negócio) de forma que os custos das perdas resultantes da realização de tais ameaças sejam minimizadas (GOTTFRIED, 1989).

A abordagem científica do gerenciamento de riscos teve seu início nos Estados Unidos e em alguns países europeus, quando do estudo da possibilidade de redução de prêmios de seguros e a necessidade de proteção da empresa frente a riscos de acidentes.

O que os americanos e os europeus na realidade fizeram foi aglutinar o que já se vinha fazendo de forma independente, em um conjunto de teorias as quais denominaram de *Risk Management* (BRASIL, 2002). A idéia principal que balizou o desenvolvimento deste conjunto de teorias refletiu tanto uma tendência para prever, planejar e alertar sobre os riscos, como a idéia de que as decisões regulamentadoras sobre os mesmos seriam menos controversas se pudessem ser estatisticamente comprovadas (STARR, 1976; RENN, 1992; apud BRASIL, 2002).

A propósito, em se tratando da área de finanças, é farta a quantidade de metodologias de medição do risco. A ênfase é dada a métodos estatísticos, geralmente com base em dados históricos. Em geral, os modelos para o gerenciamento de risco são desenvolvidos para gerenciar o risco de mercado e utilizam-se de diferentes indicadores, todos de origem estatística, para sua quantificação (PADOVEZE e BERTOLUCCI, 2005).

A idéia de gerenciar os riscos de TI com metodologias específicas vem sendo discutida desde o fim da década de 90. Um fato comum entre essas metodologias é que elas são baseadas num modelo no qual o foco esta voltado principalmente para o departamento de TI, tornando o modelo direcionado pela perspectiva de seus ativos, e não levam em consideração questões relativas ao negócio (BANDYOPADHYAY et al.,1999). Grande parte dos trabalhos inclina seus esforços para a perspectiva mais técnica, sendo comum a ênfase à área de segurança da informação.

O processo de gerenciamento de riscos pode ser dividido em quatro fases principais: identificação de riscos, análise de riscos, contramedidas de risco e monitoramento dos riscos. Bandyopadhyay et al.(1999) estudaram esse processo e criaram um modelo específico para o gerenciamento de riscos de TI. Na fase de identificação, por exemplo, esses autores classificam os riscos em níveis: nível de aplicação, nível de organização e nível inter-organizacional. Para esses autores, o modelo criado deveria prover aos gestores de TI uma visão compreensiva de todo o status do gerenciamento de riscos de TI da organização.

Westerman (2004) desenvolveu uma pesquisa sobre os riscos de TI que afetam o negócio das organizações. Na realização da pesquisa, foram entrevistados 45 gestores de TI e de negócio em 12 organizações. Tais gestores foram perguntados sobre os tipos de riscos organizacionais influenciados pelos

ativos e processos de TI. O resultado é a classificação dos riscos de TI em quatro categorias ou dimensões: Disponibilidade, Acesso, Precisãoe Agilidade.

Westerman (2004) defende ainda que os riscos de TI sejam avaliados sob a perspectiva estratégica, sendo possível até transformar um risco de TI em vantagem competitiva para o negócio. Afirma também que o gerenciamento de riscos de TI na era da informação, não pode se limitar ao gerenciamento de técnicas ou políticas de segurança da informação. Olson (2005) afirma que "o cenário dos riscos do negócio na era da informação, ao contrário do que foi no passado, agora requer que cada iniciativa estratégica considere e mitigue o potencial multidimensional dos riscos."

De fato, o aumento da influência externa sobre a organização e do relacionamento com parceiros e a diminuição do controle dos riscos sobre esses, expuseram as organizações a relações cada vez mais complexas em seu meio nas quais o gerenciamento dos riscos se torna um desafio.

De uma forma geral, esses estudos corroboram a idéia de que o gerenciamento de riscos de TI é cada vez mais necessário em detrimento da aplicação de políticas de segurança da informação, apenas, que não são suficientes para gerenciar os riscos de TI.

McFadzean et al. (2007) "examinam a percepção dos diretores de TI sobre segurança da informação e como essa percepção influencia suas ações bem como a adoção, desenvolvimento e uso de estratégias de segurança de informação."

O estudo aponta que a importância dos sistemas de informação e a percepção dos gestores sobre o risco de segurança da informação são fatores que influenciam no comprometimento dos gestores para um efetivo gerenciamento da segurança de informação. É importante que se faça uma distinção conceitual entre segurança da informação e gerenciamento de riscos de TI.

2.3.1.2 Segurança da informação e Gerenciamento de Riscos de TI

A cada dia, noticiários e organismos de segurança trazem à tona casos de vírus de última geração, ataques de negação de serviço, invasão de websites ou bugs em sistemas de segurança. Relatório do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.BR- demonstra a

evolução do número crescente de incidentes de segurança no pais, relatados voluntariamente pelas organizações brasileiras (CERT, 2009):

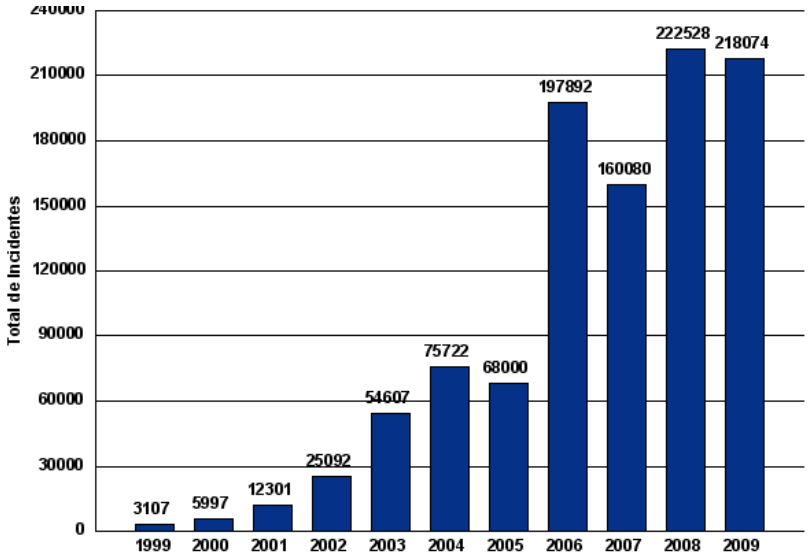

Figura 8 - Total de incidentes reportados ao CERT por ano

Fonte: CERT.BR (2009)

Também de acordo com pesquisa conduzida pela revista *Information Security Magazine* (2002), a maioria dos problemas de segurança de informação, baseado nos dados coletados a partir de 2.196 especialistas em segurança da informação, era composta por códigos maliciosos (31%), problemas com acesso de usuários (23%), TI e telecom (15%), usuários não autenticados (11%) e gerenciamento da organização (9%).

Para tentar minimizar esses eventos, é comum a confecção de políticas de Segurança da informação. Tais políticas descrevem quais seriam as informações acessadas e quem deveria ter acesso a elas. Uma vez tendo se definido uma política, o próximo passo é assegurar a sua aplicação através de um misto de processos e mecanismos técnicos. Esses processos são aplicados continuamente e as lições aprendidas em cada execução são aplicadas no próximo ciclo, num processo de realimentação. Tais processos podem ser classificados em quatro categorias:

- Medidas de proteção de ocorrência de eventos
- Medidas de detecção, que alertam o negócio quando da ocorrência de eventos
- Medidas de resposta, que lidam com as conseqüências dos eventos adversos e retornam o negócio a uma condição de segurança.
- Medidas de garantia, que validam a efetividade e a apropriada aplicação das medidas de proteção, detecção e resposta.

Os dados mostrados na **Figura 8** sugerem que a aplicação de mecanismos e processos de segurança da informação parecem não ser suficientes. BLAKLEY et al (2001) sustentam duas razões para isso: (i) "O processo de segurança da informação foca numa pequena parte do problema dos riscos de TI e (ii) não executa um bom trabalho em proteger o negócio até mesmo com relação a essa pequena parte."

Para esses autores, a segurança da informação foca primariamente na mitigação dos riscos. A análise de segurança da informação é guiada pelo desenho de cenários e confirmação de vulnerabilidades nos sistemas de informação, de forma a mitigar os riscos que as vulnerabilidades criam. Até mesmo dentro das atividades de minimização dos riscos, a segurança da informação foca mais em reduzir a probabilidade de um evento adverso do que reduzir suas conseqüências. BLAKLEY et al (2001) afirmam "ainda que a segurança da informação enquanto disciplina é geralmente baseada em mecanismos tecnológicos, lógica de hardware ou software, em vez de processos; e pouco influenciada pelo negócio. "

Uma tradução prática ocorre quando a redução das conseqüências da materialização dos riscos é implementada: as medidas tendem a focar com mais intensidade na recuperação rápida (retornar servidor de aplicações, por exemplo), do que minimizar a magnitude das perdas através de providências para evitar o crescimento dos danos. As atividades de segurança da informação raramente incluem alguma discussão sobre indenização ou transferência de riscos, por exemplo. A segurança da informação trata apenas uma fração do problema dos riscos de TI e não trabalha, portanto, de forma eficiente (BLAKLEY et al, 2001).

De acordo com um larga pesquisa conduzida pela revista *Information Security Magazine* em 2002, "a maioria dos problemas de segurança da informação é causada por negligencia humana, ao invés de eventos de ataque," por exemplo. De

acordo com a pesquisa de Crimes Virtuais e Segurança do CSI/FBI (2004), enquanto os ataques a sistemas de computadores ou o uso errado desses sistemas tem decrescido aos poucos e continuamente durante os últimos anos, as perdas anuais por organização não decresceram.

Essa tendência pode ser resultado do fato de que as organizações tem focado sua segurança para aspectos técnicos como encriptação/decriptação, controle de acesso, sistemas de detecção de intrusões etc. Entretanto, o relatório sugere que fatores econômicos e de gerenciamento de riscos se tornaram preocupações mais e mais importantes para as organizações da atualidade, e essas preocupações são complementares aos aspectos técnicos de segurança computacional, ao invés de seus substitutos (CHANG e HO, 2006).

Produtos de segurança ou tecnologias sólidos sozinhos não podem proteger a organização sem uma boa política de gerenciamento e de implementação. Tem se difundido a idéia de que segurança da informação não é primariamente um problema técnico mas sim uma questão de gerenciamento ou até mesmo do negócio (DHILLON e BACKHOUSE, 2000; VON SOLMS, 2004). Em trabalho com semelhante perspectiva, Olson (2005) afirma *que:*

> *O gerenciamento de riscos é significativamente diferente na era da informação, mais complexo do que nunca e requer uma abordagem holística englobando todas as divisões da empresa. Esse novo cenário é caracterizado por requisitos de gerenciamento complexos, pela necessidade de desenvolvimento de novas técnicas de gerenciamento bem como de novas estratégias para gerenciar o risco.*

Finalmente, Westerman e Hunter (2007) mostram que o negócio pode ser afetado pela utilização de TI, sem se quer gerar um incidente de segurança que pudesse ser contabilizado pelo CERT.BR, por exemplo, como é o caso dos riscos que afetam a agilidade na implementação de estratégias de negócio, mostrados mais adiante.

Destarte, pode-se dizer que a questão de gerenciamento de riscos é maior que a própria segurança da informação. Os trabalhos de Bandyopadhyay et al. (1999) e mais recentemente de Westerman e Hunter (2007) trazem a responsabilidade do gerenciamento de riscos para dentro da perspectiva do negócio. Essa visão é endossada pelo presente trabalho, que enfatiza as idéias contidas nesses dois modelos, procurando verificá-las experimentalmente. Na seqüência, são

explanados os dois modelos de gerenciamento de riscos utilizados no presente estudo.Dhillon e Backhouse(2000) afirmam que:

> *“ obter consenso entre os vários decisores e envolvidos com relação ao gerenciamento da segurança de informação na organização se tornou mais difícil do que resolver vários problemas técnicos que possam surgir. Os autores traçam um panorama para o que consideram o futuro do gerenciamento da segurança da informação e expandem o escopo da segurança da informação para que sejam considerados aspectos como responsabilidade dos usuários, integridade dos usuários, confiança e ética, incluindo claramente fatores organizacionais que extrapolam a dimensão técnica do problema, comumente difundida.”*

Tsohou et al. (2006) afirmam que:

> *[....] o gerenciamento de riscos envolve um número de atividades que são baseadas na forma com que os vários envolvidos percebem os riscos associados com o uso dos ativos de TI. Diagnosticam então a influência da percepção no processo. Baseados nessa visão, em seu estudo examinam o potencial da teoria da cultura como ferramenta para identificação de padrões na percepção dos envolvidos e seu efeito no gerenciamento de riscos em sistemas de informação. Para esses autores, tal ferramenta auxilia os especialistas em segurança entender e gerenciar a percepção dos envolvidos.*

2.3.3.1 Modelo de Bandyopadhyay et al. (1999): Modelo de níveis de risco em TI

Um ciclo comumente encontrado para o gerenciamento de riscos de TI na literatura contém as seguintes fases: Identificação, Análise, Elaboração de medidas de redução, Monitoramento e controle.

Diversos trabalhos deram ênfase de modo isolado a um ou mais dessas fases. O trabalho de Bandyopadhyay et al. (1999) consistiu em elaborar um modelo integrado, composto por outras propostas encontradas na literatura, formando um modelo aglutinado que atendesse a todas as fases, concentrando-se na ligação entre os seus componentes, viabilizando assim todo o sistema de gerenciamento de riscos. O referido modelo é descrito no que segue.

2.3.3.1.1 Fases do modelo

O modelo de gerenciamento de riscos de TI, para Bandyopadhyay et al. (1999) pode ser dividido em quatro fases:

a) Identificação de riscos

O gerenciamento de riscos de TI começa com o processo de identificação dos riscos, que permite a organização identificar em tempo o impacto potencial da ocorrência de ameaças internas ou externas. O primeiro passo para a identificação de riscos é definir o ambiente de TI. Para Bandyopadhyay et al. (1999) o ambiente de TI pode ser dividido em três níveis:

1. **Nível de aplicação**

O nível de aplicação se concentra nos riscos técnicos ou de falhas de implementação das aplicações de TI que podem advir do ambiente externo (desastres naturais, ações de competidores, hackers, vírus etc.) ou do ambiente interno (acesso autorizado, ou não, que resulta em abusos no uso dos sistemas). Riscos dessa categoria quando concretizados podem impactar em ativos de TI, como hardware, software, dados etc.

2. **Nível de Organização**

Nesse nível, o impacto do risco de TI é analisado ao longo das áreas funcionais da organização e da organização com um todo, ao invés de uma simples aplicação de forma isolada. Riscos nesse nível elencados por Lightle and Sprohge (1992) apud Bandyopadhyay et al. (1999) são:

- **Risco de sustentabilidade**

Refere-se ao risco de manter a vantagem competitiva gerada a partir de uma eventual aquisição de um ativo de TI por um período de tempo determinado. Sabe-se que alguns sistemas de informação podem ser facilmente adquiridos pelos

concorrentes e a vantagem competitiva inicial pode tornar-se algo comum em um determinado nicho organizacional.

- **Riscos de segurança dos dados**

As organizações correm riscos importantes dessa categoria, uma vez que é cada vez maior a dependência sobre os dados para o alcance de seu sucesso. Tais riscos abrangem desde o acesso aos dados até a perda total desses.

- **Riscos legais**

Refere-se à violação de direitos autorais de competidores e clientes através do uso da TI. A *American Air Lines*, por exemplo, foi alvo de reclamações antitruste devido ao sucesso obtido com utilização de sistemas de informação estratégicos.

3. Nível interorganizacional

Aqui, o foco é nos riscos que extrapolam as fronteiras da organização, estendendo-se a seus parceiros. Tais riscos são mais observados em organizações que utilizam sistemas de informação compartilhados por outras organizações. Loch et al. (1992) apontaram três categorias mais importantes de riscos para esse nível

- Desastres naturais
- Intrusão de hackers
- Controle fraco e ineficiente do ambiente de rede interorganizacional

b) Análise de Riscos

Na segunda fase do modelo, várias metodologias estão disponíveis para compreender e analisar os possíveis danos aos ativos de TI quando da ocorrência de ameaças externas ou internas detectadas na fase anterior. Tais metodologias são caracterizadas como quantitativas, qualitativas ou ambas.

Em seu trabalho, aqueles autores fazem uma breve compilação de algumas

técnicas utilizadas, que foge ao escopo do presente trabalho.

c) Medidas de redução de riscos

Uma vez detectados e analisados os riscos de TI no ambiente, faz-se necessário um plano de ação, composto por medidas que reduzam ou eliminem os riscos, caso a organização não o aceite. Bandyopadhyay et al. (1999) dividem as medidas de contenção possíveis nas seguintes categorias:

1. Medidas para desastres naturais
2. Medidas para computadores e vírus
3. Medidas para Riscos Estratégicos
4. Medidas para riscos legais

Cada uma dessas medidas são detalhadas no trabalho dos autores, sendo dispensável a descrição delas nesse momento.

d) Monitoramento dos Riscos

Um monitoramento de Riscos efetivo garante que as contramedidas sejam apropriadamente implementadas. Os resultados das contramedidas são avaliados para determinar se as expectativas de redução de perdas, com o gerenciamento de riscos, foram corroboradas. Dessa forma, ajustes apropriados podem ser feitos, garantindo a continuidade e efetividade do gerenciamento contra a exposição aos riscos (Bandyopadhyay et al.,1999).

Com o objetivo de quantificar os riscos de TI e identificar a efetividade das contramedidas aplicadas, BLAKLEY et al (2001) sugere “a coleta de algumas informações a respeito das vulnerabilidades identificadas, incidentes, perdas e medidas que foram eficazes.”

No que concerne a vulnerabilidades, uma lista compreensiva das vulnerabilidades de segurança identificadas precisa ser elaborada. Para cada

vulnerabilidade, as informações sobre a freqüência, modo de exploração, rapidez e facilidade de recuperação precisam ser registradas e regularmente atualizadas. As informações relativas aos incidentes sofridos pelo negócio também devem ser coletadas e devem incluir quais vulnerabilidades foram exploradas e como a resposta e a recuperação se deram.

Incidentes com vulnerabilidades desconhecidas deverão alimentar a lista desse tema. Quanto às perdas, para cada incidente identificado, a informação acerca das estimativas de perdas monetárias diretas precisa ser coletada, bem como sobre as perdas indiretas (danos à reputação e imagem da empresa).

Finalmente, informações acerca das contramedidas disponíveis, juntamente com o custo de sua execução, gerenciamento e manutenção. Para cada incidente identificado, é necessário coletar informações sobre que medidas foram utilizadas, quais foram efetivas, e quanto tempo e esforço foram despendidos para sua execução. A Figura 9 ilustra o modelo de gerenciamento de riscos de TI desses autores:

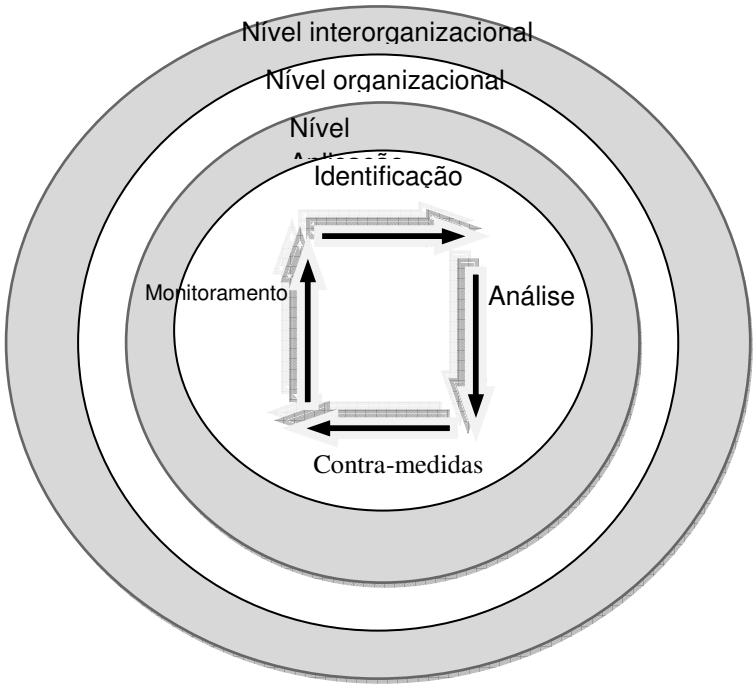

Figura 9- Modelo de Bandyopadhyay et al. (1999)

Fonte: Bandyopadhyay et al. (1999)

O modelo de Bandyopadhyay et al. (1999) acima subsidiará a avaliação da compreensão geral do processo de gerenciamento de riscos por parte dos gestores de TI.

