

A SEGURANÇA DA INFORMAÇÃO E A GERAÇÃO DE DIFERENCIAL COMPETITIVO

RESUMO DO ARTIGO

Este artigo trata do estudo sobre Segurança da Informação (SI) e sua importância como gerador de diferencial competitivo para organizações do segmento de Telecomunicações e Informática no Brasil, através da aplicação de conceitos que integram a segurança física e lógica, o treinamento e a conscientização das pessoas, buscando a otimização das ferramentas de tecnologia que visam proteger a informação.

O método utilizado foi o hipotético-dedutivo (POPPER, 1975). O referencial teórico usado foi o modelo de análise da concorrência previsto por Porter (1986) e a BS 7799-2:2002. Para cada uma das 3 hipóteses foram desenvolvidas questões-chave, que permitiram a verificação e validação em pesquisa de campo. A coleta e análise dos dados que forneceram respostas às questões-chave através dos seguintes resultados:

- Mais de 50% dos executivos entrevistados consideraram a SI fator crítico e o maior obstáculo para sua implementação nas empresas, foi a falta de consciência da direção e a falta de orçamento para aquisição e instalação dos dispositivos;

A geração de diferencial competitivo, ainda não pode ser percebida claramente nos segmentos estudados, pois os investimentos feitos pelas empresas ainda são pequena parte do montante destinado à área de Tecnologia da Informação, que não passa de 5 % do orçamento total da empresa.

Palavras chave: Segurança da Informação, Modelo de Gestão de TI, Tecnologia da Informação, Planejamento de Segurança da Informação e Análise de Risco.

A tecnologia da informação constitui um instrumento poderoso dentro das organizações nos tempos atuais. A ligação com a *Internet* e a adoção da *Intranet* se propaga de forma intensa. A informação torna-se a principal fonte de energia dentro das organizações e, portanto, a mais cobiçada também. Na idade da informação as coisas mudam rápida e incessantemente, quem tem informação passa a ter o poder. Poder de conhecer o concorrente, poder de resolver mais rápido um problema e poder de aprender com os seus erros mais facilmente. E este bem tão precioso, não deixa de ser perseguido de forma correta ou de forma ilícita, e precisa ser protegido. Sua proteção não fica só na condição de evitar que a informação seja roubada, mas também que ela esteja sempre disponível quando necessária, para quem tem autorização para utilizá-la e recuperada com agilidade e com confiabilidade. Para isto, é necessário identificar alguns dispositivos para gestão da segurança da informação, estes devem estar inseridos em um modelo universal de gestão de segurança da informação em conformidade com a norma BS 7799-2:2002, que orienta a implementação de um sistema de gestão de segurança da informação que visa garantir :

Confidencialidade - é a propriedade que visa manter o sigilo, o segredo ou a privacidade das informações evitando que as pessoas, entidades ou programas não-autorizados tenham acesso às mesmas (MOREIRA, 2001).

Integridade - Consiste em proteger a informação contra qualquer tipo de alteração sem a autorização explícita do autor da mesma (MOREIRA, 2001).

Disponibilidade - A informação deve estar disponível para a pessoa certa e no momento em que ela precisar (MOREIRA, 2001).

A situação problema do presente trabalho pode ser equacionada pela seguinte questão: Será que a aplicação do modelo de gestão de segurança da informação previsto no *framework* da BS 7799, por tratar de forma integrada a segurança física e lógica, o treinamento e a conscientização das pessoas, o entendimento dos processos críticos de negócio garantindo sua continuidade e as ferramentas de tecnologia da informação, organiza um sistema de segurança da informação que trará maiores garantias de continuidade do negócio e melhores resultados às empresas?

Para responder a esta pergunta foram entrevistadas empresas públicas e privadas que participaram da 8ª. Pesquisa Nacional da sobre Segurança da Informação, realizada pela Módulo *Security Solutions S.A* no ano de 2002.

OBJETIVOS DO ESTUDO

O trabalho se propôs discutir as questões ligadas a:

- Identificar como a implementação de um Sistema de Gestão de Segurança da Informação pode funcionar como diferencial competitivo perante o mercado.
- Identificar empresas que já aplicam os princípios de gestão de segurança da informação e verificar quais os procedimentos que são percebidos pelos gestores e clientes como garantias de segurança e continuidade do negócio.
- Estudar o modelo de gestão de segurança da informação previsto no *framework* da BS7799, como padrão de excelência para implementação de um sistema de gestão de segurança da informação que considera os aspectos físicos, lógicos e humanos da segurança da informação.

