UNIVERSIDADE FEDERAL DO PARANÁ
SETOR DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE GESTÃO DA INFORMAÇÃO

SÉRVULO GONÇALVES FILHO

SEGURANÇA DA INFORMAÇÃO NO AMBIENTE COLABORATIVO INTERORGANIZACIONAL

CURITIBA
2009

SÉRVULO GONÇALVES FILHO

SEGURANÇA DA INFORMAÇÃO NO AMBIENTE COLABORATIVO INTERORGANIZACIONAL

Trabalho apresentado à disciplina Pesquisa em Informação II, SIN030 como requisito parcial à conclusão do Curso de Gestão da Informação, Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná.

Orientador: Prof. Dr. Newton Correa Castilho Júnior

CURITIBA
2009

RESUMO

Apresenta a colaboração interorganizacional como fator estratégico e competitivo nas organizações e aponta razões para que essa estratégia seja adotada. Identifica os tipos de relacionamentos mais comuns e demonstra as vantagens das parcerias em diversos aspectos que compõem a cadeia de valor das empresas. Aborda a importância da Gestão da Informação como fator de sustentabilidade dos negócios e discorre sobre a informação como instrumento de definição de estratégias, de alavancagem dos negócios e de redução de incertezas nos ambientes intra e interorganizacionais, contribuindo significativamente para o aperfeiçoamento da pesquisa, dos processos, e do desenvolvimento de produtos e serviços. Destaca o impacto deste ativo nos negócios e a conseqüente necessidade de sua adequada proteção. Indica instrumentos que se destinam a monitorar, controlar e garantir que a informação esteja disponível quando dela se precisar, sem que haja riscos a sua integridade e confidencialidade. Analisa aspectos relativos às tecnologias mais freqüentemente utilizadas para garantir o uso seguro do acervo informacional, apontando os benefícios dos investimentos em sua proteção, comparativamente aos prejuízos em caso de sua perda ou uso indevido. Objetiva levantar os elementos, no âmbito da segurança da informação, capazes de contribuir para a redução dos riscos a que estão sujeitos os ativos informacionais das organizações e destacar a urgência do compromisso de todos os colaboradores com a preservação e o emprego apropriado do conhecimento e da informação organizacionais. Emprega, para a seleção e discussão das questões julgadas mais relevantes na condução do objetivo proposto, a metodologia de levantamento e revisão da literatura pertinente que governa à construção conceitual e a metodologia do estudo de caso na condução da pesquisa empírica. Conclui que a coleta, o tratamento e o uso da informação devem estar alinhados com as diversas medidas de segurança desse patrimônio e que os cuidados com a segurança devem ser incorporados por todas as organizações, incluindo aquelas que trabalham em regime de colaboração, de modo a ser percebidos como fator de sustentabilidade das parcerias.

Palavras chave: Colaboração interorganizacional, gestão da informação, segurança da informação.

LISTA DE FIGURAS

SUMÁRIO

1 APRESENTAÇÃO

Neste trabalho serão abordados assuntos relativos à Colaboração Interorganizacional, a Gestão da Informação e a Segurança da Informação.

1.1 INTRODUÇÃO

Com a crescente competitividade do mercado, as empresas precisam concorrer para garantir a manutenção de sua posição e, se possível, expandi-la em relação ao setor em que atuam. Gerar diferenciais competitivos passou a ser fundamental na garantia de sustentabilidade. Assim, a colaboração interorganizacional vem se tornando uma estratégia competitiva cada vez mais presente no relacionamento entre as empresas, que procuram otimizar seus processos de desenvolvimento, produção e comercialização de serviços e produtos, reduzir custos e garantir sua permanência no mercado, bem como a de seus parceiros estratégicos.

Há uma percepção, por parte das empresas, de que existe uma interdependência entre elas, seus fornecedores e clientes, e que quanto maior e melhor for sua interação com os demais agentes nessa cadeia de valor, melhores condições terá para competir. A colaboração interorganizacional se torna, então, um mecanismo capaz de proporcionar maior agilidade aos negócios, aperfeiçoar processos e desenvolver inovações.

A colaboração interorganizacional pode se dar entre empresas que atuam num mesmo segmento de mercado ou em segmentos que se complementam. Para que a colaboração atinja seus objetivos é necessário uma intensa troca de informações entre os parceiros, o que ocorre através de contatos pessoais em reuniões, troca de documentos impressos e, mais comumente, através do uso de tecnologias de informação e comunicação.

No ambiente concorrencial moderno a empresa não está isolada, tem que trabalhar com base em suas competências essenciais, tem que administrar recursos que são e que não são dela, trabalhar em sintonia com seus fornecedores, distribuidores, vendedores, lojas e outras entidades que fazem parte de uma cadeia de suprimentos. Para isso, precisam contar com uma eficiente gestão informacional

que se expande além das fronteiras internas para abarcar todas as informações que transitam no ambiente das relações interorganizacionais.

A Gestão da Informação, como ferramenta administrativa, é um instrumento de fundamental importância à tomada de decisão nas organizações e uma atividade estratégica para os processos de negócios - oferece técnicas, metodologias e recursos humanos especializados na coleta, análise, tratamento, disseminação, armazenamento e uso de dados, informação e conhecimento.

Importante fator de sustentação das organizações, a informação se faz presente nas atividades internas, nos negócios realizados pelas empresas e em seus relacionamentos colaborativos. O conhecimento e o uso da informação tornam as tomadas de decisão mais seguras, mitigando riscos. Wurman (1991) define a informação, de modo claro e objetivo, como “aquilo que reduz a incerteza”. Desnecessário dizer que, com menos incertezas, as decisões tem maior potencial de alcançar resultados positivos.

Silva (2003, p.40) discorre, de forma sucinta, sobre o valor da informação para as empresas, afirmando que “num contexto empresarial, as formas mais comuns de se mensurar o valor de uma informação são: lucro, tempo, previsibilidade e antecipação de resultados. [...]”

A Gestão da Informação fornece uma percepção precisa e objetiva dos valores da informação e do sistema de informação, bem como identifica as informações relevantes geradas e obtidas no ambiente intra e interorganizacional, tratando-as, armazenando-as e disponibilizando-as de forma a preservar sua integridade e garantir sua confidencialidade, seja por razões de marketing, de fortalecimento da imagem ou criticidade das operações e do próprio negócio.

Por sua importância, é imprescindível que a informação seja protegida contra o uso indevido, seu “vazamento”, interceptação ou perda. A segurança da informação tornou-se quase uma obsessão no mundo corporativo. Há necessidade de que os sistemas informacionais mantenham-se íntegros, que funcionários sejam conscientizados quanto ao valor dos ativos de informação, notadamente no que se refere a sua confidencialidade, para que esta não seja divulgada voluntaria ou involuntariamente a quem não deveria ter acesso a ela. Os meios de armazenagem devem ser abrigados em lugar seguro, com cópias de segurança e garantias de que

não se tornarão obsoletos, prejudicando a capacidade de recuperação da informação. Há, hoje, uma grande preocupação com os ativos informacionais em meios digitais e certa negligência com as informações contidas em documentos, relatórios impressos e, principalmente, em relação às informações e conhecimentos existentes na cabeça de cada colaborador – o conhecimento tácito.

Este trabalho analisa a importância da Segurança da Informação para a Gestão da Informação no ambiente organizacional e interorganizacional, fornecendo elementos que comprovam a necessidade das organizações em buscar, usar e administrar as informações que lhe são úteis, preservar e resguardar esse valioso bem para uso no cotidiano de suas atividades, nas decisões estratégicas que precisem ser tomadas e no compartilhamento exigido nos negócios desenvolvidos em parceria, protegendo essas informações contra as possíveis ameaças a que estão sujeitas.

1.2 PROBLEMA

A atual conjuntura econômica e social exige das organizações uma atenção especial às questões relacionadas à informação, para que essa possa ser obtida, utilizada e compartilhada com seus parceiros comerciais de modo eficaz e seguro.

Há, portanto, um problema objetivo a ser resolvido: quais elementos e ações podem ser empregados para garantir que as informações sejam protegidas quanto a sua integridade, confidencialidade e disponibilidade?

Não há uma resposta única a essa pergunta. O ambiente informacional em cada organização e as relações colaborativas com cada parceiro de negócio devem ser analisados detalhadamente para que sejam identificadas práticas capazes de reduzir riscos.

A segurança da informação precisa ser percebida, em uma visão sistêmica, como uma questão abrangente, que permeia todas as atividades da organização e suas relações com fornecedores, clientes e demais integrantes de sua cadeia de valor e de suprimentos, bem como todos os demais públicos interessados. Ela envolve processos, pessoas, recursos físicos e lógicos. Beal (2005, p.10) discorre a

respeito do assunto avaliando que “toda organização precisa adquirir uma visão sistêmica das suas necessidades de segurança, dos recursos a serem protegidos e das ameaças às quais está sujeita, para então poder identificar as medidas de proteção mais adequadas, economicamente viáveis e capazes de reduzir ou eliminar os principais riscos para o negócio”

1.3 JUSTIFICATIVA

As empresas buscam sustentar suas vantagens competitivas a partir de suas relações com o mercado e, num enfoque interno, a partir de suas competências essenciais como recursos, habilidades e conhecimentos. Para reforçar suas competências ou desenvolver competências com maior rapidez e flexibilidade, as empresas estabelecem parcerias estratégicas com outras empresas criando um relacionamento colaborativo capaz de elevar seus níveis de competitividade.

“O objetivo final da iniciativa colaborativa é um processo permanente de inovação, baseado no conhecimento compartilhado, em busca da vantagem competitiva sustentada para toda a cadeia.” (CASTILHO, 2005, p.18).

O relacionamento colaborativo tem como seu principal pilar a intensa troca de informações e, nesse campo, a Gestão da informação é, inquestionavelmente, uma das atividades de maior relevância para as empresas e vem sendo exercida por profissionais de diversas áreas, de modo mais ou menos profissional, com abordagens práticas em função de experiências conhecidas ou sistemáticas, com emprego de técnicas e profissionais especializados no assunto.

Independente da forma como as organizações lidam com a informação, os aspectos de segurança da informação constituem uma base fundamental para a sustentação dos negócios.

São muitas as ameaças ao acervo informacional das empresas. Isso se torna ainda mais concreto nos relacionamentos colaborativos, onde empresas têm acesso a uma quantidade maior de informações de seus parceiros, podendo, em alguns casos, acessar sistemas de informação pertencentes às outras empresas. Nesse particular, além das ferramentas de proteção existentes, é importante estar atento

para que a colaboração não se transforme numa ação predatória. Powell (1990) e Knight (2000) argumentam que existe sempre o risco de um comportamento oportunista por parte de um dos parceiros, que tenta capturar a maior parte dos benefícios da parceria ou o conhecimento e perícia da outra empresa.

São noticiados diariamente fatos como invasão de sistemas, prejuízos causados por funcionários descontes com a empresa e toda uma gama de problemas que resultam na perda, repasse indevido e venda de informações estratégicas pertencentes a empresas e governos.

É necessário que as organizações conheçam e administrem seu acervo informacional, protejam seus dados, informação e conhecimento organizacionais e criem políticas que favoreçam o correto uso desse patrimônio.

Em função da importância da segurança da informação nos ambientes intra e interorganizacionais, conforme exposto acima, decidiu-se estudar o assunto e utilizá-lo como foco deste trabalho.

1.4 OBJETIVOS

Os objetivos foram divididos em duas categorias: geral e específicos, conforme mostrado abaixo:

1.4.1. Objetivo Geral

Levantar os elementos, no âmbito da segurança da informação, capazes de contribuir para a redução dos riscos a que estão sujeitos os ativos informacionais das organizações.

1.4.2. Objetivos Específicos

O objetivo geral é melhor detalhado com os seguintes objetivos específicos:

a) levantar, na literatura, elementos capazes de proteger as informações presentes nas atividades internas e de relacionamento colaborativo das organizações, para que os processos de coleta, tratamento, disponibilização, armazenamento, uso e descarte desse importante ativo sejam resguardados das ameaças a que estão sujeitos;

b) realizar um estudo de caso para verificar, na prática, aspectos e visões sobre os conceitos estudados na revisão de literatura.

2 REFERENCIAL TEÓRICO

Para a realização desse trabalho foi feita uma revisão da literatura relacionada às questões abordadas, conforme exposto a seguir:

2.1 COLABORAÇÃO INTERORGANIZACIONAL

Em busca de sustentação e da elevação de competitividade, as organizações modernas estabelecem parcerias estratégicas com outras empresas criando um relacionamento colaborativo baseado nos relacionamentos que promovem junto a sua cadeia de valor, especialmente junto a seus clientes e fornecedores, de modo a compartilhar recursos de toda ordem, desde os estruturais até os de conhecimento técnico e de mercado, passando por recursos financeiros, humanos e até mesmo da cessão de sua reputação no mercado onde atua, visando reforçar suas competências ou desenvolver competências com maior rapidez e flexibilidade.

Faulkner e De Rond (2000) ensinam que:

> "(...) a colaboração influencia não só a estrutura da concorrência, mas também a velocidade em que as mudanças acontecem, pois interfere no acesso a novas tecnologias, nas oportunidades de otimização da capacidade e de capacitações, e na alteração das barreiras de entrada e saída".

Corrobora com esse pensamento Castilho (2005, p.18) quando diz que "o objetivo final da iniciativa colaborativa é um processo permanente de inovação, baseado no conhecimento compartilhado, em busca da vantagem competitiva sustentada para toda a cadeia."

Os relacionamentos interorganizacionais podem ser alicerçados por normas formais, através do cumprimento de obrigações contratuais ou, num enfoque colaborativo, por regras informais, em que as empresas percebem mais vantagens em cooperar e reconhecer que têm de agir com reciprocidade a qualquer benefício recebido.

A gradiente apresentado na figura 1, baseada em Webster (1992), aponta os diversos níveis de relacionamento colaborativo.

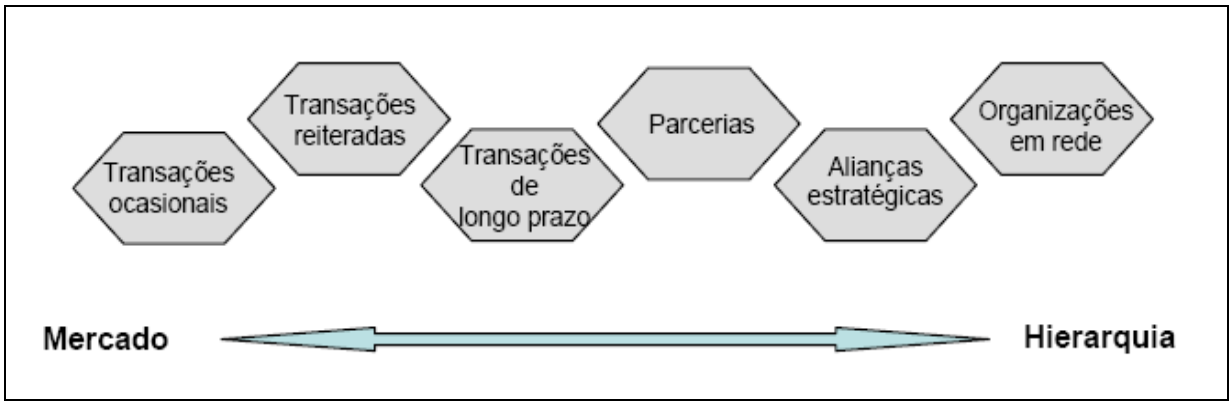

FIGURA 1 - ESTRUTURAS DE GOVERNANÇA BASEADAS NO RELACIONAMENTO
Fonte: Webster (1992)

O autor acrescenta que cada camada do gradiente deve ser entendida da seguinte forma:

a) transações ocasionais - ocorrem em razão de expectativas de maximização do lucro;

b) transações reiteradas - condição precursora do relacionamento colaborativo;

c) transações de longo prazo – sustenta-se por processo de relacionamento baseado na interdependência entre os agentes;

d) parcerias - maior interdependência das empresas, com menos parceiros envolvidos;

e) aliança estratégica - o relacionamento cria um novo empreendimento;

f) organizações em rede - relacionamentos organizados, na forma de confederação / coalizão de empresas.

