Revista de Gestão da Tecnologia e Sistemas de Informação
Journal of Information Systems and Technology Management
Vol. 4, No. 3, 2007, p. 375-397
ISSN online: 1807-1775

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: FATORES QUE INFLUENCIAM SUA ADOÇÃO EM PEQUENAS E MÉDIAS EMPRESAS

INFORMATION SECURITY MANAGEMENT: FACTORS THAT INFLUENCE ITS ADOPTION IN SMALL AND MID-SIZED BUSINESSES

Abner da Silva Netto
Marco Antonio Pinheiro da Silveira
Universidade Municipal de São Caetano do Sul – IMES, Brasil

ABSTRACT

The objectives of this study were verify in what measure the small and medium companies accomplish the management security information and identify which factors influence the small and medium companies to adopt measures of management security information. The source research was exploratory-descriptive and the design used was the survey. The sample was compound of 43 metal production industries located in ABC region. According to management information security literature and Brazilian norm of information security were identified the tools or techniques of management security information and classified it into three layers: physic, logic and human. The study identified that the human layer is the one that presents the major shortage of cares in the companies followed by the logical one. The companies get used to have the antivirus as the main security tool/technique according to the researched companies to guarantee the safety of information. Besides that, the research showed that 59% of the companies have a safety satisfactory level and the main motivator factor to adopt the management security information is "to avoid possible financial loss". On the other hand, all the inhibitors factors showed important to the researched companies like: lack of knowledge, investments value, organization culture and difficulty to measure cost/benefit.

Keywords: security information, ISO 27002, IT adoption, small and medium companies.

Recebido em/*Manuscript first received*: 10/08/2007 Aprovado em/*Manuscript accepted*: 31/10/2007

Endereço para correspondência/ *Address for correspondence*

Abner da Silva Netto, Mestrando, Universidade Municipal de São Caetano do Sul – IMES, Programa de Mestrado em Administração, Rua Santo Antonio, 50 – Centro, São Caetano do Sul – SP, Telefone: 11-4239-3324, E-mail: abner@fsa.br

Marco Antonio Pinheiro da Silveira, Professor Titular, Universidade Municipal de São Caetano do Sul – IMES, Programa de Mestrado em Administração, Rua Santo Antonio, 50 – Centro, São Caetano do Sul – SP, Telefone: 11-4239-3324, E-mail: marco.pinheiro@imes.edu.br

ISSN online: 1807-1775
Publicado por/*Published by*: TECSI FEA USP – 2007

RESUMO

Este estudo teve como objetivos verificar em que medida as pequenas e médias empresas realizam gestão da segurança da informação e identificar fatores que influenciam pequenas e médias empresas a adotarem medidas de gestão da segurança da informação. Foi realizada pesquisa de natureza exploratório-descritiva e utilizou-se como delineamento o levantamento (survey). A amostra consistiu em 43 indústrias do setor de fabricação de produtos de metal situadas na região do Grande ABC. Com base na literatura sobre gestão da segurança da informação e na norma brasileira de segurança da informação, foram identificadas as ferramentas ou técnicas de gestão da segurança da informação e classificadas em três camadas: física, lógica e humana. O estudo identificou que a camada humana é a que apresenta a maior carência de cuidados por parte das empresas, seguida pela camada lógica. O antivírus é a ferramenta/técnica mais utilizada pelas empresas pesquisadas para garantir a segurança da informação. A pesquisa relevou que 59% das empresas pesquisadas possuem um nível de segurança satisfatório e que o principal fator motivador para adoção de gestão da segurança da informação é "evitar possíveis perdas financeiras". Todos os fatores inibidores se mostraram importantes para as empresas pesquisadas: falta de conhecimento, valor do investimento, dificuldade em mensurar custo/ benefício e cultura organizacional.

Palavras-chave: segurança da informação, ISO 27002, adoção de TI, pequenas e médias empresas.

1. INTRODUÇÃO

Com a utilização dos computadores em diversas organizações, as informações começaram a se concentrar em um único lugar e o grande volume dessas informações passou a ser um problema para a segurança. Os riscos aumentaram com o uso dos microcomputadores, a utilização de redes locais e remotas, a abertura comercial da Internet e a disseminação da informática para diversos setores da sociedade.

As pequenas e médias empresas também são atingidas por estes problemas, porém dispõem de menos recursos para investir na gestão da segurança da informação.

O problema de pesquisa tratado neste trabalho é: “que fatores são capazes de influenciar a adoção da gestão da segurança da informação por pequenas e médias empresas?”

O objetivo geral foi identificar os fatores que influenciam pequenas e médias empresas a adotarem medidas de gestão da segurança da informação e avaliar o grau de importância deles. Outro objetivo foi descrever, por meio dos controles contidos na norma de segurança da informação ISO IEC 27002:2005, se as empresas pesquisadas possuem requisitos mínimos e satisfatórios de gestão da segurança da informação. Para tanto, os controles descritos na norma foram classificados em três camadas: física, lógica e humana. A empresa considerada “satisfatória” deve possuir controles efetivos nas três camadas.

Este trabalho estudou pequenas e médias empresas (PMEs) industriais presentes na região do Grande ABC, composta pelas cidades de Santo André, São Bernardo do Campo, São Caetano do Sul, Diadema, Mauá, Ribeirão Pires e Rio Grande da Serra. A categorização usada para pequenas e médias empresas foi o número de empregados, sendo: pequena empresa - de 10 a 99 empregados; média empresa - entre 100 e 499

empregados.

2 SEGURANÇA DA INFORMAÇÃO

Segurança da informação, conforme Beal (2005), é o processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade. Sêmola (2003) define segurança da informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade." A ISO/IEC 17799:2005, em sua seção introdutória, define segurança da informação como "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". Assim, podemos definir segurança da informação como a área do conhecimento que visa à proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade a fim de garantir a continuidade do negócio e minimizar os riscos.

- a integridade da informação tem como objetivo garantir a exatidão da informação, assegurando que pessoas não autorizadas possam modificá-la, adicioná-la ou removê-la, seja de forma intencional ou acidental;
- a disponibilidade garante que os autorizados a acessarem a informação possam fazê-lo sempre que necessário;
- a confidencialidade da informação é a garantia de que somente pessoas autorizadas terão acesso a ela, protegendo-a de acordo com o grau de sigilo do se conteúdo;

Sêmola (2003) acrescenta a estes três objetivos os de:

- legalidade - garantia de que a informação foi produzida em conformidade com a lei;
- autenticidade - garantia de que num processo de comunicação os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação.

A fim de garantir um nível de proteção adequado para seus ativos de informação, as organizações e seus principais gestores precisam ter uma visão clara das informações que estão tentando salvaguardar, de que ameaças e por que razão, antes de poder passar a seleção de soluções específicas de segurança (BEAL, 2005). Grande parte dos dados importantes ao negócio da empresa está armazenada em computadores, por isso as organizações dependem da confiabilidade de seus sistemas baseados em TI; se a confiança nesses dados for destruída, o impacto pode ser comparável à própria destruição do sistema.

Dessa forma, as organizações precisam adotar controles de segurança – medidas de proteção que abranjam uma grande diversidade de iniciativas – que sejam capazes de proteger adequadamente dados, informações e conhecimentos, escolhidos, levando-se em conta os riscos reais a que estão sujeitos esses ativos. (BEAL, 2005).

À medida que as empresas tornam-se mais dependentes da informática, mais vulneráveis ficam a crimes e fraudes cometidas com o uso de recursos computacionais. Na maioria dos casos ocorridos, nada é publicado, por necessidade de preservação da imagem. (CARUSO e STEFFEN, 1999).