2.3.3.2 Modelo de Westerman

Westerman (2004) elaborou um framework de riscos de TI para a organização com o objetivo de mapear os riscos do domínio técnico, para o de negócio, de modo que a equipe de TI e os executivos de negócio compartilhem uma visão única dos riscos relativos a TI que afetam a organização.

O referido autor defende que o gerenciamento adequado pode transformar os riscos de um status de ameaça para o de ativo ou diferencial competitivo. Em outras palavras, a partir do gerenciamento de riscos, a organização passa a ter o risco como vantagem competitiva.

Em seu trabalho, Westerman categoriza os riscos em quatro domínios pelos quais a organização pode sofre impacto pelo uso da TI. São eles :

1. **Disponibilidade**

Essa categoria abrange os riscos que podem afetar o funcionamento dos processos de negócio, interrompendo-os. Planejamento para recuperação de desastres deve ser uma das preocupações para minimizar os riscos dessa categoria.

2. **Acesso**

A dimensão de acesso se preocupa em garantir que as pessoas corretas tenham acesso apropriado às informações e facilidades de que precisam.

3. **Precisão**

O foco dessa dimensão reside na disponibilização de informação precisa, completa e no tempo ideal para atender às necessidades do negócio.

4. **Agilidade**

Desta vez, a preocupação é com o apoio dado pela TI em fusões organizacionais, redesenho de processos, lançamento de produtos ou serviços, que possam impactar na resposta da organização aos efeitos do mercado.

Além desses quatro domínios de riscos, Westerman e Hunter (2007) identificou empiricamente os fatores que podem afetar cada uma dessas dimensões. São seis fatores de riscos de TI identificados: Tecnologia e infra-estrutura (gerência de configuração, grau de padronização, atualização da arquitetura); aplicações e informação (complexidade da arquitetura, redundância, consistência dos dados, grau de customização); pessoas e qualificações (Rotatividade; gerenciamento de habilidades; recrutamento/treinamento, relação TI-negócio); fornecedores e parceiros (acordos de nível de serviço, uso de padrões organizacionais, fontes de recursos exclusivas, tolerância do risco dos clientes); política e processos (controle da arquitetura, grau de padronização, grau de rastreamento); e organizacionais (redução de custos, complexidade organizacional, processo de orçamento). O modelo de Westerman (2004) é sintetizado na Figura abaixo:

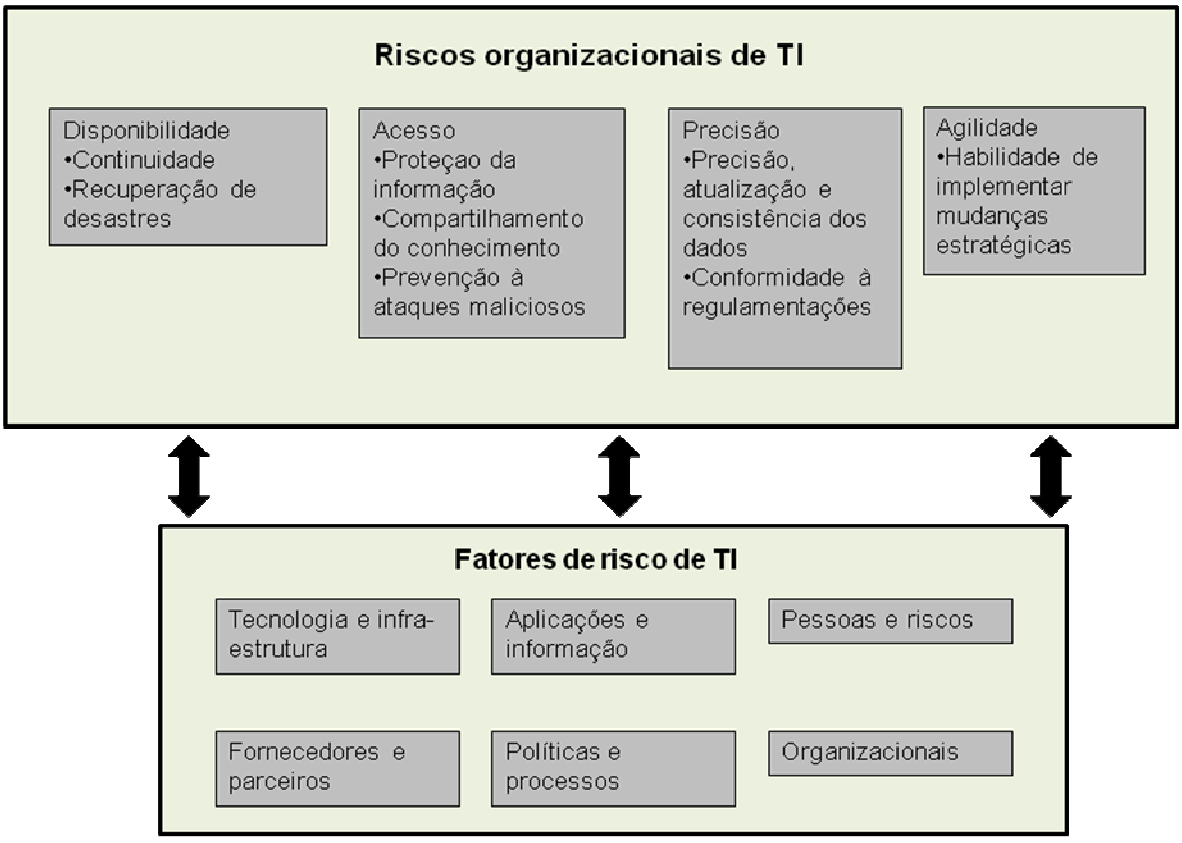

Figura 10 - Modelo de mapeamento de riscos de TI

Fonte: Westerman (2004)

Com o modelo, a organização pode identificar e gerenciar os fatores de risco, bem como saber de que forma eles podem impactar no negócio. Westerman definiu ainda o que chama de disciplinas do gerenciamento de riscos. Para ele, o processo de gerenciamento de riscos é balizado em três pilares: A cultura de conscientização sobre os riscos de TI, a governança dos seus riscos e seus fundamentos de TI.

Os fundamentos de TI consistem em práticas que procuram simplificar a sua infra-estrutura, reduzindo sua complexidade para facilitar o seu gerenciamento. O objetivo é ter uma sólida base de TI, qual seja, ativos de TI, procedimentos e pessoas, que é bem compreendida, bem gerenciada e não mais complexa do que o necessário (WESTERMAN e HUNTER, 2007). Do contrário, o gerenciamento de TI tenderá a lidar com constantes falhas, procurando remediá-las ao invés de aproveitar de uma estrutura bem construída.

A governança de riscos é conjunto de processos, políticas e estruturas que provêem uma visão corporativa dos riscos pelo qual os executivos podem priorizar e investir apropriadamente no gerenciamento dos riscos de TI, enquanto estimula que os gerentes de baixo nível gerenciem independentemente a maioria dos riscos em suas áreas. Alguns dos principais benefícios resultantes do processo de governança de riscos são: uma visão compartilhada dos riscos de toda a organização; Melhor integração do gerenciamento de riscos com a estratégia; identificação das áreas que superestimam ou subestimam o investimento no gerenciamento de riscos, dentre outros.

Por fim, a última disciplina é a cultura de conscientização dos riscos. Para os autores, ela constrói um ambiente na organização, no qual cada indivíduo, em qualquer nível, é consciente sobre os riscos, discute-os e assume um nível de responsabilidade pessoal em gerenciá-lo. Morgan (1998) define “cultura como o processo de construção da realidade que permite às pessoas verem e entenderem eventos, ações, objetos e situações de maneiras diferentes.” Considerando o estudo das organizações, a cultura é formada por valores e pressupostos básicos expressos em elementos simbólicos que ordenam, atribuem significados, constroem a identidade organizacional, agindo como elemento de comunicação e

consenso, ou ocultando e instrumentalizando as relações de dominação (ROHWEDER,2007) Segundo Westerman (2007),

> *[....] a cultura de conscientização é fator importante, pois apenas a partir de sua existência, os executivos poderão aceitar os riscos e a necessidade de gerenciá-los. Com a cultura de riscos difundida, os indivíduos também constroem uma consciência generalizada na organização sobre a natureza e as conseqüências de um comportamento considerado "de risco".*

Westerman (2007) trabalha com conceitos semelhantes daqueles discutidos no modelo de Bandyopadhyay et al. (1999), na medida em que apregoa a idéia de que os riscos de TI devem ser gerenciados não só pelo seu departamento, mas pela organização como um todo. No entanto, esses últimos autores focam na definição de um processo de gerenciamento mais clássico, definindo para ele um ciclo.

No entanto, deixam de lado a importância do redesenho ou projeto de uma boa infra-estrutura de TI e o apelo à conscientização da alta gerência para o gerenciamento de riscos, pontos contemplados no modelo de Westerman (2004).

2.3.4 Impactos do gerenciamento dos riscos de TI no negócio das organizações

Em termos de negócio, um risco é a possibilidade de um evento que pode reduzir o valor de negócio caso ele ocorra (BLAKLEY, 1997). Em estudo, o IFAC (do inglês, *International Federation Of Accountants*) apud Padoveze e Bertolucci (2005) propõe perspectivas distintas para o risco quando diz que esse pode assumir três sentidos distintos: perigo ou ameaça, incerteza e oportunidade. É possível observar as duas dimensões mais relevantes do gerenciamento de risco, quais sejam, o risco visto como uma ameaça à sobrevivência da organização, e o risco visto como algo que, quando bem administrado, pode representar potencial de crescimento (PADOVEZE;BERTOLUCCI,2005). Para esses autores, o gerenciamento dos riscos de TI, quando efetivo, pode ajudar as organizações a obter vantagem competitiva.

Existe um esforço teórico considerável traduzido em pesquisas sobre o papel dos sistemas de informação -SI- na criação de vantagem competitiva e melhoria do

desempenho organizacional (CHATZOGLOU;DIAMANTIDIS,2009). A literatura identifica uma deficiência das organizações em obter os benefícios de negócio a partir de seus investimentos em SI e em particular, suas dificuldades em obter uma vantagem competitiva sustentável a partir daqueles.

A adoção, implementação e expansão de um sistema de informação tem um importante impacto na forma como o negócio é organizado dentro da organização e não é um processo isento de riscos. Nesse sentido, um grande debate parece se instaurar atualmente, com relação à participação dos riscos de TI na performance do negócio (CHATZOGLOU;DIAMANTIDIS, 2009).

Irani (2002) apud Chatzoglou e Diamantidis (2009) classificam os impactos em duas categorias maiores: impactos financeiros, que podem ser expressos em termos monetários como lucro e custo; e não financeiros, como o trabalho de time, condutividade do trabalho.Outros pesquisadores identificaram que a implementação de TI/SI tem impacto no retorno dos investimentos e melhoria do desempenho organizacional. Finalmente, Rakesh (1996) apud Chatzoglou e Diamantidis (2009) relata que o impacto da TI na performance do negócio pode ser de natureza produtiva, coordenativa e informativa.

Os trabalhos aqui citados indicam que se a adoção de estratégias corretas é o que define o futuro de uma organização, gerenciar adequadamente os riscos a que ela se expõe significa possibilitar que a organização tenha meios de sobreviver em seu ambiente.

3 PROCEDIMENTOS METODOLÓGICOS

Nesta seção, o procedimento percorrido durante esta pesquisa será delineado. Para tanto, serão apresentados: a classificação metodológica da pesquisa, procedimento técnico, os objetos e sujeitos da pesquisa, os procedimentos utilizados na coleta de dados e os procedimentos relativos a análise e interpretação dos dados.

3.1 CLASSIFICAÇÃO METODOLÓGICA

3.1.1 Classificação quanto aos objetivos da Pesquisa

GIL (1991), considerando o objetivo ou propósito, denota três grupos possíveis para a pesquisa:

a) **Pesquisas exploratórias**: A pesquisa exploratória é o primeiro passo de todo trabalho científico. São finalidades de uma pesquisa exploratória, sobretudo quando bibliográfica, proporcionar maiores informações sobre um assunto; facilitar a delimitação de um tema; definir os objetivos ou formular as hipóteses de uma pesquisa. Portanto, a pesquisa exploratória, na maioria dos casos, constitui um trabalho preliminar ou preparatório para outro tipo de pesquisa. Estudos exploratórios têm como objeto de estudo assuntos relativamente novos e pouco estudados.

b) **Pesquisas descritivas**: descrevem as características de determinada população ou fenômeno. Os fatos são observados, registrados, analisados, classificados e interpretados, sem que o pesquisador interfira neles.

c) **Pesquisas explicativas**: são aquelas pesquisas que têm como preocupação central identificar os fatores que determinam ou contribuem para a ocorrência dos fenômenos. Pesquisa que aprofunda o conhecimento da realidade. Explica a razão, o porquê das coisas.

A presente pesquisa tem abordagem exploratória e descritiva. Quando se fala da característica exploratória da pesquisa, subentende-se que alguns estudos vão além da simples identificação da existência de relação entre as variáveis, e acabam servindo para proporcionar uma nova visão do problema. Chizzoti (2005) apud Ferreira (2007) define como sendo descritiva, a pesquisa que se restringe à descrição dos fatos.

A componente exploratória reside na preocupação em se gerar as primeiras impressões sobre o gerenciamento de riscos de TI uma vez que pouca literatura brasileira relativa está disponível sobre o assunto. Sendo assim, o estudo procura ampliar o conhecimento da área, buscando tendências, gerando hipóteses, descrevendo como se encontra atualmente a temática do gerenciamento de riscos de TI e os impactos no negócio nas organizações. O caráter descritivo reside no fato de que a pesquisa tenta descrever características do fenômeno e sua ocorrência em três organizações, procurando conhecê-lo em profundidade.

3.1.2 Classificação quanto à natureza da Pesquisa

A pesquisa é qualitativa. Richardson (1999, p.80) cita vantagens do uso de metodologia qualitativa:

> *Os estudos que empregam uma metodologia qualitativa podem descrever a complexidade de determinado problema, analisar a interação de certas variáveis, compreender e classificar processos dinâmicos vividos por grupos sociais, contribuir no processo de mudança de determinado grupo e possibilitar, em maior nível de profundidade, o entendimento das particularidades do comportamento dos indivíduos.*

Com este pensamento, a abordagem qualitativa se faz adequada aos propósitos do estudo, quando se faz necessário investigar em profundidade as variáveis que envolvem o fenômeno, o que seria dificultado em abordagem distinta. Bogdan apud Trivinos (1987) aponta características da pesquisa qualitativa que também estão presentes no estudo:

1) A pesquisa qualitativa tem o ambiente natural como fonte direta dos dados e o pesquisador como instrumento-chave.

2) A pesquisa qualitativa é descritiva.

3) Os pesquisadores qualitativos estão preocupados com o processo e não simplesmente com os resultados e o produto.

4) Os pesquisadores qualitativos tendem a analisar seus dados indutivamente.

5) O significado é a preocupação essencial na abordagem qualitativa.

3.2 CLASSIFICAÇÃO QUANTO AOS PROCEDIMENTOS TÉCNICOS (MEIOS)

Ao se escolher a estratégia da pesquisa, conforme sugere Yin (2005,p.23-24), devem-se analisar três condições: o tipo de questão de pesquisa proposta, a extensão de controle que o pesquisador tem sobre eventos comportamentais atuais e o grau de enfoque em acontecimentos contemporâneos.

Considerando a questão da pesquisa "**Como é realizado o gerenciamento dos riscos de TI nas organizações estudadas?**", adotou-se, como estratégia principal de pesquisa, o estudo de caso. O estudo de caso é a estratégia escolhida ao se examinarem acontecimentos contemporâneos, quando não é possível manipular comportamentos relevantes (YIN, 2005, p.26). Dado o escasso desenvolvimento de estudos na área e a recente discussão acadêmica, optou-se por utilizar estudo de caso, considerando também a sua adequação para a fase inicial de investigações que visam a construção de hipóteses ou reformulação do problema de pesquisa.

O estudo de caso tem constituído importante meio estratégico aos pesquisadores quando estes procuram responder às questões "como" e "por quê" certos fenômenos ocorrem, quando há pouca possibilidade de controle sobre os eventos estudados e quando o foco de interesse é sobre fenômenos atuais que só poderão ser analisados dentro de algum contexto de vida real (YIN, 2005, p.19). Em Gil (1999), pode-se constatar uma freqüência maior na utilização do estudo de caso pelos pesquisadores sociais, visto servir a pesquisas com diferentes propósitos, tais como:

a) explorar situações da vida real cujos limites não estão claramente definidos;

b) descrever a situação do contexto em que está sendo feita determinada investigação;

c) explicar as variáveis causais de determinado fenômeno em situações muito complexas que não possibilitem a utilização de levantamentos e experimentos.

Para garantir maior confiabilidade e rigor científico na execução do estudo de caso e ajudar a evitar que as evidências obtidas deixem de remeter às questões iniciais da pesquisa, convém elaborar um projeto para o estudo de caso. Yin (2005) cita cinco componentes principais a serem trabalhados:

- Questões do estudo;
- Suas proposições, se houver;
- Unidade(s) de análise;
- Lógica que une os dados as proposições ; e
- Critérios para interpretar as constatações

Essa estrutura foi seguida no presente trabalho, sendo as questões do estudo e os componentes relativos à análise dos dados agrupadas dentro do protocolo de estudo de caso (seção 3.2.3), as demais são tratadas a seguir.

3.2.1 Unidades de análise

Em um estudo de caso, a unidade de análise é o caso em investigação, podendo ser um evento, um tipo de entidade ou ainda algum tipo de processo (Rossi, 2004, p.99). Considerando a pergunta de pesquisa do estudo **Como se dá o gerenciamento dos riscos de TI nas organizações estudadas?**", naturalmente a unidade de análise a ser empregada no estudo é a própria organização. Essa simples definição é importante para ajudar na compreensão e delimitação das perguntas as quais o estudo se dispõe a realizar (YIN, 2005).

3.2.2 Proposições do estudo

As proposições oferecem base para elaboração das questões da pesquisa, que, por sua vez, responderão aos objetivos específicos da pesquisa. Cada proposição irá em direção a atenção a alguma coisa que deveria ser examinada dentro do escopo do estudo (YIN, 2005). O quadro seguinte apresenta as proposições do estudo, elaboradas a partir da reflexão sobre a teoria estudada e evidências de conhecimento comum:

Quadro 2 - Proposições da pesquisa

Fonte: Dados da pesquisa, 2009.

Objetivo específico	Proposição	Justificativa
Conhecer as práticas de governança de TI apontados por Weill e Ross(2004) em uso.	A implementação de práticas de governança de TI colabora com a adoção de mecanismos de gerenciamento de riscos de TI.	A adoção de práticas como a criação de comitês, por exemplo, pode facilitar a discussão das questões de riscos de TI junto ao negócio; A implementação de processos de comunicação da alta diretoria e intranet, pode ser usado como canal de nivelamento das informações sobre os projetos e riscos de TI; A elaboração de acordos de nível de serviço podem forçar a organização a pensar nos riscos de TI antes de assumir contratos de prestação de serviço.
Descrever a cultura de riscos existente nas organizações do sujeito da pesquisa	A existência de uma cultura de riscos difundida na organização favorece a adoção de mecanismos de gerenciamento de riscos de TI.	Uma organização que “pensa em riscos” antes de tomar suas decisões, possivelmente refletirá esse comportamento na TI.
Conhecer as práticas de gerenciamento de riscos de TI apontados por Westerman (2007) em uso.	As organizações atualmente, quando implementam mecanismos de gerenciamento de riscos de TI, esses têm essencialmente um caráter técnico em termos de TI.	Conforme apontam Bandyopadhyay et al.(1999) e Westerman(2007), predomina a ênfase nos aspectos técnicos quanto ao gerenciamento de riscos de TI.