O estudo do *framework* previsto na BS7799, foi focado no aspecto global de gestão, observando os requisitos referentes da norma que tratam da gestão da segurança da informação e seus respectivos controles. A discussão das questões sobre a gestão da continuidade do negócio estará pautada no estudo de suas características e na identificação de quais os processos e ativos que precisam de manutenção, além da identificação de argumentos que façam o pessoal da organização encarar a equipe da segurança como profissionais que contribuem para continuidade do negócio por intermédio da prevenção e não como eventuais solucionadores de problemas de segurança, quando ocorrem crises internas ou invasões (ANTUNES, 2002).

O método aplicado para realização do trabalho de pesquisa foi o método hipotético dedutivo baseado na proposta de Popper (1975), onde as fases do processo investigatório são sintetizadas na constatação de um problema – que pode ser originado dos conflitos diante de expectativas ou teorias existentes – da proposição de uma solução ou explicação testável para o mesmo – e de sua submissão a testes de falseamento, onde se tentará refutar seja pela observação ou pela experimentação, a hipótese proposta.

Para desenvolver o estudo foram enunciadas as seguintes hipóteses relacionadas as questões-chave:

HIPÓTESES	QUESTÕES-CHAVE
1. O uso das práticas de Segurança da Informação gera percepção de diferencial competitivo perante o mercado.	<p>Questão 1: Quais as vantagens competitivas identificadas pelo uso da Segurança da Informação ?</p> <p>Questão 2: Qual tipo de diferenciação que um sistema de gestão de segurança da informação pode gerar?</p> <p>Questão 3: Qual a relevância da obtenção de certificação internacional em segurança da informação - BS 7799?</p>
2. Existem barreiras sócio-culturais que dificultam a implementação do sistema de gestão de segurança da informação nas organizações.	<p>Questão 1: Quais argumentos para convencer a alta direção de uma organização da importância da implantação de um sistema de gestão de segurança da informação?</p> <p>Questão 2: Qual o grau de comprometimento das organizações com o sistema de gestão de segurança da informação implantado?</p>

	Questão 3: Quais os investimentos em Segurança da Informação feitos pelas organizações?
3. Há uma relação sistêmica entre os princípios que norteiam a implementação de um sistema de gestão da segurança da informação e os princípios que norteiam a implementação de um sistema de gestão da qualidade.	Questão 1: Quais os benefícios de implementar um sistema de gestão de segurança da informação? Questão 2: Como implementar o sistema de gestão de segurança da informação baseado no sistema de gestão da qualidade? Questão 3: É possível aplicar o PDCA (princípio da qualidade – Plan, Do, Check and Act – planejar, executar, verificar e agir corretivamente) no sistema de gestão de segurança da informação?

Quadro 1 - HIPÓTESES X QUESTÕES-CHAVE
Fonte: (CARVALHO, 2003, p.28)

REFERENCIAL TEÓRICO

O referencial teórico relacionado neste trabalho de pesquisa foi selecionado com base em pesquisa do autor entre as obras mais citadas no que diz respeito a Segurança da Informação, e são os seguintes:

Modelo de Excelência das Normas ISO 17799 e BS 7799

As normas ISO 17799 e BS 7799 são padrões de excelência internacional que orientam a organização do Sistema de Gestão de Segurança da Informação (SGSI).

Devemos observar que o desenvolvimento e implantação de um Sistema de Gestão de Segurança da Informação, além da organização da documentação exige a implementação de controles para atender aos objetivos de segurança da organização. Para isto, devem ser executados os 6 passos previstos no *framework* apresentado na BS7799:1999, parte 2. Estes passos são:

1. Definição da Política de Segurança da Informação – documento que contém de forma clara e resumida as premissas e diretrizes do Sistema de Gestão de Segurança da Informação;