Pela alta capacidade de que dados, informação e conhecimento têm de adicionar valor a processos, produtos e serviços, estes constituem recursos cada vez mais críticos para o alcance da missão e dos objetivos organizacionais (CARUSO e STEFFEN, 1999). Conseqüentemente, as informações críticas para o negócio precisam ser protegidas contra as ameaças que podem levar à sua destruição, indisponibilidade temporária, adulteração ou divulgação não autorizada. (BEAL, 2005, p. XI). Fontes (2006, p. 38) assevera "a informação é um recurso que tem valor para a organização e deve ser bem gerenciada e utilizada [...] é necessário garantir que ela esteja sendo disponibilizada apenas para as pessoas que precisam dela para o desempenho de suas atividades profissionais".

Segundo Moraes, Terence e Escrivão Filho (2004), nenhuma empresa pode escapar dos efeitos da revolução causada pela informação. Dessa forma, deve-se ter consciência de que a informação é um requisito tão importante quanto os recursos humanos, pois dela depende o sucesso ou fracasso das tomadas de decisões diárias.

Segurança - mais que estrutura hierárquica, homens e equipamentos - envolve uma postura gerencial, o que ultrapassa a tradicional abordagem da maioria das empresas. É preciso cercar o ambiente de informações com medidas que garantam sua segurança efetiva, a um custo aceitável, visto ser impossível obter-se segurança absoluta, já que a partir de um determinado ponto, os custos se tornam inaceitáveis. (CARUSO e STEFFEN, 1999).

Fontes (2006) alerta para o constante crescimento de incidentes de segurança da informação, principalmente no Brasil. De forma crescente, as organizações estão potencialmente mais expostas a novas formas de ataques, independentemente do porte ou do tipo de negócio.

Para Beal (2005), devido à alta complexidade e ao alto custo de manter os ativos da informação salvos de ameaças à sua confidencialidade, integridade e disponibilidade, é importante a empresa adotar um enfoque de gestão baseado nos riscos específicos para o negócio. Sêmola (2003) define risco como: "a probabilidade de que agentes, que são ameaças, explorem vulnerabilidades, expondo os ativos a perdas de confidencialidade, integridade e disponibilidade e causando impacto nos negócios". Os impactos são limitados por medidas de segurança, que ajudam a diminuir o risco. Assim, a gestão do risco é o conjunto de processos que permite às organizações identificarem e implementarem as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos. (BEAL, 2005).

2.1 Camadas de Segurança da Informação

A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda ordem, que buscam identificar um

ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada. (SÊMOLA, 2001, p. 18).

Para Schneier (2001), "as ameaças do mundo digital espelham as ameaças no mundo físico. Se o desfalque é uma ameaça, então o desfalque digital também é uma ameaça. Se os bancos físicos são roubados, então os bancos digitais serão roubados." O crime no ciberespaço inclui tudo o que se pode esperar do mundo físico: roubo, extorsão, vandalismo, voyeurismo, exploração, jogos de trapaças, fraude etc.

Para Sêmola (2003), a gestão da segurança da informação pode ser classificada em três aspectos: tecnológicos, físicos e humanos. As organizações preocupam-se principalmente com os aspectos tecnológicos (redes, computadores, vírus, *hackers*, Internet) e se esquecem dos outros – físicos e humanos – tão importantes e relevantes para a segurança do negócio quanto os aspectos tecnológicos. Neste trabalho, optou-se pela classificação apresentada por Adachi (2004) que estudou a gestão da segurança em *Internet Banking* dividido-a em três camadas: física, lógica e humana.

2.1.1 Camada Física

É o ambiente onde está instalado fisicamente o hardware – computadores, servidores, meio de comunicação – podendo ser o escritório da empresa, a fábrica ou até a residência do usuário no caso de acesso remoto ou uso de computadores portáteis. Para Adachi (2004), "a camada física representa o ambiente em que se encontram os computadores e seus periféricos, bem como a rede de telecomunicação com seus modems, cabos e a memória física, armazenada em disquetes, fitas ou CDs".

As pequenas e a médias empresas têm seus dados armazenados, geralmente, em servidores de rede ou em estações compartilhadas, e o acesso físico a estes equipamentos nem sempre é restrito. Na maioria das vezes, esse mesmo servidor ou estação possui acesso liberado e ilimitado à Internet, o que aumenta o risco de um incidente de segurança. Na média empresa, o cenário é menos problemático, porém não o ideal, principalmente, devido à conscientização dos funcionários sobre segurança da informação.

O controle de acesso aos recursos de TI, equipamentos para fornecimento ininterrupto de energia e firewalls são algumas das formas de se gerir a segurança desta camada.

2.1.2 Camada Lógica

A camada lógica é caracterizada pelo uso de softwares - programas de computador - responsáveis pela funcionalidade do hardware, pela realização de transações em base de dados organizacionais, criptografia de senhas e mensagens etc. Segundo Adachi (2004), é nessa camada que estão as "regras, normas, protocolo de comunicação e onde, efetivamente, ocorrem as transações e consultas".

A segurança, em nível lógico, refere-se ao acesso que indivíduos têm às aplicações residentes em ambientes informatizados, não importando o tipo de aplicação

ou o tamanho do computador. As ferramentas de controle são, em sua maior parte, "invisíveis" aos olhos de pessoas externas aos ambientes de informática; estas só os reconhecem quando têm o seu acesso barrado pelo controle de acesso. (CARUSO e STEFFEN, 1999).

Manter o software de sistema operacional atualizado com a mais recente correção de segurança disponibilidade pelo fabricante é uma forma de minimizar os riscos de segurança nesta camada.

2.1.3 Camada Humana

A camada humana é formada por todos os recursos humanos presentes na organização, principalmente os que possuem acesso aos recursos de TI, seja para manutenção ou uso. São aspectos importantes desta camada: a percepção do risco pelas pessoas: como elas lidam com os incidentes de segurança que ocorrem; são usuários instruídos ou ignorantes no uso da TI; o perigo dos intrusos maliciosos ou ingênuos; e a engenharia social (ADACHI, 2004).

Das três camadas, esta é a mais difícil de se avaliar os riscos e gerenciar a segurança, pois envolve o fator humano, com características psicológicas, sócio-culturais e emocionais, que variam de forma individual (SCHNEIER, 2001).

A gestão da segurança da informação envolve mais do que gerenciar os recursos de tecnologia – hardware e software – envolve pessoas e processos, porém algumas empresas negligenciam este fator. A política de segurança e a conscientização dos usuários são algumas das formas de se controlar a segurança desta camada.

2.2 Norma de Segurança

"Normas e padrões têm por objetivo definir regras, princípios e critérios, registrar as melhores práticas e prover uniformidade e qualidade a processos, produtos ou serviços, tendo em vista sua eficiência e eficácia." (BEAL, 2005, p. 36). Concomitantemente, Sêmola (2003) diz que "uma norma tem o propósito de definir regras, padrões e instrumentos de controle que dêem uniformidade a um processo, produto ou serviço".

Devido ao interesse internacional em uma norma de segurança da informação, em dezembro de 2000, foi publicada a norma internacional ISO 17799:2000. Em 2001, a Associação Brasileira de Normas Técnicas (ABNT) publicou a versão brasileira que ficou com a denominação de NBR/ISO 17799 – Código de Prática para a Gestão da Segurança da Informação (OLIVA e OLIVEIRA, 2003). Em setembro de 2005, a norma foi revisada e publicada como NBR ISO/IEC 17799:2005. (ISO 17799, 2005). Segundo Holanda (2006), o comitê que trata da segurança da informação na ISO aprovou a criação de uma família de normas sobre gestão da segurança da informação, batizada pela série 27000, onde a então ISO IEC 17799:2005 foi rebatizada por ISO IEC 27002:2005.

A norma define 127 controles que compõem o escopo do Sistema de Gestão de Segurança da Informação (Information Security Management System – ISMS),

agrupados em 11 seções de controles: Política de Segurança da Informação; Organização da Segurança da Informação; Gestão de Ativos; Segurança em Recursos Humanos; Segurança Física e do Ambiente; Gestão das Operações e Comunicações; Controle de Acesso; Aquisição, Desenvolvimento e Manutenção dos Sistemas de Informação; Gestão de Incidentes da Segurança da Informação; Gestão da Continuidade do Negócio e Conformidade.

