Gestão de Segurança da Informação

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.

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 armaze-

nada 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 se tornam 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).

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.

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.

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.

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.

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).

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.

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".

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.

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.

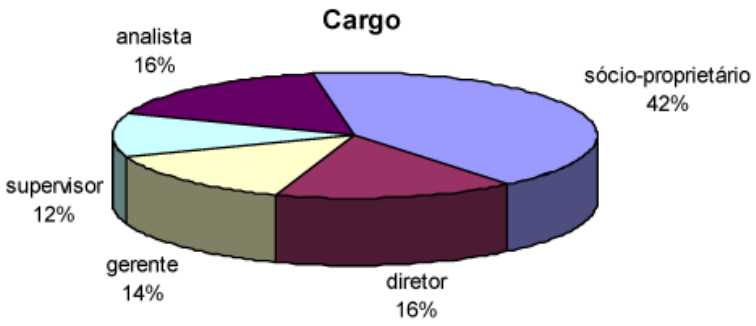

Gráfico 1: distribuição de cargos nas empresas pesquisadas

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.

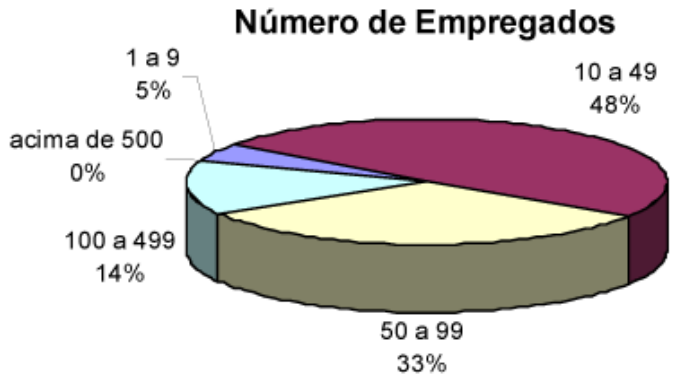

Gráfico 2: número de empregados das empresas pesquisadas

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

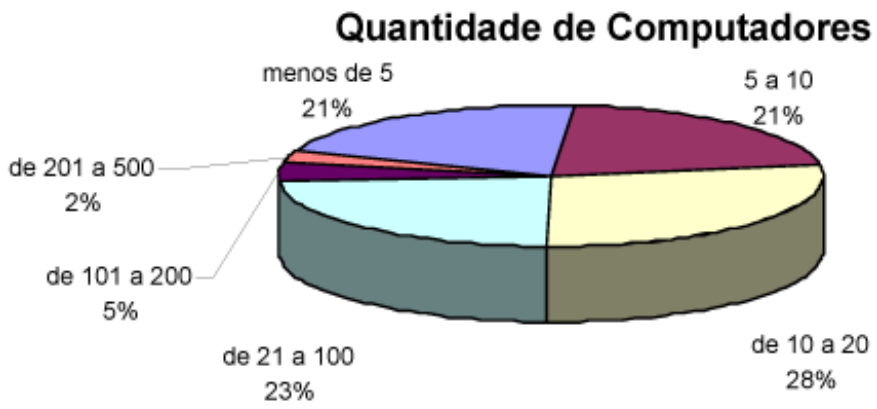

Gráfico 3: quantidade de computadores

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.

Ferramentas e Técnicas de Gestão da Segurança da Informação

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.

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.

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.

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.

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.

O avanço acelerado das Tecnologias da Informação e da Comunicação nos últimos anos, em especial a Internet e a mobilidade constituíram a Sociedade da Informação e do Conhecimento.

A nova era tecnológica tem trazido importantes ganhos para a humanidade, proporcionando crescimento e produtividade; mas, em contrapartida, tem colocado as organizações diante de riscos inerentes ao acesso ou ao ataque às informações armazenadas nos sistemas computacionais corporativos.

A informação, ativo cada vez mais valorizado, impacta diretamente na continuidade dos negócios e na sua credibilidade. Por conta disso, as empresas têm buscado soluções para mitigar esses riscos, estabelecendo um conjunto de boas práticas por meio de políticas de segurança gerenciadas em diferentes instâncias com funções e responsabilidades bem definidas. Tudo isso para assegurar o nível de segurança adequado ao negócio.

Este é o conceito de Gestão da Segurança da Informação que abrange a criação de processos voltados ao monitoramento contínuo da integridade das informações, à prevenção de ataques e ao furto dos dados, assegurando em casos emergenciais o pronto restabelecimento dos sistemas e o acesso seguro às informações das companhias.

No nosso país, o Comitê Brasileiro sobre as Normas de Gestão de Segurança da Informação (série 27000) é responsável por normatizar essa questão. O grupo é formado por especialistas que colaboram com a ISO (International Organization for Standardization) para o desenvolvimento de padrões internacionais nesta esfera.

As normas de Gestão da Segurança da Informação se fundamentam em 10 premissas básicas aplicadas em qualquer tipo de organização, sendo elas:

- Política de Segurança da Informação

- Segurança Organizacional

- Classificação e controle dos ativos de informação

- Segurança em pessoas

- Segurança Física e Ambiental

- Gerenciamento das operações e comunicações

- Controle de Acesso

- Desenvolvimento de Sistemas e Manutenção

- Gestão da continuidade do negócio e a Conformidade.

Essas premissas abrangem o conjunto de melhores práticas a serem seguidas pelas companhias tais como: a estruturação do plano diretor de segurança e de contingência; a definição da política de segurança da informação; a análise de riscos, vulnerabilidades e testes de invasão; a implementação de controles de segurança; autenticação e autorização.