3.2.3 Seleção do(s) caso(s)

As possibilidades de projeto de estudo de caso, para Yin (2005), podem ser : caso único de uma única unidade de análise; caso único de várias unidades de análise; dois ou mais casos com uma unidade de análise para cada caso; e por fim, dois ou mais casos com várias unidades de análise para cada caso. O referido autor aponta ainda caso decisivo; caso raro ou extremo; representativo ou típico; caso revelador; caso longitudinal como fundamentos para ajudar o pesquisador no processo de decisão sobre a quantidade de casos a utilizar em seu estudo.

A possibilidade de se efetuar um estudo de caso único foi descartada por não se configurar alinhamento entre o objetivo da pesquisa com os critérios de decisão de Yin (2005), citados acima. Optou-se, portanto, pela realização de um estudo de casos múltiplos. Yin (2005) afirma que “o estudo de casos múltiplos apresenta evidências mais convincentes: é mais provável que o pesquisador encontre os cenários sobre a temática que deseja investigar, em estudos exploratórios como o presente.”

Na opinião de Yin (2005), a utilização de um estudo de casos múltiplos deve seguir uma lógica de replicação (seja ela literal ou teórica) e não de amostragem, onde o pesquisador precisa escolher cada caso de forma minuciosa, orientação que foi seguida no presente estudo. As possibilidades de projetos de estudo de caso, com base na quantidade de casos passíveis de serem estudados são apresentadas em uma estrutura matricial como mostra a **Figura 11:**

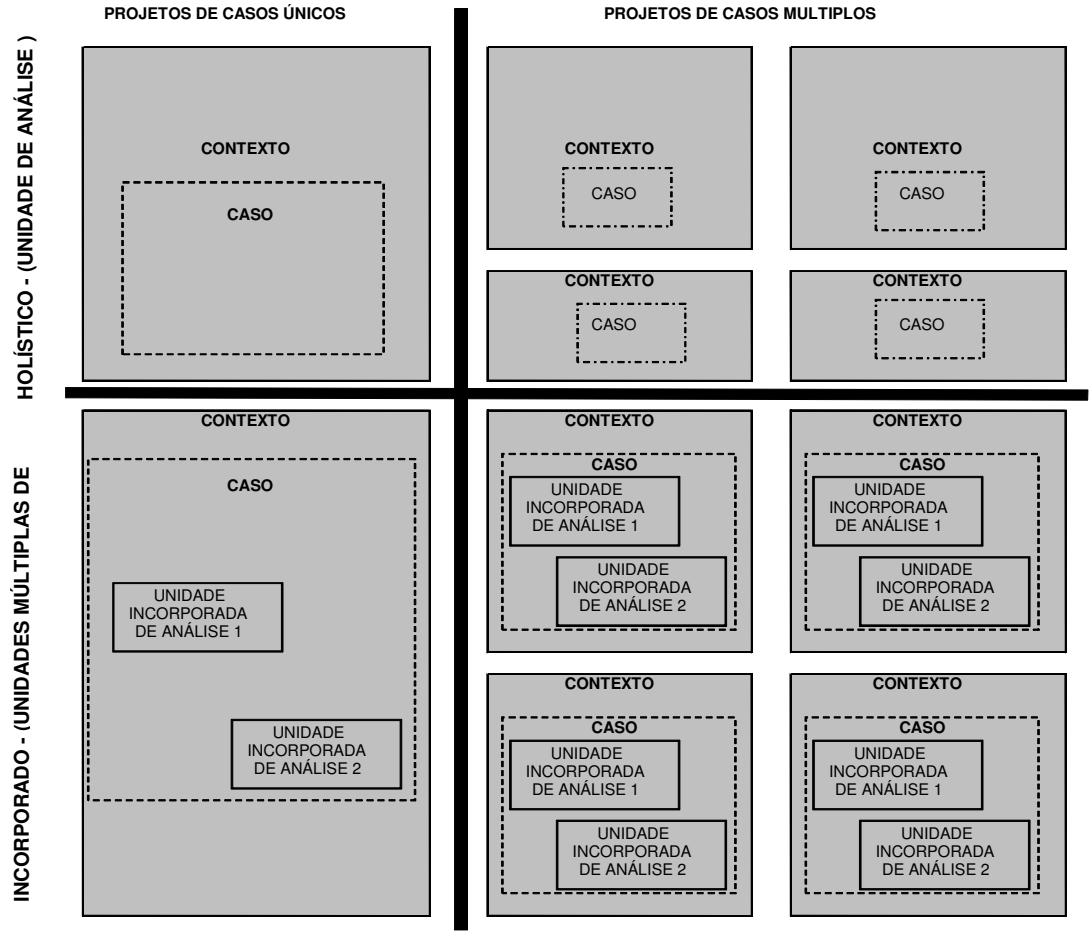

Figura 11 - Tipos básicos de projetos para estudo de caso

Fonte: Yin (2005, p.61)

Para o presente estudo de casos múltiplos, utilizaram-se dois critérios para a seleção das três organizações-alvo da replicação do estudo:

- Características das organizações escolhidas

Trata-se de organizações pertencentes ao segmento governo, que possuem quantidades de funcionários, intensidades de uso da informação, tempos de existência e natureza de negócio distintos.

- Facilidade de acesso aos seus sujeitos

Os sujeitos da pesquisa foram os gestores de TI das organizações ou indivíduo com atribuições semelhantes. A escolha dos sujeitos da pesquisa se deve ao fato destes participarem e deliberarem sobre o processo de gestão da TI em suas

organizações, sendo portanto potencialmente cientes das práticas de gerenciamento de riscos de TI eventualmente adotadas.

3.2.4 Protocolo do Estudo de Caso

Yin (2005) sugere a criação de um protocolo para o estudo de caso. Tal protocolo contém as regras a serem seguidas ao utilizar o instrumento de pesquisa. Os principais componentes de um protocolo são: visão geral do projeto; procedimentos de campo; questões do estudo; e um guia para o relatório do estudo de caso. Na seqüência é apresentado o protocolo de estudo de caso desenvolvido para a pesquisa.

3.2.2.1 Visão geral

Como parte inicial da visão geral do protocolo aqui elaborado, foi entregue à organização um termo formal de aceite sobre a participação na pesquisa, contendo o objetivo geral da pesquisa, dados do pesquisador, dentre outros contidos no Apêndice A. Foi também apresentado aos respondentes o fundamento lógico pelo qual sua organização estava sendo alvo da entrevista, conforme as justificativas descritas na seção 3.2.3.

3.2.2.2 Procedimentos de Campo

São as tarefas a serem realizadas durante a coleta e validação dos dados. A principal fonte de evidências de dados utilizada no roteiro do estudo de caso foi a entrevistas semi-estruturada (YIN, 2005, p.111). Para este estudo de caso, o procedimento de campo seguiu os seguintes passos:

1. Contato inicial com organização objeto do estudo e entrevistados, realizado por e-mail, telefone ou pessoalmente. A permissão oficial para realização da pesquisa foi concedida pelo Gestor da área de TI na organização.
2. Coleta de dados, na forma de entrevistas semi-estruturadas aplicadas através de um roteiro (Apêndice B) a gestores de TI. As coletas foram

realizadas no período de 01 a 15 de junho de 2009, em cada uma das organizações.

3. Gravação do áudio da entrevista devidamente autorizada e posterior transcrição do áudio para análise.
4. Posterior validação dos dados coletados junto aos sujeitos da pesquisa, através de resumo enviado para cada um deles, via email.

3.2.2.3 Questões do Estudo de caso

As questões do estudo de caso são como lembretes que auxiliam o pesquisador a manter o foco na pesquisa à medida que a coleta avança (YIN, 2005). As questões do estudo de caso que compuseram o roteiro de entrevista foram divididas em 6 seções, devidamente mapeadas com os objetivos específicos da pesquisa que procurarão responder, conforme pode ser observado no quadro abaixo. O roteiro de entrevista pode ser encontrado no Apêndice B.

Quadro 3 - Questões da pesquisa

Fonte: Dados da pesquisa, 2009

Objetivo	Grupo/Construto	Perguntas	Referências
Caracterizar o perfil do gestor de TI entrevistado	Perfil Gestor	Idade	O autor
		Sexo	
		Formação	
		Pós	
		Anos de experiência no cargo	
		Tipo de cargo na organização	
Caracterizar o Perfil da organização	Perfil Organização	Natureza	O autor
		Segmento	
		Número de funcionários	
		Número de funcionários do corpo de TI	
Conhecer as práticas de governança de TI apontadas por Weill e Ross(2004) em uso.	Práticas Governança TI	Conceito de governança de TI para o sujeito	Weill e Ross(2004).; Camelo (2007); ITGI (2008); Rohweder(2007);Van Grembergen(2003;)
		Grau de importância da governança de TI para o sujeito	
		Verificação das práticas abaixo: Utilização de TI nos processos Preocupação com o relacionamento negócio-TI Existência de comitê de TI Existência de comitê de arquitetura de TI	

		Realização de monitoramento de projetos Presença de acordos de nível de serviço Comunicação da alta gerência sobre decisões corporativas Existência de gestor de governança corporativa Existência de portais e intranet	
Descrever a cultura de riscos existente na organização	Cultura de Riscos	Reação dos indivíduos ao risco. Existência de confiança, consciência e conhecimento sobre riscos Compreensão dos indivíduos em relação a importância do tratamento dos riscos	Westerman (2007); Australia(1999); Olson(2005); Bandyopadhyay et al.(1999);
		Manunteção de propriedade intelectual e expertise	Westerman e Hunter(2007); Blakley et al. (2001)
		Realização de consulta a especialistas internos para decisões	
		Avaliação de riscos na tomada de decisão	
		Uso de metodologia para gerenciamento da qualidade	
		Incentivo a iniciativa das unidades	
		Documentação de vulnerabilidades	
		Documentação sobre perdas e incidentes Documentação das medidas utilizadas contra incidentes	
Conhecer as práticas de gerenciamento de riscos de TI	Abordagem utilizada para tratamento dos Riscos	Sem definição de responsável	Blakley et al (2001)
		Transferência do risco	
		Compensação por Consórcio	
		Compensação por aposta	
		Mitigação	
		Retenção/ aceitação	
	Práticas Gerenciamento de Riscos	Controle de acesso e confidencialidade dos dados para parceiros	Westerman e Hunter (2007); Bandyopadhyay et al.(1999)
		Termo de compromisso de uso dos dados para funcionários	
		Monitoramento dos usuários administradores	
		Controle de permissões dos usuários	
		Controle de logs de acesso a recursos	
		Controle de acesso ao DataCenter	
		Rastreabilidade sobre mudança das aplicações	
		Controle de versão da documentação	
		Práticas de contingência (ISO 20000)	
		Agilidade da TI para o negócio	

3.2.2.4 Relatório de análise dos dados

Para Creswell (2007) apud Gurgel (2008), o processo de análise de dados na pesquisa qualitativa consiste em extrair sentido dos dados do texto, imagens e conduzir análises diferentes. Para atingir esse objetivo, primeiramente, definiu-se a estrutura analítica geral do relatório dos estudos de caso. Conforme Yin (2005) prevê, optou-se por descrever cada caso individualmente, comparando a teoria relativa descrita no referencial, com as descobertas feitas para cada caso, relatando as conclusões e implicações numa fase posterior, comparando-as quando necessário.

Para dar suporte a esse processo, utilizou-se a análise de conteúdo, uma das várias técnicas de pesquisa que pode ser utilizada na análise de textos. Kolbert & Burnett (1991, p. 245) apud Gurgel (2008), entretanto, relatam que a utilização da técnica de análise de conteúdo deve estar pautada em processo que leve a objetividade e a confiabilidade, que, segundo os mesmos autores, se refere ao processo pelo qual categorias analíticas são desenvolvidas e usadas.

No presente trabalho, o sistema de categorias foi extraído da teoria, tendo sido necessário apenas categorizar os elementos à medida que eram encontrados.

Definiu-se o “tema” como unidade de registro para a análise de conteúdo. Para Bardin (1977), o tema pode ser definido como:

> *Uma afirmação acerca de um assunto. Quer dizer, uma frase, ou uma frase composta, habitualmente um resumo ou uma frase condensada, por influência da qual pode ser afetado um vasto conjunto de formulações singulares*.

Para Bardin (1977), a análise temática, um subtipo da análise de conteúdo, foi empregada no estudo durante o processo de categorização das entrevistas. Ela consiste em descobrir os “núcleos de sentido” que compõem a comunicação e que cuja presença ou freqüência de aparição podem significar alguma coisa para o objetivo analítico escolhido. Finalmente, o ritual metodológico executado na pesquisa está condensado na figura abaixo.

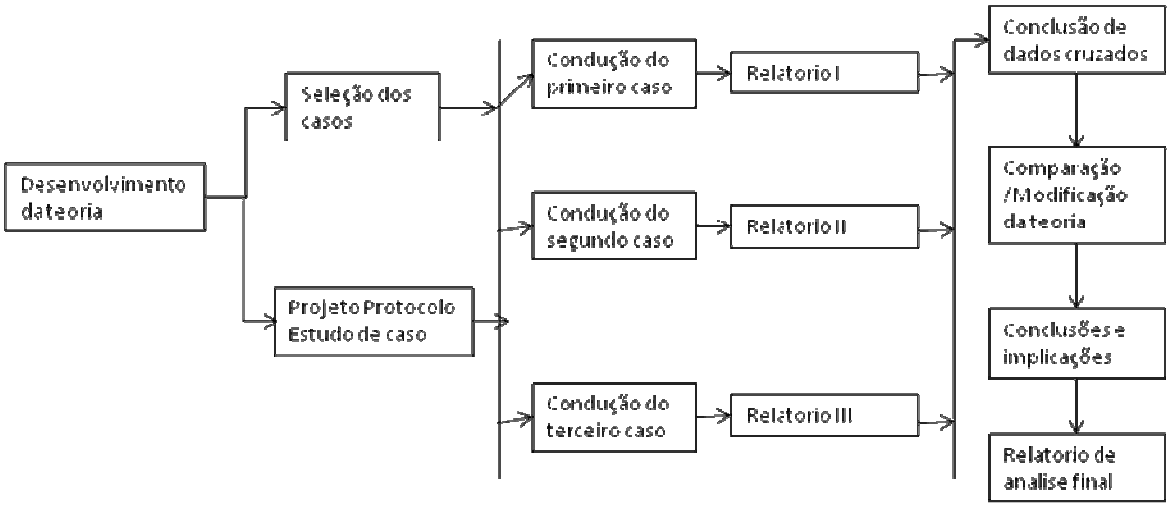

Figura 12 - Roteiro do desenvolvimento do estudo de casos múltiplos

Fonte: adaptado de Yin (2005, p.61)

3.4 CLASSIFICAÇÃO QUANTO AOS PROCEDIMENTOS DE COLETA DOS DADOS

Os dados primários foram coletados através de pesquisa de campo, utilizando-se de um roteiro de entrevista semi-estruturada que consta do apêndice B. Foi realizado um pré-teste, visando eliminar eventuais ambigüidades e dificuldades no entendimento das questões. Foram utilizados também relatórios do Diagnóstico de TI elaborado pelo governo do Estado (PERNAMBUCO, 2008).

Também foram coletados através de pesquisa bibliográfica a livros, artigos científicos, teses, dissertações, revistas e sites relevantes ao tema, configurado - se a pesquisa como bibliográfica, conforme apregoa Fachin (2003, p.125) apud DANTAS(2007) :

> *[...] Pesquisa bibliográfica diz respeito ao conjunto de conhecimentos humanos reunidos nas obras. Tem por finalidade conduzir o leitor a determinado assunto e proporcionar a produção, coleção armazenamento, reprodução, utilização e comunicação das informações coletadas para o desempenho da pesquisa.*

Os procedimentos de campo utilizados durante a coleta de dados estão explicitados na seção *3.2.2.2.* Os dados coletados resultaram em três entrevistas gravadas, com média de duração de uma hora que foram transcritas e categorizas.

3.4.1 Descrição do processo de construção do referencial teórico

É importante relatar nesta seção o processo de escolha das obras que compuseram a fundamentação teórica do presente trabalho. Pode-se falar em quatro fases:

A primeira fase do levantamento do referencial teórico consistiu na seleção de periódicos alinhados ao contexto da pesquisa, especialmente aqueles constantes do portal de periódicos da CAPES. A partir desses recursos, foram filtrados os periódicos que responderam às palavras-chave:*Information, technology, systems, security, risk, management*. No entanto, a busca não ficou limitada aquele grupo de periódicos: mecanismos de busca como o *Google scholar*, portal *Scopus*, portal *ISI web of knowledge* e fontes como o ENANPAD – Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração, ENADI – Encontro de Administração da Informação e CONTECSI – Congresso Internacional de Tecnologia e Sistemas de Informação, foram utilizados. É válido destacar que a própria escolha dessas fontes foi subjetiva e pode não representar o esgotamento de fontes a serem utilizadas.

Posteriormente, cada periódico selecionado na etapa anterior foi pesquisado procurando-se artigos com potencial contribuição à fundamentação teórica. Nessa etapa, palavras-chave como *risks, information, technology, impacts, strategic, holistic, corporative* e seus equivalentes em português, quando couberam, foram utilizados.

A terceira etapa consistiu na leitura dos resumos selecionados com vistas a identificar os artigos cujo conteúdo pudesse vir a ser relevante à pesquisa. Com a lista resultante passou-se à etapa seguinte, que consistiu na leitura do texto completo das publicações encontradas. Com a leitura dos textos foi possível identificar os artigos que não se enquadravam ao tema da pesquisa e que, portanto, foram descartados.

Ao fim deste processo, chegou-se à listagem de textos que compuseram a fundamentação teórica da pesquisa desenvolvida, resumida aos estudos de

Prodromos e Anastasios(2009), Westerman(2004), Westerman e Hunter(2007), McFadzean et al.(2007), Bandhyopadyay et al.(1999), Chang e Ho (2006), Dhillon e Backhouse (2000) e Von Solms (2004).

4. DESCRIÇÃO DOS CASOS

Os três casos estudados passam então a serem descritos neste capítulo. A identidade das organizações será preservada a pedido das mesmas, uma vez que a análise ou até mesmo o conteúdo da entrevista pode expor eventuais fragilidades por se tratar de assunto relacionado à segurança. As empresas analisadas nesta pesquisa são então identificadas como Alfa, Beta e Gama. Todas as empresas são do segmento governo com negócios distintos entre si.

O Estado de Pernambuco criou o Sistema Estadual de Informática do Governo, o chamado SEIG (PERNAMBUCO, 2006). Componente chave do SEIG, a Agência Estadual de Tecnologia da Informação – ATI – desempenha o papel de coordenação e suporte nesse sistema, possuindo as atribuições de propor e prover soluções integradoras de meios, métodos e competências, com uso intensivo e adequado da Tecnologia da Informação. A ATI atua ainda na coordenação técnica da Informática de Governo e na prestação dos Serviços Compartilhados de TI aos órgãos e entidades da administração direta e indireta, através de seus núcleos setoriais de informática – NSI (PERNAMBUCO, 2006).

As organizações aqui estudadas também fazem parte do SEIG, atuando como núcleos setoriais de informática, e de acordo com o sistema, possuem suas políticas de TI coordenadas pela ATI. A agência atua como fomentador e deliberador de programas e ações que envolvem a TI para os demais componentes do SEIG. A figura a seguir ilustra o modelo de funcionamento do SEIG e o papel da ATI, nesse contexto.