A adequação de qualquer empresa à norma ISO IEC 27002:2005 garante conformidade com as melhores práticas em gestão da segurança da informação. "As normas são criadas para estabelecerem diretrizes e princípios para melhorar a gestão de segurança nas empresas e organizações." (HOLANDA, 2006).

Para melhorar o entendimento e o estudo da gestão da segurança da informação, as seções da norma foram divididas nas três camadas conforme quadro 1.

Camada	Seção	Objetivos
Física	Gestão das operações e comunicações	Garantir a operação segura e correta dos recursos de processamento da informação.
	Segurança física e do ambiente	Prevenir o acesso físico não-autorizado, danos e interferências com as instalações e informações da organização; impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.
	Controle de acesso	Controlar acesso à informação; assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação; prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação; prevenir acesso não autorizado aos serviços da rede.
	Gestão de incidentes de segurança da informação	Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes da segurança da informação.
Lógica	Aquisição, desenvolvimento e manutenção de Sistemas de Informação	Garantir que segurança é parte integrante de sistemas de informação; prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações; proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos; Garantir a segurança de arquivos de sistema; manter a segurança de sistemas aplicativos e da informação. Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.
Humana	Organizando a segurança da informação	Gerenciar a segurança de informação dentro da organização; manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados,

		comunicados ou gerenciados por partes externas.
	Gestão de Ativos	Alcançar e manter a proteção adequada dos ativos da organização; assegurar que a informação receba um nível adequado de proteção.
	Segurança em recursos humanos	Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis e reduzir o risco de roubos, fraudes ou mau uso de recursos.
	Gestão da continuidade do negócio	Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil se for o caso.
	Conformidade	Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.
	Política de segurança da informação	Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Quadro 1: Seções da norma ISO IEC 27002 por camadas

Muitas seções da norma ISO IEC 27002:2005 possuem características das três camadas de segurança da informação (física, lógica e humana). Houve um esforço neste trabalho no sentido de classificar a seção pela camada que apresenta a maioria dos controles de uma delas.

2.3 Fatores influenciadores para adoção de TI ou Segurança da Informação em PMEs

Pouca literatura foi encontrada sobre a adoção da gestão da segurança da informação em organizações de qualquer porte. Porém, devido ao fato da maioria das empresas entenderem segurança da informação como simplesmente segurança de rede ou segurança em TI, considerou-se neste trabalho que os motivos que levam à adoção de TI estão associados ou são equivalentes aos motivos que levam à adoção da gestão da segurança da informação. Seguem os autores pesquisados que tratam da adoção de TI e suas considerações:

Thong (apud Prates e Ospina, 2004) salienta que as pequenas empresas não conhecem a importância de fatores-chave em TI, além das PMEs dispuserem de recursos reduzidos, podem estar gastando recursos e energia em fatores de pouca importância para o sucesso da implementação da TI. O autor, em pesquisa realizada com 114 pequenas empresas de Singapura, concluiu que as pequenas empresas com sucesso em TI tendiam a ter alta participação de especialistas externos.

Palvia e Palvia (1999) conduziram uma pesquisa em uma amostra de 1460 pequenas empresas para verificar os padrões de satisfação com TI, onde o proprietário

era também gerente, principal usuário, além de desempenhar as principais atividades de TI. Os autores concluíram que as características do proprietário têm impacto maior na satisfação em TI do que qualquer outro fator; para tanto foram considerados gênero, idade do proprietário, raça e habilidade em computação.

Outra pesquisa realizada com 25 pequenas empresas da macro-região de Ribeirão Preto – SP, Prates e Ospina (2004), identificaram que os principais motivos que levaram as empresas a implantarem TI foram: melhoria dos controles organizacionais, aumento de participação no mercado, aumento de produtividade e redução de custos. Em relação às dificuldades encontradas, a resistência pelos funcionários foi a mais expressiva, seguida pela cultura tradicional e ausência de pessoal qualificado.

Cragg e King (1993) pesquisaram os fatores motivadores e inibidores para utilização de computadores em pequenas empresas. Como fatores motivadores encontraram o que nomearam como *relative advantage* que se referem às economias de tempo e esforço; benefícios econômicos e diminuição de muitas tarefas repetidas. O entusiasmo de alguns proprietários com a tecnologia e a forte influência de consultores de TI também foram fatores considerados como motivadores da adoção.

Os fatores que desencorajaram o crescimento de TI foram agrupados em: educacionais, tempo administrativo, econômicos e técnicos. Os fatores educacionais são relativos à falta de conhecimento sobre os sistemas utilizados, bem como falta de pessoas com conhecimentos específicos de análise de sistemas, design e desenvolvimento. O fator tempo administrativo refere-se ao fato que muitos sistemas acabam consumindo considerável quantia de tempo dos gerentes no processo de implantação. Os fatores econômicos referem-se à situação econômica da empresa no momento e à análise informal de custo-benefício dos sistemas. Com pouco conhecimento técnico interno, pequenas empresas são muito confiantes no conselho e apoio que obtêm de seus fornecedores de TI, o que as limita, muitas vezes, ao uso de pacotes de aplicativos, à aceitação de limitações no software e a sua adaptação aos requerimentos do sistema.

Lunardi e Dolci (2006) realizaram uma pesquisa com 123 micros e pequenas empresas do Rio Grande do Sul e concluíram que os principais motivos que têm levado-as a adotarem TI estão relacionadas às pressões externas (os concorrentes diretos têm adotado ou por influência de clientes, fornecedores ou do próprio governo) que a empresa enfrenta e à existência de um ambiente organizacional favorável (funcionários em condições de utilizá-la e com uma estrutura organizacional adequada).

Relacionado à adoção da gestão da segurança da informação, Gupta e Hammond (2004) realizaram uma pesquisa com 138 pequenas e médias empresas nos Estados Unidos que apontou que somente 19% dos pesquisados tiveram um incidente de segurança nos últimos 12 meses, o que pode explicar a baixa porcentagem de pequenas empresas que desenvolve uma política de segurança e adquire proteção básica e software de backup.

Uma outra pesquisa realizada por Gabbay (2003) no Rio Grande do Norte, estudou os fatores que influenciam os Executivos e Gerentes de TI nas suas percepções em relação às diretrizes de Segurança da Informação na norma NBR ISO/IEC 17799 –

dimensão controle de acesso. Em sua conclusão, evidenciou a associação entre as variáveis, "tamanho do parque de informática" e a "freqüência dos ataques sofridos", com a variável "Nível de concordância em relação à norma NBR ISO/IEC 17799 – dimensão controle de acesso".

3 METODOLOGIA

Esta pesquisa utilizou o método exploratório-descritivo e teve como delineamento o levantamento (survey). Para realização do estudo, foi selecionado o setor de fabricação de produtos de metal, exclusive máquinas e equipamentos, localizado na região do ABC paulista. que é o mais expressivo do cadastro da CIESP – com 256 empresas cadastradas, sendo 225 classificadas como empresas de pequeno porte e 31 empresas classificadas como médio porte.

Os sujeitos da pesquisa foram os gestores (gerentes ou proprietários) que possuam algum envolvimento no processo de aquisição ou em investimentos em gestão da segurança da informação ou em TI.

Para fornecer subsídios para criação do questionário, foram realizadas entrevistas semi-estruturadas com sete gestores de quatro organizações diferentes. As entrevistas foram realizadas no mês de setembro de 2006. Foram gravadas e tiveram duração aproximada de quarenta minutos. Em três empresas, as entrevistas foram realizadas com dois gestores simultaneamente, somente em uma das empresas, a entrevista foi individual. Por serem semi-estruturadas, as entrevistas permitiram o acompanhamento da resposta e, quando necessário, foram efetuadas perguntas relacionadas, que não estavam incluídas no roteiro original. Isso ajudou, conforme recomenda Hair, Jr. et al. (2005), na descoberta de informações adicionais.