Castilho (2005, p.27) explica que

> ao estabelecer um modelo de coordenação que permita à empresa transferir algumas atividades para fornecedores mais eficientes, mantendo, internamente, somente as atividades em que seja realmente competitiva, esta consegue reduzir, significativamente, os custos de transação. O custo final será menor, devido à especialização de cada empresa participante na rede e o modelo se sustenta porque possibilita maiores retornos, no longo prazo, trazendo a confiança que contribui para a redução dos custos de transação e o valor atribuído por cada empresa ao relacionamento, o que facilita ainda mais a solução de problemas.

Powell (1990, p.305) defendeu a posição de que a reciprocidade é ampliada (*enhanced*) por uma perspectiva de longo prazo. A segurança e a estabilidade encorajam a procura de novas maneiras para o cumprimento de tarefas, promove o aprendizado e a troca de informação e gera (*engender*) confiança. O compartilhamento de riscos é fundamental para o sucesso de um relacionamento, no longo prazo. A segurança propiciada pelo relacionamento incentiva investimentos por parte dos fornecedores, confiança e dependência mútuas resultam em maior e mais rápida fluência das informações.

À medida que os projetos conjuntos ou complementares se desenvolvem, as organizações tornam-se mais confiantes no relacionamento e mais abertas em relação à troca de informações.

> […] sob condições repetitivas, a incidência da cooperação aumenta substancialmente. De forma similar, em alianças estratégicas, a cooperação é mantida conforme a firma compara os ganhos imediatos de enganar, com o possível sacrifício de ganhos futuros que possam resultar da violação do acordo [...] (PARKHE, 1993, p.227).

Para o citado autor, este modelo comportamental gera um sentimento de segurança e estabilidade que incentiva a procura por novas formas de se desempenhar tarefas, promover o aprendizado e trocar informações, além de realimentar a confiança na relação.

Fica claro que, na relação colaborativa, à medida que as empresas percebem as vantagens da união de forças, mesmo quando aplicadas a um pequeno número de atividades, passam a agir de maneira a garantir a continuidade da parceria. Segundo Castilho (2005, p.35) Esta perspectiva inibe a decisão de procurar maximizar os resultados no curto prazo, à custa do parceiro, favorecendo a idéia de contentar-se com resultados menores, investindo em ganhos futuros advindos da relação, e que é central para o entendimento e análise das formas de organização em rede.

A literatura indica que os resultados obtidos através da relação colaborativa entre empresas favorecem a competitividade, sendo esta a razão principal para a colaboração. Assim, as empresas que mantêm algum tipo de interação colaborativa têm maiores condições de competir em seus respectivos segmentos. Jarillo (1988), complementa esse pensamento quando fala da compatibilidade e da

complementaridade entre os comportamentos competitivo e colaborativo. Para Porter (1985), a vantagem competitiva é normalmente definida como a habilidade em receber retornos do investimento em níveis persistentemente acima da média do setor.

Porter (1980) construiu seus trabalhos sobre estratégia competitiva sob fundamentos hoje amplamente aceitos, sugerindo que a intensidade competitiva do setor é determinada por cinco forças fundamentais: concorrentes atuais, compradores, fornecedores, novos concorrentes (entrantes) e produtos ou serviços substitutos.

Este trabalho lista alguns dos fatores mais relevantes que conduzem ao relacionamento colaborativo, de acordo com as idéias de Kogut (1988), Powell (1990), Jarillo (1988), Einsehardt, Das e Teng (2000) e Faulkner (1995):

a) custos de transação;

b) comportamento estratégico competitivo;

c) conhecimento organizacional e aprendizado;

d) diminuição dos tempos dos ciclos de negócio;

e) necessidade de acesso a recursos e *know-how*;

f) mudanças na abordagem organizacional por especialização, foco e, possivelmente, tamanho;

g) capacidade de suplantar riscos e ineficiências;

h) disponibilização de recursos estratégicos valiosos subutilizados;

i) agregação, compartilhamento ou troca de recursos com outras empresas quando estes recursos não estão disponíveis de forma eficiente, por meio de transações no mercado ou por fusões e aquisições;

j) necessidade de minimizar custos – em clara relação com a economia de custos de transação;

k) necessidade de velocidade nas relações com o mercado – na perspectiva da Teoria da Organização da Indústria;

l) necessidade de ativos específicos ou capacidade que não possui atualmente – uma perspectiva da Visão Baseada em Recursos.

Naturalmente que esta lista sintetiza algumas das idéias encontradas na literatura estudada, não se esgotando em si as possíveis motivações que as organizações possam ter para adotar o caminho da interação e colaboração com seus parceiros de negócios, como fornecedores, clientes, demais *stakeholders* e, até mesmo, com concorrentes, quando essa postura se mostrar importante em sua estratégia competitiva.

É importante observar que, em praticamente todas as áreas, o mercado vem mantendo um dinamismo crescente, o que torna o ciclo de produção de bens e serviços cada vez mais curto resultando na necessidade, cada vez mais intensa, de aquisição de *know-how*.

O relacionamento entre empresas organizadas em parcerias, alianças e organização em redes representa uma forma rápida de ganhar acesso ao conhecimento e *know-how* que não pode ser produzido internamente, conforme explica Powell (1990).

O fortalecimento competitivo da empresa pode ser alcançado quando o relacionamento entre empresas é permeado pela cooperação mútua. Porter e Fuller (1986), já citados, relacionam o papel da colaboração com o poder competitivo, analisando que se o posicionamento afeta a lucratividade, ao empregar alianças estratégicas, os parceiros podem alcançar posições ainda mais fortes juntos, do que isoladamente. Nas palavras dos autores: “A coalizão surge quando, ao executar uma atividade em conjunto com um parceiro, o resultado apresenta-se superior àquele realizado individualmente, pela própria empresa, ou quando simplesmente terceirizado em transações ocasionais de mercado” (PORTER e FULLER, 1986).

O arranjo colaborativo ajuda a empresa a manter o foco nas áreas onde tem maior nível de especialização e competência, transferindo para seus parceiros as atividades onde estes possuem maior capacidade de atuar. Seus parceiros, por sua vez, fazem o mesmo, numa troca de competências estratégicas que têm o potencial de garantir ou fazer crescer sua posição no mercado, beneficiando e sendo beneficiada ao longo de todo esse processo. Jarillo (1988) reafirma essa noção quando explica que todos se beneficiam, por não terem de executar atividades que não lhes são essenciais ou que não apresentam vantagem competitiva.

Para Bakos e Brynjolfsson (1997), uma empresa opta por se relacionar com muitos parceiros de negócio, em uma estrutura de mercado, porque, desta forma, consegue obter custos de produção mais favoráveis, resultantes da concorrência e da eficiência. Este processo leva, contudo, a altos custos de transação, que diminuirão se forem também reduzidas, pelo estreitamento do relacionamento, as estruturas coordenativas que, no limite, com um único parceiro, assemelha-se a uma hierarquia. Portanto, a decisão de "fazer ou comprar" pode ser vista como uma escolha, entre custos de produção e de coordenação.

Embora haja considerável vantagem nessa interação, há o risco de que um dos integrantes dessa cadeia relacional utilize o conhecimento adquirido para se beneficiar isoladamente e, até mesmo abrir mão da ética, permitindo-se obter favorecimento em detrimento dos negócios da empresa com a qual compartilha habilidades e competências. Sob essa problemática, Hamel (1991) relata que a forma com que cada organização aplica os conceitos de colaboração pode ser percebida através de duas abordagens diferentes: aprendizado organizacional, aplicável ao relacionamento colaborativo e aprendizado competitivo, aplicado de forma egoísta, por uma firma, sobre as habilidades e conhecimentos de seu parceiro, de forma predatória.

É importante que se perceba que, independentemente do tipo de relacionamento que se estabeleça, a colaboração interorganizacional sofre influência da cultura local ou nacional – onde residem os valores e a cultura organizacional - composta, principalmente, de práticas (HOFSTEDE, 1991).

Gulati (1998) analisa a questão e deduz que há apenas duas formas de prever o comportamento individual em um relacionamento entre empresas. A primeira é um contrato detalhado, a outra, é a confiança.

Niederfofler (1991) associa a confiança e a boa vontade à manutenção da estabilidade em todos os níveis de desenvolvimento das relações. Castilho (2005), diz que "com uma maior tolerância, os parceiros agem proativamente, para evitar conflitos. Um bom resultado também é esperado na melhoria da comunicação entre os parceiros, aumentando, com isso, as chances de administrar e resolver eventuais desalinhamentos em suas ações, com relação aos objetivos da parceria". Segundo Granovetter (1985), a confiança é uma fonte de capital social, que afeta os custos de transação.

Ainda nessa linha, (FAULKNER e DE ROND, 2000) acrescentam que, uma demonstração de compromisso enseja um relacionamento estável e duradouro. Entre as diversas maneiras de manifestar seriedade e compromisso está o investimento de capital em um projeto cooperativo.

Outro aspecto de fundamental importância nas parcerias foi lembrado por Knight (2002). O autor diz que, normalmente, a comunicação está diretamente relacionada com o grau de desenvolvimento do comportamento nas relações colaborativas: cultura, confiança e compromisso. A comunicação tem de ser oportuna, apropriada e clara. E, também, fluir de forma desimpedida entre todos os participantes da aliança. Este fluxo de informações será maior ou menor em função dos tipos de estrutura de coordenação adotados para apoiar as transações que ocorrem entre as empresas (GULATI, 1998).

Em complemento a essas condições, Smith; Carroll; Ashford (1995) adicionam o estabelecimento de regras claras, com o conhecimento, inequívoco, dos papéis existentes e níveis adequados de influência e controle, como circunstâncias necessárias à sustentação da colaboração.

A partir desses condicionantes, pode-se perceber o grau de dependência existente dentro da parceria e corrigir seus rumos à medida que se estreitam as relações. Pfeffer (1982) corrobora com essa idéia quando destaca que “[...] porque as organizações não são auto-suficientes, elas requerem recursos ao ambiente e, portanto, tornam-se interdependentes dos elementos do ambiente com quem transacionam […]”

Observa-se que, de um modo geral, as competências que as empresas conseguem construir e fixar liderança não passam de cinco ou seis. Assim, o estabelecimento de licenciamentos ou alianças é um recurso que lhes permite anexar outras competências necessárias.

Nos casos de bens intangíveis como *know-how*, capacidade tecnológica, inovação e conhecimento tácito, cultura organizacional e outros, o intercâmbio pode ser promovido através de redes.

No julgamento de Porter e Fuller (1986) a abordagem colaborativa resulta em formas organizacionais mais rápidas no reposicionamento estratégico do que a hierarquia, além de ter custos menores e menor grau de rigidez.

Para Castilho (2005), “redes de empresas podem prover benefícios adicionais aos processos colaborativos por causa do fenômeno da inserção (tradução do autor para o termo em inglês: *embeddedness*, que define o nível de ligação entre elementos de uma rede social em função das conexões e da posição estrutural que estes ocupam na rede”. Gulati (1998) propõe duas formas de inserção: relacional e estrutural. A inserção relacional aborda a importância de relacionamentos colaborativos diretos no acesso a recursos. A estrutural é proveniente da posição estrutural que estes parceiros ocupam na rede.

Nesse contexto, verifica-se um crescente apoio das tecnologias de Informação e Comunicação (TICs) no relacionamento colaborativo, agilizando processos, ampliando a comunicação e alterando o grau de capacitação de toda a cadeia de valor.

As tecnologias baseadas na *Internet* tornaram a adoção das ferramentas de TI utilizadas para troca de informações mais fáceis e baratas para organizações de qualquer porte adicionando rapidez e flexibilidade aos relacionamentos interorganizacionais.

Um exemplo de tecnologia específica para troca de informações e que pode utilizar o ambiente da *internet* para operar é a troca eletrônica de dados, ou, em inglês EDI (*Electronic Data Interchange*), que segundo Albertin (2004): “[...] é a troca eletrônica e interorganizacional de mensagens de negócio padronizadas entre aplicações [...]” oferecendo suporte à comunicação e interconexão de processos que vão desde a colocação de pedido, até a transferência de fundos, passando por atividades de compra e venda, entre outras.

Castilho 2005 ressalta que,

> apesar de apresentar economias significativas, como redução de sistemas, baseados em papel, diminuição do índice de erros em transações interorganizacionais e agilidade de processamento destas transações, a EDI apresenta também desvantagens, relacionadas ao custo de manutenção da rede e limitações de seus padrões quanto à flexibilidade. Com a evolução acelerada da TI e o advento da Internet (WebEDI – versão Internet da EDI), parte destes problemas vem sendo resolvida pela simplificação e redução de custos, o que resulta em maior acessibilidade dos serviços e vantagens decorrentes do padrão aberto da plataforma.

A adoção de sistemas abertos, baseados no padrão TCP-IP (*Transmission Control Protocol – Internet Protocol*) possibilita a criação de portais corporativos que facilitam enormemente as comunicações interorganizacionais e possibilita a conectividade de praticamente toda a camada física, nas redes de comunicação inseridas no ambiente Web.

Dentre as ferramentas mais comuns utilizadas na integração colaborativa, estão as trocas de mensagens.

Castilho (2005) destaca que as trocas de mensagens são os serviços de tecnologia mais importantes, por ser uma ferramenta de comunicação simples e de baixo custo da plataforma *Internet*, mas que poderia ser melhor explorada se possibilitasse a identificação de presença e simultaneidade de comunicação entre as partes. O autor acrescenta que o Serviço de Mensagens Instantâneas (*Instant Messaging* – IM) possui essa característica.

Numa visão mais abrangente, dentre os sistemas utilizados nos processos colaborativos, podem-se listar os principais, numa escala que evolui do nível mais simples de comunicação, com ferramentas básicas aos mais sofisticados, cujos recursos são tantos que não seria possível listá-los no escopo deste trabalho:

a) e-mails e Serviços de Mensagens Instantâneas;

b) sistemas de Groupware;

c) sistemas de automação e gerenciamento do fluxo de trabalho (Workflow);

d) sistemas de Gestão de Documentos.

É importante destacar que estas e outras aplicações vêm sendo incorporadas aos Portais Corporativos - grandes sites, criados e gerenciados por organizações, cujas funções são basicamente as de marketing, interação com clientes e fornecedores, divulgação de políticas da instituição, informações gerais, notícias e outros conteúdos que a organização julgar importante em suas metas de comunicação.

Os sistemas de comunicação colaborativa são conhecidos como Sistemas de Informação Interorganizacionais que, conforme descreve Castilho (2005) “enfoca, principalmente, as trocas de dados que ocorrem através de fronteiras organizacionais, melhorando as ações de monitoração e coordenação, e

aumentando a eficiência, ao permitir que as empresas integrem atividades relacionáveis pela informação, sem interferir nas fronteiras legais das entidades envolvidas".

Johnston e Vitale (1988) explicam que existe uma relação de oposição entre a confiança e integração das organizações usuárias do sistema e as limitações de acesso aos dados e aos recursos de processamento um Sistema de Informação Interorganizacional - SII. Esses autores argumentam que, devido a sua extensão dentro da cadeia de valor, se comparados aos sistemas internos, os SIIs produzem maior preocupação em relação à confiabilidade, segurança, privacidade, integridade e a seu grau de impacto estratégico. Embora todas essas preocupações sejam reais, as empresas têm percebido que podem se beneficiar com os SIIs mais modernos, que já conseguem apoiar as atividades colaborativas de usuários, em diferentes empresas, permitindo consultas, coletas, análises, processamento e armazenamento de dados.

Carr (2003) reforça a utilização da informática como recurso básico nas organizações quando afirma que a TI deixou de ser considerada condição estratégica já que seus suas ferramentas são facilmente encontradas em mercados competitivos. Complementa que, um recurso para ser considerado estratégico não pode ser facilmente adquirido no mercado competitivo.

No relacionamento com fornecedores, os SIIs favorecem a integração através do processamento de dados de projeto, produção, distribuição e até mesmo financeiros, intensificando o acompanhamento das atividades desenvolvidas pelos agentes integrantes da cadeia de valor.