Toda essa orientação está prevista no Sistema de Gestão da Segurança da Informação (SGSI), um conjunto de processos e procedimentos, baseado em normas ISO, implementado para prover segurança no uso dos ativos tecnológicos de uma empresa. Tal sistema deve ser seguido por todos aqueles que se relacionam direta ou indiretamente com a infraestrutura de TI da organização.

A implantação do SGSI envolve primeiramente a análise de riscos na infraestrutura de TI para identificar os pontos vulneráveis e as falhas nos sistemas que deverão ser corrigidos. Em seguida, são definidos processos para detectar e responder aos incidentes de segurança e procedimentos para auditoria.

Este sistema garante segurança e integridade às informações das organizações. “Os bancos quando implementaram as primeiras soluções de internet banking ainda não possuíam soluções avançadas de Segurança da Informação alinhadas a esse conceito e tiveram grandes prejuízos com os roubos virtuais”, comenta José Antonio Antonioni, Diretor de Qualidade e Competitividade da SOFTEX, organização não-governamental que promove atividades de inovação e desenvolvimento por meio da educação, cultura e treinamento apropriados, de natureza técnica e mercadológica em Tecnologia de Software.

Com foco nas ameaças iminentes e na evolução constante da tecnologia, o Comitê Brasileiro trabalha neste momento no desenvolvimento de novas normativas relacionadas aos programas de auditoria do SGSI.

Essas diretrizes irão orientar a condução de auditorias internas e externas de acordo com a ISO/IEC 27001:2005 (Sistemas de Gestão de Segurança da Informação – Requisitos) formando auditores líderes no SGSI com capacidade analítica para identificar eventuais riscos e/ou oportunidades de melhoria no processo de Segurança da Informação.

A expectativa do Comitê é que as organizações realizem, o mais breve possível, a reestruturação da área de auditoria atualizando o conhecimento dos auditores e aplicando essas novas metodologias.

SGSI

É um sistema não necessariamente informatizado, embasado nas normas NBR ISO/IEC 27001:2006 e NBR ISO/IEC 27002:2006***.**

O SGSI torna-se pré-requisito à ser implementado em ambientes corporativos, educacionais, industriais, governamentais e qualquer outro que tenha por objetivo resguardar ambientes que criam, manipulam ou destroem informações relevantes.

O sistema será informatizado, caso seja necessário, conforme a peculiaridade de cada negócio (ambiente). Pois a Segurança da Informação (SI) é norteada por boas práticas, mudança de hábitos e cultura conforme o tópico “Impactos Culturais” (parte 2 do artigo) e não apenas definidas por bons softwares e ferramentas de apoio.

Tecnologias e Ferramentas de Apoio Como Segurança

Muitos gerentes, analistas e consultores de TI dentre outros, equivocadamente associam Segurança da Informação (SI) e sua totalidade a: Antivírus, Antispyware, Antiphishing, Firewall, criptografia, soluções de DLP (Data Loss Prevention), ferramentas de monitoramento, ambientes de desenvolvimento segregados, tolerância a falhas, salas cofre e muitos outros. Entretanto estes são simplesmente alguns dos requisitos de segurança que aliados a procedimentos, políticas e processos compõem a prática de SI. Notem que ainda não citei o Compliance pois nos dará conteúdo para mais um artigo ao qual falaremos em um futuro breve. Desta forma softwares e soluções informatizadas utilizados isoladamente são apenas paliativos que maquiam o ambiente e fornecem a falsa sensação de segurança.

Espinha Dorsal do Sistema

Conforme citado no primeiro tópico, as referências utilizadas são as normas, através delas e de um mapeamento prévio melhor explanado no tópico “O que Proteger?”, a PSI (Política de Segurança da Informação) é desenvolvida.

A PSI contempla as boas práticas de SI adaptadas ao cenário de cada empresa, se tornando base para criação de procedimentos e processos, juntamente com as demais políticas do âmbito de negócio e tecnologia. Após criada a PSI e antes de sua divulgação, a diretoria possui a incumbência de aprová-la e principalmente apoiá-la, pois, será fonte de consulta para tudo que envolver segurança seja ela física ou lógica.

O que proteger?

Pois bem, foram comentadas as tecnologias, normas, políticas e duas conclusões já são visíveis:

O SGSI nos dará muito trabalho para implementar;

Como protegeremos tudo?

Nos limitaremos apenas a segunda conclusão devido nosso tempo, claro que não será simples implementar, porém tudo obviamente ficaria mais trabalhoso do que apenas uma parte.

Desta forma, o que deverá ser protegido será definido pela diretoria e departamentos estratégicos da empresa, pois existem informações mais relevantes do que outras, de cunho competitivo inclusive no aspecto legal, as quais devem ter um tratamento diferenciado e o objetivo do SGSI é exatamente este, o tratamento adequado a informações do tipo restritas, sejam elas comerciais, financeiras, políticas ou até mesmo legais. O foco é definir quem são elas, cada empresa possui suas particularidades em seus respectivos segmentos e ninguém melhor do que a própria empresa para definir quais informações são importantes.

Uma vez definido o que é importante (entenda crítico) para o negócio, o SGSI baseado na PSI e com o apoio da tecnologia aplicará as medidas necessárias para classificar e tratar estas informações.

Os passos abaixo fazem parte da manipulação destas informações:

Saber quais processos de negócios envolvem ou geram estas informações;

Estar claro quem deve ter acesso;

Quais os tipos de acesso existirão;

Quem será o dono desta (s) informação (ões);

Existir classificação da informação (Pública, Restrita ou Confidencial);

Auditoria e Monitoramento periódico;

Como descartar a informação;

Existirem termos de Responsabilidade e Confidencialidade;

Estar definida uma matriz de responsabilidades;

Estes são alguns dos passos que o SGSI deverá ter bem definido para manter a confidencialidade destas informações.