Procurou-se nas entrevistas conhecer primeiramente o perfil do gestor entrevistado, questionando-o sobre incidentes pessoais de segurança ocorridos anteriormente e como ele se mantém informado sobre assuntos ligados à TI e à segurança da informação. Buscou-se levantar também o perfil da empresa e saber o conhecimento do gestor sobre incidentes ocorridos com sua empresa. O valor da informação para a empresa e o risco inerente à ela também foram objetos de questionamento, buscando-se entender como as empresas têm lidado com este tema. Por fim, a entrevista questionou-os sobre as ferramentas e técnicas de defesa implantadas na empresa e os motivos que contribuíram ou contribuiriam para elevar os investimentos em gestão da segurança da informação.

Perfil do Gestor	Não se mantêm informados sobre a área (falta de conhecimento).
Perfil da Empresa	Enfrentaram incidentes de segurança relacionados a: vírus, parada da rede ou servidor, furto de informações.
Valor da Informação e Análise de Risco	A maioria dos gestores alega preocupação com as informações armazenadas em TI; Alguns gestores alegaram que o principal risco são os funcionários.
Ferramentas e Técnicas de Defesas	Antivírus; Backup; Firewall.
Fatores	Orientação de um especialista externo;

	Importância da relação custo/benefício do investimento; Incidentes anteriores.

Quadro 2: Principais contribuições obtidas com entrevistas preliminares

O questionário utilizado na etapa do levantamento foi disponibilizado às empresas pesquisadas em um website da Internet agrupando os seguintes grupos de variáveis e quantidade de questões:

Grupo de Variáveis	O que se pretende investigar	Qtde Questões	Exemplos de Questões
Perfil do Gestor	Identificação do responsável pelos investimentos em TI e segurança da informação		E-mail, cargo, departamento, decisão de compra
Perfil da Empresa	Identificação da empresa e do parque de informática, nível de utilização dos recursos de TI		Número de funcionários, qtde de computadores, responsabilidade pela área de TI
Ferramentas e Técnicas	Importância das ferramentas e técnicas de gestão da segurança da informação e se a empresa a possui	0	Na sua empresa qual o grau de importância do uso do firewall, antivírus etc.
Fatores	Questiona sobre os fatores motivadores ou inibidores para adoção da gestão da segurança da informação		Recomendação de um especialista externo ou fornecedor da área
TOTAL DE QUESTÕES		6	

Quadro 3: Conjunto de variáveis contidas no questionário.

Este trabalho selecionou 20 controles dos 127 presentes na norma ISO/IEC 17799:2005 para serem pesquisados junto às pequenas e médias empresas. Dentre as 11 seções presentes, foi selecionado pelo menos um controle de cada seção. Entretanto, em algumas seções mais de um controle se mostrou importante por sua possível aplicação nas empresas pesquisadas. As seções da norma onde foram selecionados mais de um controle são: Gestão de Ativos (2); Segurança Física e do Ambiente (2); Gestão das Operações e Comunicações (4); Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (3); Conformidade (2).

A seleção dos controles baseou-se em pesquisas sobre segurança da informação realizadas pelo Módulo Security no Brasil, pelo FBI nos Estados Unidos, pelas recomendações da norma ABNT NBR ISO/IEC 17799:2005, por meio de entrevistas preliminares realizadas com os gestores, além da experiência profissional dos pesquisadores.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

A pesquisa foi realizada entre os meses de fevereiro e março de 2007. Foram contatadas por telefone as 256 empresas da população, sendo que destas 43 responderam ao questionário. Entre os respondentes 84% ocupam cargos gerenciais, conforme exibido no gráfico 1, e 98% dos pesquisados possuem envolvimento sobre a decisão de compra de ferramentas e técnicas de gestão da segurança da informação ou TI.

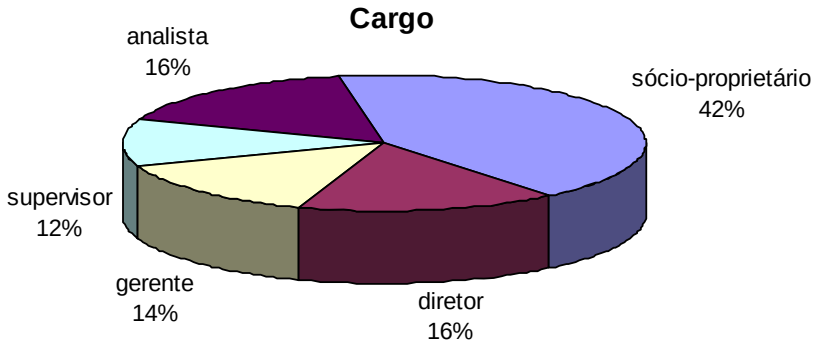


Gráfico 1: distribuição de cargos nas empresas pesquisadas

Quanto às características das empresas respondentes em relação ao porte e ao número de empregados, a amostra coletada está representada da seguinte forma, conforme o gráfico 2: 5% são microempresas (até 10 empregados), 81% são pequenas empresas (entre 10 e 99 funcionários) e 14% são médias empresas (de 100 a 499 funcionários). A delimitação da pesquisa inclui somente pequenas e médias empresas, assim as 5% consideradas microempresas foram excluídas da amostra para as análises das ferramentas/técnicas e fatores de adoção.

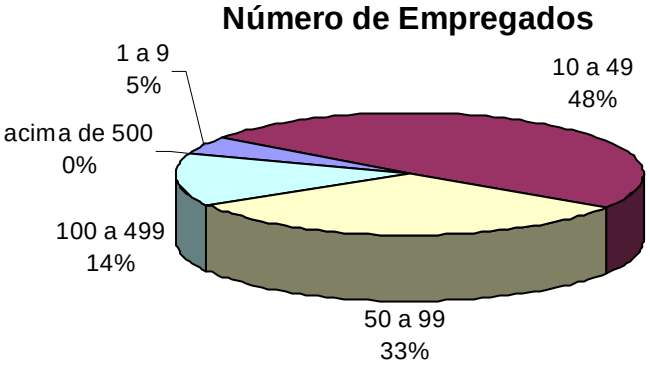


Gráfico 2: número de empregados das empresas pesquisadas

O gráfico 3 exibe a distribuição da quantidade de computadores nas empresas pesquisadas.

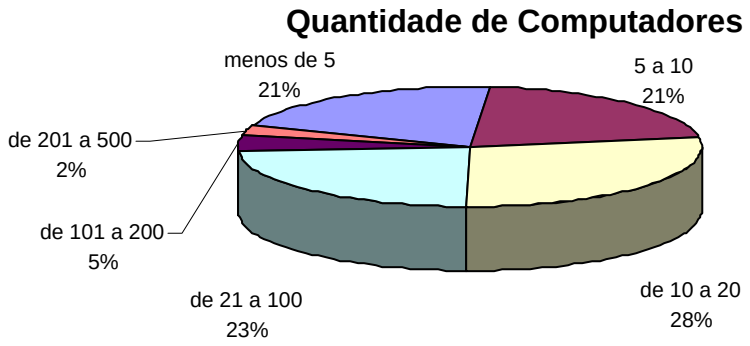


Gráfico 3: quantidade de computadores

A responsabilidade da área de TI na maioria das empresas da amostra é de um departamento interno ou funcionário (56%), enquanto os outros 44% são de empresas terceiras, sendo 23% com contrato e 21% contatadas por chamados eventuais.

Quando perguntados sobre o nível de informatização de suas operações, a maioria das empresas o considerou entre médio (65%) e alto (28%), o que pode sugerir a necessidade de uma gestão de segurança da informação mais eficaz nestas empresas devido a maior concentração de informações em computadores.

Para ajudar as empresas pesquisadas a responder sobre o nível de informatização de suas operações, foram consideradas as seguintes proposições no questionário:

- baixo: uso constante de edição de documentos, e-mails, acesso à Internet;
- médio: as considerações do nível baixo, mais uso intensivo de planilhas eletrônicas e Internet Banking;
- alto: as considerações do nível médio, mais uso de sistema integrado, acesso remoto a funcionários/fornecedores, comércio eletrônico.