Alguns estudos apontam para o uso das redes abertas, baseadas na tecnologia *Internet*, para a expansão de parcerias às empresas de porte menor, uma vez que tal tecnologia tem custo baixo e operações mais simples.

Para Sampler (1998), estamos na era da informação, uma importante transição de referenciais para a criação de redes e outros modelos de estrutura organizacional. A idéia de custo em relação à informação é alterada para a de recurso potencialmente criador de valor, com um gradual aumento do componente "informação" na produção de bens e serviços.

A figura abaixo apresenta uma síntese dos macro-conceitos da Colaboração Interorganizacional:

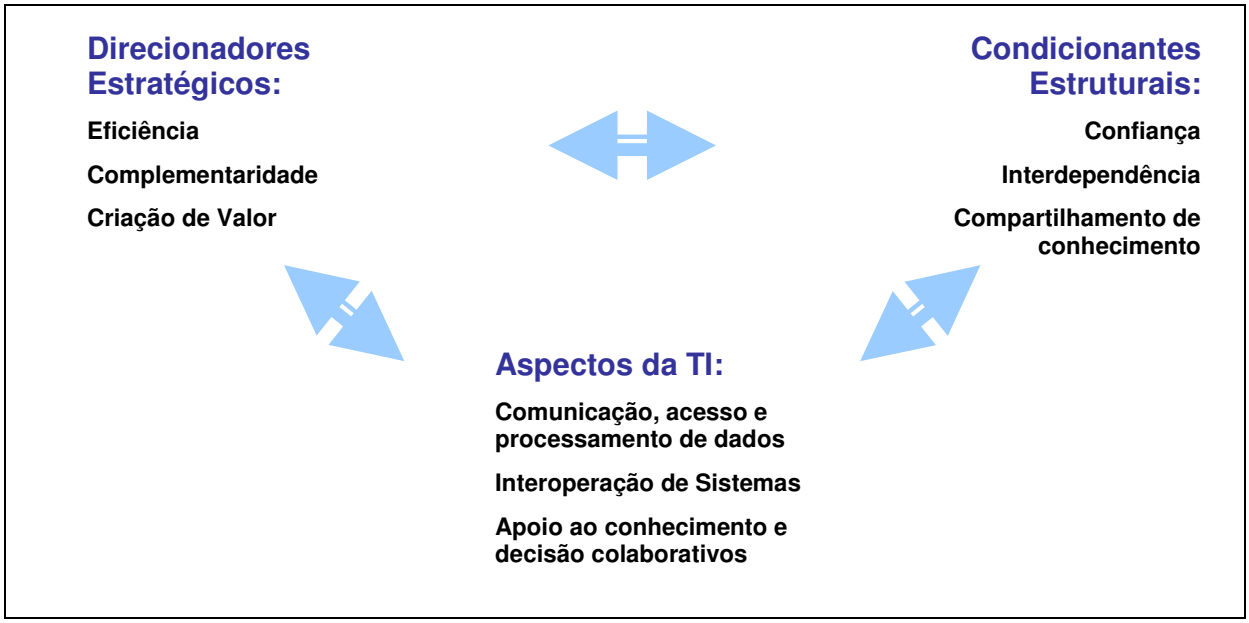

FIGURA 2 - COLABORAÇÃO INTERORGANIZACIONAL VERTICALMENTE RELACIONADA BASEADA NA TI

Fonte: Castilho (2005)

É importante salientar que algumas condutas devem ser consideradas essenciais para a implementação e continuidade do relacionamento cooperativo interorganizacional. Entre elas, pedem-se mencionar:

a) foco nos objetivos comuns;

b) suporte dos líderes da organização;

c) atendimento aos pré-requisitos e a observação dos padrões;

d) pré-disposição para a mudança;

e) identificação e cumprimento de papéis e responsabilidades;

f) confiança e transparência na comunicação entre os parceiros.

Algumas ações entre empresas cujo relacionamento se pauta em posições hierárquicas na cadeia colaborativa, são citadas por CASTILHO (2005, p.213) quando apresenta exemplos de colaboração sustentada por empresas varejistas que lideram os processos colaborativos com seus parceiros de negócios. Sob esse enfoque, uma determinada empresa varejista de grande porte oferece financiamento de equipamentos e ingresso em sua universidade corporativa aos seus parceiros. Em outro exemplo uma

empresa utiliza sua força competitiva para negociar a matéria prima, que depois é adquirida pelos fornecedores no desenvolvimento de seus produtos, na quantidade e preços acertados.

Para uma melhor compreensão dos fenômenos envolvidos no relacionamento colaborativo verticalmente relacionado, Castilho (2005) sintetiza as três Dimensões existentes, em relação aos prazos em que as parcerias são mantidas:

	Dimensões da Colaboração Interorganizacional Verticalmente Relacionada		
Duração do relacionamento/ Complexidade	**Direcionadores Estratégicos** (Por que colaborar?)	**Condicionantes Estruturais** (Sob quais condições colaborar?)	**Aspectos da TI** (Como a TI afeta a colaboração?)
Curto Prazo/Baixa	Eficiência	Confiança	Comunicação, Acesso e Processamento de Dados
Médio Prazo/Média	Complementaridade	Interdependência	Interoperação de Sistemas
Longo Prazo/Alta	Criação de Valor	Compartilhamento do Conhecimento	Apoio ao Conhecimento e Decisão Colaborativos

FIGURA 3 - MATRIZ DAS DIMENSÕES DA COLABORAÇÃO INTERORGANIZACIONAL VERTICALMENTE RELACIONADA, BASEADA EM TI E NÍVEL DE MATURAÇÃO E COMPLEXIDADE

Fonte: Castilho (2005)

Há um gradual deslocamento do eixo de motivação de uso das tecnologias de informação dos processos de otimização internos para os relacionamentos com as demais empresas da cadeia de valor.

Castilho (2005, p.247) explica que “pela redefinição conjunta de processos e produtos ou serviços, e o desenvolvimento de uma cultura colaborativa, o relacionamento interorganizacional encontrou nas TI emergentes, ferramentas estratégicas que estão tornando possível se atingir novos níveis de flexibilização, inovação e diferenciação e, portanto, uma maior capacitação.”.

O referido autor identifica alguns dos principais papéis desempenhados pela TI no suporte ao relacionamento colaborativo, conforme listado abaixo:

a) a TI torna a colaboração mais eficiente, reduzindo as restrições de tempo e distância e permitindo a redução de custos de transação entre as empresas;

b) a TI contribui para ampliar os níveis de confiança entre as empresas, ao permitir melhor coordenação e controles, além de restringir as possibilidades de comportamento oportunista;

c) a TI facilita a conectividade entre as empresas e, com isso, a comunicação e o acesso aos dados entre colaboradores;

d) a TI favorece a competitividade da parceria, ao atuar nas causas externas – ligadas ao setor, e nas internas – relativas aos recursos estratégicos;

e) a TI permite interoperabilidade entre sistemas e, portanto, automação e integração entre processos;

f) a TI influi, na padronização de processos operacionais e na diferenciação em produtos e serviços, afetando tanto à economia de escala, quanto à de escopo;

g) a TI potencializa a criatividade, a inovação e a integração de bens e conhecimentos;

h) a TI apóia novas formas de estrutura organizacional, baseadas no compartilhamento do conhecimento organizacional, que estimulam a constante reestruturação dos processos colaborativos e redefinição de escopo para os negócios;

i) a TI disponibiliza ferramental que estimula a criação e o compartilhamento do conhecimento e apóia a tomada de decisões colaborativas.

2.2 GESTÃO DA INFORMAÇÃO

A Gestão da Informação, como ferramenta administrativa e de apoio à tomada de decisão, vem se tornando uma atividade estratégica nos processos de negócios, em organizações de todos os setores e todos os portes, empregando técnicas, metodologias e recursos humanos em atividades de coleta, análise, tratamento,

disseminação, armazenamento e uso de dados, da informação gerada dentro e fora da organização e do conhecimento organizacional.

Conforme explica Marchiori (2002, p.75) “a gestão da informação tem, por princípio, enfocar o indivíduo (grupos ou instituições) e suas “situações problema” no âmbito de diferentes fluxos de informação, os quais necessitam de soluções criativas e custo/efetivas”.

Diante de um conjunto de informações confiáveis e atualizadas é possível ampliar a percepção da realidade, reduzir as incertezas e redefinir estratégias. A informação também é capaz de influenciar, sugestionar e modificar reações. Por ter todo esse potencial, a informação pode e deve ser administrada como um valioso recurso nas organizações.

A importância da informação é ratificada por Moresi (2000 p.14) cujo pensamento é:

> a importância da informação para as organizações é universalmente aceita, constituindo, senão o mais importante, pelo menos um dos recursos cuja gestão e aproveitamento estão diretamente relacionados com o sucesso desejado. A informação também é considerada e utilizada em muitas organizações como um fator estruturante e um instrumento de gestão. Portanto, a gestão efetiva de uma organização requer a percepção objetiva e precisa dos valores da informação e do sistema de informação.

Ainda nessa linha, Laureano e Moraes (2005, p.36) acrescentam que “o domínio da informação sempre teve fundamental importância para as corporações do ponto de vista estratégico e empresarial. Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente”.

A importância da informação nas atividades econômicas foi destacada por Cleveland (1983, p.8-9) quando revelou que “Todo o aumento da produção agrícola de meados da década de 1920 até meados dos anos 70 surgiu sem aumento do estoque de capital de recursos físicos. Foi tudo devido a aumentos de produtividade, com a maior parte disso devido a novos conhecimentos ou novas informações.”

Para uma melhor compreensão quanto ao conceito de informação, deve-se levar em conta que a informação é obtida a partir de dados coletados e que passa a fazer a diferença quando se transforma em conhecimento. Davenport e Prusak (1998) simplificam esses três conceitos com a seguinte estrutura:

DADOS	INFORMAÇÃO	CONHECIMENTO
Simples observações sobre o estado do mundo - facilmente estruturado; - facilmente obtido por máquinas; - frequentemente quantificado; - facilmente transferível.	Dados dotados de relevância e propósito - requer unidade de análise; - exige consenso em relação ao significado; - exige necessariamente a mediação humana.	Informação valiosa da mente humana. Inclui reflexão, síntese, contexto. - de difícil estruturação; - de difícil captura em máquinas; - frequentemente tácito; - de difícil transferência.

FIGURA 4 - DADOS, INFORMAÇÃO E CONHECIMENTO

Fonte: Davenport e Prusak (1998)

Os autores acrescentam que, em uma organização moderna, há quatro modalidades ou fluxos de informação: informação não-estruturada, capital intelectual ou conhecimento, informação estruturada em papel, informação estruturada em computadores.

Quanto às modalidades é importante ressaltar que, a despeito da importância da informação estruturada em computadores, esses mesmos autores esclarecem que,

> muitas pesquisas empíricas indicam que os administradores seniores preferem informações que não residem no computador. Vários estudos demonstram que a informação computadorizada não oferece a variedade, a atualidade ou a relevância que esses executivos exigem. Como resultado, a maioria tem nas informações verbais suas fontes mais importantes. [...].

e complementam que

> os administradores tendem a obter de fontes humanas dois terços das informações que usam. A maior parte dessa informação provém de contatos pessoais: o restante, de conversas telefônicas. No outro terço encontra-se a informação estruturada, que em grande parte vem de documentos sobre o ambiente externo, de pesquisas de mercado a revistas do setor industrial [...].

Claro está que as TICs, embora sejam um conjunto de ferramentas que têm capacidade para armazenar, processar e transmitir um grande número de dados em uma velocidade que o ser humano não poderia imitar, não bastam para garantir que as informações sejam realmente utilizadas, pois sua relevância será sempre uma avaliação humana. Para Davenport e Prusak (1998) os computadores e as redes de comunicação oferecem um acesso maior às informações, porém seus recursos são insuficientes para entender, interpretar e agregar valor à informação.

Diferentes conteúdos informacionais podem ser enfatizados por uma organização, conforme o momento que ela atravessa em seu ciclo de negócios ou em seus relacionamentos colaborativos. Os mesmos autores apresentam alguns exemplos desses conteúdos como: a obtenção de informações consistentes sobre produtos dentro das empresas, preços, mercado, logística e, até mesmo, a aquisição de informações sobre funcionários existentes e potenciais.

Em uma visão mais ampla, Davenport e Prusak (1998, p.87) resumem as exigências de informações gerenciais mais comuns na produção de bens e serviços e no acompanhamento de desempenho das organizações.

Produção Cálculo de trabalho Unidades de produção Quantidade de pedidos Especificações dos produtos	**Vendas Marketing** Pedidos Informações sobre clientes Preços de mercado
Compras / Logística Disponibilidade de estoque Preços de insumos e produtos Taxas de transporte e instalação	**Planejamento** Desempenho financeiro Eficácia do programa

FIGURA 5 - RESUMO DAS EXIGÊNCIAS DE INFORMAÇÕES GERENCIAIS

Fonte: Davenport e Prusak (1998)

O comportamento informacional tem estreita ligação com a cultura e as políticas adotadas nas organizações. Para Davenport e Prusak (1998, p.110; 112) a cultura em relação à informação significa o padrão de comportamentos e atitudes que expressam a orientação informacional de uma empresa. Ainda, segundo os autores ”[...] algumas tecnologias amplamente divulgadas podem auxiliar a obter e a disseminar o conhecimento organizacional, mas são de pouca ajuda se o pessoal envolvido ainda não estiver predisposto a usar ativamente a informação.” Sob essa ótica, Wurman (1991, p.42) observa que dados devem estar “imbuídos de forma, e aplicados de modo a se tornar significativos” como informação. Assim, segundo esse projetista de sistemas de informação, a primeira etapa do processo de dotar os dados de significado, transformando-os em informação, é exatamente a agregação de valor, processo esse capaz de incentivar o uso da informação pelos diversos atores no ambiente de negócios das organizações, individualmente ou em seus relacionamentos colaborativos.

Para que o compartilhamento e o uso da informação sejam efetivos e seguros, as organizações precisam estar atentas ao comportamento informacional de seus colaboradores, de seus parceiros e até mesmo de seus clientes. Embora essa não seja uma tarefa fácil, há um conjunto de ações que podem, segundo Davenport e Prusak (1998, p.135), atuar como táticas para que esse gerenciamento produza resultados. Entre essas ações destacam-se a de tornar claros a estratégia e os objetivos das organizações, identificar as competências informacionais necessárias, concentrar-se na administração de tipos específicos de conteúdos da informação, atribuir responsabilidades pelo comportamento informacional, criar um comitê ou uma rede de trabalho para cuidar da questão do comportamento informacional, instruir os funcionários e parceiros a respeito do comportamento informacional e apresentar a todos os problemas do gerenciamento das informações.

Nesse esforço, profissionais da informação, integrantes da equipes de Gestão da Informação - GI, com apoio das equipes de TI, devem ser destacados para agrupar, analisar, tratar, disseminar e armazenar informações que realmente possam dar apoio às decisões do negócio, bem como garantir a segurança do acervo informacional.

Conforme levantamento efetuado entre estudantes de MBA, cujos resultados são citados por Davenport e Prusak (1998, p.149), os profissionais da informação precisam ter os seguintes atributos:

a) compreensão abrangente da área de atuação e conhecimento da estrutura e da função da empresa;

b) conhecimento sobre as diferentes fontes de informação da organização;

c) facilidade de acesso às tecnologias de informação;

d) entendimento político associado à habilidade para exercer liderança;

e) fortes qualificações para relações interpessoais;

f) expressiva orientação para o conjunto do desempenho do negócio, em vez de submissão a objetivos funcionais da organização.

Marchiori (2002, p.79) identifica claramente quem é esse profissional da informação e complementa as habilidades já citadas, quando declara:

> mais do que um conjunto de técnicas e habilidades profissionais, o gestor de informação deve pensar e planejar estrategicamente, estruturar articulações políticas e analisar mercados e contextos. Para tal, exige-se dele alto nível de mobilidade pessoal e profissional, que lhe permita atuar não só como consultor e assessor, cuja competência estará igualmente sendo avaliada conforme seu grau de atualização, capacidade de empreendimentos e criatividade.

A tecnologia, apesar de suas limitações em relação à análise de informações e de sua precariedade quando comparada a atualidade do conjunto de informações que se pode obter no relacionamento pessoal, é uma ferramenta indispensável no processamento, armazenamento e distribuição da informação.