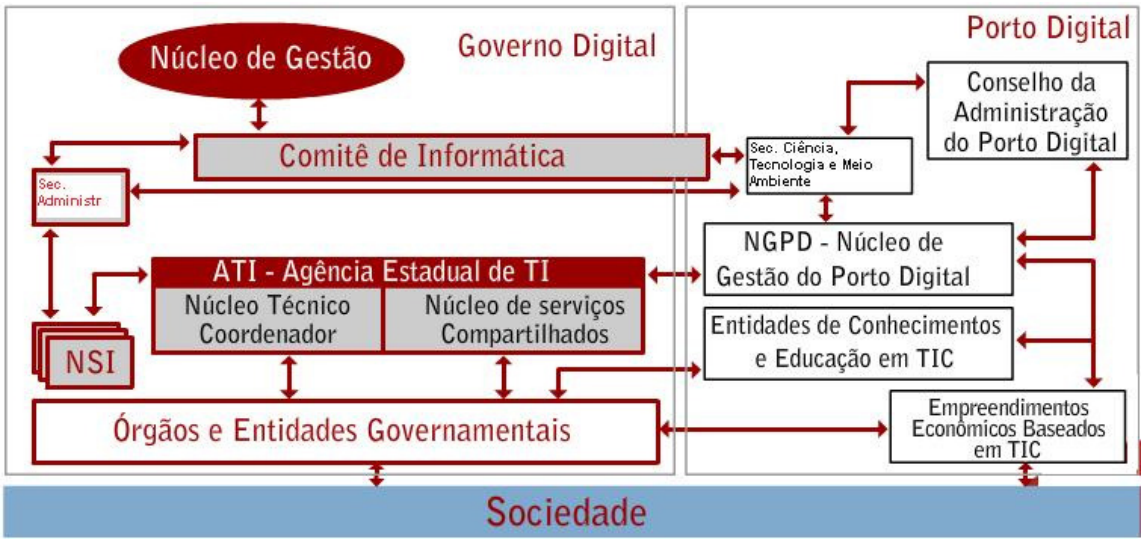

Figura 13 - Sistema Estadual de Informática de Governo de Pernambuco

Fonte: PERNAMBUCO (2006)

Na seqüência, são descritas com maiores detalhes as três organizações estudadas.

4.1 ORGANIZAÇÃO ALFA

4.1.1 Apresentação do caso

A organização Alfa é uma Secretaria do Estado de Pernambuco. Possui menos de cinco anos de existência e atua na prestação de serviços diretos ao cidadão bem como na implementação de projetos estruturais de abrangência em quase todo o Estado.

A secretaria é responsável também pelo acompanhamento das ações de outros importantes órgãos, gerindo o trabalho dos mesmos. Está centralizada numa sede física localizada na capital pernambucana.

Devido a sua recente história, a secretaria Alfa está passando por uma estruturação em seu ambiente de TI, praticamente inexistente até o início de 2008, A organização está assumindo diversos projetos prioritários do Governo nos quais estão previstos o uso intensivo de TI. Estima-se um investimento de aproximadamente R$ 800.000 (oitocentos mil reais) no prazo de um ano, apenas com projetos de TI.

O seu núcleo de TI é gerido por um profissional de 28 anos, com graduação e especialização na área de TI, juntamente com 3 técnicos, que formam o quadro

da TI. A unidade de TI não existe formalmente para a organização ainda, sendo necessário o gestor de TI se reportar a unidade Gerência Estratégica.

4.1.2 Governança de TI

Nas palavras do gestor de TI da organização Alfa, percebe-se a presença de dois dos cinco componentes citados pelo ITGI: **Alinhamento estratégico** e **Recursos de TI**. Depreende-se disso, uma visão fragmentada e reducionista de governança de TI, diversa daquela encontrada na literatura, conforme transcrito na citação abaixo:

> *[....] Governança de TI é você utilizar dos recursos de tecnologia, seja software ou hardware de forma que o uso da TI esteja alinhado com os objetivos da organização. O objetivo de toda empresa, seja publica ou privada, é ser referência no mercado. Como é que a tecnologia pode ajudar essa nisso? Provendo recursos de software e hardware. Governança de TI é gerenciar esses recursos para que os objetivos organizacionais estratégicos sejam alcançados.*

O gestor alega que o exercício do que considera "governança de TI" é necessário e procura estimular a difusão de sua importância através da sensibilização dos demais indivíduos da organização, conforme relato do mesmo "as pessoas não têm conhecimento da importância [sobre governança de TI] ou não dão a devida priorização. Algumas pessoas estão sensibilizadas, outras não. A sensibilização sobre governança é introduzida principalmente através de cases de outras organizações*."*

Quando perguntado sobre o relacionamento entre negócio e TI, mais especificamente, sobre o acesso que a TI tem ao negócio - indicador de alinhamento estratégico (LUFTMAN, 2000)- o gestor faz a seguinte afirmativa: "O relacionamento com o negócio é facilitado. Os decisores são patrocinadores da tecnologia"*.*

Apesar do conceito de governança de TI discutido por Weill e Ross (2004) não estar claro e difundido na organização, isto não impede que as práticas apontadas por esses autores estejam efetivamente implantadas. Sendo assim, procurou-se verificar a existência de cada um dos mecanismos constantes do roteiro da entrevista.

A primeira prática verificada foi o Comitê decisor de TIC. Na organização, algumas estruturas de comitês funcionam, especialmente para projetos específicos. Ainda assim, para decisões técnicas sobre TI, não existe comitê formalizado. No tocante ao envolvimento da TI nesses comitês, ele ocorre apenas quando a decisão é puramente técnica, caracterizando o que Weill e Ross (2004) chamam de Monarquia de TI para as decisões sobre tecnologia. Já para decisões relativas à TI e que não sejam essencialmente técnicas, ocorre a monarquia do negócio. O relato do gestor de TI confirma o fato "quando o negócio não tem competência de decidir se a diretriz A ou B é a mais adequada, convoca a TI. A idéia é que ajuda fosse desde o início, mas a TI só é envolvida no final."

O comitê de arquitetura de TI não existe formalmente na organização, apesar do núcleo de TI possuir algumas iniciativas na definição de normas e padrões, ocorre que a " TI tem o poder de definir a padronização, mas não tem a autoridade para institucionalizá-los na organização"- afirma o gestor de TI.

> *Não existe, formalmente, um indivíduo que cuide do relacionamento entre o negócio e TI quando das decisões comuns. Na prática o gestor de TI acumula esse papel, sendo consultado sempre que possível sobre as implicações em termos de tecnologia das decisões de negócio. Nesse tocante,"existe uma pessoa encarregada de explicar ao negócio (os desdobramentos tecnológicos das decisões de negócio).E essa pessoa é de fato, consultada. É uma das práticas que tem mais força da organização."*

A organização Alfa possui algumas iniciativas de mapeamento dos processos, como a contratação de consultoria específica para esse fim. Quanto a isso, o gestor de TI afirma que a TI teve assento desde o início desse projeto e que a organização reconhece a importância de alinhar as decisões desse projeto com a TI. O gestor de TI traz o fato à tona:

> *A organização é composta de diversas unidades e existe a preocupação dessa definição de processos. Existe um projeto estratégico que cuida dos processos dessas unidades e a TI é vista como um subsídio importante para dar continuidade e suporte. Existe uma subunidade que está fazendo um mapeamento de entradas e saídas de ações e a TI foi envolvida diretamente. Nesse projeto, a TI foi envolvida desde a primeira reunião.*

No que se refere a decisões sobre investimentos em TI, não existe formalmente um comitê de aprovação de investimentos, conforme advogam Weill e Ross (2004.). No entanto, existe um processo formal de solicitação de

investimentos no qual é exigido um parecer justificando a importância da iniciativa de TI.

O gestor de TI foi indagado sobre a existência de acordos de nível de serviço internos (JANDER et al, 2000) e se constatou que tais mecanismos não se fazem presentes, embora conste nas intenções do núcleo de TI, conforme o trecho da entrevista abaixo:

> *[...] Isso acordos de nível de serviço internos ainda não é possível porque ainda a tecnologia não está formalizada na organização. Isso é projeto. Uma vez executado e uma vez a parte operacional esteja com capital e infra-estrutura, eu terei capacidade para fazer esses contratos internos. Isso é uma meta do planejamento de tecnologia. Vou estudar um pouco sobre como vou poder aplicar isso internamente e ver se a organização está preparada para isso do ponto de vista cultural.*

Em termos de monitoramento dos projetos e ações, tem-se o seguinte diagnóstico na organização:

> *Para iniciativas externas metas do governo para a secretaria, o monitoramento é implementado naturalmente. Nesses casos, a necessidade de monitoramento vem tanto da parte de negócio como da de tecnologia. [...] Digamos que nesses casos, 90% dos projetos têm a preocupação com o monitoramento de suas ações.*
>
> *Algumas das ações internas estão sendo monitoradas dentro do possível. Quanto a ações internas, a cultura de monitoramento está difundida apenas na parte (nos projetos) de tecnologia.*

No entanto, qualquer monitoramento realizado não leva em consideração o valor da TI para a organização: “Quanto ao monitoramento valor da TI para o negócio, isso não foi feito ainda. Isso será facilmente feito através de projetos de amplitude estadual, por exemplo, e mensurar o uso do software pelo cidadão.”

Outra prática investigada foi o processo de comunicação da alta diretoria para o restante da organização. O processo de comunicação carece de formalidade, conforme externou o gestor de TI: “ As decisões geralmente são comunicadas. Existe a comunicação, feita no início, no meio ou no final do processo, ainda com algumas falhas.”

Constatou-se que a secretaria Alfa não dispõe atualmente de portais de intranet para fins de comunicação, o que dificulta o acesso às informações

corporativas, a transparência e a difusão do conhecimento. O gestor afirma que: " existe um projeto de implantação da intranet, para publicidade interna, onde os setores de imprensa e de pessoal utilizariam o serviço. Isso é uma ação de um projeto do setor da imprensa e da tecnologia. Em fase de projeto apenas."

Não existe na organização um escritório de governança corporativa. Constatou-se que o conceito não é difundido entre as unidades da organização. Finalmente, tem-se o resumo da verificação das práticas de Governança de TI na organização Alfa.

Quadro 4 - Resumo do diagnóstico das práticas de governança de TI encontradas na organização Alfa.

Fonte: dados da pesquisa (2009)

Prática de Governança de TI	**Status na organização**
Comitê de decisões de TIC	Não existe formalmente. As decisões de TI não técnicas são tomadas pelo gestor do negócio As decisões técnicas ficam para a área de TI.
Comitê de arquitetura de TIC	Não existe formalmente. Gestor de TI tem iniciativas que nem sempre são apoiadas.
CIO no relacionamento entre as decisões negócio-TI.	Não existe formalmente, embora o gestor de TI seja consultado com freqüência.
TI na Equipe de processos	TI participa suportando os processos.
Comitê de aprovação de investimentos	Não existe formalmente
Acordos de nível de serviço	Não existem.
Monitoramento dos projetos, recursos e investimentos.	Monitoramento das ações estratégicas é realizado. As ações internas são realizado apenas pela função TI.
Monitoramento do valor da TI	Não existe
Comunicação da alta diretoria	Informal
Portais baseados na web	Não existem.

4.1.3 Cultura de riscos de TI

O próximo conceito analisado na organização Alfa foi o de “Cultura de Riscos”, estudado por Westerman e Hunter (2007). Para os autores, uma cultura de riscos favorável constrói um ambiente na organização, no qual cada indivíduo, em qualquer nível, é consciente sobre os riscos, discute-os e assume um nível de responsabilidade pessoal em gerenciá-lo. Na percepção do gestor de TI, esse conceito é definido como:

> *[...] Para todo e qualquer projeto, ação ou iniciativa, você inerentemente procurar identificar os riscos, sejam positivos ou negativos e não de forma obrigatória mas sim de forma natural. Está tão intrínseco ao processo que você não consegue fugir dele. Mas para alcançar isso, deve-se ter um nível de maturidade interessante.*

Ainda com base nas idéias de Westerman e Hunter (2007), procurou-se identificar a aceitação, o nível de conhecimento e conscientização sobre o gerenciamento dos riscos, obtendo-se o seguinte relato:

> *[.....] Normalmente se colocam os riscos debaixo do tapete, pois os riscos são difíceis de tratá-los. A estratégia é deixar que eles se resolvam sozinhos. Não vejo a iniciativa pro ativa de se identificar o risco. Façamos, se acontecer alguma coisa, resolvamos. As pessoas não têm nenhuma preocupação com o risco. Eu vejo que as pessoas nem sabem do conceito, bem como da importância dessa disciplina.*

No tocante aos riscos de uma forma geral, o gestor tem intenções de implantar práticas de comunicação dos riscos eventualmente identificados para a organização, através de relatórios. Emerge nesse momento em sua fala, a dificuldade de executar tarefas relacionadas ao gerenciamento de riscos, devido ao seu excesso de tarefas e pouco recursos humanos:

“ Inclusive está nos planos se fazer um relatório semestral a ser apresentado a direção, formalizando o trabalho de gerenciamento. Infelizmente esbarro em outras tarefas. Nas situações em que o risco foi exposto, houve a compreensão por parte da diretoria.”

Quanto à verificação das práticas que estimulam o estabelecimento de uma cultura de riscos favorável, conforme discutido nos trabalhos de Westerman e Hunter (2007), a primeira a ser verificada foi a manutenção da propriedade intelectual e *expertise* dentro da organização. Nesse aspecto, o gestor se pronunciou dizendo que: “Tem uma ação de reestruturação organizacional, definição de tarefas processos, responsabilidades que visam a alcançar esse

objetivo: manter na organização a propriedade intelectual. Hoje está apenas no papel.

O Quadro cinco apresenta o resultado da verificação das práticas relacionadas com a cultura de riscos favorável, identificadas na organização Alfa.

Quadro 5 - Resumo das práticas de cultura de riscos favorável encontradas na organização Alfa

Fonte: dados da pesquisa (2009)

Práticas que favorecem a cultura de riscos favorável	**Status na organização**
Propriedade intelectual e expertise	Apenas em projeto.
Consulta a especialistas internos	Ocorre com freqüência.
Pensar em riscos antes de decisões.	Na grande maioria dos casos, pensa-se depois que a decisão é tomada.
Metodologia de gerenciamento da qualidade	Não existe. A grande maioria dos indivíduos não sabe o que é isso.
Encorajamento ao empreendedorismo	Não existe.
Responsabilidade por ações e resultados.	Não existe.
Documentação das vulnerabilidades da TI: é um objetivo/ projeto.	Não existe.
Documentação dos incidentes e respostas, recuperação:	Não. Para o gestor, isso requer um nível de maturidade que ainda não se tem.
Documentação de perdas relativas a incidentes	Não. Para o gestor, isso requer um nível de maturidade que ainda não se tem.
Desempenho das medidas, tempo, esforços	Não. Para o gestor, isso requer um nível de maturidade que ainda não se tem.

4.1.4 Tratamento formal dos riscos

Quando perguntado sobre como seria um processo de gerenciamento de riscos, o entrevistado da organização Alfa citou que em sua visão, o processo

deveria conter etapas de identificação, análise quantitativa e/ou qualitativa do risco e seu impacto, bem como de sua probabilidade de ocorrência. Mais uma vez, o gestor ressalta que “não sobra muito tempo para fazer gerenciamento de riscos” na organização.

Procurou-se investigar quais as formas de tratamento de riscos existentes na organização, para avaliar o nível de complexidade com que a questão é tratada. O Quadro abaixo retrata a situação da organização:

Quadro 6 - Resumo do diagnóstico das práticas que estimulam uma cultura de riscos de TI favorável.

Fonte: dados da pesquisa (2009)

Abordagem (BLAKLEY et al. , 2001)	**Status na organização de acordo com o gestor de TI**
a) A organização pode transferir o risco para outra parte, afirmando que não será responsável pelas conseqüências dos riscos, mas sem especificar quem será o responsável por elas. Dessa forma, não se tem responsável definido pelo gerenciamento dos riscos.	Após um processo informal de identificação de riscos, muitas vezes essa abordagem é aplicada intuitivamente.
b)A organização transfere a responsabilidade do gerenciamento das adversidades, mediante a assinatura de acordo formal com uma terceira parte.	Não existe.
c)Compensação por Consórcio: Várias unidades compartilham o custo das conseqüências de seus riscos. A idéia por trás e que dificilmente os riscos das várias unidades ocorrerão simultaneamente, distribuindo assim o custo entre os participantes desse modelo.	Não existe.
d)Compensação por aposta (hedge): A organização paga uma terceira parte para que assuma as responsabilidades dos eventos. A terceira parte aceita o risco baseando-se na probabilidade de sua ocorrência.	Não existe.
e)Mitigação: A organização trabalha para minimizar a probabilidade do risco ser concretizado ou pêra reduzir a conseqüência de seus efeitos.	Mitigação dos riscos de segurança da informação como anti-virus, firewall, backups, ainda em fase de projeto.
f)Retenção / Aceitação : A adversidade não é tão custosa ou é improvável de ocorrer, ou ainda a organização assume que os benefícios obtidos aceitando os riscos são grandes.	A aceitação pode ocorrer de maneira intuitiva

4.1.5 Práticas de gerenciamento de riscos de TI adotadas

`

No tocante aos riscos de TI que foram percebidos pelo gestor, quando indagado sobre de que forma a organização poderia sofre impactos em caso de falha da TI, o entrevistado apontou as seguintes possibilidades: " Primeiramente, a imagem da secretaria seria afetada e é o mais importante. As atividades operacionais seriam atingidas. Sem internet, infra-estrutura de TI ninguém trabalha. Se não se trabalha não se cumprem os prazos e assim se atrasam os projetos."

Existe a preocupação como acesso ou autorização da pessoa certa para ter acesso à determinada informação. O gestor relaciona também o risco da precisão das informações, quando a equipe de gestão "pode dar uma informação que não condiz com a realidade".

Conforme dito anteriormente, o gestor realiza a identificação e análise de riscos, em atividades pontuais. No entanto essa não é uma prática constante, conforme se depreende de seu depoimento: "Infelizmente eu estou sem tempo [...] Eu procuro listar os riscos para cada ação, definir riscos em termos de probabilidade e de impacto para saber se gerencio ou não o risco [...] Não tenho feito isso, mas quando fiz, fiz dessa forma."

Um problema encontrado quanto ao gerenciamento dos riscos é que, devido à falta de estrutura e formalização da TI na organização, os riscos, quando apontados, não recebem a devida importância e priorização para seu tratamento. "A TI apresenta o risco, mas o seu tratamento está fora do escopo de atuação da TI. A TI não tem autoridade para obrigar a execução do plano. Você apresenta o risco, mas não se tem tratamento dele".

Apesar da informalidade no tratamento dos riscos, a alta diretoria parece despertar para a importância de seu gerenciamento:, conforme relata o gestor Alfa: "Existiu um caso recente no qual os riscos de TI levantados pelo secretário. A parte de tecnologia não estava presente na reunião, mas o risco de TI foi considerado pelo próprio secretário."

Ainda de acordo com o gestor, há um risco potencial de catástrofe nos negócios atualmente, pois não se tem infra-estrutura mínima. O quadro abaixo traz o resumo da verificação das práticas de gerenciamento de riscos de TI na organização Alfa:

Quadro 7 -Resumo das práticas de cultura de riscos favorável encontradas na organização Alfa

Fonte: dados da pesquisa (2009)

Práticas apontadas por Westerman e Hunter (2007)	**Status na organização**
Contratos com parceiros de negócio especificam cláusulas sobre o acesso e confidencialidade dos dados. Há controle sobre os dados que os parceiros/fornecedores da organização têm acesso.	Cláusulas e contratos existem mas não há o controle sobre aquelas.
Existe um termo de compromisso sobre o uso dos dados e existem evidencias de que os funcionários leram entenderam as suas responsabilidades contidas no termo.	Não existe em prática. Apenas a intenção de fazê-la.
Existe o monitoramento das contas de usuários administradores e de duplicidade de usuários.	Não existe. Em fase de projeto.
Existe o controle sobre as permissões de cada usuário. É possível saber quais dados cada usuário tem direito a acessar.	Não existe. Em fase de projeto.
Utiliza-se o controle de acesso de quem acessou o que e quando através de logs ou similares.	Não existe. Em fase de projeto.
É possível produzir um inventario de todas as informações circulantes na organização, bem como classificar essas informações em categorias	Não existe,
Existe um controle de acesso ao Data Center ou estrutura de processamento similar.	Não existe. Em fase de projeto.
Existe controle sobre as mudanças das aplicações. As alterações podem introduzir mudanças indesejadas e não ha como controlá-las.	Não existe. Apenas a intenção de fazê-lo.
Existe controle de versionamento dos documentos da organização	Não existe. Em fase de projeto.
Está claro quem pode atualizar quais dados nos sistemas de informação. Conflitos de permissão de alteração são freqüentes.	Não existe.
Existem na organização, planos de contingência para continuidade do negocio.	Não existe.
O apoio da TI é total na execução das estratégias da empresa. Não ha dificuldades na implementação de novos projetos considerando o ambiente atual de TI.	Realidade da secretaria é distinta. Existem dificuldades de apoio da TI ao negocio.