2. Definição do Escopo do Sistema de Gestão de Segurança da Informação – que é o perímetro de abrangência que define os ativos que serão contemplados no SGSI, sejam eles sistemas, dispositivos físicos, processos ou ações do pessoal envolvido;
3. Análise de Risco – que abrange a identificação das ameaças e vulnerabilidades para os ativos cobertos pelo escopo definido, os possíveis incidentes de segurança que poderão ocorrer a partir da ação das ameaças sobre as vulnerabilidades encontradas e seus impactos no negócio. A metodologia utilizada para elaboração desta análise deve ser documentada, os critérios para identificação dos riscos precisam ser registrados e inseridos no sistema de documentação;
4. Gestão do Risco – definição do processo de gestão dos riscos identificados e critérios para atribuição das prioridades e relação custo benefício de cada ação recomendada;
5. Seleção dos Controles a serem implementados e seus respectivos objetivos. Os controle estarão apresentados em 10 itens que agrupam as principais áreas de atuação da segurança da informação: política de segurança, segurança organizacional, classificação e controle dos ativos de informação, segurança por intermédio das pessoas, segurança física e do ambiente, gerenciamento de operações e comunicações, controle de acesso, desenvolvimento de manutenção de sistemas, gestão da continuidade do negócio e conformidade legal;
6. Preparação da Declaração de Aplicabilidade – que é a justificativa clara de quais itens da norma BS7799 são aplicáveis e serão desdobrados dentro do Sistema de Gestão de Segurança da Informação da organização.

A declaração da aplicabilidade resume os passos anteriores e complementa o escopo para certificação. É também um norte para evitar que se definam controles em excesso ou que se deixe desprotegido algum ativo importante para a organização.

Gerenciamento Estratégico da Segurança da Informação

A segurança da informação deve proteger a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, visando minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio. O sistema de proteção da informação deve considerar aspectos ligados a: segurança física da informação, segurança lógica, segurança das relações financeiras, garantia da reputação e imagem da organização, aspectos legais, comportamento dos funcionários, e para com os funcionários, e todos os ativos tangíveis e intangíveis (PELTIER, 2001).

A gestão da segurança da informação necessita da participação de todos os funcionários da organização. Pode ser que seja necessária também a participação de fornecedores, clientes e acionistas. Entretanto, as metas, objetivos, direção, incentivos e definição dos papéis e responsabilidades em relação à consecução segurança da informação, devem vir da alta direção (da diretoria, ou fórum de segurança da informação) da organização, a quem compete a:

- análise crítica e aprovação da política da segurança da informação e das responsabilidades envolvidas;

- monitoração das principais mudanças na exposição dos ativos das informações às principais ameaças;
- análise crítica e monitoração de incidentes de segurança da informação;
- aprovação das principais iniciativas para aumentar o nível da segurança da informação;

A proteção da informação deve ser um meio para organização alcançar seus objetivos e não deve significar um fim em si mesma. (PELTIER, 2001)

A implementação do sistema de proteção da informação deve transpor as fronteiras da implantação de dispositivos de *hardware* ou *software*, que protegem o que está armazenado nos bancos de dados e arquivos da empresa, e muitas vezes não oferecem a segurança necessária ou esperada devido a falhas de funcionamento ou de parametrização e instalação (PELTIER, 2001). O sistema deve considerar o grau de dependência da organização da utilização da informática como ferramenta de trabalho no seu dia-a-dia, as necessidades de manutenção dos sistemas ativos em caso de desastre e o comprometimento de áreas críticas da organização, com problemas de vazamento de informações, entre outros. Para resolver estes problemas será necessário, e pode-se dizer fundamental, a definição da Política de Segurança da Informação, que é o conjunto de diretrizes do sistema de gestão de segurança da informação.

Análise da Competitividade segundo Porter

Michael Porter (PORTER, 1986) apresenta a idéia de posicionamento estratégico a partir de uma diferenciação específica, na liderança de custo ou no enfoque, que é também defendida por Philip Kotler em seu vídeo para HSM, Como Construir Marcas Fortes, de 2000. Estas são consideradas estratégias genéricas, pois são métodos que muitas das empresas de um segmento específico de indústria podem adotar para superar seus concorrentes.

A diferenciação é uma estratégia que consiste em diferenciar seu produto ou serviço o mais possível dos oferecidos pelos concorrentes. Criar um conceito de produto ou serviço que possa parecer único aos olhos do cliente. A liderança de custo está pautada na busca permanente da redução dos custos de fabricação dos produtos ou serviços. A posição de redução de custos traz com os resultados a redução de preços e por consequência diferenciação perante os concorrentes. A estratégia chamada enfoque está relacionada em manter o foco em determinado grupo de compradores, segmento de linha de produtos, ou mercado específico. Identificamos que a utilização dos dispositivos de segurança da informação de forma sistemática e organizada, poderá trazer à estratégia de diferenciação do produto aplicada pelas empresas, maior credibilidade e inovação, pois a segurança da informação trata do bem mais precioso das organizações no atual momento da gestão empresarial, e portanto, precisa de manutenção e diferenciação de tratamento tanto internamente como perante o seu cliente.