2.3 SEGURANÇA DA INFORMAÇÃO

As inúmeras possibilidades de troca de informações, viabilizadas pela TI, suscitam uma conseqüente preocupação com as questões de segurança nos espaços corporativos internos e em suas ligações com o ambiente em que se inserem, principalmente quanto às operações realizadas com seus parceiros e demais *stakeholders*. D'Andrea (2004, p.257) manifesta sua inquietação em relação

ao problema afirmando que “O enorme potencial para organizações tirarem vantagens a partir das oportunidades da conectividade sem fronteiras traz o desafio de como tratar com segurança as necessidades da inclusão digital dos parceiros de negócio.”

A informação, como elemento de fundamental importância na estratégia das organizações, no desenvolvimento de produtos e serviços e na tomada de decisões, constitui-se em ativo que precisa ser salvaguardado por todos que dela fazem uso ou por ela se responsabilizam. Dias (2003, apud LAUREANO E MOREAES, 2005) lembra que a informação é o principal patrimônio da empresa e que ela está sob constante risco. Atenta a isso, a norma NBR ISO/IEC 27002 (2005) declara que a informação é um ativo importante para os negócios dos setores públicos e privados e, conseqüentemente, necessita ser adequadamente protegida.

A segurança da informação tornou-se, nos últimos anos, assunto recorrente e de grande importância para as organizações, principalmente em função do impacto que pode provocar aos objetivos do negócio, ao seu desempenho e a noção de transparência que precisa passar ao seu público interessado.

Para Ferreira (2003, p.22) o processo de análise de impacto nos negócios contempla:

a) identificação das áreas funcionais mais relevantes (recursos humanos, financeiro, marketing, etc.);

b) análise das ameaças associadas com cada área identificada;

c) determinação do risco associado com a ameaça;

d) identificação das conseqüências que a perda de informação traria aos negócios para períodos específicos de indisponibilidade;

e) detalhamento do impacto da perda da informação;

f) preparação de relação das aplicações e recursos que suportam as funções de negócio, como o sistema de folha de pagamento e seus operadores.

Aos executivos e demais membros da alta administração precisa ser demonstrado como a segurança contribui, por exemplo, ao atendimento a leis e regulamentações, à redução dos custos operacionais, à gestão e a redução dos riscos e das responsabilidades e ao aumento da produtividade.

A importância da preservação do conhecimento das organizações deve ser entendida pelos membros da alta administração, executivos e gerentes das empresas como uma responsabilidade de vital importância para os negócios e para sua própria carreira, conforme explicam Starec, Gomes e Chaves (2006, p.285),

> dado, informação e conhecimento são considerados, por muitos gestores, ativos valiosos de suas empresas. Provavelmente aqueles que ainda não alcançaram esse entendimento o farão em um curto espaço de tempo, ou simplesmente não mais o farão na posição de gestores, após se perceberem inaptos para ocupar essa posição.

D'Andrea (2004, p. 257) explica que apenas a tecnologia não é suficiente para que uma organização atenda suas necessidades em relação à segurança de informação. Os recursos tecnológicos só têm valor quando utilizados de forma estratégica e alinhada aos processos e recursos organizacionais. O autor conclui que os pilares da segurança de informação nas organizações estão fundamentados em tecnologia, processos e pessoas.

Ferreira (2006, p.95) reforça esse raciocínio, invertendo sua ordem de modo a deslocar a tecnologia para a terceira posição na hierarquia dos itens; segundo este autor "a segurança está relacionada a pessoas e processos, antes da tecnologia".

Em face dessa conclusão, pode-se deduzir que uma das formas de garantir a segurança da informação é, também, atuar junto às pessoas que de alguma forma manipulam a informação. Programas de conscientização, treinamento e formalização de termos de confidencialidade são algumas estratégias utilizadas pelas organizações para evitar danos ao seu acervo informacional, com conseqüentes prejuízos econômicos.

Pessoas também podem se envolver em situações relacionadas ao roubo ou a sabotagem dos sistemas de informação da empresa se se sentirem ameaçadas ou, ainda, se perceberem a possibilidade de lucrar com essas ações. Para Austin e Darby (2003, p.89) "a violação do sistema de segurança na maior parte das vezes tem origem dentro da empresa, em funcionários descuidados ou vingativos". Essa ameaça pode gerar dificuldades e prejuízos não apenas ao setor onde o funcionário atua, mas a toda a organização, incluindo seus parceiros, clientes e fornecedores.

Ferreira (2003, p.123) destaca que as estatísticas do FBI (órgão americano equivalente a polícia federal) indicam que 72% dos roubos, fraudes, sabotagens e

acidentes são causados pelos próprios funcionários da organização e que, entre 15% e 20% são causados por terceiros ou consultores formalmente autorizados a acessar as instalações, sistemas e informações da organização. Assim, apenas 5% a 8% dos problemas têm origem externa a organização.

As organizações deveriam premiar os colaboradores por seus cuidados com as questões de segurança, porém poucas o fazem. Os mesmos autores explicam que "a segurança digital é invisível: você sabe que deu certo quando nada acontece. Logo, a recompensa pessoal pelo trabalho bem-feito é pequena."

A dificuldade maior para a proteção da informação está no fato de que ela está em todos os lugares e em diferentes formas, desde meios físicos, como papéis, máquinas e ferramentas até experiências e conhecimentos mantidos pela mente humana, passando, naturalmente, por bits processados por computadores, que circulam nas mais variadas redes.

Uma determinada informação pode exigir da empresa um elevado investimento em sua proteção, principalmente quando comparada ao custo e aos prejuízos que poderiam ser gerados no caso de "vazamento' ou perda da informação.

Em função disso, uma classificação dos ativos de informação deve ser viabilizada. "A informação será classificada baseada na sua capacidade crítica, exigência legais, necessidade de retenção e tipos de acesso requeridos pelos funcionários ou outros colaboradores" (FERREIRA, 2003, p.21)

Uma classificação em relação aos níveis de prioridade que podem ser atribuídos às informações pelos executivos de uma organização é proposta por Boran (1996), Wadlow (2000) e Abreu (2001) (apud LAUREANO e MORAES, 2005). Compartilha dessa mesma estrutura classificatória Ferreira (2003). Para esses autores, a informação pode ser:

a) pública: informação que pode vir a público sem maiores conseqüências danosas ao funcionamento normal da empresa, e cuja integridade não é vital;

b) interna: o acesso livre a este tipo de informação deve ser evitado, embora as conseqüências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital;

c) confidencial: informação restrita aos limites da empresa, cuja divulgação ou perda pode levar ao desequilíbrio operacional e, eventualmente, à perdas financeiras ou de confiabilidade perante o cliente externo;

d) secreta: informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número reduzido de pessoas. A segurança desse tipo de informação é vital para a companhia.

Essa classificação facilita e apóia o emprego do conceito *Need To Know – NTK*, concernente a prática de fornecer a informação apenas a quem dela necessita.

Internamente, as organizações trabalham com autorização, que é o processo de conceder ou negar direitos a usuários ou sistemas, por meio das chamadas listas de controle de acesso *Access Control Lists – ACLs*, definindo quais atividades poderão ser realizadas e produzindo os chamados perfis de acesso.

Conforme explica Ferreira (2003, p.47) os controles de acesso lógico visam assegurar que:

a) acesso apenas aos usuários autorizados;

b) acesso ao usuário apenas quando for realmente necessário para a execução de suas atividades (*NTK*);

c) acesso controlado e restrito aos recursos críticos;

d) impedimento aos usuários para execução de transações incompatíveis com a sua função.

A expansão das fronteiras tecnológicas organizações torna o gerenciamento das identidades de acesso dos usuários um desafio sem precedentes. As organizações têm uma quantidade crescente de identidades para serem gerenciadas, incluindo as que são relacionadas à sua própria força de trabalho e as identidades de acesso atribuídas aos seus fornecedores, parceiros de negócio e clientes.

Os controles de acesso não têm apenas o objetivo de impedir acessos indesejados às informações da empresa, mas também visam identificar os agentes e suas ações no espaço digital da organização e em sua extensão aos espaços

digitais das empresas parceiras, clientes, fornecedores e demais componentes das redes interligadas por empresas.

O tripé básico sobre o qual se apóia a definição de segurança da informação é constituído por critérios como confidencialidade, disponibilidade e integridade. Outros critérios podem ser atribuídos a informação para que o sistema que a administra esteja atento, também, a eles, como autenticidade, legalidade e veracidade.

Beal, (2005, p.1) define os conceitos de confidencialidade, integridade e disponibilidade da seguinte forma:

a) Confidencialidade: garantia de que o acesso à informação é restrito aos seus usuários legítimos;

b) Integridade: garantia da criação legítima e da consistência da informação ao longo do seu ciclo de vida: em especial, prevenção contra criação, alteração ou destruição não autorizada de dados e informações;

c) Disponibilidade: garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna.

A autora exemplifica os fatores citados, com situações comuns no dia-a-dia das organizações e da sociedade:

a) uma informação estatística divulgada pela imprensa, antes que possa ser usada para a tomada de decisão, deverá ter sua autenticidade verificada e sua integridade e disponibilidade protegidas.

b) uma declaração a imprensa deve ter sua integridade protegida, especialmente quanto à autenticidade e quanto ao conteúdo. Nesse caso, questões como confidencialidade e disponibilidade são superadas após a publicação.

c) uma informação relativa à estratégia de negócio deverá ter um rígido controle de acesso durante a elaboração e execução da estratégia.

Mais importante se tornam as questões relacionadas à segurança da informação quando esta tramita em uma rede formada por parceiros de negócios, clientes, acionistas e outros públicos interessados. Assim, algumas regulamentações e orientações ajudam na proteção da informação e até mesmo coíbem práticas que

coloquem em risco a segurança e a sustentação da credibilidade da informação. Entre elas podem ser citadas as normas ABNT e ISO, publicações de conselhos profissionais, Sarbanes Oxley, e o Código Civil. Conforme a NRB ISO IEC 27001-2006 um Sistema de Gerenciamento da Segurança da Informação - SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas.

Com o expressivo aumento da preocupação com a segurança, os executivos já percebem nessas normas o ponto de partida na relação entre a organização, suas divisões internas, seus clientes, parceiros e colaboradores.

A melhor política de segurança, que, conforme define Beal (2005, p.39) é um "conjunto de diretrizes e princípios adotados pela organização para proteger seus ativos de informação" será inútil se clientes, colaboradores, fornecedores e parceiros da empresa a ignorar. Por isso, é importante explicar a lógica por trás das limitações impostas, assegurando-se de que todos os envolvidos estejam conscientes dos riscos e comprometidos com a política adotada.

As organizações têm à disposição, para uso conforme as necessidades e disponibilidade de investimentos, algumas ferramentas que podem ser utilizadas para se desenvolver um processo de acreditação de terceiros,(*trusted third parties*). As ferramentas que ajudam a garantir a segurança digital dos dados que percorrem suas redes incluem o gerenciamento de chaves de criptografia e certificação digital, controles de acesso, *firewalls* e programas de monitoramento. Desnecessário dizer que o emprego dessas ferramentas depende de uma criteriosa análise de ameaças, riscos e impactos que sustentem as soluções de segurança a ser adotadas.

Na questão do desenvolvimento de programas e sistemas de informação, os técnicos precisam estar atentos às necessidades de proteção requeridas, inclusive o controle das versões criadas.

Aconselha Ferreira (2006, p.104) que os riscos inerentes ao processo de desenvolvimento de sistemas sejam minimizados através das seguintes ações:

a) detalhamento na política dos requerimentos de segurança que os sistemas devem atender obrigatoriamente;

b) atualização e armazenamento em local seguro e controlado da documentação do sistema;

c) utilização de trilhas de auditoria nas transações de negócio efetuadas pelos usuários e nos acessos aos códigos-fonte;

d) uso de criptografia de senhas;

e) emprego de interfaces automatizadas entre sistemas objetivando evitar transações incorretas;

f) segregação de funções;

g) Impedimento de acesso de usuários diretamente ao banco de dados de produção;

h) controle de acesso aos códigos fontes, visando evitar versões fraudulentas.

O autor também aconselha que a metodologia seja capaz de estabelecer formalmente os meios de documentação, análise, aprovação, desenvolvimento e homologação.

No âmbito das comunicações corporativas, D'Andrea (2004, p.259) ensina que as soluções web como portais de usuário, portais de fornecedores, *intranets* e extranets foram criados com o objetivo de reduzir custos e aumentar a capacidade colaborativa entre os parceiros de negócio e ampliar a produtividade empresarial. Para ele, a expansão das fronteiras virtuais via *Internet* exigiu mudanças na forma como a Segurança da Informação era tratada nas organizações.

O autor elenca algumas ações que devem ser implementadas pelas organizações em seus processos internos e nos relacionamentos interorganizacionais:

a) garantir que os recursos tecnológicos certos sejam conectados e disponíveis para as pessoas corretas, no momento certo;

b) assegurar que as concessões apropriadas de acesso sejam aprovadas;

c) garantir que o perímetro da organização seja protegido e monitorado;

d) assegurar que o ambiente de sistemas seja confiável e passível de recuperação;

e) assegurar que os ativos de informação atendam aos conceitos básicos de confidencialidade, integridade e disponibilidade.

Dentre o arsenal de ferramentas existentes para proteger a informação, a criptografia de arquivos digitais desempenha um importante papel de auxílio na manutenção da confidencialidade de dados, informação e conhecimento organizacionais. Conforme explica Ferreira (2003, p.61) são dois os modelos de criptografia:

a) Criptografia simétrica ou algoritmo simétrico: usa somente uma chave, tanto para criptografar como para decriptar, sendo conhecido também como algoritmo de chave secreta;

b) Criptografia assimétrica ou algoritmo assimétrico: usa duas chaves: uma pública e outra privada. A pública pode ser distribuída abertamente enquanto a privada é mantida secreta. O funcionamento se baseia na geração do par de chaves - seu detentor deve tornar público e disponível a todos os interessados a sua chave pública. A chave privada deve ficar sempre em sigilo e posse exclusiva do proprietário do par de chaves. A chave pública é utilizada para encriptar os dados, não permitindo sua decriptação, que só será possível com a chave privada.

O mesmo autor ensina que os certificados digitais simplificam a distribuição de chaves públicas garantindo que a pessoa que a está entregando é mesmo quem diz ser. Os certificados digitais funcionam de modo semelhante aos cartórios na vida real, atestando a autenticidade das informações incluídas no certificado. Eles são constituídos pelos seguintes componentes básicos: uma chave pública; informação de certificado (identificação do usuário, dados pessoais e profissionais, contatos, etc.); uma ou mais assinaturas digitais do cartório digital. Os certificados digitais podem ser distribuídos por meio das PKIs.

Para D'Andrea (2000, p.67) o ciclo de vida da segurança tem quatro fases distintas. São elas: avaliar, projetar, implementar e acompanhar. Na fase de avaliar, o objetivo é identificar riscos e vulnerabilidades. Nessa fase é importante analisar o nível de conscientização em segurança da informação das áreas envolvidas, pois existem ameaças específicas provenientes das áreas de negócio e específicas da área de tecnologia. Necessário se faz também identificar as ameaças e riscos de a

instituição não estar preparada para dar continuidade às operações críticas do negócio, dependentes ou não de tecnologia.

O autor define dois tipos de arquitetura de segurança: aberto e fechado. “No modelo de arquitetura aberto, a organização define, com base em sua cultura e modo de operação, o que será proibido do ponto de vista de segurança. Tudo que não estiver especificado está liberado. No modelo de arquitetura de segurança fechado, a organização estabelece para quais informações o acesso será permitido, e o restante estará automaticamente proibido.” (D’ANDREA, 2000, p.67)

Austin e Darby (2003) entendem que uma empresa não tem condições de reagir a toda ameaça à segurança com igual agressividade. Ainda que tivesse, comercialmente não faria sentido. Em vez disso, a gerência deve definir os riscos que apresentam maiores chances de se concretizar e quais causariam maior prejuízo aos negócios. Eles acrescentam que novas ameaças e novas formas de defesa surgem a toda hora. Mas o processo de reflexão sobre o problema não muda.