4.1 Ferramentas e Técnicas de Gestão da Segurança da Informação

4.1.1 Camada Física

Nove questões foram formuladas para representar a camada física com base nas seções: Gestão das operações e comunicações, Segurança física e do ambiente, Controle

de acesso e, Gestão de incidentes de segurança da informação.

O gráfico 4 mostra a quantidade de empresas que possui ou não a ferramenta/técnica de gestão da segurança da informação na camada física.

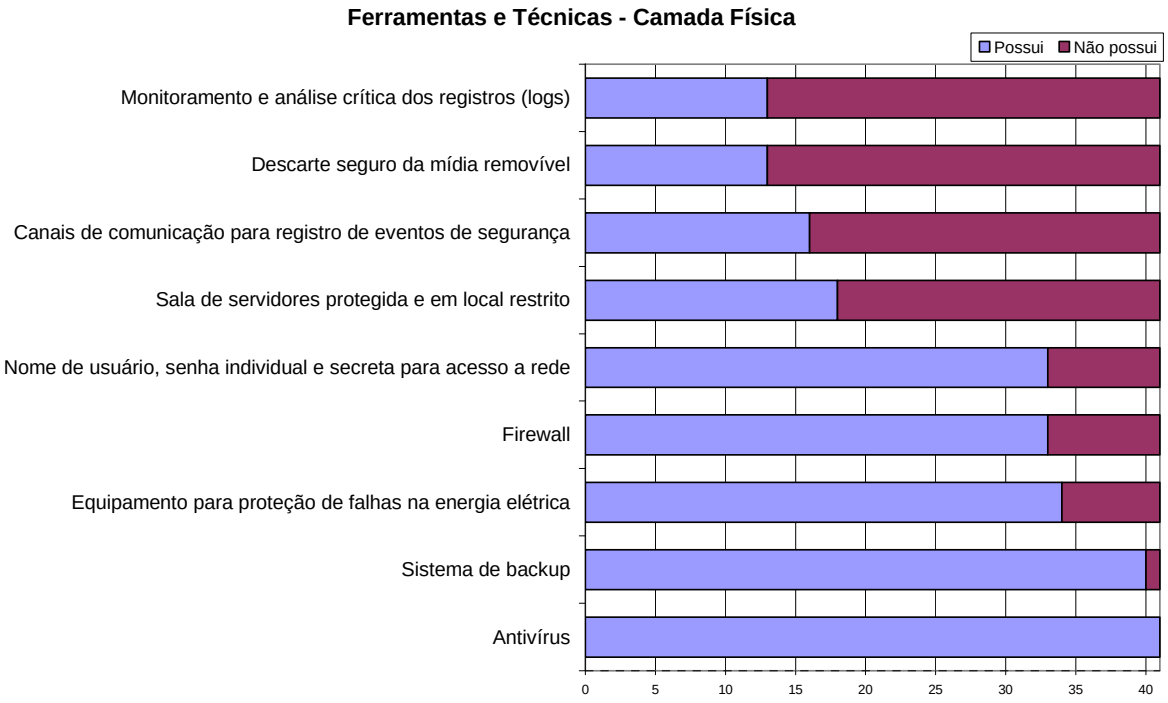


Gráfico 4: Camada Física

4.1.2 Camada Lógica

Na camada lógica, foram elaboradas três perguntas todas pertencentes à seção Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação.

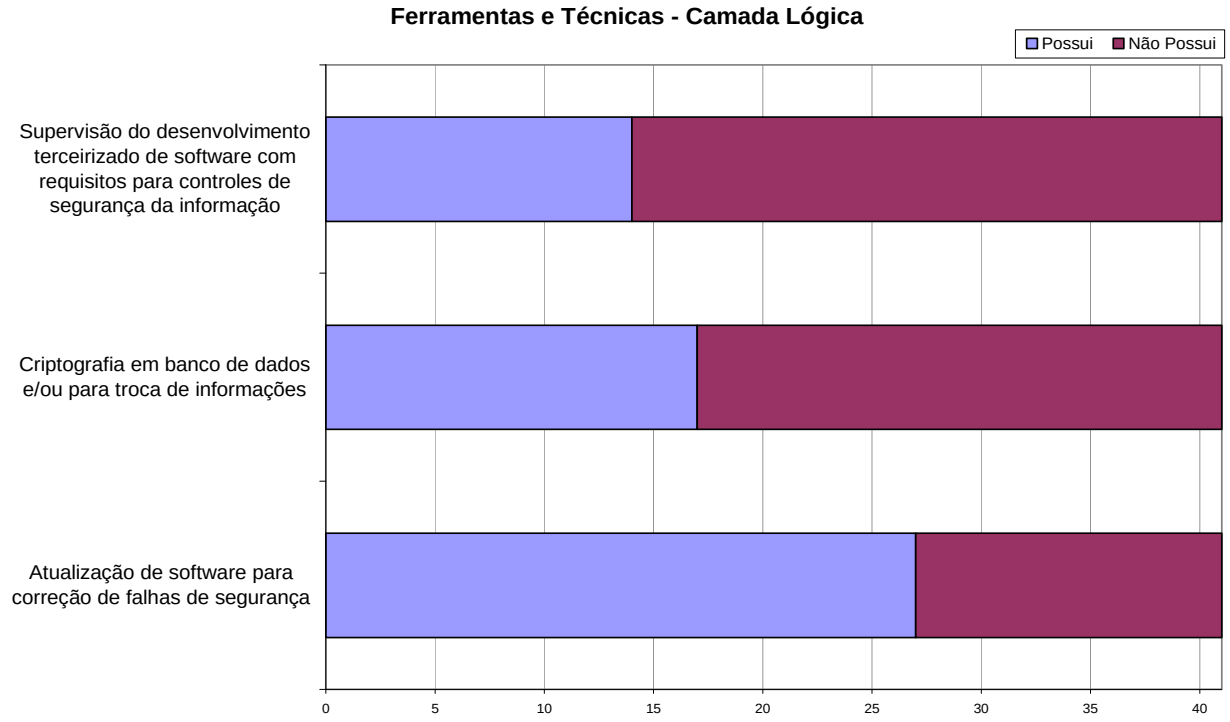


Gráfico 5: Camada Lógica

4.1.3 Camada Humana

Nesta camada, oito questões enunciadas no questionário e extraídas das seções: Política de segurança da informação, Gestão de ativos, Organizando a segurança da informação, Segurança em Recursos Humanos e Gestão da continuidade do negócio da norma tentaram conhecer a preocupação das empresas e o que efetivamente está sendo feito.