AMOSTRA PESQUISADA

A pesquisa foi realizada em âmbito nacional. Foram selecionados 129 questionários de profissionais que compõem a amostra, com intuito de obter um universo estatístico significativo, considerando 94 questionários de empresas de informática e 35 questionários de empresas de telecomunicações.

INSTRUMENTO DE MEDIDA UTILIZADO

O instrumento de medida que deu origem à coleta de dados, foi o questionário já utilizado há 8 anos pela Módulo *Security Solutions*, desenvolvido e validado com base na metodologia PESI (metodologia própria da Módulo *Security Solutions* para desenvolvimento de seus projetos de consultoria) e baseado no instrumento utilizado pela pesquisa realizada pelo CSI/FBI *Computer Security Institute/Federal Bureau of Investigations*. Foram selecionadas questões e organizadas em um questionário específicos que é um subconjunto do questionário original, para facilitar tratamento e análise dos dados obtidos a partir da 8ª Pesquisa Nacional de Segurança da Informação, buscando atender a cada referencial teórico, nos quais este estudo está baseado.

RESUMO DOS RESULTADOS OBTIDOS NA PESQUISA DOS DOIS SEGMENTOS:

Correlacionando a Hipótese I às questões-chave, obtivemos resultados muito interessantes e em alguns momentos surpreendentes e contraditórios:

- 48,57 % das empresas de Telecom têm política de segurança, contra 69,15 % das empresas de Informática. Ou seja, mais de 50 % das empresas de Informática já têm uma política de segurança formalizada.
- 31,42% das empresas de Telecom têm plano de continuidade de negócios contra 53,20% das empresas de Informática, ou seja, novamente mais de 50% das empresas de informática já têm um plano de continuidade ou estão em fase de desenvolvimento.
- Na opinião dos executivos das empresas de Telecom a segurança das informações é vital, crítica ou importante, sendo 88,57% das respostas. E 84,05% dos executivos das empresas de Informática classificam da mesma forma.
- Para os profissionais das empresas de Telecom as ameaças mais críticas são: funcionários insatisfeitos, acessos indevidos e vazamentos de informações. Já para os entrevistados das empresas de Informática são: Vazamentos de informação, funcionários insatisfeitos e vírus.

Principais ameaças às informações da empresa:	TELE COM		INFORMÁTICA	
	Freq.	No. cit.	Freq.	No. cit.
Funcionário insatisfeito	45,71%	16	61,70%	58
Espionagem industrial	22,86%	8	18,09%	17
Falhas de energia	8,57%	3	28,72%	27
Alteração indevida	17,14%	6	15,96%	15
Fraudes em e-mail	17,14%	6	23,40%	22
Incêndio / desastres	11,43%	4	12,77%	12

Acessos indevidos	25,71%	9	41,49%	39
Uso de <i>notebooks</i>	22,86%	8	31,91%	30
Divulgação de senhas	22,86%	8	32,98%	31
Vírus	22,86%	8	53,19%	50
Vazamento de informações	31,43%	11	37,23%	35
Alteração indevida de configurações	25,71%	9	14,89%	14
Roubo / furto	28,57%	10	14,89%	14
Fraudes, erros e acidentes	17,14%	6	27,66%	26
Lixo informático	8,57%	3	19,15%	18
Roubo de senhas	5,71%	2	12,77%	12
Divulgação indevida de informações confidenciais	14,29%	5	22,34%	21
<i>Hackers</i>	14,29%	5	31,91%	30
<i>Concorrentes</i>	22,86%	8	20,21%	19
<i>Superpoderes de acesso</i>	17,14%	6	15,96%	15
<i>Falhas na segurança física</i>	14,29%	5	26,60%	25
<i>Acessos remotos indevidos</i>	11,43%	4	23,40%	22
<i>Uso indevido de recursos</i>	8,57%	3	20,21%	19
<i>Pirataria</i>	2,86%	1	11,70%	11
<i>Sabotagens</i>	5,71%	2	5,32%	5
<i>Todos</i>	2,86%	1		
<i>Não responderam</i>	40,00%	14	4,26%	4
TOTAL OBS.		35		94

Tabela 1 – Principais Ameaças as Informações
 Fonte: CARVALHO, 2003, p.148

Correlacionando a Hipótese II às questões-chave, obtivemos resultados até certo ponto esperados:

- Os maiores obstáculos encontrados para implementação da segurança da informação pelos entrevistados das empresas de Telecom são: a falta de consciência dos executivos e a falta de orçamento, por último a falta de consciência dos usuários. O mesmo resultado foi obtido para empresas de Informática. Interessante que 40% dos entrevistados das empresas de Telecom consideram que não há obstáculos para implantação de um sistema de segurança da informação em suas empresas.
- Nas empresas de Telecom o principal gestor com 48,57% das indicações é a área de TI, contra 29,79% encontrado nas empresas de Informática. O *Security Officer* ainda está com índices baixos de representatividade nesta pesquisa.