Internamente, em cada organização, e também no conjunto de empresas que compõem uma rede de colaboração, pessoas responsáveis pela segurança da informação devem atuar em suas respectivas áreas de forma coordenada com o objetivo de somar esforços e complementar as atividades uns dos outros. Mesmo as pessoas, cujas denominações dos cargos não as responsabilizem diretamente pelas questões de segurança, precisam estar envolvidas nesse processo, principalmente quando as decisões que tomam possam afetar positiva ou negativamente a política de segurança de sua empresa ou das empresas parceiras.

Para os integrantes de um ambiente colaborativo, há uma forte percepção de que a segurança da informação está afeta apenas aos aspectos tecnológicos envolvidos, como senhas de acesso, identificação positiva, *time out*, bloqueio de serviços, etc. Porém, não é difícil inferir que, além de conversações fora dos escritórios e por telefone ou *internet*, dispositivos pessoais são fontes de transmissão de informações, de modo intencional ou não, para além das fronteiras tanto de uma organização em particular quanto do ambiente colaborativo. Tais dispositivos incluem *PDAs, notebooks, pen-drives*, câmeras digitais, mais uma grande gama de aparelhos eletrônicos. Complementam essa lista materiais

convencionais como fotocópias, impressos, anotações e documentos diversos pertencentes a qualquer das organizações parceiras.

A tarefa de cuidar da segurança da informação passa por dois conceitos aparentemente antagônicos, sob os quais qualquer medida deve ser criteriosamente analisada: a proteção e o compartilhamento.

Sobre essas duas vertentes no ambiente empresarial D'Andrea (2004, p. 261) faz a seguinte reflexão "O mais relevante é que a segurança é um processo empresarial estratégico para as organizações, pois o equilíbrio entre proteger e habilitar ativos de informação pode melhorar substancialmente o desempenho operacional das organizações. (...)" O autor conclui que

> como um processo estratégico, a segurança tanto protege de danos e de mau-uso os ativos de informação de uma organização, quanto habilita o acesso a esses ativos, dando suporte aos objetivos empresariais. Estes dois conceitos juntos – a segurança excluindo e protegendo, e a segurança incluindo e habilitando – definem com precisão a promessa de valor da segurança para as organizações. A forma e extensão com que é tratado o limite entre esses dois imperativos empresariais determinará o grau de conformidade ao alinhamento estratégico da organização.

Austin e Darby (2003) percebem a transferência da responsabilidade para lidar com a informação digital dos altos executivos para o pessoal técnico ou consultores e reforçam a importância da segurança da informação explicando que sua falha pode interromper operações, afastar clientes e manchar reputações. Não obstante, qualquer impropriedade de acesso pode ser razão suficiente para romper relações comerciais.

À lista acima se podem acrescentar perdas financeiras; abalo na imagem e na credibilidade institucionais, tanto pelo público interno quanto pelo externo; fuga de investimentos e outros.

Conforme o site especializado em TI "*TIinsideOnline*", uma pesquisa realizada pelo Weber Shandwick e a *Economy Intelligence Unit* revelou que 67% dos executivos no mundo inteiro estão com medo de que a reputação de suas empresas esteja em risco. Para esses executivos, a sabotagem de funcionários e o vazamento de informações internas foram muito facilitados pelo crescente uso da internet.

O que a pesquisa expõe nos dá a dimensão do desafio de se desenvolver um plano de segurança capaz de trazer mais tranqüilidade ao ambiente corporativo e ao

colaborativo, especialmente quando nos lembramos de outros agentes potencialmente ameaçadores, como ex-empregados e funcionários de empresas terceirizadas. Nesse contexto, deve-se ter em mente as duas dimensões de delitos possíveis na área de TI: os crimes cometidos com o computador – instrumento do crime – e cometidos contra o computador ou seus programas – objeto do crime.

Para a maioria dos autores pesquisados, a função dos gerentes em todas as áreas é calcular o valor comercial de seus ativos de informação, determinar a probabilidade de tais ativos serem comprometidos e, então, elaborar processos que reduzam as vulnerabilidades detectadas. “A meta não é tornar os sistemas completamente seguros, algo impossível, mas reduzir os riscos a um nível aceitável” (AUSTIN E DARBY, 2003).

Um exemplo de formação de equipe de segurança da informação, com componentes de diferentes áreas, é o caso da GlaxoSmithKline (GSK), laboratório farmacêutico europeu, que segundo Valim (2008), tem um comitê de segurança que integra o coordenador de segurança da informação e telecomunicações, uma pessoa da equipe de segurança patrimonial, uma de recursos humanos e uma do departamento jurídico.

No campo da segurança digital, defesa impenetrável é um conceito inexistente. Com boas práticas operacionais, porém, é possível mitigar os riscos. Uma ameaça que ronda o tráfego de informações entre empresas são os *software* chamados *sniffer* - literalmente um farejador - capaz de “espiar” conversas e obter senhas nas redes que se interconectam (intranets e extranets). Complementando essas ameaças há a questão que se tornou senso comum: Por causa de certa dose de complacência das organizações, colaboradores e funcionários acessam sites potencialmente perigosos, como os pornográficos, a partir de seus computadores, sob a lógica de que não sendo seus equipamentos residenciais não estarão se expondo a ataques de “pragas” virtuais. Esse raciocínio é análogo ao de que se pode descuidar de um imóvel quando este é alugado. O problema é que tal comportamento pode comprometer a rede da organização e até mesmo dos clientes, fornecedores e parceiros que se conectam a ela. Para a maioria dos autores os ataques digitais - principalmente quando usados em combinação – podem, na prática, arruinar uma empresa. Embora seja muito extensa a lista de objetivos desses ataques, podemos citar alguns com maior potencial de danos às

organizações: espionagem industrial, sabotagem de sistemas, sabotagem e vandalismo de dados, obtenção e uso de senhas secretas, artifícios para ocultar computadores com a finalidade de assumir sua identificação na rede e cometer delitos, fraudes e outros.

Algumas ferramentas capazes de ampliar a proteção das informações digitais são:

a) Utilização de firewall: aplicativo que controla o acesso às redes das organizações;

b) Adoção de Redes Privadas Virtuais – *VPNs*: funcionam como túneis virtuais criptografados entre pontos autorizados, criados através da internet, possibilitando a transferência segura de informações entre redes corporativas, usuários remotos e redes interorganizacionais, como no caso das parcerias que admitem acesso aos sistemas informacionais de seus integrantes;

c) Sistemas de detecção de intrusos – *IDSs*: programa executado constantemente em segundo plano a procura de indícios de invasões e que aciona as rotinas pré-definidas pela organização a fim de inibir tal acesso.

d) Antivírus: Identifica e permite segregar (colocar em quarentena) ou destruir programas maliciosos, como os vírus, os worms, os cavalos de tróia e outros malware.

Pastore, Gaudin e Miller (2009) explicam que “alguns profissionais de segurança estimam que metade dos *spyware* nas redes corporativas seja proveniente de acessos de funcionários à sites pornográficos e de jogos” (tradução nossa).

É consenso entre os autores da área que a segurança não deve estar fundamentada apenas em tecnologia, mas, sim, deve ser uma solução integrada ao negócio empresarial e baseada na combinação estratégica de processos, tecnologia e recursos organizacionais, principalmente humanos. Há, também, uma preocupação crescente em se estabelecer trilhas de auditoria necessárias para investigações forenses e para redução do risco de incidentes futuros.

Balizado nesses princípios, torna-se imperiosa a identificação correta das informações no que tange à sua relevância para a organização e à necessidade de sua preservação para que se possam definir as fronteiras dentro das quais a informação poderá circular.

Em relação aos limites que devem ser impostos à informação para que esta se mantenha resguardada do acesso indesejado, D'Andrea (apud VALIM, 2008) sustenta que falta ainda precisão às empresas para, por exemplo, discriminar o que é informação confidencial e para segregar informação, de modo que esta chegue somente a quem realmente precisa utilizá-la.

Embora os custos para garantir a segurança da informação possam ser elevados, estes têm que ser avaliados comparativamente ao prejuízo potencial que teria a organização caso houvesse perda ou vazamento da informação. D'Andrea (2004 p. 262) sintetiza: "Com respeito à proteção, o valor da segurança está diretamente relacionado com o valor total das perdas e danos que foram prevenidos."

Fica claro que um dos grandes desafios na condução dos negócios nas organizações é o de garantir a integridade, a privacidade, a confidencialidade e a disponibilidade dos ativos de informação. Esses ativos precisam ser, com base em uma análise de riscos abrangente, classificados de acordo com a sua criticidade e importância relativa nos processos operacionais da organização.

Conforme Starec (2006, p.288-289) o ciclo de vida da informação passa por quatro fases críticas, que expõem as informações ao risco e, por isso, devem ser diagnosticadas e trabalhadas pelas empresas: manuseio, armazenamento, transporte e descarte.

A avaliação da relação custo-benefício inerente aos investimentos em segurança e ao grau de redução de riscos envolvidos na proteção da informação pode ser visualizada por meio da figura representativa apresentada a seguir.

A aplicação desta ferramenta pode fornecer uma diretriz para adoção de controles de redução de risco.

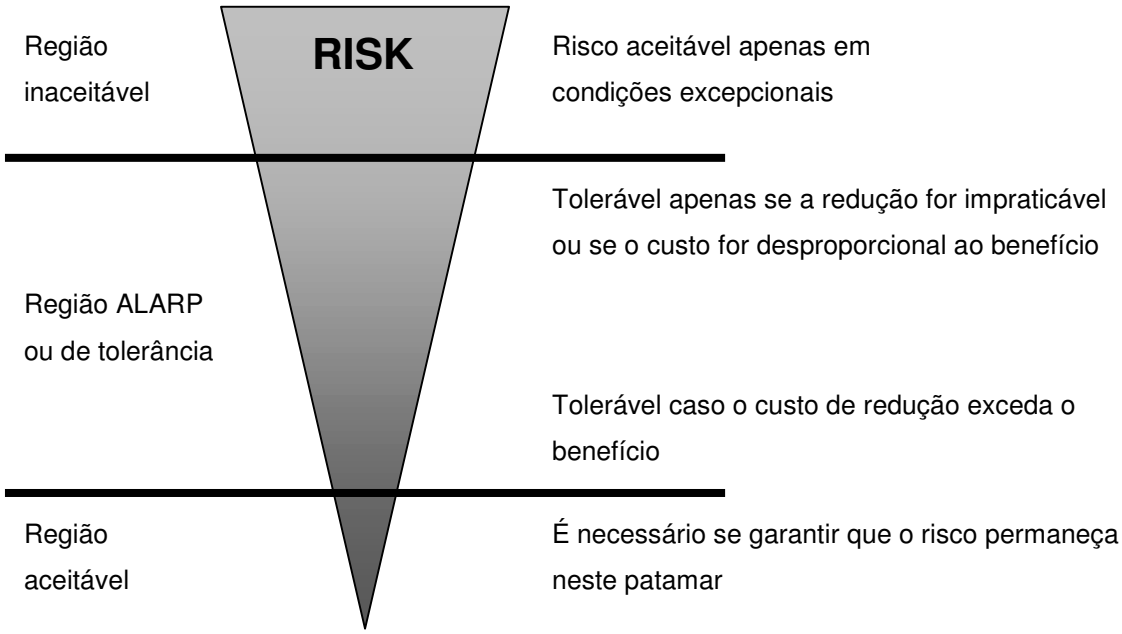

FIGURA 6 - ALARP – AS LOW AS REASONABLY PRACTICABLE

Fonte: < http://gerisco.blogspot.com/2008/03/terceira-onda-da-continuidade-de.html> por F. Saldanha

As ameaças ambientais também devem ser consideradas quanto ao seu potencial de causar danos aos ativos informacionais da organização. Dentre elas destacam-se: fogo, explosivos, fumaça, água, poeira, vibração e interferência no fornecimento elétrico.

Independente dos esforços para que as ameaças sejam neutralizadas, a organização precisa ter um planejamento de continuidade dos negócios, para o caso de alguma ameaça se concretizar provocando a parada de uma ou mais atividades da empresa e até mesmo dos processos colaborativos.

Para Ferreira (2003, p.86) o planejamento da continuidade de negócios é

> o processo de obtenção e análise de informações que gera, como produto final, uma estratégia integrada e seu plano correspondente, para reagir a uma interrupção não programada das atividades do negócio. O principal objetivo é fornecer,em um período de tempo aceitável, todos os recursos necessários para operar os processos críticos de negócio.

O autor explica que os principais objetivos de um Planejamento de Continuidade dos Negócios são:

a) garantir segurança dos empregados e visitantes;

b) minimizar dados imediatos e perdas numa situação de emergência;

c) assegurar a restauração das atividades, instalações e equipamentos o mais rápido possível;

d) assegurar a rápida ativação dos processos de negócio críticos;

e) fornecer conscientização e treinamento para as pessoas-chave encarregadas desta atividade.

Conclui o autor que um plano de contingência deve evitar o comprometimento das operações com os clientes; perda de receita e vantagem competitiva perante a concorrência e multas e sanções legais. Importante frisar que tais comprometimentos também devem atingir às empresas que atuam em colaboração.

Os riscos a que estão submetidos os acervos informacionais devem ser criteriosamente analisados para que as medidas de proteção ou de recuperação sejam planejadas de modo adequado. Para que uma avaliação possa ser obtida de forma correta, Ferreira (2003, p.88) propõe nove passos a ser seguidos:

passo 1 – caracterização dos sistemas;

passo 2 – identificação das ameaças;

passo 3 – identificação de vulnerabilidades;

passo 4 – análise dos controles de segurança;

passo 5 – determinação da probabilidade;

passo 6 – análise de impacto;

passo 7 – determinação do risco;

passo 8 – recomendações dos controles de segurança;

passo 9 – documentação dos resultados.

Ferreira (2006, p.50) apresenta o quadro abaixo, que elenca alguns dos principais itens que compõem um inventário dos ativos de informação:

Natureza do Ativo	Ativos de Informação
Informação	. banco de dados e arquivos magnéticos; . documentação de sistemas e manual do usuário; . material de treinamento; . procedimentos operacionais de recuperação; . planos de continuidade.
Documentos em papel	. contratos; . documentação da empresa; . relatórios confidenciais.
Software	. aplicativos; . sistemas operacionais; . ferramentas de desenvolvimento; . utilitários do sistema.
Físico	. servidores, desktops e notebooks; . impressoras e copiadoras; . equipamentos de comunicação (fax, roteadores); . mídias magnéticas; . gerador, *no-break* e ar-condicionado; . móveis, prédios e salas.
Pessoa	. empregados, estagiários, terceiros e fornecedores.
Serviço ou atividade	. computação (aplicação de *patches*, *backup*); . comunicação (ligações telefônicas, videoconferências); . utilidades gerais.

FIGURA 7 - INVENTÁRIO DOS ATIVOS DE INFORMAÇÃO

Fonte: Ferreira (2006)

Muitas questões relativas à segurança da informação possuem normas que ajudam as organizações a padronizar e controlar as situações de risco. Para algumas instituições a aplicação dessas normas é obrigatória, para outras funcionam como um norte na condução de suas políticas de prevenção e recuperação.

As principais normas de controle e segurança da informação, conforme apresenta Beal (2005) são:

a) *Infomation Technology Infraestruture Library (ITIL)* - Conjunto de melhores práticas para o gerenciamento de serviços em TI;

b) *Control Objectives for Information and Related Technology (COBIT)* - conjunto de práticas que auxiliam a gestão e controles em TI nas empresas. Tem como tema principal a orientação aos negócios;

c) *British Standard* (BS-15000 / *International Organization for Standartization* ISO-20000) - baseada no modelo de processos do ITIL, fornece especificações claras para implementação de processos de gestão de TI;

d) BS 7799 / ISO 17799 – código de práticas de referência para a criação de uma política de segurança;

e) ABNT NBR ISO/IEC 17799:2005 (norma brasileira baseada na ISO 17799) – código de práticas com orientações para gestão da segurança da informação.

f) ABNT NBR ISO/IEC da "família" 27000 – baseadas no modelo de processos ITIL e nas normas ISO atuais, substitui e atualiza essas últimas nas questões de segurança da informação. Seus principais códigos normativos são:

- **ISO 27000** - Publicação que define o vocabulário de Gestão da Segurança da Informação para toda a série ISO-27000,
- **ISO 27001** - Substitui a norma BS 7799-2 para certificação de sistema de gestão de segurança em organizações,
- **ISO 27002** – Substitui (re-nomeia) a ISO 17799:2005 (Código de Boas Práticas),
- **ISO 27003** - Aborda a gestão de risco, com recomendações para a definição e implementação de um sistema de gestão de segurança da informação,
- **ISO 27004** – Fornece padronização para os mecanismos de medição e de relatórios de um sistema de gestão de segurança da informação,
- **ISO 27005** - Indicações para implementação de gerenciamento de risco, monitoramento e melhoria contínua do sistema de controles, tem estreita relação com a BS 7799-3,
- **ISO 27006** – Se refere à recuperação e continuidade de negócio – *IT disaster recovery*.