4.2 ORGANIZAÇÃO BETA

4.2.1 Apresentação do caso

A segunda organização estudada é uma secretaria com mais de 300 servidores distribuídos por todo o estado de Pernambuco. Entre criação e alterações em sua estrutura, a organização tem aproximadamente cinco anos de existência. Articula políticas que tem impacto em segmentos de grande dimensão na sociedade. Está centralizada numa sede física localizada na capital pernambucana.

A secretaria realiza uma média de 2000 atendimentos diários diretamente aos cidadãos. Utiliza diversos sistemas de TI diretamente em seu negócio, intranet e no suporte das operações administrativas. O seu núcleo de TI é gerido atualmente por um profissional de 28 anos, com graduação e especialização na área de TI, juntamente com 7 técnicos, que formam o quadro da TI. A unidade de TI aparece formalmente no organograma da organização e se reporta a superintendência de gestão.

4.2.2 Governança de TI

O respondente ao ser questionado sobre o sua visão acerca de governança de TI, descreveu essencialmente a dimensão do gerenciamento de serviços de TI (ITGI, 2002), descartando componentes como alinhamento estratégico, gerenciamento de riscos, valor da TI etc. : “Já vi alguma coisa de ITIL e de COBIT relacionada a gerenciamento de serviços. É não trabalhar com o operacional [...] é querer utilizar os recursos, pensar um nível mais de pró-atividade do que apagar incêndio”.

O entrevistado ainda foi perguntado sobre os eventuais benefícios que considerava Governança de TI e, confirmando o escopo da sua visão sobre o conceito, descreveu temas relacionados ao gerenciamento de serviços de TI como registro de incidentes, atividades operacionais etc, característicos de frameworks como o ITIL (OGC, 2007), por exemplo:

> *[...] Um benefício é o controle dos incidentes, de o que está acontecendo, para podermos saber o que pode ser melhorado. [...] Quando se trabalha com o operacional acaba-se não prestando atenção no que está acontecendo. É importante a pessoa registrar o que está acontecendo para se conhecer melhor.*

O entrevistado não soube apontar práticas de governança de TI já implementadas e que no seu entendimento, contribuíssem para gerar os benefícios citados acima. Para isso, justificou a falta de apoio da organização para a implementação dessas práticas, uma vez que a organização vê na unidade da TI o suporte para "conserto de máquinas, e para apagar incêndio".

Procurou-se também, para esse caso, verificar a existência de cada uma dos mecanismos de governança de TI constantes do roteiro da entrevista. Começando pela presença de comitê específico para decisões de TI, verificou-se que a organização não possui comitê ou estrutura semelhante formalizada, sendo as decisões estratégicas de TI tomadas pela alta direção, caracterizando uma monarquia de negócio. Dentro desse arquétipo de decisão, algumas unidades fim da organização são ouvidas, mas sem poder de decisão:

> *O gerente de TI levanta o que se pode fazer para melhorar e vai para o secretario. Lá se analisava politicamente o que fazer, juntamente com a questão técnica, quando necessário. Ouvem-se as áreas que irão utilizar os sistemas, normalmente. Alguns setores solicitam novas soluções e informam a gente para ver o que podemos fazer. Agora a questão do comitê, não existe nada formalizado [...]*

Também inexiste comitê para definição da arquitetura de TI. Conforme atesta o gestor, "as demandas que aparecerem a gente resolve". Não existe comitê que pense exclusivamente em padrões. Formalmente, o gestor é responsável pelo relacionamento entre a TI com a alta direção e é consultado nas decisões que envolvem a TI, fato que já deixou de ocorrer algumas vezes.

O gerenciamento de processos em uma unidade dedicada inexiste. A TI é a única unidade que atua identificando processos, informalmente. O gestor de TI atesta a inexistência de relação da TI com qualquer iniciativa semelhante:

> *Não existe uma equipe de processos. O que acontece é que quando vai desenvolver a solução a gente procura mapear os processos para se desenvolver o sistema. Não há preocupação com melhoria de processos. Atualmente existe uma empresa de consultoria contratada para fazer o planejamento estratégico. Mas a TI não tem nenhuma relação com o trabalho dessa consultoria.*

Os investimentos em TI decorrem de projetos, alguns deles pré-formatados correlacionados com ações promovidas pelo Governo Federal, inexistindo um comitê para análise de investimentos de TI e seu retorno.

O gestor afirma que "o investimento de informática é uma conseqüência do investimento em projetos [...] é como se a informática servisse de apoio (operacional), apenas".

Quanto à presença de acordos de nível de serviço internos, o gestor afirma ser "muito difícil de conseguir (implementá-los)". Situação semelhante ocorre com o monitoramento dos recursos dos projetos, que são pontuais e sem nenhuma metodologia aparente, é o que diz o respondente nessa parte do texto:

> *Em alguns casos, existe (monitoramento dos recursos do projeto). Principalmente nas metas prioritárias do governo. Mas quanto ao monitoramento dos projetos de TI apenas o que cobram é, por exemplo, atividades como o andamento da confecção de um termo de referencia[1]. Num recente sistema, procurou-se contabilizar o custo que era antes e como se melhorou, quantos atendimentos por mês, custo de deslocamento do usuário do serviço quando não automatizado, impressões etc. Foi feito, só que nem sempre as coisas são aprovadas de acordo com isso.*

O processo de comunicação das decisões por parte da alta direção da organização, na opinião do gestor de TI, não é adequado: Pelo que ouço falar não tem muita comunicação dessas decisões. Recentemente foi decidido elaborar um sistema sem a devida comunicação à TI, sem se preocupar com os recursos disponíveis, se a gente poderia fazer. [...] Vai fazendo, vai acontecendo [...].

Finalmente, constatou-se que a Secretaria Beta faz uso de internet para disponibilizar seu site institucional e intranet para compartilhamento de informações e disponibilização de serviços.

No intuito de resumir as informações, o Quadro abaixo traz o resumo da verificação das práticas de governança de TI na organização Beta:

[1] Termo de Referência é o documento que deverá conter elementos capazes de propiciar a avaliação do custo pela Administração(governo), diante de orçamento detalhado, considerando os preços praticados no mercado, a definição dos métodos, a estratégia de suprimento e o prazo de execução do contrato em qualquer compra ou aquisição (BRASIL, 2000).

Quadro 8 - Resumo do diagnóstico das práticas de governança de TI encontradas na organização B

Fonte: dados da pesquisa (2009)

Prática de Governança de TI	Status na organização
Comitê de decisões de TIC	Não existe formalmente. As decisões não técnicas de TI são tomadas pela direção.
Comitê de arquitetura de TIC	Não existe formalmente. O gestor de TI responde reativamente caso seja necessário.
CIO no relacionamento entre as decisões negócio-TI	Não existe formalmente. O gestor de TI é consultado com freqüência. Não há formalização da necessidade dessa consulta
TI na Equipe de processos	Não existe equipe de processos ou gerenciamento desses. A TI ocasionalmente os mapeia para fins de desenvolvimento de sistemas.
Comitê de aprovação de investimentos	Não existe.
Acordos de nível de serviço	Não existem.
Monitoramento dos projetos, recursos e investimentos.	Existe parcialmente. Monitoramento das ações estratégicas é realizado. Não há acompanhamento das ações internas/adminsitrativas.
Monitoramento do valor da TI	Não existe
Comunicação da alta diretoria	Existe informalmente e é deficiente.
Escritório de governança corporativa	Não existe.
Portais baseados na web	Intranet e Site institucional

4.2.3 Cultura de riscos de TI

No caso da organização Beta, o gestor lamenta a forma com a qual a organização lida com os riscos, quando afirma que “as pessoas vão fazendo e a coisa vai acontecendo...”, sem se preocupar com a questão dos riscos.

Ele cita um caso recente em que foi tomada a decisão de se implantar um sistema de informação sem consultar a área de TI, ignorando a disponibilidade de recursos da área e eventuais riscos.

O gestor Beta afirma que “as pessoas não têm até mesmo conhecimento para falar de riscos”, de um modo geral. Assim como ocorreu no caso da implantação do sistema, a direção parece desconsiderar a existência ou a importância do gerenciamento de riscos, inexistindo uma cultura favorável à discussão sobre eventuais riscos identificados (WESTERMAN, 2007).

Em face dessas declarações, procurou-se verificar as práticas que, segundo a literatura, favorecem uma cultura de riscos favorável. O resultado é apresentado no Quadro abaixo:

Quadro 9 - Resumo das práticas de cultura de riscos favorável encontradas na organização Beta

Fonte: dados da pesquisa (2009)

Práticas que favorecem a cultura de riscos favorável (WESTERMAN e HUNTER, 2007)	**Status na organização**
Propriedade intelectual e expertise	Não existe. Segundo o gestor, “Não se tem preocupação com isso”.
Consulta a especialistas internos	Não existe.
Pensar em riscos antes de decisões.	Não existe.
Metodologia de gerenciamento da qualidade	Não existe.
Encorajamento ao empreendedorismo	Não existe.
Responsabilidade por ações e resultados.	Não existe.
Documentação das vulnerabilidades da TI: é um objetivo/ projeto.	Não existe. Existe um projeto para contratação de consultoria que realize tal trabalho.
Documentação dos incidentes e respostas, recuperação:	Não existe.
Documentação de perdas relativas a incidentes	Não existe.
Desempenho das medidas, tempo, esforços despendidos.	Não existe.

A grande maioria das práticas que favorecem o gerenciamento de riscos de TI propostas pela literatura correlata não foi encontrada na organização. A luz do que apregoam Westerman e Hunter (2007) e Blakley et al.(2001), pode-se dizer que a organização Beta também não apresenta uma cultura de riscos favorável ao gerenciamento de riscos de TI.

4.2.4 Tratamento formal dos riscos

Inicialmente, atestou-se a inexistência de qualquer processo formal de gerenciamento de riscos ou parte dele. O gestor relata que existem dificuldades na aplicação de um processo formal de gerenciamento de riscos tanto pela falta de consciência quanto de conhecimento das pessoas: “Eu até sei como funciona isso. Em alguns casos, pode-se até fazer uma parte do processo, mas na maioria dos casos, o pessoal não sabe o que é isso. Então para colocar isso em prática é difícil.”

Prosseguiu-se na verificação de quais abordagens de tratamento eram utilizadas na organização, ainda que de maneira informal. O resultado pode ser visto no quadro abaixo:

Quadro 10 - Resumo do diagnóstico das abordagens de tratamento de riscos encontradas na organização Beta

Fonte: dados da pesquisa (2009)

Abordagem (BLAKLEY et al. , 2001)	**Status na organização**
a) A organização pode transferir o risco para outra parte, afirmando que não será responsável pelas conseqüências dos riscos, mas sem especificar quem será o responsável por elas. Dessa forma, não se tem responsável definido pelo gerenciamento dos riscos.	Abordagem inexistente.
b) A organização transfere a responsabilidade do gerenciamento das adversidades, mediante a assinatura de acordo formal com uma terceira parte.	Abordagem inexistente.
c) Compensação por Consórcio: Várias unidades compartilham o custo das conseqüências de seus riscos. A idéia por trás e que dificilmente os riscos das várias unidades ocorrerão simultaneamente, distribuindo assim o custo entre os participantes desse modelo.	Abordagem inexistente.
d) Compensação por aposta (hedge): A organização paga uma terceira parte para que assuma as responsabilidades dos eventos. A terceira parte aceita o risco baseando-se na probabilidade de sua ocorrência.	Abordagem inexistente.
e) Mitigação: A organização trabalha para minimizar a probabilidade do risco ser concretizado ou pêra reduzir a conseqüência de seus efeitos.	Iniciativas pontuais de caráter mais técnico como substituição de máquinas, uso de softwares anti-vírus etc.
f) Retenção / Aceitação : A adversidade não é tão custosa ou é improvável de ocorrer, ou ainda a organização assume que os benefícios obtidos aceitando os riscos são grandes.	Abordagem é aplicada informal e inconscientemente, na medida em que não se discute os riscos.

4.2.5 Práticas de gerenciamento de riscos de TI adotadas

Quando indagado sobre de que forma a organização poderia sofrer impactos em caso de falha da TI, o entrevistado apontou com ênfase a importância da disponibilidade da internet e dos sistemas, uma vez que são realizados mais de 2000 (dois mil) atendimentos por dia na secretaria. O gestor externou a preocupação com essa questão que pode afetar a imagem da organização, afirmando que “se der uma paradinha de 5 minutos nos sistemas de informação, as pessoas ligam para cá cobrando”.

Não foram citados impactos na precisão e acesso das informações. Ainda de acordo com o gestor, a falta de recursos humanos constitui forte ameaça à agilidade dos processos da organização. Ele afirma que, atualmente, existem alguns projetos que estão parados por não se ter pessoal de TI suficiente.

O gestor não tem nenhum procedimento ou metodologia para gerenciamento de riscos de TI. Apenas em caráter informal, de forma não-sistematizada, nas reuniões com os decisores do negócio, procurava-se identificar riscos nos projetos da TI.

O Quadro abaixo traz o resumo da verificação das práticas de gerenciamento de riscos de TI na organização Beta:

Quadro 11 - Resumo das práticas de gerenciamento de riscos encontradas na organização Beta

Fonte: dados da pesquisa (2009)

Práticas apontadas por Westerman e Hunter (2007)	**Status na organização**
Contratos com parceiros de negócio especificam cláusulas sobre o acesso e confidencial idade dos dados. Há controle sobre os dados que os parceiros/fornecedores da organização têm acesso.	Não existe.
Existe um termo de compromisso sobre o uso dos dados e existem evidencias de que os funcionários leram entenderam as suas responsabilidades contidas no termo.	Em elaboração.
Existe o monitoramento das contas de usuários administradores e de duplicidade de usuários.	Prática existente
Existe o controle sobre as permissões de cada usuário. É possível saber quais dados cada usuário tem direito a acessar.	Prática existente.
Utiliza-se o controle de acesso de quem acessou o que e quando através de logs ou similares.	Prática existente
É possível produzir um inventario de todas as informações circulantes na organização, bem como classificar essas informações em categorias	Não existe
Existe um controle de acesso ao Data Center ou estrutura de processamento similar.	Não existe.
Existe controle sobre as mudanças das aplicações. As alterações podem introduzir mudanças indesejadas e não ha como controlá-las.	Não existe formalmente. Apenas intenção.
Existe controle de versionamento dos documentos da	Não existe formalmente.

organização	
Está claro quem pode atualizar quais dados nos sistemas de informação. Conflitos de permissão de alteração são freqüentes.	Não existe tal prática.
Existem na organização, planos de contingência para continuidade do negocio.	Não existe formalmente
O apoio da TI é total na execução das estratégias da empresa. Não há dificuldades na implementação de novos projetos considerando o ambiente atual de TI.	A TI enfrenta dificuldades em suportar o negócio, principalmente devido a falta de recursos humanos.

4.3 ORGANIZAÇÃO GAMA

4.3.1 Apresentação do caso

O último caso se refere a uma das mais antigas secretarias do Estado de Pernambuco, disposta entre as maiores secretarias. Seu negócio está presente em várias cidades do Estado, contando com aproximadamente 2000 (dois mil) colaboradores. Sua sede física está localizada na capital pernambucana.

Devido a sua longa trajetória, a secretaria passou por diversos estágios de evolução em termos de TI, representando hoje uma das estruturas mais robustas em termos de ativos de TI como sistemas, servidores, terminais, conectividade etc. A organização é mais madura quando comparada aos casos anteriores, com relação a algumas práticas de gestão de TI, possuindo, por exemplo, uma metodologia própria de planejamento estratégico definida e executada, iniciativas na área de gestão da qualidade, dentre outros. Faz uso intensivo de tecnologia, praticamente em todas as atividades, sejam elas atividades meio ou fim.

A secretaria Gama configura também um dos maiores corpos de TI de Pernambuco. Em 2007, seu orçamento apenas para contratos de manutenção de sistemas e renovação de licenças de software foi da ordem de R$ 1,5 milhão, aproximadamente.

A organização, que desempenha um papel estratégico para o Estado, tem seu gestor de T, com formação na área de engenharia e 40 anos de idade. A unidade de TI tem o status de superintendência e responde ao próprio secretário. É composta por assessorias e gerências com funções bem definidas.

4.3.2 Governança de TI

Dando início a discussão sobre governança de TI, o respondente da organização Gama, ao tentar definir o referido tema, expôs que “a idéia é gerir a TI, com vistas a manter seu pleno funcionamento, gerenciando projetos, controlando incidentes e riscos, garantindo a disponibilidade dos sistemas, integridade dos dados e gerenciando mudanças.”

No relato do respondente, aparecem componentes das dimensões “Gerenciamento de serviços de TI”, “Gerenciamento dos riscos”, “Alinhamento estratégico”, mas, ainda assim, representa uma visão parcial do conceito quando comparado com aqueles encontrados na literatura. O entrevistado afirma ainda que a implementação das atividades supracitadas é de alta importância para o funcionamento da organização.

Quando indagado sobre as práticas de governança de TI já implantadas, o respondente cita algumas iniciativas pertencentes ao ITIL (2007), relativas ao seu sistema de atendimento de chamados e incidentes ou *helpdesk.*

A organização estuda implantar o framework de gerenciamento de serviços de TI em suas ações futuras. Reuniões de acompanhamento e monitoramento de projetos, recursos financeiros, de pessoal, tempo também são realizadas regularmente. A existência de um planejamento estratégico de TI na organização (REZENDE, 2008) contribui para o alinhamento estratégico do negócio - TI e para explicitar o valor da TI. O Quadro abaixo traz o resumo da verificação das práticas de governança de TI:

Quadro 12 - Resumo do diagnóstico das práticas de governança de TI encontradas na organização Gama

Fonte: dados da pesquisa (2009)

Prática de Governança de TI	Status na organização
Comitê de decisões de TIC	Não existe formalmente. No entanto, As decisões são tomadas em conjunto com a TI.
Comitê de arquitetura de TIC	Não existe formalmente. Existem equipes responsáveis pela segurança da informação, gestão da qualidade que eventualmente elaboram padrões, documentos etc.
CIO no relacionamento entre as decisões negócio - TI.	O gestor de TI é consultado com freqüência.
TI na Equipe de processos	Não existe formalmente equipe de processos ou gerenciamento desses. A TI participa ativamente da definição alteração dos processos, devido ao seu uso intensivo naqueles.
Comitê de aprovação de investimentos	Não existe formalmente. Os investimentos são discutidos em reuniões bimestrais. Nas reuniões de monitoramento dos projetos.
Acordos de nível de serviço	Não existem. Apenas a intenção.
Monitoramento dos projetos, recursos e investimentos.	Existem reuniões formais bimestrais para acompanhamento através de indicadores de gestão, revisão do planejamento e do orçamento. É uma prática institucionalizada.
Monitoramento do valor da TI	Não existe a prática de demonstrar formalmente o valor da TI
Comunicação da alta diretoria	Não existe a prática sistematizada. Mas informalmente ela ocorre através de ofícios circulares, de forma impressa, avisos etc.
Escritório de governança corporativa	Não existe o conceito de governança corporativa de uma forma holística na organização.
Portais baseados na web	Existem site institucional e intranet que são utilizados pelos servidores, de acordo com o gestor.

4.3.3 Cultura de riscos de TI

O entrevistado da organização Gama foi enfático ao afirmar que “o conceito de riscos e de gerenciamento de riscos de TI não são bem entendidos dentro da organização”. As pessoas não conversam ou não são encorajadas a discutir sobre riscos, de uma forma geral.