- As empresas de Telecom na sua maioria, ou seja, 54,29% possuem um planejamento de segurança, na média para 1 ano. As empresas de Informática 48,94% possuem um planejamento, porém 40,43% não possuem qualquer tipo de plano de segurança, o que é preocupante.
- O percentual do orçamento de Tecnologia da Informação em relação ao orçamento total da empresa, para as empresas de Telecom são em média de 1 a 5 %, considerando a resposta de 31,43% dos entrevistados (vide gráfico 1). Para as empresas de Informática, a média de também de 1 a 5% considerando a resposta de 24,47% dos entrevistados (vide gráfico 2).

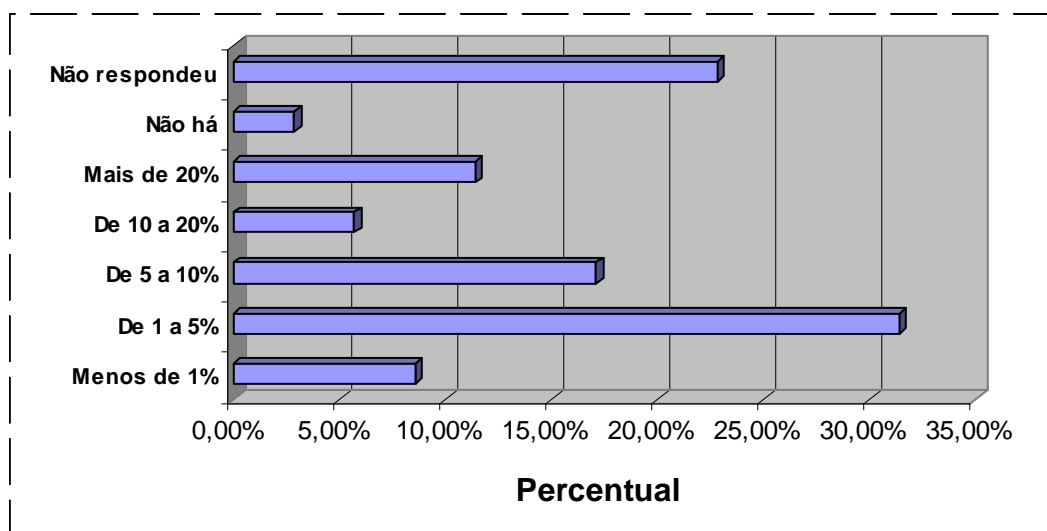


Gráfico 1: Percentual do Orçamento de TI em relação do orçamento total da empresa no segmento de Telecom
 Fonte: (CARVALHO,2003, p. 140)

- O percentual do orçamento de Tecnologia da Informação em relação ao orçamento total da empresa, para as empresas de Informática, a média de também de 1 a 5% considerando a resposta de 24,47% dos entrevistados (vide gráfico 2).