A série ISO 27000 se alinha à ISO-9001 (Sistemas de gerenciamento da qualidade) e ISO-14001 (Sistemas de gerenciamento do meio-ambiente) em termos de estrutura geral e de ajuste às melhores práticas com os padrões de certificação.

Baseado nessas normas, resume-se, aqui os aspectos fundamentais que devem ser observados pelas organizações para a administração da segurança da informação, tanto no âmbito interno, quanto nos relacionamentos que estas mantêm com as organizações parceiras, clientes, fornecedores, órgãos governamentais e demais públicos interessados:

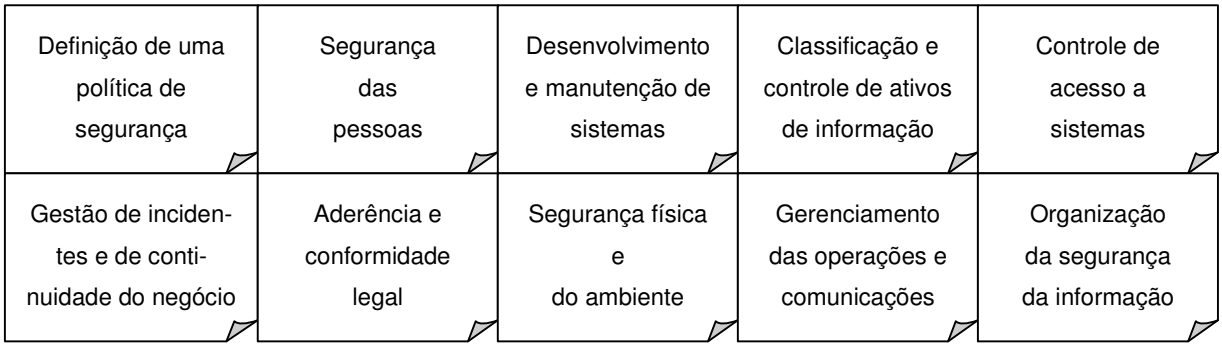

FIGURA 8 - ASPECTOS FUNDAMENTAIS DA SI
Fonte: O autor (baseados nas normas NBR ISO/IEC 27001)

Reforça-se aqui a condição *sine qua non* para implementação de quaisquer normas, medidas ou ações gerenciais em relação à segurança da informação: O envolvimento da alta-administração em cada etapa do processo.

Seguir normas somente não garante que informações possam não ser perdidas ou tornadas inúteis quando necessárias. Segundo o site especializado TI Inside, além das medidas preventivas técnicas, há que se observar também medidas para fazer frente às demandas legais. Em artigo publicado no referido site, com informações fornecidas por Patrícia Peck Pinheiro do escritório PPP advogados, as empresas correm o risco de ter seus servidores apreendidos para elucidar questões legais, o que está amparado pelos artigos 798, 839, 840 e 842 do Código de Processo Civil e artigos 13 e 14 da Lei de *Software* (Lei 9.609/98). Nesses casos, falta conhecimento às empresas para lidar adequadamente com a situação.

Conforme explicou a advogada, os incidentes mais comuns que resultam na apreensão de computadores são, na ordem de freqüência: mau uso da ferramenta de trabalho tecnológica, uso não autorizado da marca na internet, contaminação por vírus ou trojan, vazamento de informação confidencial, problemas com contratos de TI, pirataria e downloads, furto de dados, *cyber/typosquatting*, ofensa de direitos autorais e fraude eletrônica.

Para a advogada as empresas têm de ter cuidado aos usos e costumes que não tenham embasamento legal. "Quem não conhece alguém que imprime um e-mail importante para guardar e apaga o original eletrônico".

A pesquisa realizada pela autora mostrou que os objetos mais freqüentes de ações judiciais são: 43% identificação de autoria; 22% retirada de conteúdo do ar; 12% infração a propriedade intelectual; 9% quebra de acordo de nível de serviço (SLA) e falha de serviço; 5% dados por ofensa na web; 4% desenvolvimento de *software*; 3% fraude eletrônica; 1% abuso de reclamação e 1% contrafação e afins. Contribuiu com o artigo publicado por TI Inside o especialista Alexandre Maiali, para quem as "empresas têm de mapear processos para evitar processos. Geralmente as empresas têm política de backup, mas não de *restore*. É comum ver documentos armazenados que são sobrescritos, com títulos como documento final, documento final 1, documento final revisado". Para esses casos, o planejamento da política de TI é fundamental. O especialista propõe que as empresas tracem um Plano Legal Diretor de Informática que agregue valor jurídico aos documentos desde sua origem.

3 METODOLOGIA

Para que a pesquisa fosse realizada, a definição dos procedimentos metodológicos foi condição fundamental para se alcançar os objetivos almejados.

O presente trabalho pode ser caracterizado como uma pesquisa aplicativa (motivada pela necessidade de resolver problemas concretos; tem finalidade prática) e ao mesmo tempo bibliográfica, visto que está alicerçado por material escrito em livros, sites especializados, artigos científicos e normas ISO/IEC/NBR.

A revisão da literatura visou basicamente verificar quais textos relacionados ao assunto estudado foram publicados e conhecer a forma como esse assunto foi abordado e analisado em estudos anteriores. Também auxiliou na identificação das variáveis do problema em questão.

O método utilizado, conhecido como Estudo de Caso é, conforme define Yin (2001, p.32) “uma investigação empírica de um fenômeno contemporâneo observado na vida real, onde não há uma clara delimitação entre o fenômeno investigado e o contexto em que está inserido”.

O estudo de caso realizado trouxe em seu bojo uma abordagem monográfica, que, conforme define Lakatos e Marconi (2007, p.97) “parte do princípio de que qualquer caso que se estude em profundidade pode ser considerado representativo de muitos outros casos semelhantes. As autoras concluem esse pensamento explicando que esse método “consiste no estudo de determinados indivíduos, profissões, condições, instituições, grupos ou comunidades, com a finalidade de obter generalizações”.

Dessa forma, este trabalho investigou, analisou e teceu considerações sobre as ações e comportamentos empresariais observados na empresa pesquisada, quanto às questões relacionadas à Segurança da Informação no âmbito interno e externo da empresa, notadamente em seus relacionamentos colaborativos, incluindo-se o conjunto dos *stakeholders* com os quais direta ou indiretamente ela se relaciona.

A revisão da literatura foi efetuada a partir da seleção de trabalhos realizados nas áreas de colaboração interorganizacional, gestão da informação e segurança da informação. Inicialmente pretendeu-se estudar artigos relacionados à segurança da

informação no ambiente colaborativo, porém, sem êxito, visto serem escassos trabalhos sobre esse tema.

A literatura utilizada foi obtida em diferentes fontes, como a biblioteca do Setor de Ciências Sociais Aplicadas, artigos disponibilizados pelo orientador (pertencentes ao seu acervo pessoal), portal de periódicos Capes, sites especializados em segurança da informação, material colecionado das diversas disciplinas do curso de Gestão da Informação e livros emprestados por professores.

Durante a leitura de cada fonte de informação, foram extraídos e os trechos considerados mais relevantes ao propósito deste trabalho que, na seqüência, foram digitados conforme sua abordagem, com o cuidado de usar aspas para lembrar que ainda precisariam ser analisados. Também se cuidou para que fossem anotadas todas as referências.

Concluída essa etapa, procedeu-se a análise de cada texto para uma seleção mais apurada em relação aos conteúdos que, depois foram incorporados ao trabalho.

Em relação à aplicação do método de estudo de caso, foram empregados os seguintes instrumentos de pesquisa:

a) leitura de documentos corporativos por meio de pesquisa documental, corrente e retrospectiva, que, conforme Lakatos e Marconi (2007) é a busca de materiais como correspondências, avisos, agendas, relatórios, etc.

b) entrevistas (semi-estruturadas ou não estruturadas):

   - entrevista, que segundo Martins (2009, p.27) é uma “técnica de pesquisa de coleta de dados cujo objetivo básico é entender e compreender o significado que os entrevistados atribuem a questões e situações, em contextos que não foram estruturados anteriormente, com base nas suposições e conjecturas do pesquisador”;

   - as entrevistas tiveram o objetivo de levantar a situação atual da empresa em relação aos procedimentos relacionados à segurança da informação, de modo a verificar, em ambiente real, a prática desses procedimentos. As entrevistas foram estruturadas conforme apêndice A.

c) observação direta: cujos procedimentos, conforme explica Martins (2009, p.23) consiste em “procedimentos empíricos de natureza sensorial” Aconselha o autor que, em um estudo de caso, o próprio pesquisador deve se envolver com o fenômeno e o ambiente pesquisado, i.é, ser um observador participante.

Os métodos de coleta de informações são escolhidos de acordo com a tarefa a ser cumprida. [Bell, 1989].

Antes do início dos trabalhos, porém, foram determinados os dados que devem ser coletados, com base na revisão bibliográfica realizada. Também foi necessário cuidar dos preparativos para a realização dos estudos, que incluíram:

a) autorização de acesso à organização e às pessoas-chave;

b) material necessário: computador pessoal, papel, lápis, clips e um local calmo para tomar notas;

c) envelopes e pastas para transporte do material até o local de estudo;

d) agenda clara das atividades de coleta de dados e respectivo cronograma;

e) obtenção prévia do organograma com nomes e cargos para facilitar os contatos;

f) meios de transporte adequados ao cumprimento do programa;

g) preparo para acontecimentos inesperados, como: mudança de disponibilidade de entrevistados, alterações do humor e da motivação do pesquisador e do entrevistado.

No momento da pesquisa, o papel do pesquisador deve ser claro para quem lhe presta informações, para que seu trabalho não seja confundido com inspeção, avaliação ou supervisão das atividades. Por esse motivo, foi obtida a permissão da diretoria da empresa que formalmente comunicou a todos os colaboradores o papel a ser desempenhado pelo pesquisador.

4 O CASO ESTUDADO

Com o objetivo de observar, na prática, as ameaças a que estão sujeitos os acervos informacionais das organizações, decidiu-se estudar o caso de uma empresa de produção de *software* e aplicar nela métodos de pesquisa que pudessem ajudar no entendimento da questão.

A empresa estudada tem como principal foco de atuação o desenvolvimento de sistemas de gerenciamento empresarial para operadoras de planos de saúde. Sua carteira de clientes se estende por vários estados brasileiros, nas cinco regiões do país.

Inicialmente foi verificada a predisposição da empresa em fazer parte da pesquisa, permitindo que o pesquisador a estudasse em profundidade, em questões que poderiam colocá-la em posição de vulnerabilidade, visto estar-se trabalhando com aspectos de segurança. Para isso, foi assumido o compromisso de que a empresa não seria identificada no trabalho e que os dados apresentados seriam criteriosamente tratados para que uma identificação indireta fosse impedida.

Em seguida foi preparado um protocolo com base nos preceitos expostos por Yin (2001) e demais literaturas pesquisadas, com todos os passos de realização da pesquisa, conforme apêndice B. Esse conjunto de procedimentos auxiliou no seqüenciamento das ações a ser implementadas. O descritivo desses procedimentos pode ser visto abaixo, juntamente com observações quanto a sua execução:

a) obtenção das devidas autorizações para a realização da pesquisa no ambiente de trabalho da empresa, incluindo-se as autorizações para contatos com os colaboradores e análise de documentos, bem como para observação e anotações sobre o desempenho dos trabalhos desenvolvidos no ambiente organizacional;

b) essas autorizações foram obtidas diretamente com diretoria da empresa, sob a condição de fornecimento dos resultados aos seus executivos para que pudessem avaliar seu grau de conformidade com as melhores práticas levantadas no estudo. Outra condição imposta, que já era esperada, diz respeito ao sigilo quanto à identificação da empresa. Ambas as condições foram formalmente aceitas;

c) na etapa seguinte foi levantada a estrutura organizacional da empresa. O objetivo dessa etapa era o de conhecer os setores e colaboradores, a fim de identificar aqueles que possuíssem informações relevantes para a execução dos trabalhos;

d) na seqüência foram definidas as pessoas que responderiam as questões diretamente relacionadas à Segurança da Informação - SI. A escolha dessas pessoas foi feita em conjunto com o diretor da empresa, a quem coube a palavra final sobre o assunto;

e) na etapa seguinte foram definidas as fontes de informação que seriam usadas na pesquisa. Também nessa etapa houve participação direta do diretor da organização. Seguem abaixo algumas fontes onde a busca de informações foi autorizada, precedidas das respectivas ações:

   - análise do portal da empresa;
   - observação do comportamento individual dos colaboradores e suas relações com os clientes;
   - leitura e análise de documentos em arquivo e outros registros impressos;
   - acompanhamento, à distância, de conversas telefônicas;
   - análise de um conjunto de comunicações eletrônicas mantidas através do correio eletrônico da empresa;
   - verificação de registros mantidos pelos colaboradores como apoio às suas atividades, incluindo-se cadernos de anotação, planilhas eletrônicas e agendas.

Para que a técnica da observação participante fosse aplicada, definiu-se os seguintes aspectos a ser observados ao longo da rotina de trabalho de todos os integrantes da empresa estudada:

a) informações repassadas à clientes ou parceiros sobre casos ocorridos com outros clientes ou parceiros (por qualquer meio);

b) cuidados com a proteção de programas-fonte que poderiam ser utilizados e copiados nos ambientes externos à organização;

c) utilização de equipamentos móveis, como *note-books, palmtops, pendrives* e outros;

d) cuidados com o uso de *e-mails*, notadamente no que tange a material anexado e preenchimento dos campos “com cópia – cc” e “com cópia oculta – cco”;

e) sites visitados nos horários de intervalo e de almoço, em que os funcionários ficam livres para utilizar a Internet. (inclui-se aqui especial atenção aos jogos virtuais, sites pornográficos e material ofensivo que possam ser oriundos de endereços eletrônicos da empresa);

f) atenção ou descaso com informações expostas nas telas dos computadores e em documentos sobre as mesas.

A escolha desses aspectos deve-se ao fato de que, conforme levantado na literatura pertinente, referem-se a atitudes que podem comprometer a segurança da informação. Ademais, a abordagem por meio de questionário ou entrevista possivelmente produziria distorções, uma vez que dificilmente um colaborador forneceria respostas que pudessem comprometê-lo, mesmo com o compromisso do pesquisador de que manteria sigilo em relação às informações fornecidas.

A partir da análise dos resultados obtidos nas etapas acima relacionadas, foi elaborado e aplicado um questionário para obtenção de informações complementares (apêndice A).