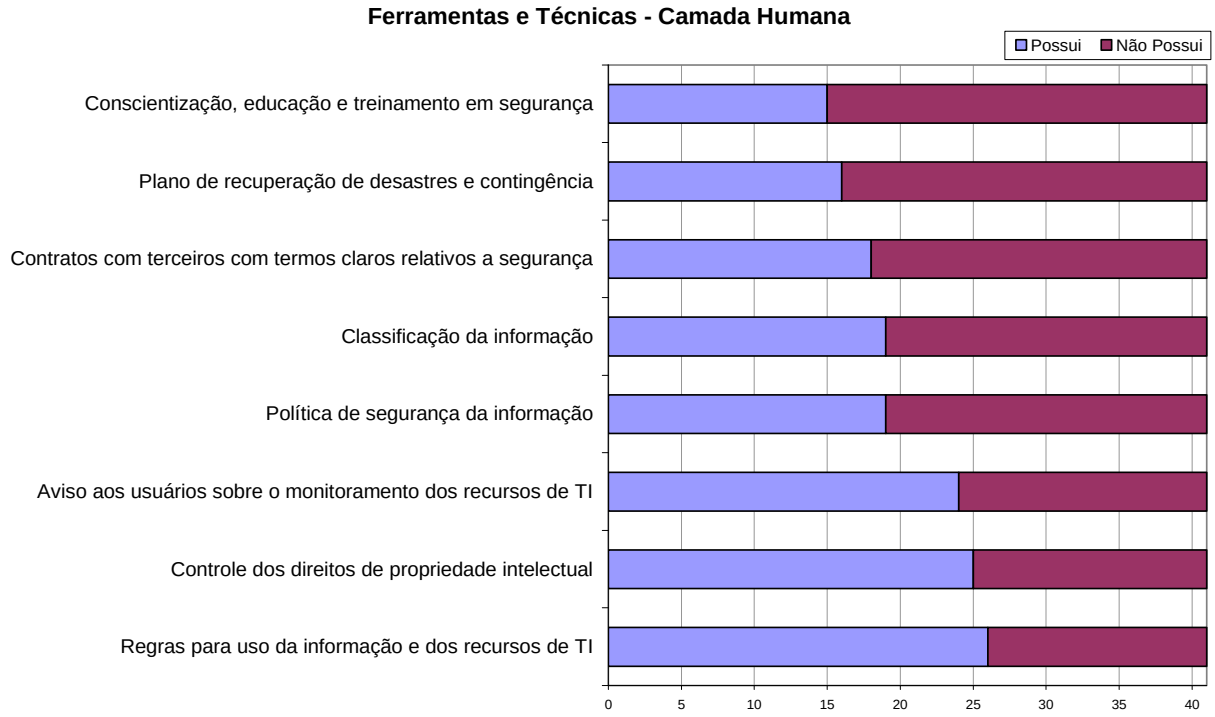


Gráfico 6: Camada Humana

Se observarmos os gráficos de adesão das três camadas: física, lógica e humana pelas empresas pesquisadas, percebe-se que a camada humana, devido ao número de ferramentas/técnicas, é a que apresenta maior carência de cuidados por parte dos administradores. Esta constatação confirma as alegações de Schneier (2001) e as preocupações de Fontes (2006). O interessante é que muitas das ferramentas/técnicas listadas neste trabalho na camada humana não são de difícil implementação, requerem, na maioria dos casos, baixo investimento em ferramentas computacionais, tempo e dedicação da gerência. O que confirma as considerações de Sêmola (2003) quando diz que as empresas se preocupam mais com os aspectos tecnológicos da segurança da informação do que com os aspectos físicos e humanos.

O gráfico 7 representa o grau de importância atribuído a todas as ferramentas ou técnicas de gestão da segurança da informação independentemente da camada a que foi categorizado: a maior ameaça e causa de perda de dinheiro com fraudes pelas empresas são os vírus de computador.

A implementação de uma Política de Segurança da Informação ficou em 11º lugar entre as 20 ferramentas/técnicas pesquisadas, uma posição modesta perante à importância que vários autores estudados atribuem à ferramenta.

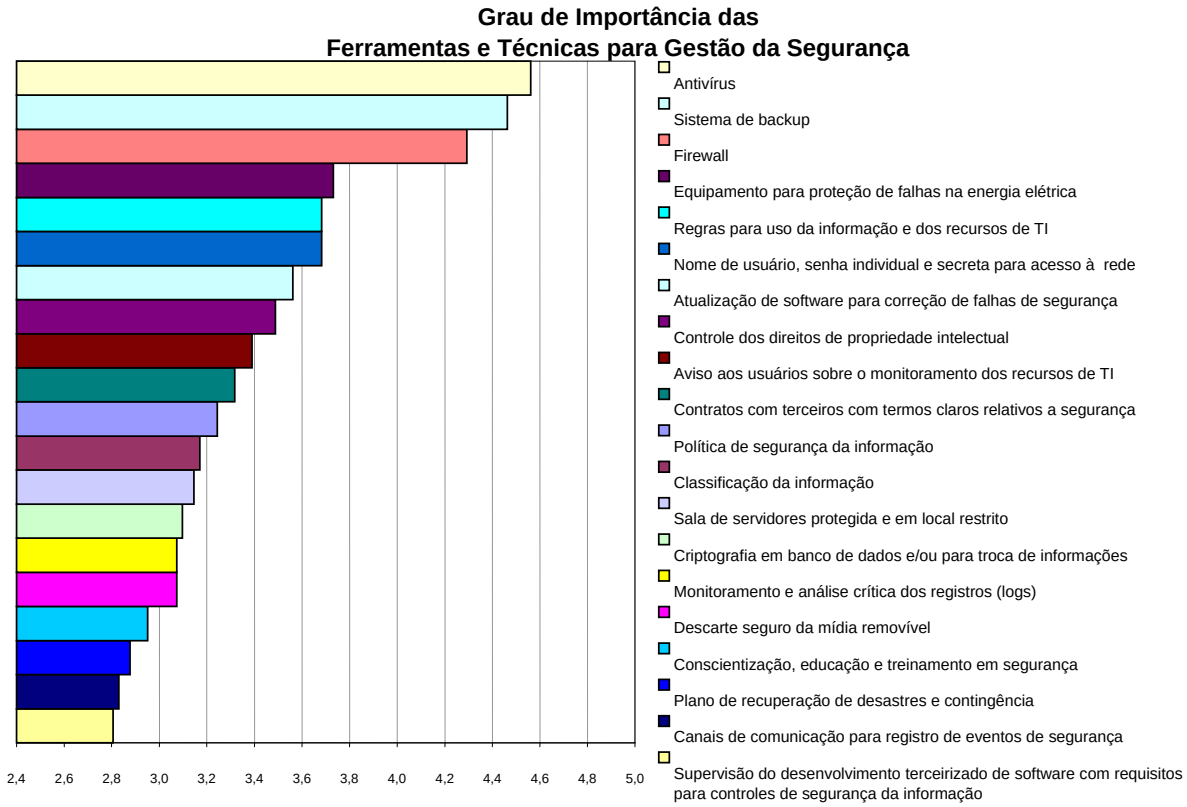


Gráfico 7: Grau de importância da Ferramentas/Técnicas

4.2 Gestão da Segurança da Informação nas Três Camadas

A fim de avaliar o nível de gestão da segurança da informação implementadas nas pequenas e médias empresas pesquisadas e, conseqüentemente, sua adequação a alguns itens da norma ISO IEC 27002:2005 foi desenvolvida a seguinte metodologia:

- verificar se a empresa possui pelo menos uma ferramenta/técnica instalada em cada uma das camadas de segurança: física, lógica e humana;
- verificar se a porcentagem das ferramentas/técnicas que a empresa possui instalada é maior ou igual a 50%, independentemente da camada de segurança;
- caso a empresa atenda às condições determinadas no item a e b, sua gestão da segurança da informação é classificada como satisfatória, caso contrário é classificada como insatisfatória.

A maioria das empresas pesquisadas (59%) se enquadrou no nível satisfatório, o que indica que existe uma preocupação da maioria das empresas com as três camadas da segurança.

O gráfico 8 representa a distribuição das ferramentas/técnicas instaladas nas

empresas pesquisadas. A maior distribuição de freqüência encontrada está no intervalo entre 60% a 80% das ferramentas/técnicas instaladas, com 13 empresas. Acima de 80% encontram-se nove empresas. Somando as duas freqüências, temos que 53,7% das empresas pesquisadas possuem mais que 60% das ferramentas/técnicas instaladas, o que pode inferir que a maioria encontra-se adequada à gestão da segurança da informação, independentemente da camada.

Ao diferenciar as pequenas empresas das médias empresas, pôde-se observar que somente em uma das médias empresas a gestão da segurança da informação foi categorizada como insatisfatória, pois não atende aos requisitos mínimos estabelecidos. Todas as demais consideradas insatisfatórias são representadas por pequenas empresas, por possuírem menos recursos financeiros e humanos acabam não conseguindo atender às três camadas efetivamente.