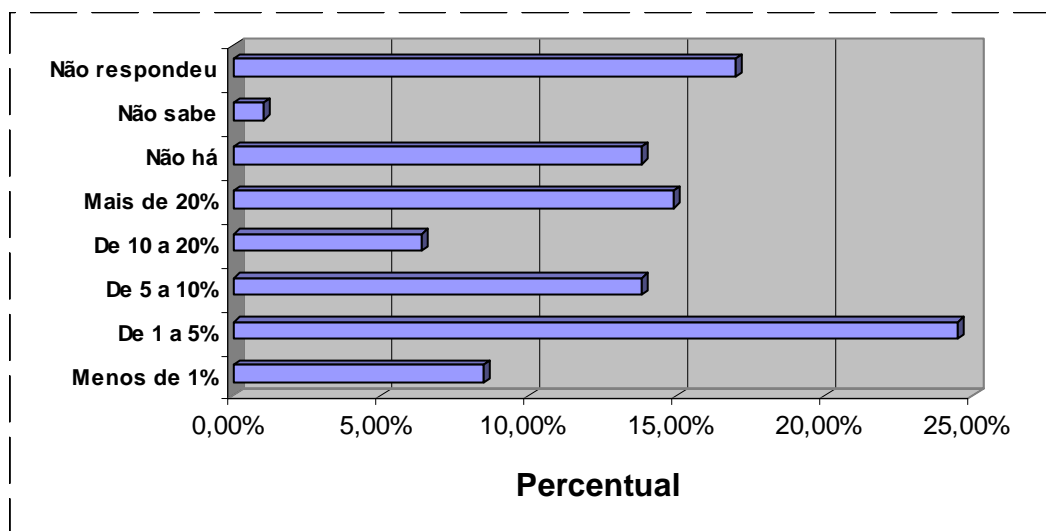


Gráfico 2: Percentual do Orçamento de TI em relação do orçamento total da empresa no segmento de Telecom
 Fonte: (CARVALHO,2003, p. 155)

- O percentual do orçamento de Segurança em relação ao orçamento com Tecnologia da Informação, em ambos os segmentos foi menor que 5%.
- 45,71% dos entrevistados das empresas de Telecom, deixam de comprar em *sites* de *E-Commerce* por causa da sensação da falta de segurança. Contra 57,45% dos entrevistados das empresas de Informática. Ou seja, mais ou menos a metade dos entrevistados deixa de comprar por causa da sensação de falta de segurança.
- 56,38% dos entrevistados das empresas de Informática fornecem o número de seu cartão de crédito em compras *on line*. Porém, somente 25,71% dos entrevistados das empresas de Telecom fornecem número de seu cartão de crédito em compras *on line*.
- A opinião dos entrevistados sobre o que está faltando em termos de serviços ou produtos de segurança da informação no mercado brasileiro, foi divergente e pulverizada. O item mais indicado pelos entrevistados nos dois segmentos, foi *Ampla Divulgação*, e em seguida *Capacitação Técnica*.

Correlacionando a Hipótese III às questões-chave, obtivemos coincidentes com o dia-a-dia da autora. Sendo para esta hipótese foram elencadas questões-chave que não são relacionadas às perguntas do questionário, e portanto, serão respondidas com base no referencial teórico, considerando a opinião dos autores referenciados e a própria experiência da autora deste trabalho de pesquisa:

- 28,57% das empresas de Telecom possuem Certificação ISO 9000 e 2,86% possuem ISO 14000. Já 22,34% das empresas de Informática possuem ISO 9000, 7,45% das empresas estão se preparando para certificação BS 7799, sendo que 2 empresas do segmento já estão certificadas (Módulo e SERASA-SP), e 1,06% possuem certificação CMM (Capability Maturity Model).

Os resultados encontrados nesta pesquisa servirão de fundamento para as conclusões que serão apresentadas ao final deste artigo, mas podemos afirmar que a utilização dos sistemas de gestão de segurança nos segmentos estudados ainda está abaixo do desejado, ou melhor dizendo, abaixo do necessário, considerando que estes segmentos (informática e telecom) são em geral provedores de serviços de vital importância para garantia da continuidade dos negócios das organizações, e responsáveis pela viabilização dos próprios sistemas de gestão de segurança em seus clientes. Cabe neste momento a seguinte reflexão, como implementar ou viabilizar sistemas ou dispositivos de gestão para redução dos riscos de violação da segurança da informação em seus clientes, se as empresas provedoras ainda não estão conscientes de sua real importância e não utilizam plenamente estes dispositivos?

RESULTADOS GERAIS OBTIDOS

A análise dos dados coletados forneceu respostas às questões-chave e permitiu que este estudo fosse concluído com observações significativas sobre o uso da segurança da informação como diferencial competitivo nos setores de informática e telecomunicações em nosso país.

- Os executivos da amostra estudada, mais de 50% consideraram a segurança da informação fator crítico para o negócio e, as empresas onde trabalham já possuem um planejamento de segurança para um período de 6 meses a 1 ano;
- O maior obstáculo para implementação da segurança da informação nas empresas, indicado pelos entrevistados, foi a falta de consciência da alta direção e a falta de orçamento para obtenção e implementação de dispositivos de proteção da informação, sejam eles dispositivos físicos, lógicos, treinamentos e desenvolvimento de normas e procedimentos;
- Apesar de a Segurança da Informação ser um assunto antigo na pauta dos pesquisadores, ainda há falta de conhecimento e divulgação sobre a gestão de segurança da informação, sua importância para a garantia da continuidade dos negócios das empresas e os prejuízos e perdas com falhas na segurança da informação.