Diagrama das principais fontes de informação usadas para constatação dos fatos relativos a SI na empresa:

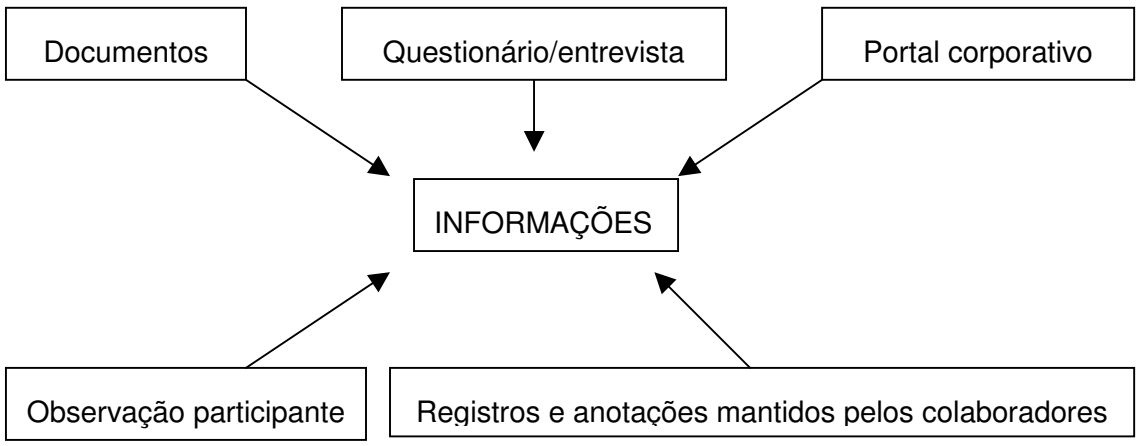

FIGURA 9 - DIAGRAMA DE FONTES DE INFORMAÇÃO
Fonte: o autor

Por meio da comparação do *modus operandi* da empresa com as normas e melhores práticas em SI, conforme o referencial teórico estudado, foi possível identificar algumas vulnerabilidades, bem como itens de conformidade.

Para contextualização, é importante observar que a empresa pesquisada mantém parcerias com empresas congêneres, porém focadas em diferentes nichos de mercado, além de parcerias com fornecedores e clientes que compõem sua cadeia de valor.

As observações feitas *in loco* e a leitura de documentos forneceram exemplos dessas parcerias e permitiram a identificação de práticas colaborativas que ampliam suas competências.

Em um de seus relacionamentos colaborativos, a empresa se associa a outra que também desenvolve *software* para, em conjunto, desenvolver sistemas complexos, onde cada uma fica responsável por um aspecto relacionado ao projeto. Assim, enquanto a empresa pesquisada desenvolve as rotinas e os bancos de dados dos sistemas, a empresa parceira se encarrega de criar módulos capazes de integrar os sistemas desenvolvidos com as ferramentas *web*, de forma a atender a demanda de sistemas gerenciais que permitam aos clientes das empresas clientes utilizar seus portais para agendar consultas, emitir boletos de pagamento, obter informações sobre os profissionais credenciados e receber um grande número de serviços *online*. A empresa estudada acompanha as freqüentes regulamentações emanadas da agência reguladora da atividade de seus clientes, no caso a ANS, e informa sua parceira quanto aos aspectos que devem ser observados em relação à disponibilização dos serviços de saúde *online*.

Esse trabalho conjunto favorece a empresa no desenvolvimento de novas competências, tendo em vista que seus técnicos trabalham em conjunto com os da empresa parceira. A empresa parceira se beneficia igualmente desse trabalho conjunto quando amplia seu conhecimento sobre sistemas de gerenciamento empresarial. Ademais, os contratos em que clientes solicitam ambas as competências são firmados sob a forma de consórcio, onde cada empresa fica responsável por atender as necessidades em sua área de competência, tendo o objetivo comum de atender as demandas do mercado.

Em outro exemplo de parceria, a empresa mantém com alguns de seus clientes uma intensa troca de informações quanto à legislação e novas necessidades das operadoras, utilizando-se de consultores especializados pertencentes aos quadros desses clientes para aprimorar e expandir seus sistemas. Esse comportamento traz benefícios mútuos às empresas envolvidas, visto que as empresas clientes passam a contar com sistemas capazes de atender a todas as suas necessidades, enquanto a empresa fornecedora amplia e aprimora sua uma linha de produtos, com recursos mais abrangentes e soluções que lhe permitem conquistar e fidelizar novos clientes.

Sob a ótica da segurança da informação foi possível constatar que a diretoria da empresa pesquisada tem uma grande preocupação com a segurança da informação que tramita nos ambientes internos e externos da empresa, incluindo-se as informações acessadas de parceiros e clientes, bem como as acessadas por esses últimos.

Mais especificamente no caso da empresa estudada, em função de sua atividade fim – o desenvolvimento de *software* – deve ser seguida uma metodologia que oriente o desenvolvimento de sistemas em consonância com as práticas de segurança da informação, conforme aconselha Ferreira (2006) – ver página 34.

As normas NBR/ISO/IEC 27000 e suas regulamentações declaram que a empresa deve tomar alguns cuidados quando da manutenção e testes de hardware e *software*, principalmente quanto à proteção dos dados contidos em equipamentos submetidos à manutenção, inclusive com a retirada dos discos rígidos.

Em seu relacionamento com empresas parceiras, a empresa formaliza cláusulas contratuais que protejam os processos e programas por ela desenvolvidos, antes do fornecimento dessas informações às empresas que atuam em regime de colaboração, com o cuidado de disponibilizar apenas as informações, códigos e acessos que sejam fundamentais aos objetivos da parceria. Adicionalmente, os contratos firmados também prevêem o cumprimento dos requerimentos previstos em lei, de modo que o desenvolvimento e o produto desenvolvido estejam em conformidade com as normas e regulamentações legais e contratuais. Para isso, a empresa conta com uma assessoria jurídica que trata de toda a documentação necessária, além de fornecer aconselhamento jurídico especializado.

Essa mesma assessoria está, no momento, fornecendo sustentação jurídica para a criação de normas internas que incluam punições aos colaboradores e parceiros que violem os requisitos de segurança estabelecidos pela empresa.

Algumas práticas de proteção da informação já estão consolidadas na organização, porém, é patente a necessidade de formalização de ações que possam mitigar os riscos e neutralizar ameaças a partir de uma política de segurança da informação, com normas, princípios e diretrizes que se coadunem com as atividades e tipo de negócio da empresa.

5 ANÁLISE DOS RESULTADOS

Analisando-se os dados obtidos e confrontando-os com os autores estudados na revisão bibliográfica, percebeu-se que a empresa aplica práticas de segurança em um grande número de suas atividades, porém ainda precisa corrigir processos que apresentam pontos de vulnerabilidade e adequar atividades que estão em oposição às normas e melhores práticas em SI.

Em relação à gestão de pessoas, que para D'Andrea (2004) formam um dos três pilares da segurança da informação nas organizações, junto com processos e tecnologia, há, na empresa estudada, algumas deficiências:

a) inexiste um programa de treinamento específico em relação à segurança da informação para os usuários, tanto os internos quanto os pertencentes aos quadros das empresas parceiras, o que torna o ambiente informacional interno e externo, especialmente o relacionamento colaborativo, extremamente vulnerável. Sobre este quesito, a empresa está construindo um projeto de conscientização e adoção de práticas de segurança;

b) não são formalizadas ou aplicadas quaisquer sanções disciplinares aos colaboradores que ajam de modo negligente ou que façam uso indevido das informações da organização ou das empresas parceiras.

Ainda sob a ótica da gestão de pessoas foram consideradas positivas as seguintes práticas:

a) contratação de funcionários por meio de processos que prevêem a investigação do desempenho e comportamento do candidato em empregos anteriores e a avaliação de seu perfil a partir de entrevistas previamente estruturadas e preenchimento de formulário com dados pessoais que possam ser confirmados pela empresa;

b) nos processos de desligamento de funcionários são suspensas permissões de acesso aos sistemas, ao e-mail corporativo e aos documentos impressos, sendo permitido ao funcionário o retorno ao seu local de trabalho somente para resgate de seus pertences, o que evita ações predatórias por

funcionários vingativos, que, segundo Austin e Darby (2003) podem dar origem a violações do sistema de segurança;

c) uso de termo de confidencialidade incorporado aos contratos de trabalho de todos os colaboradores e parceiros, incluindo-se cláusulas relativas à propriedade intelectual e aos diretos autorais;

d) uso de sistema de controle das comunicações feitas através de contas de e-mail corporativas que permite a identificação dos usuários e destinatários de e-mails que contenham anexos.

Em uma abordagem técnica/operacional/administrativa, foram observados elementos que contribuem de modo eficaz com a SI, entre os quais se destacam:

a) realização de *backups* diários do conteúdo do servidor da empresa, em mídia móvel, armazenada em local externo, conforme preconiza Ferreira (2006);

b) controle de acesso aos arquivos digitais da empresa, por colaboradores e parceiros através de *logins* e senhas;

c) registro dos acessos remotos aos sistemas da empresa, especialmente quando oriundos das empresas parceiras, criando-se trilhas de auditoria que possam revelar eventuais usos indevidos;

d) uso de certificação digital que permite a identificação segura da empresa por órgãos governamentais e por organizações que utilizam essa técnica em seus relacionamentos de negócios, notadamente no ambiente colaborativo;

e) as entradas para dispositivos móveis estão desativadas em todos os computadores, à exceção dos computadores da diretoria;

f) descarte de mídias digitais por meio de incineração dos suportes. Starec (2006) inclui o descarte da informação em seu ciclo de vida da informação;

g) informações confidenciais são criptografadas antes de seu envio em redes externas, a exemplo do que ensina Ferreira (2006);

h) programas de proteção contra “pragas virtuais”, com emprego de firewall e programas anti-vírus/anti-spam são sempre atualizados e mantidos em

funcionamento na rede da empresa, havendo também um servidor Proxy que abriga os arquivos disponibilizados para os parceiros. Igual procedimento é solicitado aos parceiros, porém não há garantias de que efetivamente eles o cumpram. Na verdade, todo o material recebido de empresas parceiras é verificado antes de seu uso;

i) existe um cuidado com as informações expostas nas telas dos computadores e em documentos sobre as mesas;

j) a empresa emprega um mecanismo de segregação de funções no qual cada colaborador é responsável por uma etapa do processo, não conhecendo todos os passos que o compõem, conforme aconselha Ferreira (2006). O mesmo vale para as empresas parceiras que, em contra-partida adotam o mesmo sistema;

k) em caso de envio de equipamentos para manutenção, são retiradas / apagadas informações residentes nos equipamentos;

l) uso de equipamentos do tipo *no-break* nos servidores da empresa para garantia de manutenção das atividades por período de tempo suficiente até que os arquivos sejam salvos, em caso de interrupção repentina de energia. Esse tipo de equipamento é citado por Ferreira (2006) em sua lista de ativos de informação.

Em oposição às boas práticas de segurança, observou-se alguns procedimentos técnicos / operacionais / administrativos, que contribuem para elevação do nível de vulnerabilidade das informações pertencentes à empresa conforme relacionados abaixo:

a) inexiste qualquer preocupação com o descarte de documentos impressos, independente de seu conteúdo. O descarte desses documentos deveria ser controlado, conforme aconselha Starec (2006);

b) as estações de trabalho de colaboradores que lidam com informações confidenciais não são monitoradas por meio de *software* específicos. Nesse caso a empresa utiliza-se, apenas, de um programa de captura de telas para acompanhamento das atividades dos colaboradores;

c) as informações não têm uma classificação formal em relação a sua criticidade para as atividades da empresa ou quanto ao grau de risco a que estão sujeitas, o que caracteriza a não conformidade com as normas NBR ISO/IEC do grupo 27000;

d) embora não haja procedimentos que garantam a proteção do acesso aos sistemas de informação dos clientes e parceiros, a empresa está preocupada com o assunto e pretende adotar medidas para esse fim.

e) não há um inventário dos ativos informacionais da organização que também desconhece a existência de tal inventário nas empresas clientes. Conforme explica Ferreira (2006), esse documento é uma das ferramentas utilizadas na Segurança da Informação;

f) não existe qualquer controle de acesso dos colaboradores aos sistemas das empresas parceiras ou das empresas clientes, o que torna os sistemas desses *players* vulneráveis, independente dos cuidados com a segurança existentes naquelas empresas;

g) os técnicos das empresas parceiras, quando desenvolvem seus sistemas no escritório da empresa pesquisada, não são segregados em sala separada, o que lhes permite observar o trabalho dos colaboradores da empresa e ouvir os contatos telefônicos mantidos com outros parceiros e com os clientes;

h) também não há preocupação com a segurança da informação no que concerne aos visitantes e prestadores de serviços da empresa, o que não se coaduna com as normas que deveriam ser colocadas em prática para maior segurança do acervo informacional, conforme explica Ferreira (2003);

i) inexiste um plano de recuperação de contingências para o caso de algum incidente resultar na interrupção das atividades da empresa, que também desconhece a existência de um plano de contingência nas empresas parceiras. Essa situação torna vulnerável o processo de desenvolvimento de sistemas em que haja dependência do trabalho daquelas empresas. A norma ISO/IEC 27006 determina que se construa um plano de continuidade dos negócios para o caso de ocorrência de contingências;

j) os ativos intangíveis da empresa não possuem qualquer cobertura de seguro;

k) os sistemas da empresa não possuem uma ferramenta de rastreamento capaz de identificar os agentes causadores de problemas, quando o acesso à rede interna é feito através de uma estação de trabalho da própria empresa;

l) ausência de detectores de fumaça que possam acionar mecanismos de controle ou alertar sobre o perigo;

m) não há cofres para a guarda de documentos ou mídias digitais que deveriam ser protegidos;

n) não há uma clara identificação dos “proprietários” da informação, tanto interna quanto externamente em relação aos parceiros e clientes;

o) inexiste normas que definam os sites e procedimentos que não serão aceitos, como: *upload/download* de material ofensivo, que contenham carga preconceituosa ou que externem comportamento ameaçador / violento ou ainda que estejam relacionados a atividades ilegais (essa preocupação também se aplica aos colaboradores das empresas parceiras que trabalham no ambiente interno da empresa pesquisada);

p) a empresa não utiliza programas específicos de acompanhamento das atividades dos colaboradores que lidam com informações confidenciais;

q) não há sistema de Controle de Versão ou de projetos;

r) não existe qualquer procedimento que proteja o acervo informacional do emprego de técnicas de engenharia social.

Alguns aspectos legais também foram analisados durante a pesquisa e, foram considerados pontos positivos os seguintes itens:

a) não é permitida a utilização de cópias ilegais e há o cuidado de se verificar a conformidade de todos os aplicativos em relação à legislação em vigor;

b) igual cuidado é exigido das empresas com as quais a empresa estudada mantém parcerias, por meio de cláusula contratual específica para esse fim;

c) adicionalmente, é exigida a homologação de qualquer sistema desenvolvido em parceria.

O presente estudo de caso demonstrou que a preocupação com a segurança da informação começa a se deslocar do eixo das práticas experimentais e de um conjunto de procedimentos convencionais para o eixo do tratamento profissional e especializado, onde são aplicadas sofisticadas técnicas e metodologias que permitam a minimização dos riscos em níveis aceitáveis, lançando mão de assessoria jurídica e tecnologias modernas para atingir esse objetivo. Também pôde ser observada uma crescente preocupação com o comportamento e as ações das empresas parceiras, no que se refere à proteção de informações sensíveis da organização e aos objetivos das parcerias estabelecidas;

A empresa estudada, cujas características são semelhantes à maioria das empresas que desenvolvem *software* no país - conforme informação de seu diretor - pode ser tomada como exemplo do que ocorre com grande parte das empresas do setor, o que pressupõe a necessidade de maior atenção às questões do gerenciamento da segurança da informação.

6 CONCLUSÕES

Ao longo da literatura estudada foi visto que, por sua natureza dinâmica, a informação que permeia as organizações, interna e externamente, por ser um ativo capaz de proporcionar condições de sustentabilidade dos negócios, deve ser cuidadosamente analisada, contextualizada, armazenada e protegida, de modo a atender à tomada de decisão dos executivos dessas organizações, seus parceiros e público interessado. Não há meios para evitar todas as ameaças que rondam o acervo informacional das organizações, porém, algumas medidas podem reduzir os riscos e evitar maiores prejuízos. Evidenciou-se que, tanto no âmbito de seus processos internos, quanto no de seus parceiros, a segurança da informação só será garantida se for construída uma cultura que estimule um comportamento seguro e alinhe as ações de segurança aos objetivos do negócio. Para que essa condição seja alcançada será necessária a participação de todos os colaboradores da organização e, sobretudo, o efetivo comprometimento da alta direção.

Qualquer normatização que objetive a manutenção dos aspectos centrais de confidencialidade, integridade e disponibilidade de ativos de informação precisam ser permanentemente reavaliadas e revisadas, tendo em vista as mudanças que se operam nos ambientes de negócios e a constante evolução das técnicas de invasão de sistemas.