Há deficiência na própria consciência individual bem como no conhecimento da maioria dos indivíduos sobre a temática.

O entrevistado tem o conhecimento do que seriam as fases de um “processo padrão” de gerenciamento de riscos, conforme mostrado em Austrália (1999), mas afirma que “não existe tal processo de gerenciamento dentro da organização.” Ele cita um caso recente em que se deixou de decidir uma melhoria em um processo da organização porque não havia como medir o risco inerente a implantação dessa ação. A organização então deixou de agregar agilidade e inovação ao seu negócio por não ter os meios com os quais pudesse identificar analisar ou mitigar os riscos inerentes à decisão, conforme externado em trecho da entrevista:

> *[....] Existe aqui uma dúvida sobre a possibilidade do trabalho de um grupo de servidores ser realizado em casa. Até se acredita que isso trará benefícios para a organização, embora sabendo que existem fatores culturais envolvidos. Mas a questão é que não se decidiu até hoje a questão por não se ter como medir quantitativa ou qualitativamente esse risco que se imagina existir*.

Dito isto, foi verificada a existência das práticas que favorecem a criação de uma cultura de riscos favorável (WESTERMAN E HUNTER, 2007) na organização Gama e os resultados constam no Quadro abaixo:

Quadro 13 - Resumo das práticas de cultura de riscos favorável encontradas na organização Gama

Fonte: dados da pesquisa (2009)

Práticas que favorecem a cultura de riscos favorável(WESTERMAN e HUNTER, 2007)	**Status na organização**
Propriedade intelectual e expertise	Não existe. Existe Apenas a preocupação com o tema.
Consulta a especialistas internos	Existe.
Pensar em riscos antes de decisões.	Não existe.
Metodologia de gerenciamento da qualidade	Existe
Encorajamento ao empreendedorismo	Não existe
Responsabilidade por ações e resultados.	Não existe
Documentação das vulnerabilidades da TI	Não existe
Documentação dos incidentes e respostas, recuperacao:	Não existe
Documentacao de perdas relativas a incidentes	Não existe
Documentacao do Desempenho das medidas, tempo, esforcos envidados.	Não existe

4.3.4 Tratamento formal dos riscos

A unidade se segurança da informação, composta por dois analistas, realiza atividades técnicas que podem ser vistas como medidas de mitigação, como é o caso de instalação de softwares anti-vírus, *spywares,* configuração de permissões, *firewalls ,*dentre outros. A aplicação dessas medidas é feita de forma intuitiva, com base na experiência dos analistas, não existindo um processo formal de gerenciamento de riscos composto por fases e que seja seguido em sua grande parte.

“ Isso acontece apesar de haver a compreensão sobre o que seria um processo formal de gerenciamento”, como o disposto em AUSTRALIA (2004).

Mesmo identificando que a organização Gama não possui processo de gerenciamento de riscos bem definido, procurou-se identificar quais abordagens de tratamento eram aplicadas, ainda que de forma pontual ou informal. Pode-se observar os resultados encontrados no Quadro abaixo:

Quadro 14 - Resumo do diagnóstico das abordagens de tratamento de riscos encontradas na organização Gama

Fonte: dados da pesquisa (2009)

Abordagem (BLAKLEY et al. , 2001)	**Status na organização**
a) A organização pode transferir o risco para outra parte, afirmando que não será responsável pelas conseqüências dos riscos, mas sem especificar quem será o responsável por elas. Dessa forma, não se tem responsável definido pelo gerenciamento dos riscos.	Abordagem inexistente.
b) A organização transfere a responsabilidade do gerenciamento das adversidades, mediante a assinatura de acordo formal com uma terceira parte.	Abordagem inexistente.
c) Compensação por Consórcio: Várias unidades compartilham o custo das conseqüências de seus riscos. A idéia por trás e que dificilmente os riscos das várias unidades ocorrerão simultaneamente, distribuindo assim o custo entre os participantes desse modelo.	Abordagem inexistente.
d) Compensação por aposta (hedge): A organização paga uma terceira parte para que assuma as responsabilidades dos eventos. A terceira parte aceita o risco baseando-se na probabilidade de sua ocorrência.	Abordagem inexistente.
e) Mitigação: A organização trabalha para minimizar a probabilidade do risco ser concretizado ou pêra reduzir a conseqüência de seus efeitos.	Iniciativas pontuais de caráter mais técnico.
f) Retenção / Aceitação : A adversidade não é tão custosa ou é improvável de ocorrer, ou ainda a organização assume que os benefícios obtidos aceitando os riscos são grandes.	Abordagem é aplicada algumas vezes, de forma mais intuitiva, sem adesão a um processo de gerenciamento.

4.3.5 Práticas de gerenciamento de riscos de TI adotadas

Quando indagado sobre de que forma a organização poderia sofrer impactos devido a falhas da TI, o respondente destacou a importância de se manter a integridade, confidencialidade e disponibilidade dos dados.

Essa afirmação coincide com os impactos estudados por Westerman e Hunter (2007) nos seus domínio de acurácia, disponibilidade e acesso.

De acordo com a percepção do entrevistado, a infra-estrutura de tecnologia utilizada em sua organização não oferece riscos a agilidade do negócio.

A pesar de não se tratar os riscos de TI de forma metódica, o respondente afirmou que os riscos eventualmente identificados podem ser discutidos com a alta direção, que possui um estrito canal de comunicação com a TI, mas que isso não é um fato regular.

O Quadro abaixo traz o resumo da verificação das práticas de gerenciamento de riscos de TI na organização B.

Quadro 15 - Resumo das práticas de gerenciamento de riscos encontradas na organização Gama

Fonte: dados da pesquisa (2009)

Práticas apontadas por Westerman e Hunter (2007)	**Status na organização**
Contratos com parceiros de negócio especificam cláusulas sobre o acesso e confidencial idade dos dados. Há controle sobre os dados que os parceiros/fornecedores da organização têm acesso.	Não existe formalmente
Existe um termo de compromisso sobre o uso dos dados e existem evidencias de que os funcionários leram entenderam as suas responsabilidades contidas no termo.	Prática existente
Existe o monitoramento das contas de usuários administradores e de duplicidade de usuários.	Prática existente
Existe o controle sobre as permissões de cada usuário. É possível saber quais dados cada usuário tem direito a acessar.	Prática existente
Utiliza-se o controle de acesso de quem acessou o que e quando através de logs ou similares.	Prática existente
É possível produzir um inventario de todas as informações circulantes na organização, bem como classificar essas informações em categorias	Não existe formalmente

Existe um controle de acesso ao Data Center ou estrutura de processamento similar.	Prática existente
Existe controle sobre as mudanças das aplicações. As alterações podem introduzir mudanças indesejadas e não ha como controlá-las.	Prática existente
Existe controle de versionamento dos documentos da organização	Prática existente
Está claro quem pode atualizar quais dados nos sistemas de informação. Conflitos de permissão de alteração são freqüentes.	Prática existente
Existem na organização, planos de contingência para continuidade do negocio.	Não existe formalmente.
O apoio da TI é total na execução das estratégias da empresa. Não há dificuldades na implementação de novos projetos considerando o ambiente atual de TI.	Prática existente

5. ANÁLISE E DISCUSSÃO DOS RESULTADOS

Uma vez apresentada a descrição dos casos sob investigação, passa-se neste capítulo à análise comparativa dos casos. Trata-se da análise das principais similaridades e diferenças encontradas, à luz do que pensam os autores apresentados no Capítulo dois.

5.1 ANÁLISE COMPARATIVA DA CARACTERIZAÇÃO DOS GESTORES E DE SUAS ORGANIZAÇÕES

Os sujeitos ou respondentes possuem formação em computação ou engenharia. Os dados que caracterizam os sujeitos e os objetos da pesquisa estão dispostos no Quadro abaixo:

Quadro 16 - Comparativo da caracterização dos gestores de TI entrevistados na pesquisa

Fonte: dados da pesquisa (2009)

	Organização Alfa	**Organização Beta**	**Organização Gama**
Idade do gestor	28 anos	28 anos	42 anos
Sexo	Masculino	Masculino	Feminino
Formação acadêmica	Ciências da Computação	Ciências da computação	Outras engenharias
Pós Graduação	Engenharia de Software	Engenharia de Software	Não possui
Cargo atual exercido na organização	Gestor de TI	Gestor de TI	Superintendente de TI
Tempo no cargo	1 ano	1 ano	1 ano

Os três gestores são funcionários de carreira do governo. A única discrepância ocorre na organização Gama, que possui o gestor mais experiente em termos de quantidade de anos. Para os dois primeiros casos, os gestores passam por suas primeiras experiências em cargos não-técnicos. Já o gestor da organização Gama possui dez anos de experiência em funções de gerência.

Quanto às características das três organizações estudadas, todas do segmento governo, puderam-se observar diferenças que variaram desde o número de funcionários, quanto a aspectos de infra-estrutura de TI e, até mesmo, em termos de práticas de gestão de TI empregadas. Dessa forma, procurou-se estudar organizações que estivessem em estágios distintos quando considerado o uso da TI.

Quadro 17 - Comparativo da caracterização das organizações objeto da pesquisa

Fonte: dados da pesquisa (2009)

	Organização Alfa	**Organização Beta**	**Organização Gama**
Anos de existência	Menos de 5	5	Mais de 50
Número de funcionários:	60	300	Mais de 2000
Número de funcionários de TI:	4	7	200
Número de estações de trabalho	100	300	Mais de 2000
Outras características	Bom relacionamento com a alta direção; TI participa das ações estratégicas e prioritárias do governo; Unidade de TI não é formalizada e passa por processo de estruturação.	TI é forte no suporte operacional. Unidade de TI é formalizada.	Uso intensivo da TI. Possui planejamento estratégico definido e gestão da qualidade, gestão da segurança da informação. Uso intensivo da TI.

5.2 GOVERNANÇA DE TI

O ITGI decompõe o processo de Governança de TI em cinco subprocessos: Gerenciamento de recursos de TI, Alinhamento Estratégico, Gerenciamento de riscos, Retorno de investimento e Mensuração de performance.

Nas falas do gestor de TI da organização Alfa, percebe-se a presença de dois dos cinco componentes citados pelo ITGI: **Alinhamento estratégico** e **Recursos de TI**. Depreende-se, uma visão fragmentada e reducionista de governança de TI, diversa daquela encontrada na literatura. De forma semelhante, o entrevistado da organização Beta descreveu essencialmente a dimensão do

gerenciamento de serviços de TI, como se reduzisse o conceito de governança de TI para o de gerenciamento de serviços de TI, apenas.

Para deixar clara a diferença entre os conceitos de Governança e de gerenciamento, recorre-se a distinção entre os conceitos feita por Bird apud Webb et al.(2006):

> *[...] Enquanto os executivos e gerentes administram, desenvolvem, implementam e monitoram as estratégias do negócio no cotidiano, comitês e outras estruturas de governança lidam globalmente com as políticas da organização, cultura e direcionamento estratégico. É como se os executivos gerenciassem as organizações com a autoridade delegada por aqueles que a governam.*

Resgatando-se a fala do gestor da organização Gama, pode-se observar também a incompletude do conceito que o gestor entende por Governança de TI. Na transcrição abaixo, aparecem componentes das dimensões "Gerenciamento de serviços de TI", "Gerenciamento dos riscos", "Alinhamento estratégico", mas ainda assim, representa uma visão parcial do conceito quando comparado com aqueles encontrados na literatura: "a idéia é gerir a TI, com vistas a manter seu pleno funcionamento, gerenciando projetos, controlando incidentes e riscos, garantindo a disponibilidade dos sistemas, integridade dos dados e gerenciando mudanças. "

Todos os entrevistados incorreram na mesma insuficiência conceitual em suas definições quando essas são comparadas com aquelas encontradas na literatura, que também variam entre si conforme discutido na seção 2.2.1, especialmente nos estudos do ITGI (2008) e Weill e Ross (2004). Para Webb et al.(2006) essa falta de clareza sobre o conceito de governança de TI não é surpresa:

> *[.....] dado que a disciplina de sistemas de informação é relativamente nova e que emergiu de uma maneira orgânica sobre uma variedade de diferentes disciplinas incluindo, mas certamente não limitada a, ciências sociais e ciências da computação. A ramificação e a diversidade de disciplinas base e a natureza emergente da disciplina, resultou, talvez naturalmente, em muitos termos e conceitos relativos a sistemas de informação, sendo fragilmente definidos e carentes de consenso pelos pesquisadores e praticantes do tema.*

Webb et. al.(2006) procuraram sintetizar uma definição a partir de uma revisão de literatura sobre o tema. Para eles Governança de TI 'é o alinhamento

estratégico entre a TI e o negócio tal que o máximo do valor do negócio é obtido, através do desenvolvimento e manutenção de um controle efetivo, da prestação de contas, gerenciamento de performance e de riscos de TI."

Tal definição também não foi encontrada nas falas dos entrevistados. O receio é que essa deficiência identificada na compreensão sobre o conceito de Governança de TI, apregoado na literatura, tenha impacto nos processos fundamentais da governança de TI, dentre eles o gerenciamento de riscos. Uma vez não percebido como componente essencial dentro do processo de governança, as organizações podem desconsiderar ou não priorizar as práticas de gerenciamento de riscos de TI. Tal hipótese poderia ser examinada em estudos específicos sobre a questão.

Todos os entrevistados reconheceram a importância das práticas de governança de TI. No entanto, quando indagados sobre quais delas implementavam em suas organizações, apenas a organização Gama citou práticas como *service desk*, reuniões de acompanhamento de projeto, implementação do planejamento estratégico.

Os dois outros gestores não relataram ou não souberam opinar. Foram investigadas também as práticas levantadas pelos executivos de TI pesquisados nos trabalhos de Weill e Ross (2004). De acordo com os autores, as práticas levantadas correspondem às ações de maior impacto e que eram implantadas com maior freqüência. Procurou-se investigar o status dessas práticas nas organizações, procurando compreender a aderência da organização às mesmas.

Passando-se a análise das práticas nas organizações, tem-se que a organização Alfa não exerce formalmente nenhuma das práticas consideradas. Vale salientar que, informalmente, algumas decisões de TI são tomadas em conjunto pela TI e Negócio. Outras iniciativas estão em fase de implantação ou figuram entre os anseios do gestor, como por exemplo, TI participando do desenho dos processos, acordos de nível de serviço, criação de portais baseados na web, dentre outros.

A organização Alfa age pró-ativamente na definição de padrões e normas, antecipando-se à necessidade do negócio. A TI da organização Beta trabalha de forma reativa, quanto à definição de padrões. Também não existem estruturas de decisão formalizadas, a comunicação da diretoria sobre suas decisões é deficiente, apesar do uso de intranets e portais.

O cenário encontrado na organização Beta se torna mais preocupante porque não se verificou a intenção de implementar outras práticas de governança no curto prazo. O cenário encontrado na organização Gama apresentou uma maior maturação na implementação de algumas práticas em relação aos outros casos. Foram identificados o monitoramento dos projetos, comunicação da alta diretoria, comitê informal de arquitetura e segurança da informação, dentre outros. Mas ainda nesse caso, as práticas não estão formalizadas.

De uma forma geral, pode-se dizer que as três organizações estudadas aplicam poucos mecanismos de Governança de TI, alguns deles, ainda informalmente, sendo que a minoria são práticas consolidadas. Um retrato preocupante que está em consonância com o relatório do ISACA (2008), realizado em 23 países com mais de 700 respondentes, mostra que a importância dada ao gerenciamento de riscos de TI é maior nas organizações que possuem mais maturidade em termos de governança de TI, conforme pode ser observado na **Figura 13:**

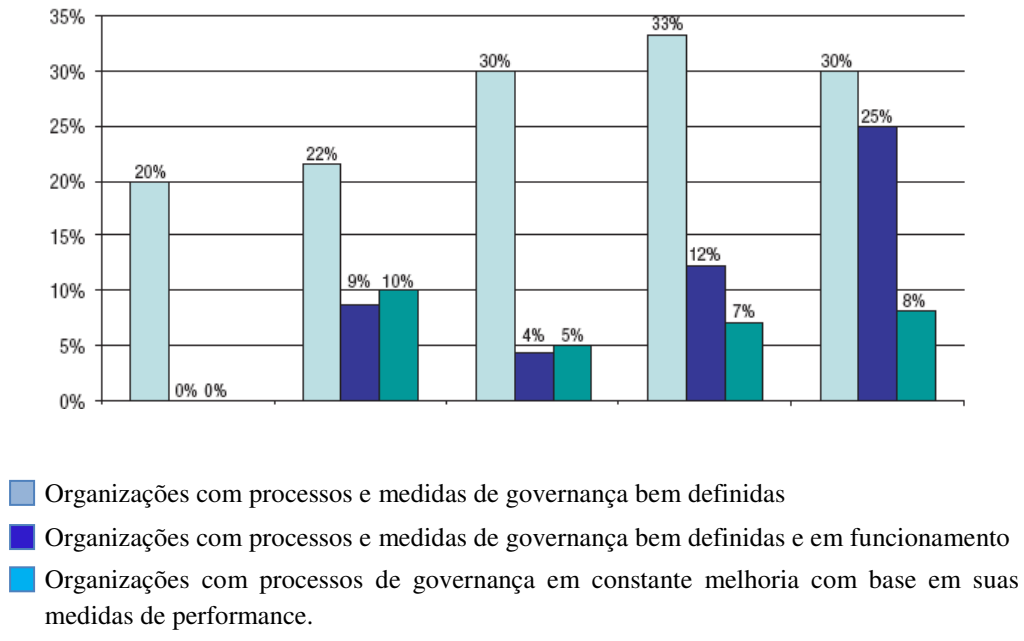

Figura 14 - Cruzamento de dados sobre maturidade de governança em TI e a importância do gerenciamento de riscos de TI
Fonte: (ITGI, 2008)

De acordo com a Figura 17, as organizações que possuem os processos de governança de TI em constante melhoria são também as que dão mais importância ao gerenciamento de riscos de TI. Para as organizações do outro extremo da escala de maturidade, a alternativa à governança é um desordenado conjunto de mecanismos implementados em diferentes momentos, cada um atacando um problema específico e geralmente local.

Esta estrutura é improvável que seja efetiva em focar as práticas de TI nos objetivos estratégicos da organização (WEILL e WOODHAM, 2002).

5.3 CULTURA DE RISCOS

Uma cultura de riscos favorável constrói um ambiente na organização, no qual cada indivíduo, em qualquer nível, é consciente sobre os riscos, discute-os e assume um nível de responsabilidade pessoal em gerenciá-lo (WESTERMAN; HUNTER, 2007). Essa é a característica que se espera encontrar num ambiente organizacional que apóie a execução das práticas de gerenciamento de riscos.

No entanto, os resultados mostraram realidades distintas dessa. No caso da organização Alfa, foi relatado que “normalmente se colocam os riscos debaixo do tapete, pois os riscos são difíceis de tratá-los. A estratégia é deixar que eles se resolvam sozinhos.” Falta de consciência gera pontos fracos na cadeia que forma os ativos de TI bem como pode minimizar a eficiência do processo de gerenciamento de riscos (WESTERMAN e HUNTER, 2007).

De maneira semelhante, na organização Beta o andamento dos processos ocorre de forma que “as pessoas vão fazendo e a coisa vai acontecendo [...] sem se preocupar com a questão dos riscos”. Ainda segundo o gestor da organização Beta, “as pessoas não tem até mesmo conhecimento para falar de riscos”, caracterizando o que Westerman e Hunter (2007) chamam de cultura avessa ao risco. Por fim, a organização Gama sustenta que “as pessoas não conversam ou não são encorajadas a discutir sobre riscos, de uma forma geral.”

Não existe a cultura de riscos disseminada, não há o conhecimento sobre a temática. Sem consciência, a organização não pode evitar os riscos, apenas sofrer suas conseqüências (WESTERMAN e HUNTER, 2007).

Os pressupostos de consciência, conhecimento e confiança não foram confirmados para nenhum dos casos. A quase totalidade das práticas que propiciam o surgimento de uma cultura de riscos favorável também não foi identificada nas três organizações, conforme pode ser visto nos Quadros 4,8 e 11, relativos aos casos Alfa, Beta e Gama, respectivamente. O Quadro 17 traz o resumo do diagnóstico das abordagens de tratamento de riscos nos três casos estudados.