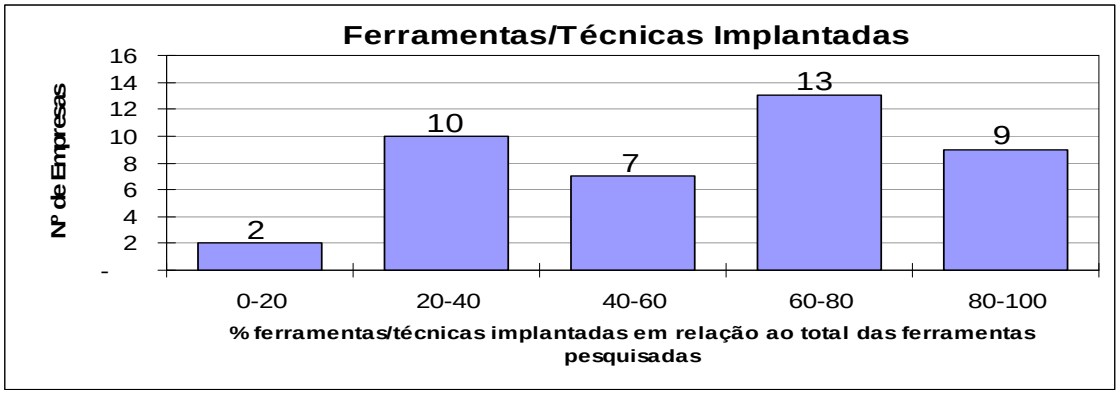
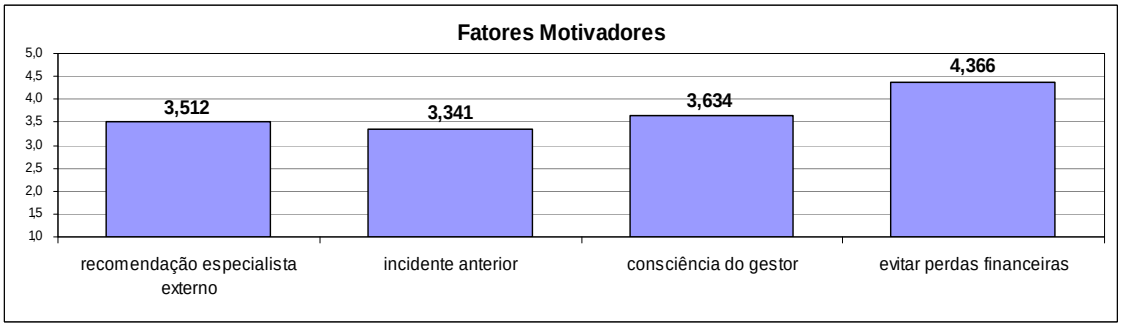


Gráfico 8: Quantidade de ferramentas/técnicas implantadas, por faixa, nas 43 empresas pesquisadas

4.4 Fatores motivadores e inibidores

Além de levantar as principais ferramentas e técnicas utilizadas pelas pequenas e médias empresas pesquisadas, este trabalho teve como foco principal verificar os fatores motivadores e inibidores para uso e a aplicação da gestão da segurança da informação. Os fatores pesquisados bem como os resultados das médias de cada um encontram-se exibidos no gráfico 9.



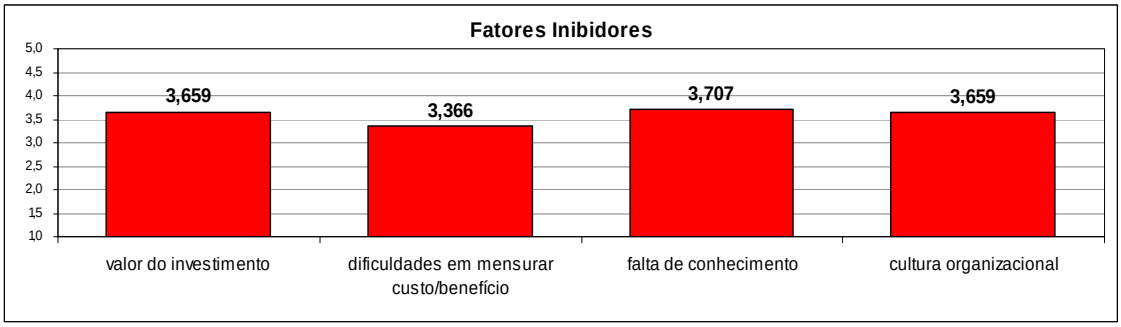


Gráfico 9: Fatores Motivadores e Inibidores

O gráfico 9 exibe que o fator motivador que obteve a maior média na pesquisa foi "evitar perdas financeiras" seguido por "consciência do gestor". Em fatores inibidores, a maior média ficou com o fator "falta de conhecimento".

Para verificar a significância das médias apresentadas no gráfico 9, foram realizados os seguintes testes com o uso do software SPSS: teste Shapiro-Wilk para verificar a normalidade dos dados, teste Kruskal-Wallis para verificar a significância entre as médias, teste Mann-Whitney para verificar a média que apresentava maior significância;

O teste Shapiro-Wilk revelou um valor de $p < 0,0001$, para tanto a distribuição não pode ser considerada normal, o que inviabilizou o uso de testes paramétricos como ANOVA – *Analysis of Variance*. Assim, procedeu ao uso de testes não-paramétricos.

O teste Kruskal-Wallis realizado com as médias dos fatores motivadores e com as médias dos fatores inibidores revelou que: em fatores motivadores, nem todas as médias são iguais estatisticamente ($p < 0,0001$), porém as médias dos fatores inibidores não apresentaram diferenças significativas entre si ($p = 0,429$); ao nível de confiança de 95%, o que pode inferir que todos os fatores inibidores têm a mesma importância para a amostra de empresas pesquisadas.

Para confirmar entre os fatores motivadores a média que apresentava diferença significativa foi realizado o teste Mann-Whitney, comparando a média de cada fator entre si. Os resultados estão apresentados na tabela 1:

Tabela 1: Teste Mann-Whitney

Fatores	Mann-Whitner U	Wilcoxon W	Z	Asymp.Sig (2-tailed)
especialista interno x incidente anterior	773,000	1634,000	-0,648	0,517
especialista interno x consciência do gestor	775,500	1636,500	-0,626	0,531
especialista interno x evitar perdas	482,000	1343,000	-3,529	0,000

financeiras				
incidente anterior x evitar perdas financeiras	443,500	1304,500	-3,870	0,000
consciência do gestor x evitar perdas financeiras	529,000	1390,000	-3,061	0,002

Dentre as médias analisadas, a que apresentou diferença significativa entre as demais foi a do fator "evitar perdas financeiras", com $p < 0,05$, inferindo que o fator motivador para as empresas implantarem ferramentas/técnicas de gestão da segurança da informação se dá, principalmente, para evitar possíveis perdas financeiras ou operacionais.

Apesar dos testes estatísticos revelarem que os demais fatores motivadores têm a mesma significância em termos de média, o fator "consciência do gestor" (segunda maior média) merece atenção por indicar certa incoerência com os fatores inibidores que mostram a "falta de conhecimento" com a maior média, pois é estranho identificar que o gestor tem consciência dos perigos que sua empresa corre com relação às informações, porém não se preocupa em ter o conhecimento adequado para sanar os problemas. Fato que também ficou claro nas entrevistas preliminares.

Nas entrevistas realizadas para criação do questionário ficou evidenciado que incidentes anteriores tinham um peso considerável na adoção de gestão da segurança da informação, assim como pesquisado por Gabbay (2003), porém nesta pesquisa não se apresentou como fator importante, o que pode indicar que as pequenas e médias empresas não têm sofrido incidentes de segurança da informação como apontado por Gupta e Hammond (2004) ou não têm monitorado (como apresenta o baixo grau de importância nas ferramentas/técnicas no item anterior) seus recursos para descobrir evidências de ataques aos ativos de informação, o que pode representar um sério risco à continuidade do negócio e/ou vazamento de segredos industriais e processos a concorrentes.