Ademais, a pesquisa mostrou que embora as informações em meios digitais sejam as que atraem maior atenção dos executivos para o estabelecimento de mecanismos de proteção, outros registros informacionais também são merecedores de igual atenção, podendo-se citar os documentos impressos, como contratos, relatórios, manuais técnicos, etc. Independente do formato da informação, riscos físicos, como incêndio, enchente, roubo de equipamentos e outros podem se concretizar, prejudicando seriamente as atividades da organização.

Uma das mais importantes constatações que este estudo permitiu diz respeito à participação humana como principal fonte de vulnerabilidade das ações e políticas de segurança da informação. O comportamento das pessoas e suas condições psicológicas podem abrir brechas que comprometam a segurança. A engenharia social é um dos instrumentos que exploram essas condições.

Assim, o treinamento e a conscientização dos colaboradores, dos parceiros de negócios e dos clientes – como no caso da empresa estudada - são fundamentais para a redução dos riscos.

A realização do estudo de caso permitiu a confrontação dos conceitos obtidos na literatura com a prática de segurança em uma empresa de desenvolvimento de *software* de Curitiba. Pode-se notar que algumas vezes o problema foi tratado da forma considerada adequada, porém, em outras, a empresa utiliza métodos baseados em sua própria percepção sobre o problema e sobre a forma de se proteger.

Por fim, constatou-se que não é possível às organizações se protegerem de todas as ameaças ao seu acervo informacional e, portanto, cada risco deve ser analisado em relação à possibilidade de sua concretização e ao conseqüente prejuízo que possa dela advir. A partir daí será possível estabelecer parâmetros de custo para as ações de proteção a ser adotadas.

7 CONSIDERAÇÕES FINAIS

O principal problema que motivou o presente trabalho foi a necessidade de se refletir sobre as questões relacionadas ao tratamento da informação nas organizações e em seus relacionamentos colaborativos.

Como objetivo geral ficou estabelecido que fossem apresentados elementos que pudessem contribuir para a redução dos riscos informacionais em ambientes intra e interorganizacionais.

Em relação aos objetivos específicos definiu-se que seriam apresentados, com base na literatura, procedimentos para a melhoria da segurança das informações que permeiam o relacionamento interorganizacional bem como para a proteção do acervo informacional das organizações, apontando formas de redução de vulnerabilidades.

Esses objetivos foram alcançados através da pesquisa bibliográfica, onde os diversos autores apresentaram métodos e técnicas de segurança da informação, cuja análise permitiu a realização do estudo de caso em uma empresa de desenvolvimento de *software* na cidade de Curitiba. Procedeu-se, então, a uma investigação aprofundada das questões referentes à segurança informacional da empresa em relação às suas atividades internas e às atividades colaborativas existentes entre esta e seus parceiros de negócios.

O resultado do estudo de caso demonstrou a preocupação da empresa pesquisada quanto à segurança da informação e sua postura diante do desafio para mitigar os riscos a que está sujeito seu acervo informacional, que, nesse caso específico, compreende inclusive seu principal ativo: os programas e sistemas desenvolvidos pela empresa e por seus parceiros.

Este trabalho poderá servir de ferramenta para que as pessoas que tenham interesse no assunto da segurança da informação possam compreender as questões básicas que envolvem o tema.

8 LIMITAÇÕES E FUTURAS OPORTUNIDADES DE APROFUNDAMENTO DOS ESTUDOS

Um estudo dessa natureza esbarra em limitações impostas pelas próprias organizações, que, por razões óbvias, não podem disponibilizar todas as informações quanto aos seus procedimentos de segurança. Por outro lado, há material bibliográfico que trata do assunto, além de fóruns de discussão, congressos e outros eventos com o mesmo tema.

Maior abrangência desse estudo poderia ser obtida caso fossem realizados mais estudos de caso sobre como as organizações estruturam seus procedimentos e normas relacionadas à segurança da informação.

Por ser uma área instigante da Gestão da Informação, há interesse em dar prosseguimento a este trabalho, ampliando a pesquisa, procurando novas empresas onde verificar mecanismos de segurança e participando de eventos que tragam novos conhecimentos sobre o tema.

REFERÊNCIAS

ALBERTIN, A. **Comércio eletrônico**: modelo, aspectos e contribuições de sua aplicação. 5. ed. São Paulo: Atlas, 2004.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Tecnologia da informação - Técnicas de segurança - Código de pratica para a gestão de segurança da informação. Rio de Janeiro, 2005.

AUSTIN, Robert; DARBY, Christopher. The mith of Secure Computing. **Harvard Business Review**, [*S.l.*] p. 12-126, June 2003.

BAKOS, Y.; BRYNJOLFSSON, E. Organizational partnership and the virtual corporation. In: **Information technology and industrial competitiveness**: how Information technology shapes competition. [*S.l.*]: Kluwer Academic Publishers, 1997.

BEAL, Adriana. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BELL, Judith. **Doing your research project**: a guide for the first-time researchers in education and social science. England: Open University Press, 1989.

CARR, N. It doesn't matter. **Harvard Business Review**, [*S.l.*] May 2003.

CASTILHO, N. C. **Tecnologia de informação e colaboração interorganizacional**: um estudo no varejo de grande porte no setor de confecção. São Paulo, 2005. Tese (Doutorado em Administração) EAESP.

CLEVELAND, Harlan. A Informação como um recurso. **Diálogo,** Rio de Janeiro, v.16, n.3, p.7-11, 1983.

D'ANDREA, Edgar R. P. Segurança da informação: uma visão estratégica para as organizações. In: ALBERTIN, Alberto; MOURA, Rosa (Orgs). **Tecnologia de informação**. São Paulo: Atlas, 2004. p.253-277.

D'ANDREA, Edgar R. P. **Segurança em Banco Eletrônico**. São Paulo: PricewaterhouseCoopers, 2000.

DAS, T.; TENG, B. A Resource-based theory of strategic alliances. **Journal of Management,** v. 26, n 1, p. 31-61, 2000.

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

EINSEHARDT, K.; SCHOONHOVEN, C. Resource-based view of strategic alliance formation: strategic and social effects of entrepreneurial firms. **Organization Science**, [*S.l.*], v. 7, p. 136-50, 1996.

FAULKNER, D. International Strategic Alliances: Co-operating to Compete. **Maidenhead**: McGraw-Hill, 1995.

FAULKNER, D. O.; ROND, M. **Cooperative strategy**: economic, business, and organizational issues. Oxford: Oxford University Press, 2000. 397p.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação**. Rio de Janeiro: Editora Ciência Moderna, 2003.

FERREIRA, Fernando; TADEU, Marcio. Política **de Segurança da Informação**: guia prático para embalagem e implementação. Rio de Janeiro: Editora Ciência Moderna, 2006.

GRANOVETTER, M. Economic action and social structure: The problem of embeddedness. **American Journal of sociology**, [S.l.], v. 91, n. 3, p. 481-510, 1985.

GRANOVETTER, Mark. **Ação econômica e estrutura social**: o problema da incrustação. In: MARQUES, R; PEIXOTO, J. (Org.) A nova sociologia econômica. [*S.l.*] Celta, Deiras, 2003. p.69-102.

GULATI, R. Alliances and networks. **Strategic Management Journal,** Hoboken, NJ v. 19, p.293–317. 1998.

HAMEL, G. Competition for competence and interpartner learning within international strategic alliance. **Strategic Management Journal**, [*S.l.*], v. 12, p. 83-103, 1991

HOFSTEDE, G. **Culturas e Organizações**: Compreender a nossa programação mental. Silabo: Lisboa. 1991.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 17799:2005** Information technology — Security techniques — Code of practice for information security management. [*S.l.*], 2005.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27006:2007**: Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems. [*S.l.*], 2007.

JARILLO, J. On Strategic Networks. **Strategic Management Journal**, [S.l.], v. 9, p.31-41, 1988.

JOHNSTON, H.; VITALE, M. Creating competitive advantage with interorganizational information systems. **MIS Quarterly**, Minneapolis, v.12, n.2, p. 153-65, 1988.

KNIGHT, L. Learning to Collaborate: a study of individual and organizational learning, and Interorganizational Relationships. **Journal of Strategic Marketing**, [S.l.], v. 8, p. 121-38, 2000.

KNIGHT, L. Network learning: exploring learning by interorganizational networks, **Human Relations, v**.55, n 4. 2002.

KOGUT, B. Joint Ventures: Theoretical and empirical perspectives. **Strategic Management Journal,** [*S.l.*], v. 9, p. 319, 332, 1988.

LAKATOS Eva Maria; MARCONI, Marina de Andrade. **Metodologia Científica**. São Paulo: Atlas. 2007.

LAUREANO, Marcos Aurélio Pchek, MORAES Paulo Eduardo Sobreira. Segurança como estratégia de Gestão da Informação. **Revista Economia e Tecnologia**, São Paulo, v. 8, n.3, p.38-44, 2005.

MARCHIORI, Patrícia Zeni. A ciência da informação: compatibilidades no espaço profissional. **Ciência da Informação**, Brasília, v.31, n.2, p.72-79, maio/ago.2002.

MARTINS, Gilberto. **Estudo de Caso: uma estratégia de pesquisa**. São Paulo: Atlas, 2009. 102p.

MORESI, Eduardo Amadeu Dutra. **Ci. Inf.** Brasília, v.29 n.1, p.14-24, jan./abr. 2000.

NIEDERFOFLER, M. **The Evolution of Strategic Alliances**: Opportunities for managerial Influence. Journal of Business Venturing, v6 i4. p. 237-257, 1991.

PARA EXECUTIVOS, reputação das empresas corre mais riscos com a web. **TI Inside Online**. Disponível em <http://www.tiinside.com.br/News.aspx?ID=117198&C=265>. Acesso em: 06 fev 2009.

PARKHE, A. Messy research, methodological predispositions, and theory development in international joint ventures. **Academy of Management Review**, [*S.l.*], v. 18, p. 227 - 268, 1993.

_____. **Empresas precisam implantar melhores práticas de segurança**, alerta advogada. Disponível em <http://www.tiinside.com.br/News.aspx?ID=132884&C=265>. Acesso em 30 maio 2009.

PASTORE M.; GAUDIN S.; MILLER D. **Inside Spyware**: A guide to finding, removing and preventing online pests. Disponível em: <http://www.scribd.com/doc/7364774/A-guide-to-findingremoving-and-preventing-onlive-pest>. Acesso em: 25 fev 2009.

PFEFFER, J. **Organizations and organization theory**. Cambridge: Ballinger Publishing Co., UK. 1982.

PORTER, M. E. **Estratégia Competitiva**: técnicas para Análise de Indústrias e da Concorrência. Campus: Rio de Janeiro, 1985.

PORTER, M.; FULLER, M. Coalitions and Global Strategy, In: M. Porter (ed.). **Competition in Global Industries**. Boston: Harvard Business School Press, 1986.

_____. **Vantagem Competitiva**: Criando e Sustentando um Desempenho Superior. Campus: Rio de Janeiro, 1980.

POWELL, W. Neither Markets nor Hierarchy: Network forms of organization. In: STAW, B.; CUMMINGS, L. (Eds.) **Research in Organizational Behavior**. Greenwich, CT: JAI Press, 1990, v. 12, p. 295-336.

SAMPLER, J. Redefining Industry Structure for the Information Age. **Stategic Management Journal,** USA, v. 19, p. 343-355, 1998.

SILVA, Welington. D. F. da. **Introdução à gestão da informação**. Campinas, Alínea: 2003.

SMITH, K.; CARROLL, S.; ASHFORD, S. Intra- and Inter-organizational Cooperation: Toward a research Agenda. **Academy of Management Journal**, [*S.l.*], v. 38, n.1, p. 7-23, 1995.

STAREC, Cláudio; GOMES, Elisabeth B. P.; CHAVES, Jorge B. L.. Gestão Estratégica da Informação e Inteligência Competitiva In:_____(Org). **Gestão da segurança da informação**. São Paulo: Saraiva, 2006.

VALIM, Carlos Eduardo. **Acesso negado**. Disponível em <www.informationweek.com.br/ noticias/artigo.asp?id=26876>. Acesso em: 12 dez, 2008.

WEBSTER, Frederick E., Jr. The Changing Role of Marketing in the Corporation**. Journal of Marketing**, Chigago v.56, n.3, Out., 1992.

WURMAN, Richard Saul. **Ansiedade de informação**: como transformar informação em compreensão. São Paulo: Cultura Editores Associados, 1991.

YIN, R. K. **Estudo de caso**: planejamento e métodos. Tradução Daniel Grassi. 2. ed. Porto Alegre: Bookman, 2001.

APÊNDICE A – Roteiro de entrevista

Aplicado ao diretor da empresa

Com o objetivo de levantar o comportamento da organização em relação à segurança da informação e suas preocupações com a proteção de seu ativo informacional, foi aplicado o questionário abaixo, cujas respostas deram origem às análises apresentadas anteriormente, resultando em uma visão aprofundada da situação da empresa.

Aspectos relacionados às pessoas:

A empresa exige a assinatura de termo de confidencialidade de seus funcionários?

O acesso físico e lógico aos ativos de informação é retirado no momento do desligamento de um colaborador?

Há algum controle dos e-mails da empresa?

Há processos adequados para a contratação de pessoal, como investigação de antecedentes de colaboradores e prestadores de serviço?

Há um programa de treinamento e conscientização dos colaboradores quanto à importância e os procedimentos de segurança da informação?

Há uma política de sanções disciplinares que coíba a negligência ou o uso indevido da informação da empresa ou de seus parceiros?

Aspectos técnicos:

A empresa possui uma sistemática para a realização de backups?

Há medidas de proteção para o acesso remoto de um funcionário à rede interna?

Nesse caso, os acessos remotos são registrados para obtenção de trilhas de auditoria.

A empresa utiliza certificação digital em procedimentos sensíveis junto aos seus parceiros ou outros órgãos?

Aspectos técnicos/operacionais:

Os procedimentos de backup e restauração estão devidamente documentados e os responsáveis por sua execução formalmente identificados?

Como a empresa controla o uso de pendrives e outras mídias removíveis?

O descarte de documentos e mídias é feito de forma segura?

A empresa adota soluções de criptografia para informações confidenciais?

Há procedimentos de segurança para o descarte de documentos impressos?

As estações de trabalho de colaboradores que lidam com informações confidenciais são monitoradas por meio de *software* específicos?

Aspectos legais

Os sistemas desenvolvidos por seus parceiros estão em conformidade com as exigências legais?

É permitida a utilização de sotfware pirata pela empresa ou por seus parceiros?

Recursos

A empresa utiliza programas de proteção contra pragas virtuais e exige esse comportamento de seus parceiros?

Aspectos administrativos

A empresa classifica seus ativos de informação conforme o nível de criticidade, vulnerabilidade e confidencialidade?

Em função da possibilidade de acesso aos sistemas de informação dos clientes e parceiros, há procedimentos que garantam a proteção dessas informações?

Há uma política de mesa limpa e tela limpa?

A empresa adota o método de segregação de funções para evitar que um determinado colaborador administre todas as etapas de um processo?

Há normas que coíbam ações de roubo de informação por terceiros que visitam o ambiente organizacional?

Há um inventário dos ativos informacionais?

Aplicado aos colaboradores

Complementarmente ao questionário aplicado à diretoria da empresa, foi aplicado aos colaboradores o questionário que se segue:

Aspectos técnicos/operacionais/administrativos:

Há algum cuidado adotado para o envio de equipamentos para manutenção?

Você envia e-mails com todos os destinatários no campo para ou no campo com cópia?

Você já recebeu algum treinamento da empresa sobre a prevenção de ações de engenharia social?

APÊNDICE B – Protocolo para o estudo de caso

Protocolo

1- Obtenção de autorização para realização da pesquisa;

2- Levantamento da estrutura organizacional da empresa;

3- Escolha dos colaboradores que responderiam às questões levantadas;

4- Definição das fontes de informação;

5- Preparação do questionário (apêndice 1);

6- Confrontamento do modo de operação da empresa com as melhores práticas em SI levantadas na pesquisa.