Quadro 18 - Principais práticas de Governança de TI e seus objetivos

Fonte: dados da pesquisa (2009)

Práticas que favorecem a cultura de riscos favorável	**Status na organização**		
	Alfa	Beta	Gama
Propriedade intelectual e expertise	Apenas em projeto.	Não existe.	Não existe.
Consulta a especialistas internos	Ocorre com freqüência.	Não existe.	Existe.
Pensar em riscos antes de decisões.	Não existe.	Não existe.	Não existe.
Metodologia de gerenciamento da qualidade	Não existe	Não existe.	Existe
Encorajamento ao empreendedorismo	Não existe.	Não existe.	Não existe
Responsabilidade por ações e resultados.	Não existe.	Não existe.	Não existe
Documentação das vulnerabilidades da TI	Não existe.	Não existe.	Não existe
Documentação dos incidentes e respostas, recuperação:	Não existe.	Não existe.	Não existe
Documentação de perdas relativas a incidentes	Não existe.	Não existe.	Não existe
Documentação do Desempenho das medidas, tempo, esforços envidados.	Não existe	Não existe.	Não existe

O Quadro 18 mostra uma realidade preocupante, já que “a conscientização sobre riscos é essencial, uma vez que até mesmo os melhores processos podem falhar se eles forem definidos num ambiente de pessoas desinformadas ao passo que encorajam uma cultura na qual o risco é discutido e gerenciado abertamente.” (WESTERMAN e HUNTER, 2007).

Sem uma cultura de gerenciamento de riscos construída, a organização não consegue consolidar uma visão holística sobre os riscos, desde o seu nível operacional, tático até o estratégico, pois os indivíduos não estão preparados para discutir ou conversar sobre o tema.

Esses comportamentos desejáveis não foram identificados nas organizações estudadas, o que pode se traduzir para aquelas em perdas diretas e indiretas. Como exemplo, um dos grandes benefícios ao se gerenciar riscos de TI é a melhora na capacidade de se prover a infra-estrutura para dar suporte ao crescimento da organização e às mudanças nas estratégias do negócio, o que não foi evidenciado em um projeto específico da organização Gama.

5.4 ABORDAGENS DE TRATAMENTO DOS RISCOS

Neste quesito, procurou-se verificar a existência de um processo de gerenciamento de riscos de TI, tomando-se como referência os modelos discutidos em AUSTRALIA(2004), Bandyopadhyay et al.(1999) e Tsohou et al.(2006). Identificaram-se as semelhanças entre os modelos e partiu-se para a verificação das fases de identificação, análise, avaliação, tratamento e monitoramento nos casos.

No caso da organização Alfa, o entrevistado citou que em sua visão, o processo deveria conter etapas de identificação, análise quantitativa e/ou qualitativa do risco e seu impacto, bem como de sua probabilidade de ocorrência.

No entanto, essas etapas são realizadas de forma independente e não ocorre regularmente. O gestor ressaltou que “não sobra muito tempo para fazer gerenciamento de riscos” na organização. Os gestores das organizações Beta e Gama afirmaram também conhecer o processo de gerenciamento de riscos delineado sem, no entanto aplicá-lo.

Quanto às abordagens de tratamento possíveis citadas por Blakley et al. (2001), foram identificados três tipos utilizados pontualmente em alguns projetos: Transferência de responsabilidade sem definição de responsável formal, aceitação dos riscos e mitigação. Quando a mitigação ocorre, é realizada sem as fases prévias de identificação de riscos, análise e avaliação e tem como base a experiência dos gestores com ocorrências anteriores de incidentes, resumindo-se

basicamente a mitigar questões técnicas como atualização de antivírus, substituição de equipamentos antigos, dentre outros.

A aceitação também não é antecedida de fases formais de um processo de gerenciamento de riscos, sendo, de certa forma o caminho natural e intuitivo para o tratamento dos riscos.

Quadro 19 - Principais abordagens de tratamento de riscos de TI encontradas

Fonte: dados da pesquisa (2009)

Abordagem (BLAKLEY et al. , 2001)	**Status na organização de acordo com o gestor de TI**		
	Alfa	Beta	Gama
a) A organização pode transferir o risco para outra parte, afirmando que não será responsável pelas conseqüências dos riscos, mas sem especificar quem será o responsável por elas. Dessa forma, não se tem responsável definido pelo gerenciamento dos riscos.	Abordagem inexistente.	Abordagem inexistente.	Abordagem inexistente.
b) A organização transfere a responsabilidade do gerenciamento das adversidades, mediante a assinatura de acordo formal com uma terceira parte.	Abordagem inexistente.	Abordagem inexistente.	Abordagem inexistente.
c) Compensação por Consórcio:	Abordagem inexistente.	Abordagem inexistente.	Abordagem inexistente.
d) Compensação por aposta (hedge):	Abordagem inexistente.	Abordagem inexistente.	Abordagem inexistente.
e) Mitigação:	Mitigação dos riscos de segurança da informação como anti-vírus, firewall, backups, ainda em fase de projeto.	Iniciativas pontuais de caráter mais técnico como substituição de máquinas, uso de softwares anti-vírus etc.	Iniciativas pontuais de caráter mais técnico de segurança da informação.
f) Retenção / Aceitação : A adversidade não é tão custosa ou é improvável de ocorrer, ou ainda a organização assume que os benefícios obtidos aceitando os riscos são grandes.	A aceitação pode ocorrer de maneira inconsciente.	Abordagem é aplicada informal e inconscientemente, na medida em que não se discute os riscos.	Abordagem é aplicada algumas vezes, de forma mais intuitiva, sem adesão a um processo de gerenciamento.

Em suma, as abordagens em utilização ainda são incipientes, corroborando as palavras de Bandhyopadyay et al.(1999), Chang e Ho (2006), Dhillon e Backhouse (2000) Von Solms (2004), Westerman e Hunter (2007), quando afirmam

que “as organizações se preocupam principalmente com os riscos mais técnicos, focando seus esforços para dentro do “silo da TI ”.

5.5 GERENCIAMENTO DOS RISCOS DE TI E PRÁTICAS IMPLANTADAS

Neste item, procurou-se identificar que dimensões da organização poderiam ser afetadas em caso de eventuais falhas da TI, se os riscos eram considerados nas decisões da alta diretoria. Verificou-se ainda a metodologia de gerenciamento de riscos utilizada e a adesão às práticas apontadas por Westerman e Hunter (2007).

O gestor de TI Alfa relatou que “a imagem da secretaria seria afetada e é o mais importante”. Citou ainda que “as atividades operacionais seriam atingidas. Sem internet, infra-estrutura de TI ninguém trabalha”. Riscos de precisão e acesso também foram citados como preocupação para esse gestor. O gestor Beta corrobora os prejuízos para a imagem de sua organização, caso a TI falhe, corrobora os riscos de agilidade que a TI pode causar, mas não cita riscos como o de acurácia e acesso.

Finalmente, o gestor Gama destacou a importância de se manter a integridade, confidencialidade e disponibilidade dos dados. Segundo ele, a TI pode impactar também na agilidade das mudanças de processos do negócio.

Todos são unânimes em afirmar que a TI está intrinsecamente ligada às atividades de suas organizações e parecem perceber as dimensões de riscos mapeadas por Westerman e Hunter (2007) e Chatzoglou et al.(2009), “sem no entanto implementar efetivamente um processo de gerenciamento de riscos de TI, reduzindo-o a riscos eventualmente identificados em reuniões, que variam de acordo com o canal de comunicação estabelecido com a alta direção. Todas são iniciativas informais, não fazendo parte dos processos consolidados na organização.”

A direção da organização Alfa começa a pensar riscos de TI em seu nível estratégico, assim como algumas questões chegam à diretoria das organizações Beta e Gama. No entanto, falta para essas organizações, à luz das proposições dos (BANDYOPADHYAY et al, 1999; SOLMS, 2001; WESTERMAN, 2004), “a adoção

de um processo efetivo de gerenciamento de riscos integrado ao processo de decisões estratégicas para que essas mesmas organizações possam extrair os benefícios esperados, minimizando eventuais perdas."

Com relação às práticas de gerenciamento de riscos de TI adotadas, observaram-se três cenários distintos. O primeiro deles é o da organização Alfa, no qual a maioria das práticas inexiste, apesar de haver a intenção de adotá-las. Vale ressaltar que a referida organização passa por um estágio de estruturação de seus processos, inclusive os de TI. Com o maior número de práticas identificadas, encontra-se a organização Gama, indicando os esforços que a TI da organização envida para a questão do gerenciamento de riscos de TI nas dimensões precisão, disponibilidade e acesso.

O Quadro 20 apresenta o resumo das práticas de gerenciamento de riscos de TI apontadas por Westerman e Hunter (2007) identificadas neste trabalho.

Quadro 20 - Principais práticas de gerenciamento de riscos de TI nas três organizações

Fonte: dados da pesquisa (2009)

Práticas apontadas por Westerman e Hunter (2007)	**Status na organização**		
	Alfa	Beta	Gama
Contratos com parceiros de negócio especificam cláusulas sobre o acesso e confidencial idade dos dados. Há controle sobre os dados que os parceiros/fornecedores da organização têm acesso.	Cláusulas e contratos existem mas não há o controle sobre aqueles.	Não existente.	Não existe formalmente
Existe um termo de compromisso sobre o uso dos dados e existem evidencias de que os funcionários leram entenderam as suas responsabilidades contidas no termo.	Apenas a intenção de fazê-la.	Em elaboração.	Prática existente
Existe o monitoramento das contas de usuários administradores e de duplicidade de usuários.	Não existente. Em fase de projeto.	Prática existente	Prática existente
Existe o controle sobre as permissões de cada usuário. É possível saber quais dados cada usuário tem direito a acessar.	Não existente. Em fase de projeto.	Prática existente.	Prática existente
Utiliza-se o controle de acesso de quem acessou o que e quando através de Logs ou similares.	Não existente. Em fase de projeto.	Prática existente	Prática existente
É possível produzir um inventario de todas as informações circulantes na organização, bem como classificar essas informações em categorias	Não existente.	Não existente	Não existe formalmente
Existe um controle de acesso ao Data Center ou estrutura de processamento	Não existente. Em fase de projeto.	Não existente.	Prática existente

similar.			
Existe controle sobre as mudanças das aplicações. As alterações podem introduzir mudanças indesejadas e não há como controlá-las.	Apenas a intenção de fazê-lo.	Apenas a intenção.	Prática existente
Existe controle de versionamento dos documentos da organização	Em fase de projeto.	Não existente.	Prática existente
Está claro quem pode atualizar quais dados nos sistemas de informação. Conflitos de permissão de alteração são freqüentes.	Não existente.	Não existente. Apenas a intenção.	Prática existente
Existem na organização, planos de contingência para continuidade do negocio.	Não existente.	Não existente.	Não existe formalmente.
O apoio da TI é total na execução das estratégias da empresa. Não há dificuldades na implementação de novos projetos considerando o ambiente atual de TI.	Existem dificuldades da TI em suportar o negocio.	A TI enfrenta dificuldades em suportar o negócio, principalmente devido a falta de recursos humanos.	A TI, em termos de infra-estrutura está preparada para suportar o negócio. A TI oferece riscos a agilidade do negócio da organização.

Uma consideração sobre os achados, corroborada com o estudo de Tsohou et al (2006), “é que o número de práticas de gerenciamento de risco é baseado na forma com que os vários *stakeholders* percebem os riscos associados com os ativos de TI,” o que de certa forma foi retratado no Quadro 19.

A percepção de riscos por parte dos gestores de TI existe, conforme pode ser observado no Quadro 20 e nas falas dos respondentes. Parece faltar um mecanismo de comunicação efetivo dessa percepção para os demais envolvidos na organização, para que seja adotado um processo de gerenciamento formal de riscos de TI, no qual as decisões sobre riscos de TI sejam levadas em consideração no nível estratégico do negócio.

6 CONSIDERAÇÕES FINAIS

A dependência da TI nas organizações em todos os seus níveis cresceu a ponto de ser impensável uma realidade sem a qual a TI não suporte a maioria de seus processos. Essa dependência trouxe consigo alguns riscos que precisam ser gerenciados em caso de falha da TI, seja no suporte aos antigos ou na criação de novos processos de negócio. Esta pesquisa teve como objetivo investigar como as organizações gerenciam esses riscos decorrentes do uso da TI e que afetam os seus negócios.

Para tanto, foram realizados três estudos de caso em organizações públicas do governo do Estado de Pernambuco, nas quais este estudo foi replicado, analisado, no Capítulo 4, e comparado no Capítulo 5.

Diante do cenário corroborado por diversos autores Bandhyopadyay et al. (1999), Chang e Ho (2006), Dhillon e Backhouse (2000), Solms (2004), Westerman e Hunter (2007), “no qual o gerenciamento de riscos de TI é reduzido à implementação de práticas de segurança da informação,” quando requer espaço nas mesas de decisões estratégicas, torna-se necessário conhecer como esse fenômeno se apresenta nas organizações brasileiras.

Até o momento da conclusão deste trabalho, essas organizações não havia sido investigadas do ponto de vista dessa temática. Daí a necessidade de um estudo de caráter descritivo/exploratório que trouxesse as primeiras amostras do fenômeno para discussão acadêmica.

Além do objetivo geral, foram elencados alguns objetivos específicos que passam a ser discutidos. O primeiro deles tratou da caracterização dos gestores de TI, descrita em detalhes no Capítulo 5. De uma forma geral, os perfis apresentaram uniformidade, variando basicamente em termos de tempo de experiência profissional. Já as organizações, todas da esfera pública estadual, possuíam práticas de TI que variaram bastante entre si. Houve um caso em que a TI sequer aparecia no organograma da organização; em alguns casos havia déficit de recursos humanos de TI; práticas de gerenciamento de projeto eram implementadas, alguns possuíam unidades dentro da TI com funções específicas

como gestão da qualidade e segurança da informação, parques computacionais distintos em número, bem como volume de investimentos diversos.

O segundo objetivo se destinou a conhecer as práticas de governança de TI exercidas pelas organizações. Primeiramente, foi identificada uma visão parcial sobre o conceito de governança de TI considerando a literatura correlata. O receio é que essa deficiência, identificada na compreensão do significado diferente daquele apregoado na literatura, tenha impacto nos processos fundamentais da governança de TI (LAINHAT, 2001), dentre eles o gerenciamento de riscos. Quanto às práticas propriamente ditas, pode-se dizer que as três organizações estudadas aplicam poucos mecanismos de Governança de TI, alguns deles, ainda informalmente, sendo que a minoria corresponde a práticas consolidadas. Apesar disso, todos os entrevistados reconheceram a importância das práticas de governança de TI como forma de maximizar o uso da TI na organização.

No que tange à cultura de riscos, as organizações apresentam o que Westerman e Hunter (2007) chamam de cultura de aversão ao risco, um ambiente no qual as pessoas não tem conhecimento, consciência ou abertura para discutir sobre riscos. Nos ambientes analisados foram comuns frases do tipo: “as pessoas vão fazendo e a coisa vai acontecendo [...] “sem se preocupar com a questão dos riscos” ou “normalmente se colocam os riscos debaixo do tapete”. Diante do exposto, pode-se afirmar que a disciplina “cultura de riscos” estudada por Westerman e Hunter (2007), encontra-se em estágio incipiente nas organizações estudadas, assim como demonstra também o Quadro 17.

Os resultados decorrentes do terceiro objetivo permitem reportar que em nenhum dos casos investigados foi identificado um processo formal de gerenciamento de riscos de TI, apesar de se ter algumas iniciativas pontuais que aplicaram parte do processo considerado em Austrália (1999), Bandyopadhyay et al.(1999) e Tsohou et al.(2006). Ademais, das cinco abordagens possíveis para a fase de tratamento de riscos de acordo com Blakley et al. (2001), apenas a retenção ou aceitação do risco foi identificada, ainda assim, ocorrendo independente do fluxo delineado na Figura 6.

É importante destacar a gravidade que representa a ausência de mecanismos de gerenciamento de riscos de TI, especialmente em se tratando do contexto governamental, no qual o volume de recursos financeiros é alto e as informações

são de interesse coletivo. Essa questão deve ser levada à debate pelos agentes públicos.

Finalmente, o último objetivo procurou conhecer as práticas de gerenciamento de riscos de TI apontadas por Westerman e Hunter (2007) em uso nos casos estudados. O que pôde se constatar foi a aplicação de grande parte das práticas recomendadas pelo autor, ou ainda a intenção de fazê-lo, especialmente na organização Alfa. Todas as práticas eram voltadas para os riscos que afetam as dimensões precisão, acesso e disponibilidade. Para gerenciar a dimensão "agilidade", a TI precisa envolver mais o negócio, sendo o primeiro passo, o estabelecimento de um processo efetivo de comunicação dos riscos.

Considerando a pergunta central da pesquisa, pode-se concluir que as organizações não possuem metodologias de gerenciamento de riscos de TI formalmente definidas nem executadas.

No entanto, exercem a maior parte das práticas indicadas pela referência central da pesquisa, sem alinhamento com os processos de gerenciamento de riscos. Pode-se colocar em dúvida a eficácia dessas atividades em gerenciar os riscos que podem impactar na organização, uma vez que eles representam a visão da TI sobre os riscos existentes

6.1 LIMITAÇÕES DO ESTUDO

Como em qualquer esforço de pesquisa, há limitações e preocupações a serem consideradas a respeito das conclusões alcançadas pela pesquisa. Para uma melhor compreensão, as limitações foram divididas em dois tipos, que seguem descritos.

6.1.1 Limitações conceituais

Um fator limitante inicial é a impossibilidade de serem traçadas generalizações para outros contextos dada a natureza do estudo, permitindo apenas sustentar as conclusões e evidências para os casos estudados. Soma-se a esse fato a escassa quantidade de referências de estudos correlatos encontrados

que dificultam a comparação ou mesmo o apoio na análise dos casos estudados bem como na construção do referencial teórico.

6.1.2 Limitações operacionais

A escolha dos sujeitos da pesquisa se deu com base no critério de acessibilidade do autor para com os respondentes. Como porta-vozes de suas respectivas organizações, estas pessoas tinham a responsabilidade de preservar a imagem da organização, isto é, descrevê-la de forma a evidenciar seus pontos positivos e, assim, cuidar da imagem da empresa, do setor ao qual pertencem e de si próprias. Em adição, a temática de riscos pode ter causado inibição aos respondentes no sentido de não revelarem as fragilidades existentes em suas organizações. Aliado a esse fato, o pesquisador e a natureza de seu vínculo com as organizações estudadas pode ter limitado a franqueza das respostas dos sujeitos da pesquisa, uma vez que em tese, os sujeitos do estudo devem seguir as orientações da agência que coordena a execução da política de TI que deve ser seguida pelas organizações pesquisadas. Em outras palavras, os sujeitos podem ter sido intimidados ou influenciados em suas respostas, dada a representatividade do órgão regulador na pessoa do pesquisador.

A pesquisa ganharia significativamente em representatividade caso fosse realizada também sob a perspectiva dos gerentes de negócio, o que possibilitaria a análise das eventuais percepções de riscos de TI sobre o negócio, sob o prisma do negócio. No entanto, esse caminho se demonstrou inviável, dada a dificuldade de acesso aos gestores do negócio nas organizações pesquisadas.

6. 2 RECOMENDAÇÕES AOS GESTORES DE TI

As organizações do estudo, à luz do referencial teórico pesquisado, precisam implantar um efetivo gerenciamento de riscos de TI. De acordo com Westerman(2007), são três as disciplinas fundamentais para a construção de um processo como esse: infra-estrutura de TI, governança de riscos de TI e cultura de riscos favorável.