A importância da recomendação de um especialista externo ou fornecedor da área também ficou clara nas entrevistas e foi apontada nas pesquisas sobre adoção de TI de Cragg e King (1993) e Thong. Porém não apresentou média significativa como fator motivador na adoção de gestão da segurança da informação na amostra pesquisada.

Nos fatores inibidores não foi possível destacar o mais importante, visto as médias encontradas não apresentarem diferenças significativas. Porém, de acordo com as entrevistas preliminares a falta de conhecimento do gestor é um fator inibidor que merece certa atenção, pois ficou explícito nas entrevistas que não existe uma preocupação dos gestores em se manterem informados sobre assuntos ligados à gestão da segurança. Em relação aos outros fatores inibidores, conclui-se que para as empresas o valor do investimento e sua mensuração em razão do custo/benefício não são dispendiosos e, portanto, fáceis de serem aprovados no orçamento e implementados. A cultura organizacional também não mereceu destaque entre os fatores inibidores, possivelmente pela crescente divulgação de notícias relacionadas a incidentes de

segurança da informação na mídia em geral, e a conseqüente conscientização das pessoas com relação à mesma.

5 CONCLUSÃO

Das empresas pesquisadas, 80% possuem pelo menos um controle em cada uma das camadas de segurança (física, lógica e humana), o que indica que as PMEs se mostram preocupadas com a gestão da segurança da informação. Quando utilizada a classificação presente neste estudo sobre a gestão da segurança da informação, 59% das empresas pesquisadas podem ser consideradas satisfatórias com os controles implantados. A ferramenta mais utilizada foi o antivírus, presente em 100% das empresas pesquisadas, seguida por sistema de backup (97,6%) e *firewall* (82,9%). Todos estes controles relativos à camada física.

A camada humana é a que carece de maior atenção por parte das empresas, pois foi a que apresentou o menor índice de controles implantados. Os dados confirmam que as empresas investem principalmente em controles tecnológicos para diminuir o risco de incidentes de segurança da informação, porém esquecem que o fator humano é uns dos grandes responsáveis por falhas na segurança.

Em relação às seções da norma ISO IEC 27002:2005, foi verificada uma baixa adequação das pequenas e médias empresas, o que pode demonstrar que a norma requer muitos controles que a maioria não está preocupada em implantar ou não possui tempo ou dinheiro para isso. Contando que a norma sugere 127 controles e neste trabalho foram selecionados somente 20, esperava-se uma grande adequação aos controles.

Evitar perdas financeiras foi o fator motivador para adoção de gestão da segurança da informação que apresentou maior média e o único que apresentou diferença significativa das médias comparando com os demais fatores. O fator reforça a preocupação das empresas com o lado financeiro, visto ser mais fácil de mensurar do que perda de produtividade ou imagem, por exemplo. Os demais fatores motivadores, conforme comprovaram os testes estatísticos, podem ser considerados com pesos iguais.

Não foi possível indicar o principal fator inibidor na adoção da gestão da segurança da informação, pois os testes estatísticos revelaram que todos os fatores possuíam o mesmo nível de significância. Porém, nas entrevistas realizadas com os gestores a falta de conhecimento apareceu como um possível fator inibidor e, após a realização das pesquisas quantitativas, apresentou a maior média matemática.

O presente estudo mostrou que as pequenas e médias empresas, apesar de considerarem a perda financeira como o principal fator para adoção da gestão da segurança da informação, são carentes de informações sobre a correta gestão da segurança da informação.

Para estudos futuros, recomenda-se aplicar a pesquisa em outros setores da economia como empresas de serviços ou comércio, a fim de verificar a amplitude das análises. Uma amostra maior de empresas também poderia relevar mais informações e possibilitar a indicação de um fator inibidor. Recomendam-se também estudos para verificar a causa da falta de conhecimento dos gestores em gestão da segurança da

informação e TI. Haveria uma falta de interesse por parte das empresas ou dos gestores?

REFERÊNCIAS

ADACHI, Tomi. Gestão de Segurança em Internet Banking – São Paulo: FGV, 2004. 121p. Mestrado. Fundação Getúlio Vargas – Administração. Orientador: Eduardo Henrique Diniz.

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

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. Segurança em Informática e de Informações – São Paulo: Editora SENAC São Paulo, 1999.

COMITÊ GESTOR DA INTERNET NO BRASIL. Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil 2005. Disponível em <http://www.mct.gov.br/upd_blob/10819.pdf>. Acesso em 27/12/2006 às 20h48min.

CRAGG, Paul B.; KING, Malcolm. Small-Firm Computing: motivators and inhibitors – MIS Quarterly, março/1993, p. 47-60.

FONTES, Edison. Segurança da Informação: o usuário faz a diferença - São Paulo: Saraiva, 2006.

GABBAY, Max Simon. Fatores influenciadores da implementação de ações de Gestão de Segurança da Informação: um estudo com executivos e gerentes de tecnologia da informação em empresas do Rio Grande do Norte. 01/06/2003. 1v. 150p. Mestrado. Universidade Federal do Rio Grande do Norte - Engenharia de Produção. Orientador(es): Anatália Saraiva Martins Ramos. Biblioteca Depositaria: BCZM

GUPTA, Atul; HAMMOND, Rex. Information systems security issues and decisions for small business: an empirical examination – Information Management & Computer Security, 2004, pg. 297-310. Disponível em <http://www.emeralinsight.com/0968-5227.htm>. Acesso em 09/09/2006.

HAIR, JR Joseph F.; BABIN, Barry; MONEY Arthur H.; SAMOUEL, Phillip. Fundamentos de Métodos de Pesquisa em Administração - Porto Alegre: Bookman, 2005.

HOLANDA, Roosevelt de. O estado da arte em sistemas de gestão da segurança da Informação: Norma ISO/IEC 27001:2005 – São Paulo: Módulo Security Magazine, 19 jan 2006. Disponível em <http://www.modulo.com.br> seção documentos - artigos.

ISO 17799. ABNT NBR ISO/IEC 17799:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas – Rio de Janeiro: ABNT, 2005.

MÓDULO. 9ª Pesquisa Nacional de Segurança da Informação – Rio de Janeiro: Outubro/2003. Disponível em <http://www.modulo.com.br/pdf/nona_pesquisa_modulo.pdf>.

MORAES, Giseli Diniz de Almeida; TERENCE, Ana Claúdia Fernandes; ESCRIVÃO

FILHO, Edmundo. A tecnologia da informação como suporte à gestão estratégica da informação na pequena empresa – Revista de Gestão da Tecnologia e Sistemas da Informação, v.1, n.1, 2004, p. 28-44.

LUNARDI, Guilherme Lerch; DOLCI, Pietro Cunha. Adoção de Tecnologia da Informação e seu Impacto no Desempenho Organizacional: um estudo realizado com micro e pequenas empresas – Salvador: ENANPAD - 30º Encontro da ANPAD, 2006.

OLIVA, Rodrigo Polydoro; OLIVEIRA, Mírian. Elaboração, Implantação e Manutenção de Política de Segurança por Empresas no Rio Grande do Sul em relação às recomendações da NBR/ISO17799 – ENANPAD, 2003.

PALVIA, Prashant C.; PALVIA, Shailendra C. An examination of the IT satisfaction of small-business users. Information & Management. Amsterdam: Mar 8, 1999.Vol.35, Iss. 3; p. 127, 11 p..

PRATES, Gláucia Aparecida; OSPINA, Marco Túlio. Tecnologia da Informação em Pequenas Empresas: fatores de êxito, restrições e benefícios – RAC, v.8, n.2, Abr/Jun-2004, p. 09-26.

ROCHA, Luís Fernando. Governança em TI e Segurança: COBIT e ISO 17799 no mercado financeiro – Modulo Security Magazine, 29/09/2003. Disponível em <http://www.modulo.com.br> seção documentos - artigos.

SCHNEIER, Bruce. Segurança.com: segredos e mentiras sobre a proteção na vida digital – Rio de Janeiro: Campus, 2001.

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