Estes fatos podem indicar que ainda há uma longa trajetória a ser traçada pelas empresas para alcançar um nível satisfatório de implementação de sistemas de gestão de segurança da informação nos segmentos estudados.

CORROBORAÇÃO E REFUTAÇÃO DAS HIPÓTESES

Pela originalidade do assunto e a falta de conscientização geral sobre o uso dos princípios básicos sobre a segurança da informação e por consequência, a visão distorcida de alguns executivos sobre o alto custo da implementação de um sistema de gestão de segurança, baseado nas melhores práticas internacionais, não foi possível identificar efetivamente se a implementação de um sistema de gestão de segurança da informação gera diferencial competitivo perante a concorrência, e portanto, espera-se que os próximos 10 anos sejam de relevante significado para o movimento de instauração de uma consciência crítica sobre o tema. As características do estudo conduzido não permitiram corroborar ou refutar nenhuma das hipóteses. Os dados coletados foram analisados de modo que fosse possível determinar exclusivamente a plausibilidade ou a implausibilidade das hipóteses através dos critérios estabelecidos.

CONCLUSÕES

Assim, os resultados obtidos por intermédio do questionário foram organizados como exposto, onde a autora procurou relacionar as questões chaves com os argumentos de validação encontrados por intermédio da pesquisa de campo e das informações obtidas na revisão de literatura. Os tópicos abaixo são uma síntese das conclusões que a autora chegou com presente trabalho de pesquisa.

Conclusões sobre a Hipótese I: O uso das práticas de Segurança da Informação gera percepção de diferencial competitivo perante o mercado:

- Não foi possível medir se as empresas que já empregam o modelo de gestão de segurança da informação obtiveram vantagem competitiva, porém sabemos que os princípios primários de garantia da confidencialidade, integridade e disponibilidade podem:
 - Preservar a *informação* que é um bem inestimável para as empresas;

- Evitar vazamentos de informações confidenciais;
 - Garantir de Continuidade do negócio;
 - Preservar a imagem de segurança perante o cliente;
 - Reduzir a probabilidade de ocorrência de incidentes de segurança;
 - Reduzir danos/perdas causados por incidentes de segurança;
 - Facilitar a recuperação dos danos em caso de desastre/incidente.
- As principais barreiras apontadas pela pesquisa são: a falta de consciência dos executivos e a falta de orçamento, por último a falta de consciência dos usuários. Interessante que 40% dos entrevistados das empresas de Telecom consideram que não há obstáculos para implantação de um sistema de segurança da informação em suas empresas, isto demonstra a típica atitude da negação à realidade e por conseqüência, uma barreira para implementação do sistema.
- Não identificamos se efetivamente é relevante para os entrevistados dos dois segmentos obter uma certificação em segurança da informação. Os padrões internacionais são tidos como muito rígidos e geram altos custos de implantação, na opinião dos usuários de forma geral.

Conclusões relacionadas a Hipótese II: Existem barreiras sócio-culturais que dificultam a implementação do sistema de gestão de segurança da informação nas organizações. Esta hipótese têm uma abordagem que visa a identificar o envolvimento e o comprometimento da alta direção com o sistema de segurança da informação:

- Os principais argumentos para obtenção da aprovação da alta direção para um projeto de implementação da segurança da informação são a análise de risco e a pontuação que os ativos críticos recebem dos responsáveis pelos processos internos de negócio da empresa. Saber qual é o retorno sobre o investimento feito em segurança não é o mais importante, e sim, saber qual será o prejuízo se ocorrer um incidente de segurança, como por exemplo um vazamento de informação.
- A responsabilidade sobre a segurança da informação ainda está na área de TI, e a figura do Executivo de segurança (*Security Officer*) ainda não participa das decisões estratégicas, pois em geral está em posição de nível tático, subordinado aos Diretores de tecnologia da Informação.
- Os investimentos em Segurança da Informação são baixos e restritos à implantação de dispositivos de detecção de intrusões nas redes, sistemas de *back-up* e instalação de antivírus e *firewall*.

Conclusões relacionadas a Hipótese III: Há uma relação sistêmica entre os princípios de gestão da segurança da informação e os princípios de gestão da qualidade. A identificação dos elementos fundamentais de proteção da informação, estudados por Peltier e a BS7799-2:2002 foram validados pelas questões-chave propostas para esta hipótese, que teve o objetivo de identificar o método de implementação e melhoria contínua do sistema de segurança da informação.

- O sistema de gestão de segurança da informação tem a finalidade de diminuir o nível de exposição aos riscos em todos os ambientes para que a empresa possa estender a

segurança aos seus produtos e serviços, resultando em uma satisfação maior por parte dos clientes.

- O modelo de Peltier (2001, cap. 10, p.175), no que se refere aos elementos fundamentais para proteção da informação, lista como principais objetivos:
 1. Alinhamento com a estratégia e os objetivos de negócios da empresa;
 2. O sistema de segurança requer comprometimento da alta direção;
 3. Os investimentos de segurança devem ser compatíveis com o nível de segurança desejado, ou necessário para suportar os negócios da empresa;
 4. Responsabilidade sobre segurança da informação é de todos;
 5. O acesso à informação deve ser autorizado pelos seus proprietários;
 6. Análise e revisões sistemáticas do sistema de segurança deverão ser feitas visando a tomada de ações corretivas e preventivas;
 7. Há necessidade de auditorias e testes para verificação de falhas ou desvio no sistema;
 8. A segurança da informação deve fazer parte da cultura da empresa;

- Os estudos feitos pela autora e apresentados na revisão de literatura e no referencial teórico indicam que o modelo de gestão de segurança da informação previsto na norma NBR ISO/IEC 17799 e na BS7799-2:2002, Introdução p. 4; Requisito 4.2; Processo p.7-11, garante um nível satisfatório de requisitos para implementação e melhoria do sistema de gestão de segurança em qualquer empresa.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBUQUERQUE, RICARDO E RIBEIRO, BRUNO. Segurança no desenvolvimento de software : como garantir a segurança do sistema para seu cliente usando a ISO/IEC. Rio de Janeiro, Ed. Campus, 2002.

AMARAL, MARCOS P. Segurança da Informação em Ambientes Computacionais Complexos: uma abordagem baseada na gestão de projetos. Minas Gerais, CEFET-MG, 2001.

ANTUNES, E. Planejamento de contingência e continuidade do negócio. São Paulo. Disponível em: <<http://www.modulo.com.br>>. Acesso: junho de 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Tecnologia da Informação – Código de prática para a gestão da segurança da informação, NBR ISO/IEC 17799:2001. Rio de Janeiro: ABNT, 2001.

BRITISH STANDARD. Information security management – Part 2: Specification for information security management systems, BS 7799-2:1999. London: BSI, 1999.

CARUSO, CARLOS A. A.; STEFFEN, Flávio Deny. Segurança em informática e de Informações. São Paulo: Senac, 1999.

CARVALHO, ROSÂNGELA C. A aplicação de um modelo de gestão de segurança da informação e a sua influência na percepção de competitividade no setor de telecomunicações e informática, UFF, Niterói, 2003.

GHEMAWAT, PANKAJ. A Estratégia e o Cenário dos Negócios; textos e casos. BookMan / IBMEC, Porto Alegre, 2000.

MÓDULO SECURITY SOLUTIONS S.A. 8ª pesquisa sobre segurança de informação, 2001. Disponível em: <http://www.modulo.com.br>. Acesso em 1 set. 2002.

- MOREIRA, NILTON S.** Segurança Mínima - uma visão corporativa da segurança de informações. Rio de Janeiro, Axcel Books, 2001.
- PELTIER, THOMAS.** Information Security Policies, Procedures, and Standards – Guideline for effective Information Security Management, Florida, Auerbach, 2001.
- PORTER, MICHAEL E.** Competição: estratégias competitivas essenciais, Rio de Janeiro, Ed. Campus, 1999.
- POPPER, KARL R.** A lógica da pesquisa científica. São Paulo, Cultrix/USP, 1975.
- PORTER, MICHAEL E.** Vantagem Competitiva, Rio de Janeiro, Ed. Campus, 1986.
- QUINTELLA, HEITOR M.** Tecnologia da Informação e Avaliação da Competitividade no Brasil. Revista Suma Econômica, Rio de Janeiro, p. 46-47, ago. 1998.
- TIPTON, HAROLD F. KRAUSE, MICKI.** Information Security Management Handbook. Volume 1, 2, 3 e 4. Flórida, Auerbach, 1998.