Como sugestão para os contextos pesquisados, os gestores de TI precisam comunicar efetivamente o negócio da existência e da importância do gerenciamento dos riscos de TI, buscando sensibilizá-los para a questão, favorecendo assim o surgimento de uma cultura de riscos dentro da organização. O próximo passo será a composição de um comitê para discutir os riscos e deliberar sobre o processo de gerenciamento de riscos de TI adotado. A composição dos modelos de Bandhyopadhyay et al.(1999) e Westerman(2004) podem servir de base para esse fim. Finalmente, com o processo de gerenciamento de riscos de TI definido e implantado, o resultado será a implementação de ações preventivas e corretivas que certamente minimizarão ou evitarão os impactos de falhas ou mau uso da TI.

6.3 Recomendações para trabalhos futuros

Pode-se elencar algumas possibilidades de trabalhos futuros. A primeira delas seria investigar de que forma a governança de TI pode colaborar na maturidade do gerenciamento estratégico de riscos de TI, uma vez que as estruturas de decisão e de comunicação, típicas práticas de governança, podem ser utilizadas no gerenciamento dos riscos de TI, facilitando a construção de uma visão holística e compartilhada desses riscos. É necessário compreender também por que organizações como as ora estudadas a pesar de ter seus gestores de TI conscientizados sobre as dimensões possíveis de serem impactadas, não conseguem implementar um processo de gerenciamento de riscos de TI que envolva o negócio à mesa de discussão. Aprofundando-se nesse tópico, pode-se investigar de que forma o modelo centralizador e coordenador de políticas de TI adotado no Estado impacta na implementação das políticas de gerenciamento de riscos de TI em cada uma das organizações estudadas. Em outras palavras, cabe perguntar se as organizações estudadas não deliberaram suas políticas próprias de gerenciamento de riscos de TI por entenderem não ser seu papel, em consonância com o que prega o SEIG, ou seja, as organizações estudadas vêem na ATI a entidade deliberativa sobre a questão. Qual será a realidade em organizações com modelos de gestão de TI diversos do aqui tratado?

Pode-se investigar que fatores organizacionais inibem ou facilitam o estabelecimento de uma cultura de riscos de TI favorável.

Por todo o exposto, o tema gerenciamento de riscos de TI necessita de um número maior de estudos, para que se possa construir o panorama atual sobre o tema, permitindo assim definir diretrizes de pesquisas mais específicas. Pesquisas de natureza quantitativa que pudessem inferir parâmetros de uma população maior têm no gerenciamento de riscos de TI, um campo novo a ser explorado.

REFERÊNCIAS BIBLIOGRÁFICAS

ABRAB, A., Buglione, *L. A* multidimensional performance model for consolidating *Balanced Scorecards*. **Advances in Engineering Software**, v. 34, p. 339-349 ,2003.

ALVARES, Elismar e LANK, Alde G. **Governando a Empresa Familiar**. Ed. Qualitymark: Belo Horizonte, MG. Fundação Dom Cabral, 2003.

ANDERSON**,** Evan e CHOOBINEH**,** Joobin**.** Enterprise information security strategies. **Computers & Security**. v. 30, p. 1-8, 2008.

ARNAUD, Victor Gonçalves; Melo. **Governança de Tecnologia da Informação**: em busca do alinhamento com a estratégia da organização. Rio de Janeiro, 2007.165p. Dissertação (Mestrado) – Departamento de Engenharia Industrial, Pontifícia Universidade Católica do Rio de Janeiro. 2007.

ARRUDA, Péricles Alves Ferreira. **Governança de Tecnologia da Informação para micro e pequenas empresas**: estudo de caso na cidade de Fortaleza. Fortaleza, 2006. 129p. Dissertação (Mestrado) – Mestrado em informática aplicada, Universidade de Fortaleza. 2006.

AUSTRALIA, Risk Management. AUSTRALIA STANDARDS 4360. 2004. Disponível em http://www.cqurire.com/htm/paper/risk/Aust_Standards_4360-2004.pdf Acesso em 20 jan 2009.

BANDYOPADHYAY K.; MYKYTYN P. P. e MYKYTYN, K. A framework for integrated risk management in information technology. **Management Decision**, v. 37, p. 437-445, 1999.

BARDIN, L. (1977). **Análise de Conteúdo**. Lisboa, Portugal: Edições 70. Hair, J.F.;

BLAKLEY, B; MCDERMOTT, E.; GEER, D. Information Security is Information risk Management. In: XXX WORKSHOP ON NEW SECURITY PARADIGMS, 2002, New Mexico. **Proceedings**.. New Mexico: ACM, 2002.

BRASIL. **Decreto nº 3.555, de 8 de agosto de 2000.** Aprova o Regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.. Disponível em <http://www.planalto.gov.br/ccivil_03/Decreto/D3555.htm> Acesso em 10 mai 2009.

BRASIL. MINISTÉRIO DA PREVIDÊNCIA SOCIAL. Previdência Social e o Gerenciamento de Riscos. 2002.Disponível em < http://www.previdenciasocial.gov.br/arquivos/office/3_081014-104627-289.pdf> Acesso em 23 out 2008.

CAMELO, S. B. **Governança corporativa, processo sucessório e estratégia competitiva**: associações com o desempenho de grandes empresas no Brasil. Recife, 2007. Dissertação (Mestrado) Mestrado em Administração, Faculdade Boa Viagem. 2007.

CARR, N.G. **IT doesn't matter**. Harvard Business Review, v. 81, n. 5, p.41-49, 2003.

CERT. Estatísticas dos Incidentes Reportados ao CERT.br 2009. Disponível em http://www.cert.br/stats/incidentes/ Acesso em 10 maio 2009.

CHANG , Shuchih Ernest; HO, Chienta Bruce. Organizational factors to the effectiveness of implementing information security management. **Industrial Management & Data Systems**, 2006, p. 345-361.

CHATZOGLOU , P. d e DIAMANTIDIS, A. D. IT/IS implementation risks and their impact on firm performance. **International Journal of Information Management** v. 29, p.119–128. 2009.

CSI/FBI (2004), 2004 CSI/FBI Computer Crime and Security Survey. Computer Security Institute, San Francisco, CA, Disponível em <www.gocsi.com>

DENCKER, A. de F. m. **Pesquisa em Turismo:** Planejamento, métodos e técnicas. São Paulo: Futura, 2007.

DHILLON, G.,; Backhouse, J. Risks in the use of information technology within organization. **International Journal of Information Management,** v. 10, p. 65–74.1996.

ESTADOS UNIDOS. Sarbanes-Oxley Act of 2002. Disponível em <http://news.findlaw.com/cnn/docs/gwbush/sarbanesoxley072302.pdf>

HARDY, Gary. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges, **Information Security Technical Report**, v. 11, n, 1, p. 55-61, 2006.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 3. ed. São Paulo: Atlas, 1991.

GOTTFRIED, I.S. When disaster strikes, **Journal of Information Systems Management**, p.86-9. 1989.

GURGEL, Giovane Montine Moreira. **A Gestão da informação sob a luz do Enterprise Content Management (ECM)***:* Um estudo de caso em uma universidade pública. Natal, 2008.110p. Dissertação (Mestrado) – Programa de Pós Graduação em Administração, Universidade Federal do Rio Grande do Norte. 2008.

HALLIDAY, Sharon; BADENHORST, Karin e Solms, Rossouw. A business approach to effective information technology risk analysis and management **Information Management & Computer Security**. V. 4, p.19-31, 1996.

HENDERSON, J. e VENKATRAMAN. N. Strategic alignment: Leveraging information technology for transforming organizations. **IBM systems journal.** v**.** 32, 1993.

Instituto Brasileiro de Governança Corporativa,Relatório Anual, 2008. Disponível em <http://www.ibgc.org.br/RelatoriosAnuais.aspx⊥ > Acesso em 10 jun 2009.

ITGI, IT Governance Global Status Report,2008. Disponível em < http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=50272&TEMPLATE=/ContentManagement/ContentDisplay.cfm> Acesso em 20 nov 2008.

Office for Government Commerce. ITIL. Information Technology Infrastructure Library. 2007. Disponível em <http://www.itil-officialsite.com/home/home.asp> Acesso em 10 jan 2009.

JANDER, M. , STURM , R. e MORRIS , W. **Service Level Management - Fundamentos Do Gerenciamento De Níveis De Serviço.** São Paulo: Campus, 2000.

JURISON, J.Toward more effective management of information technology. **Journal of Strategic Information Systems. v.**5, p. 263-274. , 1996.

KANG, H., Bradley, G. Measuring the performance of IT services: An assessment of SERVQUAL. **International Journal of Accounting Information Systems.** v. 3 p. 151–164, 2002.

LAINHAT, J. W. COBIT as a Risk Manager framework. ITGI. Disponível em <HTTP:// *strategic.tistory.com/attachment/48e1b2d1e8db278.ppt* >

LUFTMAN, J. Assessing Business-IT alignment Maturity. Communications of Association for Information Systems. 2000.

LUFTMAN, Jerry. Assessing Business-IT Alignment Maturity. **Communications of the Association for Information Systems**. v.4, p.1-50. 2000.

MCFADZEAN, E.; EZINGEARD, J. e BIRCHALL, D. Perception of risk and the strategic impact of existing IT on information security strategy at board level. **Online Information Review.** v. 31, n. 5, 2007

MECKLING, William H.; JENSEN, Michael C..Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. **The Journal Of Financial Economics**, 1976.

Organization for Economic Co-Operation and Development .**Principles of Corporate Governance**, Paris, 2004 .

OLIVEIRA, Jayr Figueiredo. **Sistemas de Informação versus Tecnologias da Informação**: um impasse empresarial. São Paulo: Érica, 2004, 1. ed.

PADOVEZE, C. L. BERTOLUCCI, R. G. Proposta de um modelo para o gerenciamento do risco corporativo. XXV ENCONTRO NACIONAL DE ENGENHARIA DE PRODUÇÃO. 2005. **Anais..**

PERNAMBUCO. Diagnóstico de TI do Estado. 2008

PESLAK, A. R. Organizational information systems: Rate of return and influencing variables as viewed by top financial executives. **Industrial Management & Data Systems** v. 108, p. 43-59 , 2008.

REZENDE, D. A. **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.

RICHARDSON, Roberto Jarry. **Pesquisa Social**: Métodos e Técnicas. 3. ed. São Paulo. Atlas, 1999.

ROSSI, Ruth Ferreira Roque. **Modelo de governança de TI para organizações brasileiras**. 2004. Florianópolis, 1 v. Tese (Doutorado) - Centro Tecnológico. Programa de Pós-Graduação em Engenharia de Produção, Universidade Federal de Santa Catarina. 2004.

SILVIUS, G. A. J. (2007). Business and IT alignment in theory and practice. HAWAII INTERNATIONAL CONFERENCE ON SYSTEMS SCIENCES, 40., 2007. Hawaii. **Proceedings**… Hawaii, 2007.

SOLMS, B. V. Corporate governance and information security, **Computers & Security**, v. 20 No. 3, pp. 215-228.2001.

TRIVIÑOS, Augusto Nibaldo Silva. **Introdução à pesquisa em ciências sociais**: a pesquisa qualitativa em educação. São Paulo: Atlas, 2008.

TSOHOU, A., KARYDA, M., KOKOLAKIS, S. e KIOUNTOUZIS, E. Formulating information systems risk management strategies through cultural theory. **Information Management & Computer Security** v. 14, n. 3, p. 198-217, 2006.

WEILL, P. e WOODHAM, R. **Don't Just Lead, Govern:** Implementing Effective IT Governance Sloan School f Management. Massachusetts Institute of Technology. Disponível em <http://web.mit.edu/cisr/working%20papers/cisrwp341.pdf>. Acesso em 10 mai. 2009.

WEILL, Peter; ROSS, Jeane. **IT Governance: How top performers manage IT decision rights for superior results**. 1. ed.Boston:Harvard Business School Press, 2004.

WESTERMAN, G. **Understanding the enterprise's IT risk profile**. Center for Information Systems Research - Massachusetts Institute of Technology. v. 4, 2004.

Disponível em http://web.mit.edu/cisr/working%20papers/cisrwp351.pdf Acesso em 15 jul 2008.

WESTERMAN, G., HUNTER R. . **IT Risk**: Turning business threats into competitive advantage. Boston: Havard Business School Press, 2007.

YIN, Robert K. **Estudo de caso**: planejamento e métodos. 3. ed. Porto Alegre: Bookman, 2005.

APÊNDICE A - CARTA DE APRESENTAÇÃO

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS DA ADMINISTRAÇAO

Recife, ____ de Junho de 2009.

Dissertação de Mestrado: ASPECTOS DO **GERENCIAMENTO DE RISCOS DE TI NAS EMPRESAS: Estudo de casos múltiplos**

Aluno: Alixandre Thiago Ferreira de Santana

Prezado (a) Gestor (a),

Sou aluno do Programa de Pós-Graduação em Ciências da Administração da Universidade Federal do Rio Grande do Norte.

A minha dissertação de mestrado está relacionada com o estudo do gerenciamento dos riscos de TI que tem impacto no negócio das organizações e está sendo realizada sob a orientação do Professor Doutor Manoel Veras de Souza Neto

A presente proposta de Estudo de caso, vem requisitar a participação do colega GESTOR de TI e tem apenas como objetivo recolher dados para fundamentar a pesquisa no referido estudo.

Sua participação é fundamental para esta pesquisa, pois a partir dela, poderão ser validadas algumas hipóteses acerca do gerenciamento dos riscos de TI nas organizações.

Os dados fornecidos serão confidenciais e destinam-se apenas a fins acadêmicos.

Alixandre Thiago F de Santana

Mestrando em Administração

APÊNDICE B - ROTEIRO DE ENTREVISTA SEMI-ESTRUTURADA

QUESTÕES DO ESTUDO DE CASO

- Idade
- Sexo
- Formação acadêmica:
- Pós Graduação
- Cargo atual exercido na organização ou último cargo ocupado
- Tempo no cargo
- Número de funcionários da organização:
- Número de funcionários de TI na organização:

I – Governança de TI

Hipótese1: A presença de instrumentos de governança favorece a adoção de práticas de gerenciamento de riscos de TI.

- Definir conceito de governança de TI no entendimento do entrevistado
- Definir grau de importância das práticas de governança de TI para o entrevistado
- Identificar práticas de governança implantadas e apontadas pelo entrevistado
- Fazer checklist das práticas abaixo:

a) Comitê, ou estrutura semelhante, dedicado a tomar decisões de TI, na totalidade ou subconjunto delas, com ou sem participação de membros da TI (monarquia, duopólio, federalismo), de acordo com o modelo decisório sobre TI.
b) Existe um comitê ou estrutura semelhante que cuida da arquitetura de TI (padronização, normas, diretrizes para os projetos etc) da organização.
c) Preocupação com o relacionamento entre as decisões do Negócio e da TI. Um ou mais profissionais são responsáveis por esse relacionamento (CIO, geralmente).
d) Existe equipe que cuida dos processos da Organização juntamente com membros da TI.

e) Comitê de aprovação de investimento *f) Acordos de nível de serviço* *g)Monitoramento do andamento dos projetos e dos recursos (pessoas, dinheiro etc.) consumidos.* *h)Monitoramento do valor da TI nos projetos*
i) Comunicações da alta diretoria *l) Portais baseados na Web e intranets para a TI.*

II – Cultura de Riscos

H2: Cultura de riscos estimula a aplicação de práticas de gerenciamento de riscos de TI

- Identificar como as pessoas reagem/encaram os riscos
- Identificar existência de **consciência, confiança e conhecimento** para discutir sobre riscos enfrentados pela organização.
- Identificar qual o comportamento da organização ao se pedir prorrogação de um projeto, alegando-se risco no mesmo.
- Fazer checklist das práticas abaixo:

a) Manter a Propriedade intelectual e expertise (especialistas) é crítico para nosso sucesso.
b) Nós cultivamos especialistas internos, como por exemplo, analistas ou engenheiros, e os escutamos em nossas decisões.
c) Nós pensamos em riscos, em tudo que nós fazemos e antes que se tome alguma decisão importante.
d) Nós utilizamos uma metodologia de gerenciamento da qualidade, como Controle de Qualidade Total ou Seis Sigma, para melhorar nossas operações e decisões.
e) Nós encorajamos as unidades da organização a terem iniciativas

empreendedoras e algum nível de autonomia.
f) Nós encorajamos empregados em todos os níveis hierárquicos a assumirem responsabilidade por suas ações e resultados.
g) Nossa organização é alvo de ataques de ativistas sociais ou políticos ou ainda de criminosos.
h) Nós conhecemos e documentamos as vulnerabilidades identificadas na TI.
i) Nós conhecemos e documentamos os incidentes pelos quais passamos, incluindo as respostas dadas e como se deu a recuperação
j) Para cada incidente, documentamos as perdas diretas (monetárias) e indiretas (reputação, oportunidades) de sua ocorrência.
k) Para cada incidente, informações sobre as medidas utilizadas, seus desempenhos, tempo e esforços requeridos são documentados.

III - Tratamento formal dos riscos

H3: Está relacionado com a cultura de riscos e favorece as práticas de gerenciamento de riscos de TI.

- Definir, na opinião do entrevistado, o que seria um tratamento formal
- Identificar a existência de um processo formal de tratamento dos riscos
- Enquadrar o tratamento do risco da organização em um das opções abaixo:

a) A organização pode transferir o risco para outra parte, afirmando que não será responsável pelas conseqüências dos riscos, mas sem especificar quem será o responsável por elas. Dessa forma, não se tem responsável definido pelo gerenciamento dos riscos.
b) A organização transfere a responsabilidade do gerenciamento das adversidades, mediante a assinatura de acordo formal com uma terceira parte.
c) Compensação por Consórcio: Várias unidades compartilham o custo das conseqüências de seus riscos. A idéia por trás e que dificilmente os riscos das várias unidades ocorrerão simultaneamente, distribuindo assim o custo entre os participantes desse modelo.
d) Compensação por aposta (hedge): A organização paga uma terceira parte para que assuma as responsabilidades dos eventos. A terceira parte aceita o risco baseando-se na probabilidade de sua ocorrência.
e) Mitigação: A organização trabalha para minimizar a probabilidade do risco ser concretizado ou pêra reduzir a conseqüência de seus efeitos.
f) Retenção / Aceitação : A adversidade não é tão custosa ou é improvável de ocorrer, ou ainda a organização assume que os benefícios obtidos aceitando os riscos são grandes.

IV - Gerenciamento de Risco de TI e práticas

H4: As organizações não despertaram para a a importância dos riscos de TI no processo decisório do negócio.

- Identificar em quais dimensões a organização pode ser afetada por uma falha de TI.
- Identificar as práticas de gerenciamento de TI adotadas
- Verificar situações em que o negócio levou em consideração nas decisões, algum risco de TI.
- Discorrer sobre risco de agilidade. Verificar se há adequação com uma das frases:
    1. "Há um risco potencial de catástrofe nos negócios"
    2. A tecnologia atual pode ser substituída para suportar uma nova estratégia de negócio
    3. Migração de tecnologia melhorará a perfomance dos negócios.

- Fazer checklist das práticas abaixo:

a) Contratos com parceiros de negócio especificam cláusulas sobre o acesso e confidencialidade dos dados. Há controle sobre os dados que os parceiros/fornecedores da organização têm acesso.
b) Existe um termo de compromisso sobre o uso dos dados e existem evidencias de que os funcionários leram entenderam as suas responsabilidades contidas no termo.
c) Existe o monitoramento das contas de usuários administradores e de duplicidade de usuários.
d) Existe o controle sobre as permissões de cada usuário. É possível saber quais dados cada usuário tem direito a acessar.
e) Utiliza-se o controle de acesso de quem acessou o que e quando através de logs ou similares.
f) Não é possível produzir um inventario de todas as informações circulantes na organização, bem como classificar essas informações em categorias
g) Existe um controle de acesso ao Data Center ou estrutura de processamento similar.
h) Não existe controle sobre as mudanças das aplicações. As alterações podem introduzir mudanças indesejadas e não ha como controlá-las.
i) Não existe controle de versionamento dos documentos da organização
j) Não esta claro quem pode atualizar quais dados nos sistemas de informação. Conflitos de permissão de alteração são freqüentes.
k) Não existem não organização, planos de contingência para continuidade do negocio.
l) O apoio da TI é total na execução das estratégias da empresa. Não ha dificuldades na implementação de novos projetos considerando o ambiente atual de TI.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo