RODRIGO DINIZ LARA

ANÁLISE DA SEGURANÇA DA INFORMAÇÃO DAS SECRETARIAS DE ESTADO DE MINAS GERAIS

Belo Horizonte
2004

RODRIGO DINIZ LARA

ANÁLISE DA SEGURANÇA DA INFORMAÇÃO DAS SECRETARIAS DE ESTADO DE MINAS GERAIS

Monografia de conclusão de curso apresentada ao Curso Superior de Administração – habilitação em Administração Pública promovido pela Escola de Governo da Fundação João Pinheiro, para aprovação na disciplina Estágio Supervisionado II e requisito para obtenção do título de Bacharel no referido curso.

Orientador: Sérgio Martins Barbosa
Supervisor: Marconi Martins de Laia

Belo Horizonte
2004

Dedico este trabalho aos meus pais, que não mediram esforços para a minha formação acadêmica, e as minhas irmãs, pela paciência e carinho.

Agradeço,

A Deus, por ter me guiado nessa longa caminhada.

À Cecília, pelo amor e carinho.

Ao meu orientador, Sérgio Martins Barbosa, cuja experiência e apoio me ajudaram a concluir este trabalho de forma conclusiva.

À SCGE e a Adriene, pelo apoio na marcação das entrevistas.

Aos profissionais das Secretarias de Estado de Minas Gerais que participaram dessa pesquisa, pela cordialidade ao longo das entrevistas.

À Helena Schirm, pela ajuda na normalização desse trabalho.

Ao Moreira, Elieth, Silvana e coordenadoras do PROAP, pela experiência profissional adquirida ao longo do curso.

Aos professores e funcionários da Escola de Governo da Fundação João Pinheiro, pelo conhecimento adquirido e estrutura oferecida ao longo do curso.

Aos amigos e familiares, pelos momentos felizes vividos juntos.

Ao X CSAP, turma inesquecível.

A todos, meus sinceros agradecimentos por terem me ajudado nesse trabalho acadêmico e ao longo do Curso Superior de Administração Pública.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

RESUMO

Tendo em vista a importância da informação no contexto organizacional atual, o presente trabalho tem como objetivo geral realizar um diagnóstico da situação em que se encontra a segurança da informação nas Secretarias de Estado de Minas Gerais, buscando analisar como estas instituições têm lidado com a proteção de suas informações. Para a realização do trabalho foi feita uma revisão bibliográfica sobre o macro-tema segurança da informação e, posteriormente, foi realizada uma pesquisa em todas as 15 Secretarias de Estado de Minas Gerais que compõe o Poder Executivo em 2004, com o intuito de investigar qual a situação em que se encontra a segurança da informação nestas organizações. Esta pesquisa foi baseada na Pesquisa Nacional de Segurança da Informação, realizada pela empresa Módulo Security Solutions, e na NBR ISO/IEC 17 799, norma nacional que estabelece um código de boas práticas relativas à gestão da segurança da informação. Como resultado da pesquisa, conclui-se que existe uma longa trajetória a ser traçada pelas Secretarias de Estado de Minas Gerais para alcançar um nível satisfatório para a proteção de suas informações. O alto índice de organizações que tiveram problemas com segurança da informação nos últimos seis meses, a falta de implementação das melhores práticas em segurança da informação sugeridas pela NBR ISO/IEC 17 799 e a inexistência de um fórum de gestão da segurança da informação, indicam uma situação crítica em relação à proteção da informação nas Secretarias de Estado de Minas Gerais.

Palavras-chave: Segurança da informação – NBR ISO/IEC 17 799 – Gestão da segurança da informação.

SUMÁRIO

1 INTRODUÇÃO

Ao longo das últimas décadas, a informação vem sendo tratada como o recurso principal e mais valioso das organizações. Hoje se vive na chamada Sociedade da Informação, também denominada por Castells (2003) como a Sociedade em Rede, em que o ambiente *pode ser visto com um emaranhado de fluxos de informação a que indivíduos* e organizações têm que se readaptar.

A informação adquiriu o *status* de recurso fundamental para as organizações, em decorrência do desenvolvimento da Tecnologia da Informação e Comunicação (TIC)[1], que tornou a informação cada vez mais difusa nas últimas décadas. Com o avanço na disponibilidade da comunicação, do computador e da Internet, as sociedades ganharam importantes ferramentas para a disseminação da informação. Na Administração Pública já existe um grande número de serviços disponíveis em forma eletrônica, e alguns, como a Declaração de Imposto de Renda, já são amplamente utilizados pelos cidadãos.

Na sociedade atual, quem tem a informação, passa a ter o poder. No contexto do Estado, a partir de informações adequadas e que se tem o poder de realizar uma análise da realidade social e subseqüente elaboração, aplicação e controle de políticas públicas mais eficientes e eficazes para a sociedade.

Tendo em vista a importância da informação no ambiente organizacional, é de grande relevância zelar pela sua segurança. Informações adulteradas sem autorização do proprietário, indisponíveis no momento em que se necessita dela, e sob o conhecimento de pessoas ou organizações não-autorizadas a terem acesso às mesmas, podem comprometer significativamente o andamento dos processos organizacionais, sendo possível até inviabilizar a continuidade dos serviços da organização se não for dada a devida atenção à segurança de suas informações.

---

[1] "A informação, não só como conceito, mas também como ideologia, está intrinsecamente ligada ao desenvolvimento do computador durante e após a II Guerra Mundial (Kumar, 1997). Dois pontos focais aparecem como determinantes para a formação da sociedade da informação: a computação e a comunicação, que por sua vez, são diretamente ligadas a 'dois objetos tecnológicos': o microcomputador e a rede Internet (BELL *apud* Kumar, 1997)" (AKUTSU; PINHO, 2002, p. 726)

Sêmola (2003) coloca que a crescente valorização da informação como principal ativo das organizações, somada a alguns fatores como a dependência dos processos organizacionais em relação aos sistemas de informação; o crescimento contínuo da digitalização das informações; o crescimento exponencial da conectividade da organização; o crescimento do compartilhamento das informações; a maciça utilização da Internet; a grande diversidade e compartilhamento de técnicas de ataque e invasão; a carência de mecanismos legais de responsabilização em ambiente virtual; e a diversificação dos tipos de ameaças (funcionários insatisfeitos, cracker, hacker, pragas virtuais, spam, engenharia social, etc); tem influenciado para que a segurança da informação seja considerada uma real necessidade e um requisito estratégico, que interfere na capacidade das organizações de realizarem suas atividades com eficiência e eficácia.

Considerando o contexto descrito acima, esse estudo se pauta pelo seguinte problema de pesquisa: "As Secretarias de Estado de Minas Gerais, órgãos responsáveis pela execução das funções essenciais do Governo Estadual, têm implementado mecanismos de segurança eficazes para a proteção de suas informações, recursos indispensáveis para o funcionamento adequado de qualquer organização, especialmente aquelas que prestam serviços essenciais para a população?"

Levando em consideração o problema de pesquisa levantado, esse trabalho monográfico possui como objetivo geral realizar um diagnóstico da situação em que se encontra a segurança da informação nas Secretarias de Estado de Minas Gerais, buscando analisar como estas instituições têm lidado com a proteção de suas informações.

Para se atingir o objetivo da monografia foi feita uma revisão bibliográfica sobre o macro-tema segurança da informação e, posteriormente, foi realizada uma pesquisa em todas as 15 Secretarias de Estado de Minas Gerais, com o intuito de investigar qual a situação em que se encontra a segurança da informação na organização. A pesquisa elaborada foi baseada na Pesquisa Nacional de Segurança da Informação, realizada pela empresa Módulo Security Solutions, e também na NBR ISO/IEC 17 799, norma nacional de segurança da informação, que estabelece um código de boas práticas relativas à gestão da segurança da informação.

Este trabalho acadêmico divide-se em mais cinco seções, um apêndice e um anexo, além desta introdução. A segunda seção constitui-se de uma revisão bibliográfica sobre o macro-tema segurança da informação e enfocará quatro assuntos: os principais conceitos de segurança da informação; as principais ameaças aos ativos da organização; a NBR ISO/IEC 17 799; e o Sistema de Gestão da Segurança da Informação, com as ações de segurança mais características de cada fase desse modelo. A terceira seção apresenta os procedimentos metodológicos e operacionais para a realização desse trabalho. A quarta seção contém a apresentação e a análise dos resultados da pesquisa. A quinta seção apresenta as principais conclusões do trabalho. A sexta seção contém as referências bibliográficas utilizadas. Por fim, é apresentado o apêndice A, que contém o formulário utilizado na pesquisa, e o anexo A, que contém uma descrição resumida das principais tecnologias em segurança da informação.

2 SEGURANÇA DA INFORMAÇÃO

Nessa seção é realizada uma revisão bibliográfica sobre o macro-tema segurança da informação focando quatro assuntos que são a base teórica para a compreensão desse trabalho acadêmico. A seção **2.1** abordará os principais conceitos de segurança da informação com o intuito de facilitar a compreensão das seções posteriores. A seção **2.2** apresentará alguns tipos mais comuns de ameaças que os ativos das organizações atualmente estão expostos. A seção **2.3** abordará a norma nacional de segurança da informação, denominada NBR ISO/IEC 17 799, considerada uma fonte relevante de controles em segurança da informação. Por fim, a seção **2.4** apresentará o Sistema de Gestão de Segurança da Informação, um modelo que serve de base para o gerenciamento da segurança da informação nas organizações.

2.1 Conceitos de segurança da informação

Esta seção busca apresentar de forma clara alguns termos que são bastante utilizados no ambiente de segurança da informação com o objetivo de embasar a leitura e a compreensão das seções posteriores. É importante destacar que a definição de segurança da informação será apresentada no final da seção, depois que forem apresentados os termos essenciais para a sua compreensão.

2.1.1 Ativos

O primeiro termo a ser definido neste trabalho acadêmico é o que vem a ser um ativo no ambiente de segurança da informação, já que a NBR ISO/IEC 17 799 menciona que "a informação é um ativo, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida." (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003, p.2)

Ativo é todo elemento que manuseia direta ou indiretamente a informação, a contar a própria informação (SÊMOLA, 2003; MOREIRA, 2001; MAIA, 2002), e são os elementos que a segurança da informação visa proteger. Sêmola (2003) dividi os ativos em seis grupos:

1°) equipamentos; este grupo contempla os computadores, notebooks, disquetes, cd-roms, os servidores, ou seja, todos os instrumentos tecnológicos onde a informação é armazenada, transportada e processada;

2°) aplicações; este grupo corresponde aos programas de computador que processam e armazenam as informações, como banco de dados, sistemas operacionais (Windows, Linux), sistemas de informação[2], programas de correios eletrônicos, entre outros;

3°) usuários; este grupo corresponde a todas as pessoas que utilizam a informação na organização, como os seus funcionários, prestadores de serviço, estagiários, entre outros;

4°) ambientes; este grupo corresponde à estrutura física da organização onde estão localizados os outros grupos de ativos, como as salas e armários, bibliotecas, cofres etc;

5°) informações[3]; como expõe a NBR ISO/IEC 17 799, a informação pode existir em muitas formas, podendo "[...] ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas." (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003, p. 2); e

6°) processos; este grupo corresponde ao conjunto de atividades realizadas para o funcionamento da organização, como o pagamento dos funcionários, a prestação de serviços para os clientes, aquisição de equipamentos e etc.

2.1.2 Princípios da segurança da informação

Segundo vários autores (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003; MOREIRA, 2001; SÊMOLA, 2003; AMOROSO *apud* VELOSO, 2002), para se garantir a segurança das informações deve-se preservar três princípios básicos:

---

[2] O Governo do Estado de Minas Gerais possui grandes sistemas de informação corporativos, como por exemplo, o Sistema de Informações Institucionais (SINFI), o Sistema Integrado de Administração Financeira de Minas Gerais (SIAFI/MG) e o Sistema Integrado de Administração de Materiais e Serviços (SIAD).

[3] Existem várias definições para o termo informação. Uma das definições que se adapta ao contexto da segurança da informação é a constante na apostila de Castelo Branco (2003, p. 5), que considera ela como um " 'ativo' resultante do tratamento de dados, que auxilia as funções de planejamento, organização, direção e controle, reduzindo a incerteza no processo decisório."

a) a confidencialidade, que consiste que as informações somente serão acessíveis para indivíduos e organizações autorizadas;

b) a disponibilidade, que consiste que a informação e seus ativos correlatos sempre estarão disponíveis no momento em que as pessoas e organizações autorizadas necessitarem; e

c) a integridade, que consiste na proteção da informação contra qualquer tipo de alteração de pessoas ou organizações não autorizadas.

A preservação dos três princípios básicos da segurança da informação possibilita que a organizações garanta as condições essenciais para o desenvolvimento de suas atividades em um ambiente seguro.

Outros aspectos, alinhados com os princípios básicos da segurança da informação, também são mencionados como elementos a serem considerados para a gestão da segurança da informação nas organizações. Podemos destacar a autenticidade, o não repúdio e a legalidade dentre esses elementos.

A autenticidade é a garantia de que a informação ou usuário da mesma sejam autênticos, ou seja, atesta com exatidão a identidade dos elementos que estão compondo o processo de comunicação (SÊMOLA, 2003; BRASIL, 2000).

O não-repúdio é a capacidade de provar tecnicamente a origem das informações e confirmar a distribuição das informações, ou seja, demonstra-se que a transmissão ocorreu de fato, entre o remetente e o receptor. Desta forma, impede o remetente de negar o envio da informação, ou o receptor de negar a recepção da informação. (BRASIL, 2000; MOREIRA, 2001).

A legalidade, segundo Sêmola (2003, p. 47) é a "característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes". O aspecto da legalidade é um item essencial para a prática da segurança da informação na Administração Pública já que, a Constituição Federal de 1988,

em seu Art. 37[4], o considera como os dos cinco princípios que devem nortear as ações dos indivíduos que trabalham na Administração Pública.

2.1.3 Ameaças

Ameaças são agentes ou condições que podem gerar incidentes de segurança que atingirão os ativos por meio da exploração de suas vulnerabilidades, atingindo negativamente os princípios básicos da segurança da informação, acarretando dessa forma, em impactos as atividades da organização (SÊMOLA, 2003; MOREIRA, 2001).

Sêmola (2003, p. 47-48) adotando o critério da intencionalidade, agrupa as ameaças em três tipos:

> a) naturais, ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição etc;
>
> b) involuntárias, ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia etc;
>
> c) voluntárias, ameaças propositais causadas por agentes humanos como hac*kers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

2.1.4 Vulnerabilidades

No âmbito da segurança da informação, vulnerabilidades são as falhas ou fraquezas presentes em um ativo ou grupo de ativos que abrem a possibilidade para que as ameaças explorem tais pontos fracos ensejando um incidente de segurança, atingindo os princípios básicos da segurança da informação: confidencialidade, integridade e disponibilidade (SÊMOLA, 2003).

As vulnerabilidades podem estar presentes em qualquer ambiente de uma organização. Segundo, Moreira (2001, p. 22), "todos os ambientes são vulneráveis, partindo do pressuposto de que não existem ambientes totalmente seguros".

---

[4] "**Art. 37.** A administração pública direta, indireta ou fundacional, de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de **legalidade**, impessoalidade, moralidade, publicidade [...]." (destaque nosso).

Como exemplos de vulnerabilidades podemos citar: a falta de extintores, detectores de fumaça e de outros recursos para o combate a incêndio; a falta de treinamento dos trabalhadores; a utilização de mídias (disquetes, fitas magnéticas) antigas ou de baixa qualidade; a troca de informações confidenciais sem proteção adicional; erros ou problemas durante a instalação de um *hardware*; erros na instalação ou na configuração de um *software* que podem provocar acessos indevidos; instalações prediais fora do padrão; o compartilhamento de informações confidenciais como senhas; a não execução de rotinas de segurança; entre outras inúmeras vulnerabilidades (SÊMOLA, 2003; MOREIRA, 2001).

A identificação das vulnerabilidades presentes nos ambientes corporativos é de extrema importância, pois possibilita um diagnóstico de quais ameaças podem afetar negativamente os ativos, possibilitando aos gestores a escolha de mecanismos eficazes de segurança da informação (MOREIRA, 2001).

É importante destacar que as vulnerabilidades isoladamente não provocam incidentes, "[...] pois são elementos passivos, necessitando para tanto de um agente causador ou condição favorável, que são as ameaças." (SÊMOLA, 2003, p. 48)

2.1.5 Risco

A informação e os ativos relacionados a ela são elementos considerados de grande valor para as organizações independentemente do setor em qual a organização está inserida atualmente. Todos os processos organizacionais são baseados em informações (SÊMOLA, 2003; MOREIRA, 2001).

Entretanto, prover a segurança da informação é uma tarefa árdua já que todos os ativos da organização "[...] estão sujeitos a vulnerabilidades em maior ou menor escala e, neste caso, estas vulnerabilidades proporcionam riscos [para a organização]". (MOREIRA, 2001, p.21)

Segundo Sêmola (2003, p. 50), o risco, no ambiente de segurança da informação, é a "probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios [ou atividades da organização]."

Os riscos surgem a partir da presença de vulnerabilidades nos ativos da organização que posteriormente podem ser exploradas por ameaças causando incidentes de segurança (MOREIRA, 2001).

2.1.6 Incidentes de segurança / Impacto

Um incidente de segurança é qualquer evento que provêem de uma ameaça efetiva, que explorou algum tipo de vulnerabilidade presente no ambiente de trabalho, que ocasionou à perda dos princípios básicos da segurança da informação gerando impactos negativos aos processos organizacionais (SÊMOLA, 2003; MOREIRA, 2001).

Moreira (2001) relata que cada ameaça pode acarretar vários tipos de incidentes de segurança, e cita como exemplo, o vírus (ameaça) que quando infecta uma máquina pode ocasionar vários incidentes, entre eles, a perda de informações, parada do sistema e lentidão da máquina infectada.

O termo impacto possui uma relação direta com os incidentes de segurança e pode ser definido, segundo Sêmola (2003, p. 50), como a "abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio."

2.1.7 Medidas de segurança

Medidas de segurança são as práticas, os procedimentos e os mecanismos utilizados para proteger a informação e seus ativos dos incidentes de segurança, tentando reduzir ao máximo as vulnerabilidades presentes no ambiente de forma que diminua a probabilidade de que as ameaças explorem-nas (SÊMOLA, 2003; MOREIRA, 2001).

As medidas de segurança podem assumir as seguintes características:

a) preventivas, que são as medidas de segurança baseados na precaução, com o objetivo de prevenir que os incidentes de segurança venham a ocorrer (SÊMOLA, 2003). Podemos dar como exemplos, às políticas de segurança da informação, campanhas e palestra de conscientização de usuários, treinamento de funcionários e ferramentas técnicas como *firewall* e o antivírus;

b) detectáveis, que são as medidas de segurança que procuram localizar possíveis condições ou agentes, ou seja, ameaças, com o intuito de impedir que as mesmas explorem as vulnerabilidades causando incidentes de segurança (SÊMOLA, 2003). Podemos dar como exemplo a análise de riscos, os sistemas de detecção de intrusão e as câmeras de vigilância; e

c) corretivas, que são medidas de seguranças que procuram corrigir a estrutura física, humana e tecnológica afetada por um incidente de segurança com o intuito de recuperar e dar continuidade às atividades da organização. (SÊMOLA, 2003; MOREIRA, 2001). Podemos dar como exemplo dessa medida o Plano de Contingência.

Sêmola (2003) destaca que uma medida de segurança pode assumir mais de uma característica e cita o exemplo do Plano de Contingência, que quando elaborado funciona como uma ação preventiva e quando é utilizado é uma ação de caráter corretiva.

2.1.8 Ciclo da segurança da informação

A luz dos conceitos apresentados anteriormente cabe agora definir o que vem a ser segurança da informação. Sêmola (2003, p.43) relata que a segurança da informação é "[...] uma área do conhecimento dedicada à proteção dos ativos da informação contra acessos não autorizados, alterações indevidas ou a sua indisponibilidade", ou seja, preservando os três princípios básicos da segurança da informação. Ainda segundo o autor, a segurança da informação, de forma mais ampla, pode ser considerada como a "[...] a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação". (SÊMOLA, 2003, p. 43)

Segurança da informação, conforme exposto pela norma NBR ISO/IEC 17 799, "protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio". (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003, p. 2). Ainda segundo a norma, a segurança da informação é caracterizada pela preservação da confidencialidade, integridade e disponibilidade da informação.

Dentre os conceitos apresentados, podemos perceber que todos eles giram em torno da preservação dos três princípios básicos da segurança da informação: integridade, confidencialidade e disponibilidade da informação.

Por fim, cabe apresentar o ciclo resumido da segurança da informação (fig. 2.1), relacionando os diversos conceitos apresentados nessa seção. Todas as atividades da organização dependem dos ativos para sua execução. Os ativos da organização, por sua vez, podem conter falhas ou fraquezas denominadas vulnerabilidades. Estas vulnerabilidades podem ser exploradas pelas ameaças, expondo os ativos a riscos de segurança. A ameaça, quando explora alguma vulnerabilidade do ativo, compromete os princípios básicos da segurança da informação (confidencialidade, integridade e disponibilidade), causando impactos sobre as atividades organizacionais. Para reduzir e administrar os riscos de segurança na organização são implementadas controles físicos, tecnológicos e humanos, ou seja, medidas de segurança, que eliminam ou reduzem as vulnerabilidades dos ativos levando a organização a atingir o nível de segurança adequado para a realização de suas atividades.

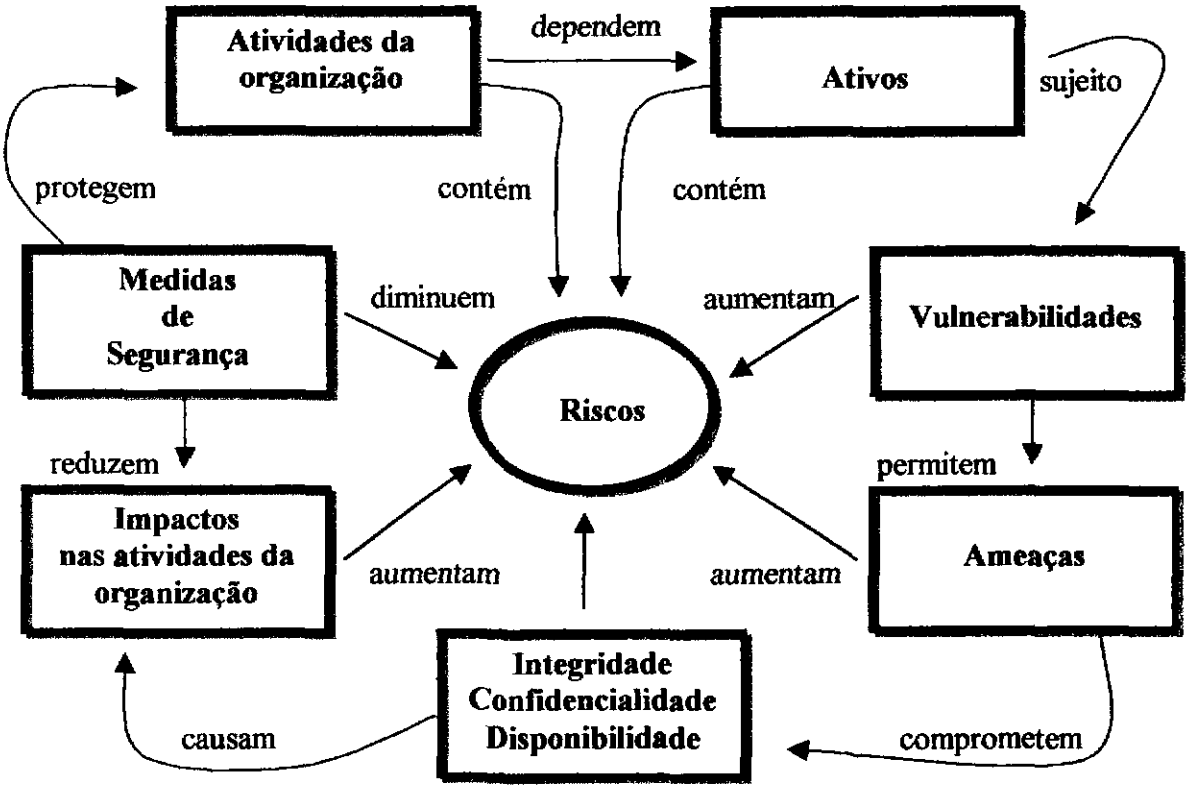


Figura 2.1 Ciclo da Segurança da Informação
Fonte: Adaptado de: MOREIRA, Nilton Stringasci. **Segurança mínima:** uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001. p. 21.

2.2 Ameaças aos ativos

As ameaças, como exposto na seção **2.1.3**, são agentes ou condições que podem gerar incidentes de segurança que atingirão os ativos por meio da exploração das vulnerabilidades atingindo negativamente os princípios básicos da segurança da informação, acarretando dessa forma, em impactos as atividades da organização (SÊMOLA, 2003; MOREIRA, 2001).

Para garantir a proteção dos ativos da organização é importante conhecer as ameaças e as técnicas de ataques utilizados pelos indivíduos, para então aplicar as medidas e ferramentas adequadas para a salvaguardar esses ativos.

Esta seção tem o intuito de apresentar alguns tipos de ameaças existentes, sem com tudo esgotar o assunto, pois a idéia é mostrar os tipos mais comuns para que o leitor da monografia possa verificar a necessidade e a importância de estudar e aprofundar neste tema. É necessário ressaltar que os responsáveis pela segurança das informações nas organizações necessitam dedicar uma parte do seu tempo para aprendizado e atualização das novas ameaças.

2.2.1 Ameaças internas

As ameaças de origem internas estão presentes nos ambientes das organizações independentemente se tais estão conectadas à Internet ou não. Geralmente os funcionários insatisfeitos e/ou mal treinados são apontados pelas pesquisas como as principais ameaças internas da organização. Outros agentes que podem ser considerados como ameaças internas são os prestadores de serviço e funcionários terceirizados que trabalham para a organização. A seguir serão apresentadas alguns tipos mais comuns de ameaças internas:

a) erros humanos

A 9ª Pesquisa Nacional de Segurança da Informação relatou que 41% dos entrevistados consideram os erros e acidentes humanos como uma das principais ameaças à segurança da informação nas organizações (MÓDULO SECURITY SOLUTIONS, 2003). {Moreira (2001, p. 49) destaca que "[...} em geral, a falta de treinamento e de suporte [e]

omissões por parte dos funcionários [...]" acabam por se tornarem as principais causas dos erros e acidentes humanos. Podemos dar como exemplos de incidentes ocasionados por essa ameaça, o uso incorreto de ferramentas de trabalho e o apagamento acidental de dados.

b) roubo de informações

Moreira (2001) expõe que o roubo de informações não se caracteriza apenas quando os computadores e *notebooks* da organização são roubados fisicamente, mas também quando são subtraídas as informações que eles contém. Os meios pelos quais as informações são retiradas dos ativos tecnológicos podem ser de diversas formas. Podemos ter como exemplos à cópia dos dados em algum tipo de dispositivo de armazenamento (disquete, cd-rom e etc.) ou por e-mail.

c) funcionários insatisfeitos

As três últimas Pesquisas Nacionais de Segurança da Informação (2001, 2002, 2003) apontam os funcionários insatisfeitos entre as duas principais ameaças à segurança da informação nas organizações pesquisadas. Segundo reportagem da ABC News (2002),

> antigamente, funcionários insatisfeitos procuravam vingança contra a empresa roubando acessórios do escritório ou espalhando boatos maldosos sobre seus chefes. Hoje, com o avanço do ambiente de informática nas empresas, o ataque desses mesmos funcionários mudou. Por isso, a constatação que o maior perigo de invasões e destruição [de] importantes arquivos do sistema [da organização] ser interno.

Moreira (2001) relata que o roubo de senhas, o uso indevido de conta e senha com grande nível de acesso na rede interna, decodificação seguida de alteração de programas executáveis e, acesso e alteração de dados direto em Banco de dados são os incidentes de segurança mais comuns causados por funcionários insatisfeitos:

2.2.2 Ameaças externas

Ameaças externas "[...] representam todos os ataques oriundos de fora do ambiente da organização com o objetivo de explorar as vulnerabilidades de um determinado sistema computacional para uma finalidade qualquer." (MOREIRA, 2001. p. 60).

Geralmente as ameaças externas são causadas por indivíduos que não pertencem à organização e possuem conhecimentos aprofundados na área de informática. As causas que levam tais agentes a obterem acesso remoto não-autorizados aos sistemas da organização são variadas. Abaixo são apresentados alguns motivos para a ação de tais agentes:

a) os ganhos financeiros adquiridos decorrentes da invasão a banco de dados financeiros que possibilitem a transferência de valores para contas ilícitas, a redução de dívidas de alguns indivíduos ou captação de alguns dados relevantes (números de CPFs e cartões de créditos) com o intuito de vender para pessoas interessadas em tais dados. Os ganhos financeiros são uma das principais razões para invasão de sistemas (MOREIRA, 2001);

b) vingança, já que ex-funcionários podem ter alguma restrição a organização por considerarem que a sua demissão foi injusta e se tornam uma ameaça potencial se não houver o cancelamento do seu acesso remoto a sistemas e outros recursos computacionais. Moreira (2001, p. 62) afirma que "os estudos de casos sugerem que a vingança é a mais provável de resultar em problemas ou danos a sistemas do que a maioria dos outros motivos.";

c) a necessidade de aceitação ou respeito dos invasores perante a um grupo. Geralmente, membros de clubes de hackers necessitam, por exemplo, invadir sistemas computacionais de grandes organizações para ganharem prestigio perante o grupo (MOREIRA, 2001);

d) questões ideológicas. Segundo reportagem da Vnunet.com de 20 de junho de 2002, estatísticas da mi2g, empresa em segurança da informação, revelam que durante "[...] a tensão vivida entre Índia e Paquistão no mês de maio de 2002, cerca de 111 sítios comerciais indianos sofreram ataques e tiveram seus serviços prejudicados. Esses ataques foram assumidos por grupos de crackers ligados a movimentos antiisraelitas e pela libertação da Cashemira";

e) a espionagem industrial que se caracteriza pela ação de indivíduos ou organizações que procuram desenvolver ações ilegais procurando explorar os sistemas de outras organizações a fim de capturar softwares a serem comercializados e projetos

importantes com o intuito de obter uma vantagem competitiva em relação a outras organizações (MOREIRA, 2001).

Ultimamente, todos os invasores externos, independentemente do motivo de tal agente estar acessando um sistema é denominado *hacker*. Alguns autores (OTILIO, 2000; MOREIRA, 2001; SCUA SEGURANÇA DA INFORMAÇÃO, 2004) mencionam que nos últimos anos vêm se criando uma confusão em relação à definição do termo *hacker*. Existem diferenças entre esses agentes e os autores relatam que o grupo de invasores externos podem ser classificados em três sub-grupos principais:

1°) *Hacker*

Indivíduo que se especializa em estudar os ativos tecnológicos (computadores, sistemas, redes) e testar seus limites, explorando suas fraquezas e falhas. Tem grande facilidade de assimilação e estuda exaustivamente algo até dominar o assunto. Depois que o hacker invade um sistema, ele não altera as informações, pois o seu intuito é o divertimento ou o desafio de poder invadir os sistemas. Apesar de não alterarem as informações, *os hackers* ferem outro princípio da segurança da informação, a da confidencialidade.

2°) *Cracker*

Agente que conhece várias linguagens de programação e sabe tanto quanto um hacker sobre invasão de sistemas. Contudo, usa seus conhecimentos para roubar dados e arquivos, números de cartão de crédito, modificar sítios e pode ser contratado para fazer espionagem industrial.

3°) Pheaker

Especialista em telefonia que procura conseguir por meio dos seus conhecimentos fazer ligações internacionais gratuitas, obter códigos de segurança de celulares, reprogramar centrais telefônicas e, principalmente, invadir remotamente um sistema sem deixar rastro.

2.2.3 Engenharia social

Engenharia social é o método utilizado para a obtenção de informações importantes de uma organização ou acesso indevido a determinado ativo organizacional, por meio da utilização de técnicas de persuasão que procuram explorar a ingenuidade e confiança dos indivíduos que possuem alguma relação com a organização, como os seus funcionários e prestadores de serviço. Os ataques que procuram utilizar a engenharia social geralmente são realizados por meio de telefonemas, envio de mensagens por correio eletrônico, salas de bate-papo e até mesmo pessoalmente (MAIA, 2001; VARGAS, 2002).

Existem diversas técnicas que utilizam a engenharia social como método de ataque. Para exemplificar tal ameaça, abaixo serão apresentados três casos típicos de engenharia social, citados pela NIC BR Security Office (2003, p. 8-9), sendo um realizado pelo telefone e dois por mensagens de *e-mail*:

> **Exemplo 1:** algum desconhecido liga para a sua casa e diz ser do suporte técnico do seu provedor. Nesta ligação ele diz que sua conexão com a Internet está apresentando algum problema e, então, pede sua senha para corrigi -lo. Caso você entregue sua senha, este suposto técnico poderá realizar uma infinidade de atividades maliciosas, utilizando a sua conta de acesso à Internet e, portanto, relacionando tais atividades ao seu nome.
>
> **Exemplo 2:** você recebe uma mensagem de *e-mail*, dizendo que seu computador está infectado por um vírus. A mensagem sugere que você instale uma ferramenta disponível em um *site* da Internet, para eliminar o vírus de seu computador. A real função desta ferramenta não é eliminar um vírus, mas sim permitir que alguém tenha acesso ao seu computador e a todos os dados nele armazenados.
>
> **Exemplo 3:** você recebe uma mensagem *e-mail*, onde o remetente é o gerente ou o departamento de suporte do seu banco. Na mensagem ele diz que o serviço de *Internet Banking* está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem. A execução deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso a conta bancária, aguardando que você digite sua senha. Na verdade, este aplicativo está preparado para furtar sua senha de acesso à conta bancária e enviá-la para o atacante. (grifo do autor)

Percebe-se que a engenharia social procura enfocar os seus ataques aproveitando as vulnerabilidades residentes na baixa conscientização dos membros da organização a respeito de cuidados de segurança. Dessa forma é importante oferecer palestras aos funcionários alertando e conscientizando-os do assunto.

O *cracker* Kevin Mitnick[5], conhecido por invadir sistemas usando a engenharia social, alertou que muitas organizações não estão preparadas para combater ataques baseados na engenharia social. Mitnick expõe que "[...]muitas pessoas pensam que não são fáceis de se enganar, que não podem ser manipuladas. No entanto, não existe verdade absoluta. A ameaça de engenharia social é significativa. As pessoas deveriam saber que você pode comprar a melhor tecnologia no mundo, que não protegerá a organização contra a engenharia social". (INFOCONOMY.COM; MÓDULO SECURITY MAGAZINE, 2002)

2.2.4 Pragas virtuais

Com o advento da Internet e a maciça utilização do e-mail, o ambiente da área de segurança da informação começou a ser ameaçado de forma significativa pela rápida disseminação de pragas virtuais pelo mundo. Estas pragas virtuais são códigos maliciosos que podem acarretar vários tipos de incidentes aos ativos de uma organização. Normalmente, as pragas virtuais são chamadas de vírus, mas tecnicamente, existem outras nomenclaturas mais específicas. As diversas pragas virtuais são classificadas pela forma como se comportam, como são ativadas ou como se espalham. A seguir será apresentada uma descrição dos principais grupos que constituem as pragas virtuais.

a) Vírus

Segundo NIC BR Security Office (2003, p. 9), "vírus é um programa capaz de infectar outros programas e arquivos de um computador. Para realizar a infecção, o vírus embute uma cópia de si mesmo em um programa ou arquivo, que quando executado também executa o vírus, dando continuidade ao processo de infecção". As formas mais comuns de se infectar um sistema com um vírus, atualmente são:

- anexos de arquivos enviados por e-mails;

---

[5] "Em 15 anos de carreira no meio hacker, Mitnick ficou famoso pela utilização perfeita de técnicas de engenharia social. No entanto, por causa disso, ficou preso durante quase cinco anos por ter invadido redes da Novell, da Motorola, da Nokia, entre outras empresas. Suas ações incluíam fraudes com uso do computador, fraudes online e interceptação de comunicações. Em janeiro de 2000, ele foi solto e cumpre a pena em liberdade condicional. Conseguiu ainda permissão federal para trabalhar como consultor de segurança e escrever colunas em sítios na Internet. Calcula-se que os prejuízos causados por Mitnick tenham chegado a cinco milhões de dólares". (INFOCONOMY.COM; MÓDULO SECURITY MAGAZINE, 2002)

- instalar programas de procedência duvidosa ou desconhecida, obtidos pela Internet;

- abrir arquivos armazenados em outros computadores, por meio de compartilhamento de recursos utilizando disquetes e CD-ROM.

Os problemas causados pela infecção por vírus podem ser variados. Os vírus podem ser programados exclusivamente para prejudicar o computador corrompendo programas, excluindo arquivos ou reformatando o seu disco rígido. Outros não são desenvolvidos para provocar danos, mas puramente para se reproduzirem e chamarem a atenção sobre a sua presença com mensagens de texto, vídeo e áudio. Entretanto, mesmo esses vírus que não causam aparentemente nenhum dano, podem consumir recursos na memória do computador podendo acarretar quedas dos sistemas de informação.

b) *Worm* (Verme)

Worm é um programa que possui a capacidade de se propagar automaticamente por meio de redes, sem a necessidade da intervenção humana, enviando cópias de si mesmo de computador para computador. Este programa se propaga explorando as vulnerabilidades existente ou falhas nos ativos computacionais (computadores, redes). (NIC BR SECURITY OFFICE, 2003; GALVÃO, 2002)

O maior problema ligado à contaminação desse programa é o fato dele poder consumir muitos recursos dos ativos computacionais devido a sua facilidade de auto-replicação, acarretando em um atraso ou interrupção dos processos de negócios da organização (NIC BR SECURITY OFFICE, 2003), e dessa forma, afetando um dos princípios básicos da segurança da informação: a disponibilidade da informação.

c) *Trojan Horse* (Cavalo de Tróia)

A denominação dada ao programa *trojan horse* é uma analogia a famosa história grega do Cavalo de Tróia[6]. Esse tipo de programa procura parecer ter alguma função

6 "No século XII A. C. iniciou-se o conflito entre Grécia e Tróia. Estas guerras perduraram por 10 anos, onde os gregos sempre perseguiam os troianos, mas nunca conseguiram vencer porque a cidade de Tróia era muito

útil ou inofensiva, como protetores de tela ou jogos, para que possam ser instalado e executado pelos usuários. Entretanto, quando são executados, eles realizam funções prejudiciais aos computadores, como a alteração e destruição de arquivos; roubo de senhas e informações relevantes; e a inclusão de *backdoors* (ver seção **2.2.4** - alínea d), que possibilitam que o invasor consiga ter o controle total sobre o computador infectado. (NIC BR SECURITY OFFICE, 2003; GALVÃO, 2002)

A principal característica que difere o *trojan horse* do *worm* e do vírus e que ele não possui a capacidade de auto-replicação, além de necessitar ser executado para instalar-se automaticamente (GALVÃO, 2002; MOREIRA, 2001; NIC BR SECURITY OFFICE, 2003). Segundo NIC BR Security Office (2003, p. 13), "podem existir casos onde um cavalo de tróia contenha um vírus ou *worm*. Mas mesmos nestes casos é possível distinguir as ações realizadas como conseqüência da execução do cavalo de tróia propriamente dito, daquelas relacionadas ao comportamento de um vírus ou *worm*."

d) *Backdoors*

Segundo Virus & Cia (*apud* Gonçalves, 2002), *backdoors* são programas que instalam uma porta de entrada nos computadores com o objetivo de permitir o acesso remoto da máquina por meio das redes sem que os usuários percebam tal ação. Com a presença dos *backdoors* nos computadores é possível ter o controle total da máquina por outro computador possibilitando ao invasor acessar os arquivos armazenados, ler e-mails, apagar ou alterar arquivos, executar programas instalados, formatar o disco rígido entre várias outras funções.

A inclusão de um *backdoor* em um computador, segundo NIC BR Security Office (2003), pode ser realizada sem necessariamente depender de uma invasão podendo também ser decorrente da instalação de um *trojan horse* ou a instalação e má configuração de um programa de administração remota. A NIC BR Security Office (2003, p. 12) alerta que "alguns fabricantes incluem/incluíam *backdoors* em seus produtos (software, sistemas operacionais), alegando necessidades administrativas. É importante ressaltar que estes casos constituem uma séria ameaça à segurança de um computador que contenha um destes

---

protegida. A alternativa encontrada pelos gregos foi a construção de um cavalo de madeira com a sua parte interna oca, e como estratégia presentearam os troianos com o cavalo carregado de soldados no seu interior. O cavalo foi deixado no meio da cidade e a noite os soldados saíram e abriram os portões, onde os restantes da tropa, que estavam lá fora, entraram e dominaram Tróia." (CANDEÁ, 2002, p. 28)

produtos instalados [...]", pois apesar dos fabricantes serem conhecidos, isto possibilita que eles tenham acesso irrestrito a essas máquinas, podendo afetar o princípio da confidencialidade da informação.

2.2.5 Lixo eletrônico

Com a disseminação do e-mail como meio de comunicação pelo mundo começaram a surgir em proporções de crescimento alarmantes mensagens eletrônicas que possuem conteúdo que não agregam nenhum valor para o usuário, podendo ser consideradas como um lixo eletrônico. Nesse grupo de lixo eletrônico se destacam os spams e os *hoaxes* (boatos) que serão descritos abaixo.

a) Spam

Segundo a NIC BR Security Office (2002, p. 3), spam "é o termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do inglês *Unsolicited Commercial Email*)".

O spam pode ocasionar uma gama de impactos para as organizações. Dentre os prejuízos relacionados à circulação deste lixo eletrônico pela Internet podemos destacar:

- o não recebimento de *e-mails*, já que uma boa parte dos provedores de internet possui uma limitação do tamanho da caixa postal do usuário no seu servidor. Se o número de spams recebidos pelo indivíduo for elevado, corre se o risco de se esgotar a capacidade da caixa postal, e dessa forma, o não recebimento de e-mails a partir desse momento (NIC BR SECURITY OFFICE, 2003);

- perda de produtividade do trabalhador, já que este terá que dedicar um espaço de tempo maior do seu trabalho para ler, identificar o e-mail como spam e removê-lo da caixa postal. Devido ao grande número de spams, isto pode dificultar a seleção dos e-mails por parte dos trabalhadores acarretando na possibilidade de mensagens relevantes não serem lidas, serem lidas com um certo atraso ou apagadas por engano. (NIC BR SECURITY OFFICE, 2003; ROCHA, 2004b);

- aumento de custos, já que as organizações que possuem acesso discado à Internet estão pagando alguns segundos a mais de ligações para apagar cada spam recebido. (NIC BR SECURITY OFFICE, 2003; ROCHA, 2004);

- perda de credibilidade do e-mail como meio de comunicação (ROCHA, 2004b; FAULHABER, 2004); e

- o envio de spams tem sido utilizado nos últimos tempos como ferramenta de disseminação de vírus e fraudes *on-line*. (ROCHA, 2004b)

b) *Hoaxes* (Boatos)

Hoaxes são e-mails que contém informações de teor alarmante ou falso e que geralmente possuem como remetente de grandes empresas e órgãos governamentais. (NIC BR SECURITY OFFICE, 2003; CANDÉA, 2002)

Geralmente, o objetivo da pessoa que cria um boato é verificar o quanto ele se propaga pela Internet e verificar quanto tempo ele permanece no ar. Os problemas mais típicos relacionados aos boatos são ocupar espaços nas caixas de e-mails de usuários e espalhar a desinformação pela Internet. Entretanto, existem alguns boatos com fins maliciosos que podem, por exemplo, induzir os usuários a fornecerem informações importantes como o número do seu CPF e do seu cartão de crédito (NIC BR SECURITY OFFICE, 2003; CANDÉA, 2002).

2.3 NBR ISO/IEC 17 799 – Norma brasileira de segurança da informação

Desde a última década, as organizações vêm criando consciência da enorme relevância que tem para o desenvolvimento de suas atividades, a proteção adequada de seus ativos, elementos de sustentação dos processos organizacionais. Entretanto, um dos maiores obstáculos à implementação da segurança da informação nas organizações é a falta de padrões com relação à metodologia de implementação de soluções (COBB *apud* MACHADO, 2002a).

Devido a essa necessidade de estabelecimento de padrões, foram desenvolvidos esforços internacionais para o desenvolvimento de uma norma que pudesse

subsidiar a gestão da segurança da informação no mundo, englobando mecanismos eficientes e universais para proteger a informação de ameaças que pudessem afetá-la, provocando a perda de sua confidencialidade, integridade e disponibilidade. Tais esforços resultaram em uma norma internacional de segurança da informação, no ano 2000, intitulada ISO/IEC[7] 17 799, que posteriormente foi transformada pela Associação Brasileira de Normas Técnicas (ABNT) na primeira norma nacional de segurança da informação, denominada NBR ISO/IEC 17 799 – Tecnologia da informação – Código de prática para a gestão da segurança da informação.

2.3.1 Histórico

O governo britânico, em 1987, através do departamento de comércio e indústria do Reino Unido - *Departamente of Trade Center* (DTI) -, criou um centro de segurança de informações denominado *Comercial Computer Security* Centre (CCSC), que possuía como objetivos a elaboração de critérios para a avaliação da segurança de empresas britânicas que comercializavam produtos para a segurança de Tecnologia da Informação (TI) e a criação de um código de segurança para os usuários das informações. Em 1989, foi publicada a primeira versão do código de segurança, intitulado PD 0003 – Código de Gerenciamento de Segurança da informação (SOLMS *apud* CASANAS; MACHADO, 2001).

No ano de 1995, o PD003 foi revisado e publicado como uma norma britânica (BS), a BS 7 799-1:1995. Em 1996, esta norma foi indicada à ISO para homologação, porém não foi aceita. Após a publicação da BS 7 799-1:1995, começou a ser elaborada a segunda parte deste documento, que foi publicada em novembro de 1997 para consulta e avaliação pública. Em 1998, a segunda parte foi publicada com o nome de BS7 799-2:1998 e, após uma revisão, em 1999, juntamente com a primeira parte, foram publicadas como BS 7 799:1999 (HEFFERAN *apud* CASANAS; MACHADO, 2001).

---

[7] "ISO significa International Standartization Organization. Trata-se de uma organização internacional formada por um conselho e comitês com membros oriundos da maioria dos países. Seu objetivo é criar normas e padrões universalmente aceitos sobre como realizar as mais diversas atividades comerciais, industriais, científicas e tecnológicas. IEC, significa International Engineering Consortium. É uma organização voltada para o aprimoramento da indústria da informação. Uma associação entre as duas instituições produz normas e padronizações internacionais." (MACHADO, 2002b)

Durante o seu desenvolvimento, a BS 7 799:1999 já estava sendo utilizada por outros países, além da Inglaterra, destacando-se os países de língua inglesa como a Austrália, Nova Zelândia e África do Sul (SOLMS *apud* CASANAS; MACHADO, 2001). A primeira parte deste documento, ou seja a BS 7 799-1, foi entregue novamente a ISO para homologação, através do mecanismo de *Fast Track* , para um trâmite mais rápido. Em outubro de 2000, na reunião do comitê da ISO em Tóquio, a norma foi aprovada pela maioria dos representantes e foi homologada como ISO/IEC 17 799:2000 (CASANAS; MACHADO, 2001).

Após a homologação da norma ISO/IEC 17 799, a ABNT, acompanhando a tendência mundial, em abril de 2001, apresentou para consulta pública o projeto 21:204.01-010, que era uma "tradução literal" da norma internacional de Segurança da Informação - ISO/IEC - 17 799 (GONÇALVES, 2004). Em setembro de 2001, "[...] após pequenos ajustes sugeridos pelos comitês em consulta pública" (SÊMOLA, 2003, p. 70), a ABNT homologou a NBR ISO/IEC 17 799 – Tecnologia da informação – Código de prática para a gestão da segurança da informação, a primeira norma brasileira do gênero.

2.3.2 Controles

A NBR ISO/IEC 17 799 possui como escopo fornecer

> [...] recomendações para a gestão da segurança da informação para uso por aqueles que são responsáveis pela introdução, implementação ou manutenção em suas organizações. [A Norma] tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão de segurança, e prover confiança nos relacionamentos entre as organizações. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003, p. 4)

A norma brasileira sobre segurança da informação apresenta-se na forma de notas de orientação e recomendações bem abrangentes e procura englobar todos os aspectos da segurança da informação (humanos, físicos e tecnológicos). A norma brasileira segue a mesma estrutura da ISO/IEC 17 799 e é composta de dez domínios, reunidos em 36 objetivos, que resultam em 127 controles ou medidas de segurança. Abaixo será apresentada uma síntese de cada um dos dez domínios que compõem a NBR ISO/IEC 17 799:

1°) Política de segurança

Este domínio ressalta a importância do estabelecimento de uma política de segurança da informação para a organização, pois esta política estabelece uma direção e a base para a gestão da segurança da informação. A política deve ser estabelecida em um documento, que deve ter o apoio da direção da organização e deve ser divulgado adequadamente para toda a organização, de forma que as pessoas envolvidas entendam e respeitem as suas normas. Esta política deve ter um gestor que tenha a responsabilidade de mantê-la sempre atualizada em relação às mudanças que venham a ocorrer no ambiente ou em relação ao surgimento de novas vulnerabilidade e ameaças.

2°) Segurança organizacional

Este domínio sugere que uma infra-estrutura específica seja criada dentro da organização, com o intuito de facilitar a gestão da segurança da informação. A coordenação dessa estrutura pode ser gerenciada por um fórum multifuncional que englobe diretores de todos os departamentos mais importantes da organização.

Outro aspecto mencionado neste domínio é a necessidade de manter um controle sobre o acesso de prestadores de serviço aos ativos da organização, com o objetivo de manter as normas e políticas de segurança da informação colocadas pela organização. Este controle pode ser realizado através do estabelecimento requisitos de segurança nas cláusulas dos contratos entre os prestadores de serviço e a organização.

3°) Classificação e controle dos ativos de informação

Este domínio expõe que os ativos devem ser inventariados e classificados de acordo com o valor e a importância que possuem para a organização, de forma a fornecer níveis de proteção adequados para cada um deles. É importante que os principais ativos tenham um responsável, com as funções de manutenção adequada dos controles de segurança, e prestação de contas do ativo.

4°) Segurança em pessoas

Este domínio engloba a necessidade de:

a) informar aos funcionários da organização, por meio dos seus contratos, sobre as suas responsabilidades na realização de sua tarefas sempre mantendo a segurança da informação;

b) treinar e educar os usuários nos procedimentos de segurança e na manipulação correta dos ativos, com o objetivo de reduzir os incidentes de segurança; e

c) remeter ao departamento responsável, no menor tempo possível, por meio de canais adequados e que sejam do conhecimento dos funcionários da organização, todos os incidentes de segurança ocorridos ou suspeitos, ameaças e vulnerabilidades do ambiente, para que se possa tomar as providências cabíveis, com o objetivo de reduzir os impactos às atividades da organização. Convém que a organização catalogue as características dos incidentes, das vulnerabilidades e das ameaças reportadas, de forma a criar uma base de conhecimento que oriente as suas ações futuras.

5°) Segurança física e do ambiente

Este domínio aborda a importância de se implementar perímetros de segurança, por meio de barreiras de segurança pertinentes, como controles de entrada física baseados em cartões de identificação, para formar áreas de segurança em que os ativos essenciais da organização sejam salvaguardados de acessos não autorizados, danos e interferências.

A proteção física dos equipamentos (inclusive os que se encontram fora do ambiente físico da organização) contra ameaças ambientais e acessos não autorizados é importante para garantir a integridade, disponibilidade e confidencialidade das informações. O estabelecimento de políticas de mesa limpa para papéis e mídias removíveis; uma política de tela limpa para recursos de processamento da informação; e controles para a retirada dos ativos da organização também são englobados neste domínio para evitar a exposição e roubos dos ativos.

6°) Gerenciamento das operações e comunicações

Este domínio estabelece controles para a garantia do funcionamento seguro e adequado dos dispositivos de tratamento da informação. Para que isto ocorra:

a) os procedimentos e responsabilidades pela manipulação dos ativos têm que ser definidos;

b) um planejamento da capacidade e aceitação dos novos sistemas de informação tem que ser realizado para reduzir o risco de falhas;

c) controles devem ser adotados para prevenir e detectar a introdução de softwares que prejudiquem a integridade da informação;

d) cópias de segurança de dados e de softwares importantes aos processos organizacionais devem ser realizados;

e) uma gama de controles deve ser implementada para proteção das informações em redes e da infra-estrutura que o suporta;

f) procedimentos para a proteção física e o controle das mídias devem ser estabelecidos, inclusive no momento do seu descarte;

g) controles para a troca de informações e softwares devem ser implementados, para prevenir a perda e garantir a integridade dos ativos.

7°) Controle de acesso

Este domínio identifica a necessidade da monitorar e controlar o acesso aos ativos da organização (informações, sistemas de informações, redes, recursos computacionais), para garantir a sua integridade e confidencialidade.

8°) Desenvolvimento e manutenção de sistemas

Este domínio reafirma a idéia de que o desenvolvimento e a manutenção de todos os sistemas de informação tem que focar a segurança em todas as suas etapas, introduzindo controles, como a criptografia e a assinatura digital, para garantir a integridade, confidencialidade, disponibilidade e autenticidade das informações.

9°) Gestão da continuidade do negócio

Este domínio engloba a necessidade das organizações em implementar controles que reduzam, a um nível aceitável, os efeitos das interrupções dos processos organizacionais, e protejam os ativos essenciais da organização de falhas ou desastres maiores, garantindo que as atividades voltem à escala normal de trabalho no menor tempo possível.

10°) Conformidade

Este domínio expõe que as organizações têm que observar a legislação vigente em cada país, para implementação dos seus controles de segurança. Este domínio também aborda a necessidade de uma análise periódica da segurança dos sistemas e um controle em relação aos processos de auditoria de sistemas, com o intuito de proteger a integridade da informação e prevenir o uso indevido das ferramentas de auditoria.

Os controles constantes na NBR ISO/IEC 17 799 giram em torno da preservação dos três princípios básicos da segurança da informação: disponibilidade, confidencialidade e integridade da informação. Afirmar que um ambiente é aderente a esta Norma significa dizer que o mesmo utiliza os recursos adequados para garantir a preservação dos três princípios básicos mencionados acima.

A seleção dos controles de segurança da informação a serem utilizados é uma tarefa difícil que deve levar em consideração as características do ambiente organizacional e deve ser precedida de uma identificação dos requisitos de segurança (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003). A NBR ISO/IEC 17 799 aponta três fontes principais para a identificação dos requisitos de segurança: a avaliação de risco; a legislação

que a organização, seus parceiros, contratados e prestadores de serviço têm que respeitar; e os conjuntos de princípios e objetivos da organização. A Norma dá um destaque maior à avaliação de risco como ferramenta para identificar os requisitos de segurança. Esta ferramenta, também denominada análise de riscos, será tratada detalhadamente na seção **2.4.2.1**. Cabe neste momento apresentar a sua definição constante na NBR ISO/IEC 17 799: "avaliação das ameaças, impactos e vulnerabilidades da informação e das instalações de processamento da informação e da probabilidade de sua ocorrência." (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003, p. 4)

Apesar de sempre reiterar a necessidade de uma avaliação de risco para selecionar os controles a serem implementados na organização, a NBR ISO/IEC 17 799 aponta um conjunto de controles que são considerados essenciais para o início da implementação da segurança da informação e que geralmente podem ser aplicados na maior parte das organizações e dos ambientes de trabalho. Estes controles apresentados como melhores práticas de segurança da informação segundo a NBR ISO/IEC 17 799 são:

a) uma política de segurança da informação documentada: visa estabelecer um conjunto de normas, métodos e procedimentos que delineiam as diretrizes da organização para a gestão da segurança da informação. É importante que esta política tenha apoio da alta direção da organização e seu conteúdo seja bem divulgado, de forma que os usuários a compreendam;

b) definição das responsabilidades na segurança da informação: apresentar os responsáveis por salvaguardar cada ativo da organização e, dessa forma, facilitar a comunicação com os mesmos quando o ativo sofrer algum problema de segurança;

c) educação e treinamento em segurança da informação: é necessário que todas as pessoas envolvidas com os ativos da organização sejam treinadas e tenham a consciência da importância da sua segurança, antes de ter seu acesso definido, de forma a possibilitar a utilização correta do ativo;

d) relatórios de incidentes de segurança: a elaboração de tais documentos, que dependem da colaboração dos funcionários e prestadores de serviços em notificar o mais rápido possível os incidentes de segurança ao departamento responsável, possibilita-se a

criação na organização de um banco de dados que reúna todas as informações sobre os incidentes, e que poderá ser utilizado, por exemplo, em treinamentos, de forma a educar os usuários a saberem como proceder diante da possibilidade da ocorrência de tal incidente; e a

e) gestão da continuidade do negócio: através da junção de controles que mesclam prevenção e recuperação, visa diminuir para um nível aceitável, as suspensões das atividades ocasionadas por incidentes de segurança.

Após a seleção dos controles de segurança a serem utilizados na organização, a próxima fase corresponde a sua implementação. A NBR ISO/IEC 17 799 menciona que existem alguns fatores que são considerados críticos para o sucesso da implementação da segurança da informação dentro de uma organização:

> a) política de segurança, objetivos e atividades, que reflitam os objetivos do negócio;
>
> b) um enfoque para implementação da segurança que seja consistente com a cultura organizacional;
>
> c) comprometimento e apoio visível da direção;
>
> d) um bom entendimento dos requisitos de segurança, avaliação de risco e gerenciamento de risco;
>
> e) divulgação eficiente da segurança para todos os gestores e funcionários;
>
> f) distribuição das diretrizes sobre as normas e política de segurança da informação para todos os funcionários e fornecedores;
>
> g) proporcionar educação e treinamento adequados;
>
> h) um abrangente e balanceado sistema de medição, que é usado para avaliar o desempenho da gestão de segurança da informação e obtenção de sugestões para a melhoria. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003, p. 3-4).

Segundo dados da 9ª Pesquisa Nacional de Segurança da Informação, o principal obstáculo para a implementação da segurança da informação nas organizações, na visão de 23% dos entrevistados, é a falta de consciência dos executivos, ou seja, da direção da organização. (MÓDULO SECURITY SOLUTIONS, 2003) Este dado reforça a idéia apresentada pela NBR ISO/IEC 17 799 que aponta o comprometimento e apoio visível da direção como fatores a serem considerados na implementação da segurança da informação nas organizações.

2.3.3 Considerações sobre a utilização da NBR ISO/IEC 17 799

A primeira parte da BS 7 799, que originou a ISO/IEC 17 799, e posteriormente a NBR ISO/IEC 17 799, como já exposto, é um Código de Prática de Gestão da Segurança. Por se tratar de um código de prática, ou seja, um guia de recomendações em segurança da informação e não especificar como implementar tais recomendações, esta parte não é objeto de certificação (SÊMOLA, 2003; BASTOS, 2002).

A segunda parte da BS 7 799, que contém um *framework* de segurança denominado Sistema de Gestão de Segurança da Informação (SGSI)[8], está em consulta pública, com o intuito de gerar a versão ISO correspondente, para que quando for homologada, juntamente com os controles de segurança expostos pela ISO/IEC 17 799, ser a base para a certificação das organizações (SÊMOLA, 2003). Sêmola (2003, p. 141) expõe que "[...] enquanto isso não ocorre, a alternativa é buscar a conformidade e a certificação BS 7 799, que já poderia representar uma pré-certificação para a ISO/IEC 17 799."

Machado (2002b) relata que as normas ISO/IEC 17 799 e NBR ISO/IEC 17 799 foram criadas originalmente para as organizações comerciais e, portanto, se ajustam melhor a elas. O autor coloca que as instituições de ensino, instituições públicas e outras com características parecidas podem ter dificuldades em implantar certos controles da norma devido ao fato de seus ambientes corporativos serem distintos dos de uma empresa comercial. Mesmo assim, Machado (2002b, p. 2) ressalta que "[...] qualquer organização pode aproveitar grande parte dos controles da norma para implementar segurança da informação em suas instalações."

A Associação Brasileira de Normas Técnicas (2003, p.4) relata na introdução da NBR ISO/IEC 17 799 "[...] que nem todas as recomendações e os controles desta Norma podem ou devem ser integralmente aplicados. Além disso, controles adicionais não incluídos nesta Norma podem ser necessários e complementares."

[8] O *framework* de segurança intitulado Sistema de Gestão de Segurança da Informação (SGSI), possui o objetivo de proporcionar uma base para gerenciar a segurança da informação nas organizações (SÊMOLA, 2003).

Em relação a essa passagem, Sêmola (2003, p.71-72) afirma que existe a

> [...] preocupação em desvincular a norma do sentido figurado de um TRILHO, atribuindo à mesma o papel figurado de uma TRILHA, capaz de apontar a direção sem, no entanto, gerar obrigatoriedade e padronização inflexível que, certamente, não seria compatível com o dinamismo das empresas, seus ambientes e as mudanças em seus ativos físicos, tecnológicos e humanos.

Seguindo a mesma linha de argumento de Sêmola (2003), Symantec do Brasil (2002) considera que "a flexibilidade e imprecisão do ISO 17 799 (e conseqüentemente da NBR ISO/IEC 17 799) é intencional, pois é muito difícil criar um padrão que funcione para todos os variados ambientes de TI, e que seja capaz de crescer com a mutante paisagem tecnológica atual."

Em suma, apesar da NBR ISO/IEC 17 799 e da ISO/IEC 17 799 não serem objeto de certificação, elas são reconhecidas nacionalmente e internacionalmente, como uma base sólida e eficiente de recomendações em segurança da informação; e as organizações mundiais e brasileiras devem utilizá-las como fonte de consulta para aprimorarem a sua gestão de segurança da informação, com o intuito de preservar a disponibilidade, integridade e confidencialidade de suas informações.

2.4 Sistema de Gestão da Segurança da Informação

A segunda parte da Norma BS 7 799, conforme relatado superficialmente na seção **2.3.3**, contém um *framework* de segurança denominado Sistema de Gestão da Segurança da Informação (SGSI), ou em inglês, *Information Security Management System* (ISMS). Um SGSI "é o resultado da aplicação planejada de objetivos, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para segurança da informação." (MACHADO, 2002b, p. 2), ou seja, proporciona uma base para gerenciar a segurança da informação nas organizações.

Nos últimos 21 meses, o número de organizações pelo mundo certificadas BS 7 799 aumentou consideravelmente. Em 20 de fevereiro de 2003, eram 202 organizações (ROCHA, 2004a). Em novembro de 2004, esse número mais que quadruplicou, passando para 950 organizações mundiais, conforme está presente no sítio da ISMS International User

Group (IUG)[9], que gerencia uma lista atualizada e completa das organizações que obtiveram tal certificado. O Japão é o país com o maior número de organizações certificadas (449), seguido do Reino Unido (168). O Brasil possui três organizações: a Módulo Security Solutions, o Banco Matone e o Serasa.[10]

Machado (2004) relata que as organizações que adotam um SGSI, e posteriormente são certificadas, comprovam "[...] que a segurança da informação está garantida de forma efetiva, o que não significa, contudo, que a organização esteja imune a violações de segurança."

O SGSI sugerido pela segunda parte da Norma BS 7 799 é baseado no modelo PDCA (*Plan, Do, Check, Act*), adotado na ISO 9001[11], que representa um ciclo de melhoria contínua dos processos de segurança da informação formado por quatro fases: *Plan* (planejar); *Check* (analisar); *Do* (implementar); e *Act* (monitorar) (SÊMOLA, 2003). A seguir será apresentada a finalidade de cada fase no processo de gestão da segurança da informação[12], com a descrição mais aprofundada dos instrumentos que mais caracterizam cada etapa.

2.4.1 *Plan* (Planejar)

Esta fase corresponde ao planejamento do processo de segurança da informação. Tal fase abrange o momento de definir quais os objetivos que se quer atingir, planejar o que será feito e definir os métodos que permitirão alcançar o que foi proposto (SÊMOLA, 2003). A Política de Segurança da Informação e o Plano de Contingências são instrumentos elaborados nessa fase.

2.4.1.1 Política de Segurança da Informação

A Política de Segurança da Informação (PSI) é um conjunto de diretrizes, normas, procedimentos e instruções destinadas a orientar a gestão da segurança da informação

---

[9] O sítio da ISMS International User Group (IUG) é http://www.xisec.com.

[10] O Estados Unidos, com 12 organizações certificadas, e o Canadá, com nenhuma organização, são países que não tiveram uma grande adesão a BS 7 799 e a ISO 17 799. Gonçalves (2004) expõe que "[...] na época da homologação da ISO 17 799, [Estados Unidos e Canadá já possuíam] uma longa tradição na área de segurança da informação e, por assim dizer, 'sua própria maneira de fazer as coisas', razão pela qual tendem a resistir em adotar soluções que não foram criadas por eles."

[11] A ISO 9001 apresenta um Sistema de Gestão da Qualidade (SGQ), na qual são exigidas todas as etapas do planejamento – sintetizada pela sigla PDCA (CAUBIT, 2002).

[12] A descrição de cada fase do SGSI será baseada na obra de SÊMOLA (2003).

Group (IUG)[9], que gerencia uma lista atualizada e completa das organizações que obtiveram tal certificado. O Japão é o país com o maior número de organizações certificadas (449), seguido do Reino Unido (168). O Brasil possui três organizações: a Módulo Security Solutions, o Banco Matone e o Serasa.[10]

Machado (2004) relata que as organizações que adotam um SGSI, e posteriormente são certificadas, comprovam "[...] que a segurança da informação está garantida de forma efetiva, o que não significa, contudo, que a organização esteja imune a violações de segurança."

O SGSI sugerido pela segunda parte da Norma BS 7 799 é baseado no modelo PDCA (*Plan, Do, Check, Act*), adotado na ISO 9001[11], que representa um ciclo de melhoria contínua dos processos de segurança da informação formado por quatro fases: *Plan* (planejar); *Check* (analisar); *Do* (implementar); e *Act* (monitorar) (SÊMOLA, 2003). A seguir será apresentada a finalidade de cada fase no processo de gestão da segurança da informação[12], com a descrição mais aprofundada dos instrumentos que mais caracterizam cada etapa.

2.4.1 *Plan* (Planejar)

Esta fase corresponde ao planejamento do processo de segurança da informação. Tal fase abrange o momento de definir quais os objetivos que se quer atingir, planejar o que será feito e definir os métodos que permitirão alcançar o que foi proposto (SÊMOLA, 2003). A Política de Segurança da Informação e o Plano de Contingências são instrumentos elaborados nessa fase.

2.4.1.1 Política de Segurança da Informação

A Política de Segurança da Informação (PSI) é um conjunto de diretrizes, normas, procedimentos e instruções destinadas a orientar a gestão da segurança da informação

---

[9] O sítio da ISMS International User Group (IUG) é http://www.xisec.com.

[10] O Estados Unidos, com 12 organizações certificadas, e o Canadá, com nenhuma organização, são países que não tiveram uma grande adesão a BS 7 799 e a ISO 17 799. Gonçalves (2004) expõe que "[...] na época da homologação da ISO 17 799, [Estados Unidos e Canadá já possuíam] uma longa tradição na área de segurança da informação e, por assim dizer, 'sua própria maneira de fazer as coisas', razão pela qual tendem a resistir em adotar soluções que não foram criadas por eles."

[11] A ISO 9001 apresenta um Sistema de Gestão da Qualidade (SGQ), na qual são exigidas todas as etapas do planejamento – sintetizada pela sigla PDCA (CAUBIT, 2002).

[12] A descrição de cada fase do SGSI será baseada na obra de SÊMOLA (2003).

na organização. (SÊMOLA, 2003) Segundo a NBR ISO/IEC 17 799, a Política de Segurança da Informação tem o objetivo de "prover à direção uma orientação e apoio para a segurança da informação" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003, p. 4). Moreira (2001) destaca que um dos objetivos de uma Política de Segurança é informar a todas as pessoas da organização quais são os mecanismos de segurança que serão utilizados para a proteção de seus ativos de acordo com nível de segurança estabelecido pela organização.

Sêmola (2003) relata que a Política de Segurança da Informação deve ser *formada por três grandes blocos: diretrizes, normas e os procedimentos e instruções de* trabalho, que são ligadas, respectivamente, ao nível estratégico, tático e operacional.

A primeiro bloco da Política de Segurança da Informação corresponde às diretrizes. Sêmola (2003, p. 105) expõe que as diretrizes "têm papel estratégico, precisam expressar a importância que a empresa dá para a informação, além de comunicar aos funcionários seus valores e seu comprometimento em incrementar a segurança à sua cultura organizacional." Em suma, as diretrizes expõem regras gerais que irão nortear a elaboração de todos os controles constantes na Política de Segurança da Informação.

As normas correspondem ao segundo bloco da Política de Segurança da Informação e possuem papel tático. As normas se caracterizam por serem regras mais específicas que as diretrizes, "detalhando situações, ambientes, processos específicos e fornecendo orientação para o uso adequado das informações" (SÊMOLA, 2003, p. 105). Algumas normas que são características de uma Política de Segurança da Informação são: critérios normatizados para admissão e demissão de funcionários; criação e manutenção de senhas; descarte de informações em mídia magnética; uso da internet; e classificação da informação. (SÊMOLA, 2003)

Os procedimentos e as instruções correspondem ao terceiro nível da Política de Segurança da Informação e apresentam um caráter operacional. Os procedimentos e as instruções são um conjunto de ações que irão descrever os passos necessários para executar o que foi proposto pela norma. (SÊMOLA, 2003).

Para exemplificar as camadas da Política de Segurança da Informação, Sêmola (2003, p. 107) coloca que:

> [...] enquanto a diretriz orienta estrategicamente para a necessidade de salvaguardar as informações classificadas como confidenciais, e a norma define que estas deverão ser criptografadas em tempo de envio por e-mail, o procedimento e a instrução específica para esta ação tem de descrever os passos necessários para executar a criptografia e enviar o e-mail.

A presença de uma infra-estrutura de segurança da informação na organização é um fator importante para iniciar o processo de elaboração da PSI, bem como para estar coordenando a sua implementação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003). Brasil (2003) destaca que, para a efetividade da política, é importante que a sua elaboração conte com o suporte e aceitação da maioria das áreas da organização. Outro fator que é levantado por vários autores para que a política seja reconhecida dentro da organização é o apoio formal da sua alta direção. Este apoio da alta direção à política de segurança tem intuito de legitimar o conjunto de diretrizes, normas e os procedimentos e instruções estabelecidos, para que tais sejam respeitados e cumpridos por todos os indivíduos que possuem algum vínculo com a organização (SÊMOLA, 2003; ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003; LUZ *apud* GONÇALVES, 2002; BRASIL, 2003; FONTES *apud* GONÇALVES, 2002).

O conteúdo presente na política de segurança vai variar de uma organização para a outra, pois dependerá das suas características, como por exemplo: o seu grau de informatização, a sua área de atuação, o tamanho da organização, a sua cultura organizacional, como também o nível de segurança que foi estabelecido pela organização a ser seguido. (SÊMOLA, 2003; BRASIL, 2003). Brasil (2003, p. 29) menciona o seguinte em relação ao conteúdo da PSI:

> a Política de Segurança de Informações deve extrapolar o escopo abrangido pelas áreas de sistemas de informação e recursos computacionais. Ela não deve ficar restrita à área de informática. Ao contrário, ela deve estar integrada à visão, à missão, ao negócio e às metas institucionais, bem como ao plano estratégico de informática e às políticas da organização concernentes à segurança em geral.

Como foi exposto acima, cada organização deve elaborar a sua PSI de acordo com a suas características e necessidades. Entretanto, alguns itens são apontados, por alguns autores, como requisitos mínimos a serem contemplados na elaboração de uma Política de Segurança da Informação. Os itens freqüentemente apontados são:

a) o conceito de segurança da informação e explanação de sua importância como mecanismo que possibilita o compartilhamento de informações (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003; BRASIL, 2003);

b) definição de responsabilidades gerais e específicas dos membros da organização na gestão da segurança das informações (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003; BRASIL, 2003, MOREIRA, 2001; SÊMOLA, 2003);

c) políticas de controle de acesso a recursos e sistemas computacionais (BRASIL, 2003; FONTES *apud* Gonçalves, 2002; SÊMOLA, 2003);

d) classificação das informações[13] (BRASIL, 2003; SÊMOLA, 2003);

e) princípios legais (leis locais, estaduais e federais) que devem ser observados quanto à tecnologia da informação (direitos de propriedade de produção intelectual, direitos sobre software, normas legais correlatas aos sistemas desenvolvidos, cláusulas contratuais) (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003; BRASIL, 2003; MOREIRA, 2001; FONTES *apud* GONÇALVES, 2002; SÊMOLA, 2003);

f) conseqüências das transgressões das regras estabelecidas na PSI (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003; BRASIL, 2003; MOREIRA, 2001; FONTES *apud* GONÇALVES, 2002);

g) princípios da gestão da continuidade das atividades da organização em casos de contingências (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003; BRASIL, 2003; FONTES *apud* GONÇALVES, 2002; SÊMOLA, 2003);

h) plano de treinamento e conscientização em segurança da informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003; BRASIL, 2003; SÊMOLA, 2003).

---

[13] Sêmola (2003, p.107) expõe cinco níveis para classificar as informações: extra confidencial, confidencial, restrito, interno e público.

Depois de elaborada a PSI é fator crítico de sucesso a realização de uma campanha de divulgação para toda a organização, de forma que os trabalhadores possam compreender todo o seu conteúdo e a sua importância, com o intuito de criar uma cultura de segurança dentro da organização (MARINHO, 2003; ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003; BRASIL, 2003). Outro fator importante para o sucesso da implementação da política é que ela sempre deve estar acessível a todos da organização que precisarem consultá-la (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003).

Por fim, cabe mencionar que é importante que a Política de Segurança da Informação da organização, depois de elaborada, "tenha um gestor que seja responsável por sua manutenção e análise crítica" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003, p. 5), a fim de avaliar freqüentemente a efetividade da política de segurança, o custo e o impacto dos controles na eficiência das atividades da organização e atualizar a PSI sempre que ocorrer mudanças que afetem a última Análise de Riscos realizada pela organização, como por exemplo, novas vulnerabilidades. (BRASIL, 2003).

Em suma, a existência de uma Política de Segurança da Informação contribui para a proteção dos ativos da organização, preservando sua integridade, disponibilidade e confidencialidade, pois fornece, quando bem formulada, uma base sólida que irá auxiliar a gestão da segurança das informações organizacionais.

2.4.1.2 Plano de Contingências

Um Plano de Contingências, também denominado por alguns autores como Plano de Continuidade de Negócios (PCN), segundo definição de Brasil (2003, p. 35) é um

> [...] conjunto de estratégias e procedimentos que devem ser adotados quando a instituição ou uma área depara-se com problemas que comprometem o andamento normal dos processos e a conseqüente prestação dos serviços. Essas estratégias e procedimentos deverão minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade. O Plano de Contingências é um conjunto de medidas que combinam ações preventivas e de recuperação.

Caruso (*apud* Calheiros, 2002) menciona que o objetivo de um Plano de Contingência é funcionar como um guia que irá delinear as ações a serem tomadas para a continuidade dos serviços considerados essenciais para as organizações em casos de

incidentes de segurança. Brasil (2003), a NBR ISO/IEC 17 799 e Sêmola (2003) ressaltam também como um dos objetivos do Plano de Contingências assegurar que o funcionamento das atividades da organização sejam restabelecidas no menor tempo possível, a fim de reduzir ao máximo os impactos dos incidentes de segurança.

Brasil (2003, p. 38), relata que, geralmente, um Plano de Contingências contempla itens como:

> a) condições e procedimentos para ativação do Plano (como se avaliar a situação provocada por um incidente);
>
> b) procedimentos a serem seguidos imediatamente após a ocorrência de um desastre (como, por exemplo, contato eficaz com as autoridades públicas apropriadas: polícia, bombeiro, governo local);
>
> c) a instalação reserva, com especificação dos bens de informática nela disponíveis, como hardware, software e equipamentos de telecomunicações;
>
> d) a escala de prioridade dos aplicativos, de acordo com seu grau de interferência nos resultados operacionais e financeiros da organização. Quanto mais o aplicativo influenciar na capacidade de funcionamento da organização, na sua situação econômica e na sua imagem, mais crítico ele será;
>
> e) arquivos, programas, procedimentos necessários para que os aplicativos críticos entrem em operação no menor tempo possível, mesmo que parcialmente;
>
> f) sistema operacional, utilitários e recursos de telecomunicações necessários para assegurar o processamento dos aplicativos críticos, em grau pré-estabelecido;
>
> g) documentação dos aplicativos críticos, sistema operacional e utilitários, bem como suprimentos de informática, ambos disponíveis na instalação reserva e capazes de garantir a boa execução dos processos definidos;
>
> h) dependência de recursos e serviços externos ao negócio;
>
> i) procedimentos necessários para restaurar os serviços computacionais na instalação reserva;
>
> j) pessoas responsáveis por executar e comandar cada uma das atividades previstas no Plano (é interessante definir suplentes, quando se julgar necessário);
>
> l) referências para contato dos responsáveis, sejam eles funcionários ou terceiros;
>
> m) organizações responsáveis por oferecer serviços, equipamentos, suprimentos ou quaisquer outros bens necessários para a restauração;
>
> n) contratos e acordos que façam parte do plano para recuperação dos serviços, como aqueles efetuados com outros centros de processamento de dados.

Para mostrar-se eficaz, o Plano de Contingência deve receber o apoio da direção da organização. Brasil (2003, p. 105) relata que o Plano "é de responsabilidade direta da alta gerência, é um problema corporativo, pois trata-se de estabelecimento de

procedimentos que garantirão a sobrevivência da organização como um todo e não apenas da área de informática."

Por fim, para garantir que o Plano de Contingências atinja todos os seus objetivos é necessário: treinamento e conscientização dos funcionários da organização em relação aos procedimentos estabelecidos no Plano (BRASIL, 2003); testes periódicos, com o intuito de perceber se as medidas a serem adotadas conseguiriam resolver as possíveis contingências, sobretudo por ser a última medida de proteção a ser adotada, depois que todas as demais fracassaram (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003; BRASIL, 2003; SÊMOLA, 2003); e atualizações, de forma a contemplar sempre as modificações (físicas, tecnológicas e humanas) que estão ocorrendo na organização que podem influir nas situações de contingência (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003; BRASIL, 2003; SÊMOLA, 2003).

2.4.2 *Check* (Analisar)

Esta fase envolve ações que procuram dimensionar a situação real em que se encontra a segurança da informação na organização, por meio da identificação dos seus ativos, bem como das vulnerabilidades, ameaças, riscos e impactos para as atividades da organização decorrentes de incidentes de segurança no ambiente organizacional. A partir dessa análise é possível identificar quais as medidas de segurança mais apropriadas para se atingir o nível de segurança estabelecido pela organização (SÊMOLA, 2003). A Análise de Riscos é um instrumento característico dessa fase.

2.4.2.1 Análise de riscos

Os autores que versam sobre o tema segurança da informação, entre eles Marcos Sêmola e Nilton Moreira, relatam que não existe segurança total das informações, ou seja, o risco sempre estará presente nos ambientes organizacionais. Dessa forma, é necessário que cada organização, de acordo com as suas características, encontre um nível de risco adequado para o desenvolvimento de suas atividades (SÊMOLA, 2003; MOREIRA, 2001). O nível de risco tem que ser bem dimensionado, para que não ocorra a possibilidade de que uma organização escolha um nível de risco além do necessário, podendo acarretar a implementação de controles de segurança que gerem alguns efeitos indesejados, como a perda da velocidade dos processos em decorrência de sua excessiva burocratização (SÊMOLA,

2003). Dentro deste contexto, surge a análise de riscos, um processo chave para determinar o nível de risco ideal em que as organizações deverão operar. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003).

A análise de riscos, também conhecida como avaliação de riscos, "[...] consiste em um processo de identificação e avaliação dos fatores de risco presentes e de forma antecipada no ambiente organizacional, possibilitando uma visão do impacto negativo [...]" que será causado às atividades da organização se as ameaças explorarem as vulnerabilidades do ambiente (MOREIRA, 2001, p. 11). Este processo pode analisar toda a organização, apenas um departamento dela ou um elemento de um sistema de informação; isto irá variar de acordo com a necessidade da organização. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003; MOREIRA, 2001)

Para se realizar uma análise de riscos, existem alguns métodos que, de acordo com Sêmola (2003), são norteados basicamente por duas metodologias: quantitativa e qualitativa. A metodologia quantitativa procura dimensionar os impactos financeiros ocasionados por uma quebra de segurança, levando em consideração a valoração dos ativos. A metodologia qualitativa é conduzida por critérios que possibilitam estimar os impactos que as atividades organizacionais sofrerão com a perda da confidencialidade, integridade e disponibilidade das informações, conseqüência da exploração de uma vulnerabilidade por parte de uma ameaça.

O primeiro passo para a realização de uma análise de riscos é a identificação dos ativos e dos processos de negócios e classificá-los de acordo com a sua relevância para a organização. O objetivo dessa etapa é conhecer o ambiente ou o item a ser analisado para posteriormente detectar a presença de riscos. (SÊMOLA, 2003; MOREIRA, 2001). Sêmola (2003) menciona que, apesar da importância que os ativos tecnológicos possuem no contexto organizacional atual, a análise de riscos não pode focar-se exclusivamente nestes, pois eles constituem apenas uma parte do ambiente organizacional. Uma análise de riscos deve possuir uma visão mais abrangente da organização, e conseqüentemente dos seus riscos, com o intuito de englobar além dos aspectos tecnológicos, os aspectos legais, físicos, humanos e uma gama de fatores que interferem direta ou indiretamente na proteção dos ativos.

Segundo Moreira (2001, p.12), a análise de riscos deverá fornecer para as organizações, no mínimo, as seguintes informações:

a) pontos vulneráveis do ambiente;
b) ameaças potenciais ao ambiente;
c) incidentes de segurança causados pela ação de cada ameaça;
d) impacto negativo para o negócio a partir da ocorrência dos incidentes prováveis de segurança;
e) riscos para o negócio a partir de cada incidente de segurança;
f) medidas de proteção adequadas para impedir ou diminuir o impacto de cada incidente.

A partir das informações adquiridas com a análise de risco, "[...] é possível determinar as prioridades de ação em função do risco identificado, para que seja atingido o nível de segurança desejado pela organização." (MOREIRA, 2001, p.11) Sêmola (2003, p.109) reafirma o papel da análise de riscos ao mencionar que ela é um "[...] instrumento perfeito para dimensionar a situação da segurança atual [da organização] , tornado-a consciente dos riscos e orientando-a buscar soluções que a conduzam para o patamar de risco aceitável."

Em suma, a análise de riscos propicia para a organização uma base de informações que permite conhecer melhor os problemas que envolvem segurança da informação, de forma a subsidiar a escolha de medidas de segurança adequadas para a proteção dos ativos contra tais problemas.

2.4.3 *Do* (Implementar)

Esta fase compreende a execução do que foi planejado, ou seja, compreende implementação dos controles físicos, tecnológicos e humanos que foram estabelecidos na fase de planejamento de segurança. Por sua vez, estes controles foram definidos de acordo com a fase de diagnóstico da segurança da informação, que levantou as necessidades da organização e indicou quais medidas seriam necessárias a fim de se atingir o nível de risco adequado para a execução das atividades da organização (SÊMOLA, 2003). A implementação de controles de segurança e o treinamento e conscientização dos funcionários em segurança da informação são ações a serem realizadas nessa fase.

2.4.3.1 *Implementação de controles de segurança da informação*

Após a identificação das fragilidades do ambiente organizacional e a seleção das medidas de segurança que serão adotadas para reduzir as vulnerabilidades do ambiente, o próximo passo é a implementação dos controles de segurança. Segundo Sêmola (2003, 116), no que tange à segurança da informação, "implementar é adquirir, configurar e aplicar os mecanismos de controle de segurança a fim de atingir o nível de risco adequado." Não basta ter uma Política de Segurança formalizada, com apoio da alta direção da organização, para reduzir os problemas com segurança na organização. As medidas ou controles de segurança estabelecidos na Política devem ser implementados por meio da instalação de ferramentas de segurança, capacitação e conscientização dos funcionários em relação aos procedimentos a serem adotados, dentre outras várias medidas.

Atualmente existe uma grande variedade de controles de segurança que podem ser implementados na organização para garantir a confidencialidade, integridade e disponibilidade das informações. Sêmola (2003) menciona que existência dessa multiplicidade de controles esta relacionada à questão deles serem destinados a atuarem em três esferas: humana, física e tecnológica.

Os controles humanos buscam atuar no elo considerado mais fraco para a implementação da gestão da segurança da informação nas organizações, o ser humano (MOREIRA, 2001; SÊMOLA, 2003; RAMOS; 2004; TEÓFILO, 2002). A implementação dos controles humanos possui como um dos seus objetivos a criação de uma cultura de segurança na organização, com o intuito de reduzir os riscos de segurança. Podemos ter como exemplo desse tipo de controle: os seminários de sensibilização em segurança, cursos de capacitação, campanhas de divulgação da Política de Segurança, procedimentos para a contratação e demissão de funcionários, entre outros. Pelo papel fundamental que o treinamento e a conscientização em segurança tem no processo de gestão da segurança da informação, sendo considerado pela NBR ISO/IEC 17 799 como uma das melhores práticas para a segurança da informação, tais controles serão abordados com maior aprofundamento na seção **2.4.3.1.1**.

A implementação dos controles físicos tem a função de "controlar o acesso e as condições de ambientes físicos, sinalizando, registrando, impedindo e autorizando acessos e estados [...]" (SÊMOLA, 2003, p. 117). Podemos ter como exemplo de controles físicos: roletas de controle de acesso físico, detectores de fumaça, extintores de incêndio, salas-cofre, alarmes e sirenes, fragmentadoras de papel, dispositivo para armazenamento de cd-rom e disquetes, entre outros.

Ao longo do processo de evolução da segurança da informação, à medida que as ameaças vêem aumentando vertiginosamente em decorrência da maciça utilização dos computadores e da Internet, foram desenvolvidos uma gama de controles tecnológicos destinados a proteger os ativos da organização. Os controles tecnológicos podem atuar garantindo a privacidade das informações, como a criptografia, assinatura digital e a *Virtual Private Network* (VPN); combater ataques e invasões, como o *Firewall,* o anti-vírus e o *Intrusion Detection System* (IDS); ou garantir a confidencialidade da informação por meio de processos que oferecem acesso aos ativos apenas para indivíduos autorizados, como a senha (SÊMOLA, 2003). O apêndice B apresentará a descrição resumida das principais ferramentas tecnológicas utilizadas nas organizações para a implementação da segurança da informação.

2.4.3.1.1 Treinamento e conscientização em segurança da informação

O elemento humano é apontado por vários autores, entre eles, Moreira (2001), Sêmola (2003), Ramos (2004) e Teófilo (2002), como o elo mais fraco na implementação do processo de gestão da segurança da informação. Sêmola (2003, p. 129) expõe que esta questão se confirma pelo fato de que os seres humanos "não possuem um comportamento binário e previsível em que se possa eliminar todas as vulnerabilidades presentes. O ser humano é uma máquina complexa, dotada de iniciativa, criatividade e que sofre interferência de fatores externos, provocando comportamentos nunca antes experimentados."

Os funcionários e prestadores de serviço podem ser a principal causa da perda de integridade, confidencialidade e disponibilidade das informações nas organizações, devido a vários fatores, entre eles, acidentes e erros ocasionados por más condutas ou práticas descuidadas com os ativos manuseados. As organizações podem adquirir várias tecnologias avançadas em segurança da informação, entretanto, para que tais medidas de proteção sejam

eficientes e eficazes, os indivíduos da instituição são elementos chaves, pois são os responsáveis pelo processo de implementação e manutenção de tais controles.

Sêmola (2003) relata que é necessário criar uma cultura de segurança na organização para minimizar os riscos ligados aos seres humanos no processo de gestão da segurança da informação. Para criar esta cultura, programas de treinamento e campanhas de conscientização em segurança da informação são apontadas como medidas de segurança essenciais para que se incorpore tal cultura nas atividades realizadas pelos indivíduos ligados à organização (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003; TEÓFILO, 2003; RAMOS, 2004; MOREIRA, 2001; SÊMOLA, 2003).

Moreira (2001) expõe que o objetivo do treinamento em que se foca a segurança da informação é capacitar todos os funcionários a utilizarem os ativos conforme políticas e procedimentos estabelecidos pela organização. Dessa forma, Ramos (2004) coloca que o primeiro passo para se iniciar um programa de treinamento em segurança é estabelecer quais as ações deverão ser seguidas pelos funcionários. Nesse ponto, a Política de Segurança da Informação é um instrumento essencial e complementar ao programa de treinamento, já que esta estabelece diretrizes, normas, procedimentos e instruções que orientam as ações da segurança da informação na organização. Marinho (2003) também destaca a importância da Análise de Riscos no processo de treinamento dos funcionários, pois, por meio deste instrumento, pode-se selecionar quais assuntos devem ser abordados prioritariamente, de acordo com o levantamento das principais vulnerabilidades e ameaças ao ambiente organizacional.

Os profissionais ligados diretamente à área de segurança da informação devem realizar cursos específicos periódicos sobre novos métodos e técnicas de segurança, bem como devem estar cientes das novas vulnerabilidades e ameaças dos ambientes organizacionais, a fim de estarem preparados para administrarem novas situações de risco (SÊMOLA, 2003).

Moreira (2001, p. 164 -165) menciona que

> [...] todo esforço de treinamento, independente da forma, faz parte da implementação de um programa de conscientização dos usuários. À medida que os funcionários vão entendendo sobre o assunto, passam a aplicar as regras no seu dia-a-dia [...] e ao educar os funcionários em relação a melhor e a mais segura maneira de se comportar durante o uso da Internet ou dos recursos tecnológicos, a empresa [ou organização] sentirá uma grande diminuição da probabilidade da ocorrência de incidentes de segurança no ambiente.

Outra forma de sensibilizar e conscientizar os usuários sobre a importância da segurança da informação é a realização de palestras focando a importância da colaboração dos funcionários no processo, os prejuízos atuais causados com a falta de segurança da informação e os cenários futuros caso nada seja realizado (RAMOS, 2004).

Enfim, com a combinação de programas de treinamento com campanhas de conscientização em segurança da informação espera-se que os funcionários aumentem o seu conhecimento em relação aos procedimentos adequados para proteger as informações, assim como, mudem suas atitudes de forma a privilegiar uma constante melhoria da segurança da informação em toda a organização.

2.4.4 *Act* (Monitorar)

Esta fase compreende atividades que procuram administrar o nível de segurança da organização, por meio da monitoração da eficiência dos controles implementados. A partir dessa monitoração, é possível constatar se o nível de segurança estabelecido não foi atingido e se existe a necessidade de realizar algum ajuste no processo de gestão da segurança da informação. Sêmola (2003, p. 85) coloca que essa é a "fase que representa o elo de ligação com as demais, formando um ciclo contínuo, dando vida ao verdadeiro processo de gestão dinâmica." Em suma, esta fase se caracteriza pela administração e monitoração da segurança da informação.

2.4.4.1 Administração e monitoração da segurança da informação

A fase da administração e monitoração da segurança da informação na organização corresponde à etapa que tem por objetivo aferir se os resultados obtidos com a implementação das medidas de segurança estão de acordo com o nível de risco estabelecido

pela organização, de forma a constatar se existe a necessidade de alteração dos controles implementados (SÊMOLA, 2003).

A equipe responsável pela segurança da informação na organização deve criar índices e indicadores de segurança que permitam medir o quanto é eficaz cada medida adotada (GONÇALVES, 2002; SÊMOLA, 2003). A partir da medição constante desses indicadores e índices de segurança

> [...] torna-se possível perceber desvios de conduta, sobrecarga de infra-estruturas, tentativas de ataque e invasão, ineficiência dos controles implementados e, principalmente, presença de mudanças físicas, tecnológicas ou humanas que venham a provocar a oscilação do nível de segurança (SÊMOLA, 2003, p. 133).

O processo de monitoração da segurança da informação pode ser realizado por meio de uma auditoria de segurança que implica examinar e avaliar a adequação e eficiência das medidas de segurança implementadas (GONÇALVES, 2002). Moreira (2001) relata que a auditoria de segurança possibilita entre várias funções, a identificação de acessos não autorizados às redes da organização; a avaliação da integridade de arquivos essenciais para a organização, como por exemplo, a folha de pagamento de funcionários; e testar se as atividades realizadas pelos funcionários estão em conformidade com as diretrizes, normas e instruções estabelecidos pela organização na sua Política de Segurança da Informação.

O relatório dos incidentes de segurança, apontado pela NBR ISO/IEC 17 799 como uma das melhores práticas para a segurança da informação, é um instrumento essencial para a realização de uma administração e monitoração de segurança efetiva na organização. O relatório de incidentes atualizado é um fonte de informação importante "para medir o grau de aderência dos funcionários, o índice de eficiência dos controles e, ainda, para perceber falhas de segurança que permaneceram mesmo depois dos controles implementados" (SÊMOLA, 2003, p. 133), já que tais relatórios funcionam como um banco de dados que contém registros de todos os incidentes de segurança e as medidas de segurança adotados para a sua resolução.

Em suma, o ciclo do Sistema de Gestão de Segurança da Informação, esquematizado na Figura **2.2**, envolve primeiramente a fase do planejamento que estabelece um conjunto equilibrado de medidas de segurança em conformidade com as ameaças, vulnerabilidade e riscos identificados na organização na fase de análise do ambiente; o próximo passo é implementar efetivamente as medidas de segurança estabelecidas na fase

anterior, a fim de garantir que os riscos mantenham-se em níveis toleráveis para o desenvolvimento das atividades organizacionais; por fim, para o sucesso do processo de gestão da segurança da informação na organização é essencial uma administração e monitoração efetiva do processo, a fim de constatar possíveis falhas, novas vulnerabilidade e ameaças ao ambiente organizacional, com o objetivo de fornecer informações para a primeira fase, de modo a subsidiar as modificações que serão necessárias para atingir o nível de segurança estabelecido pela organização, mantendo um processo de melhoria contínua da segurança da informação na organização.

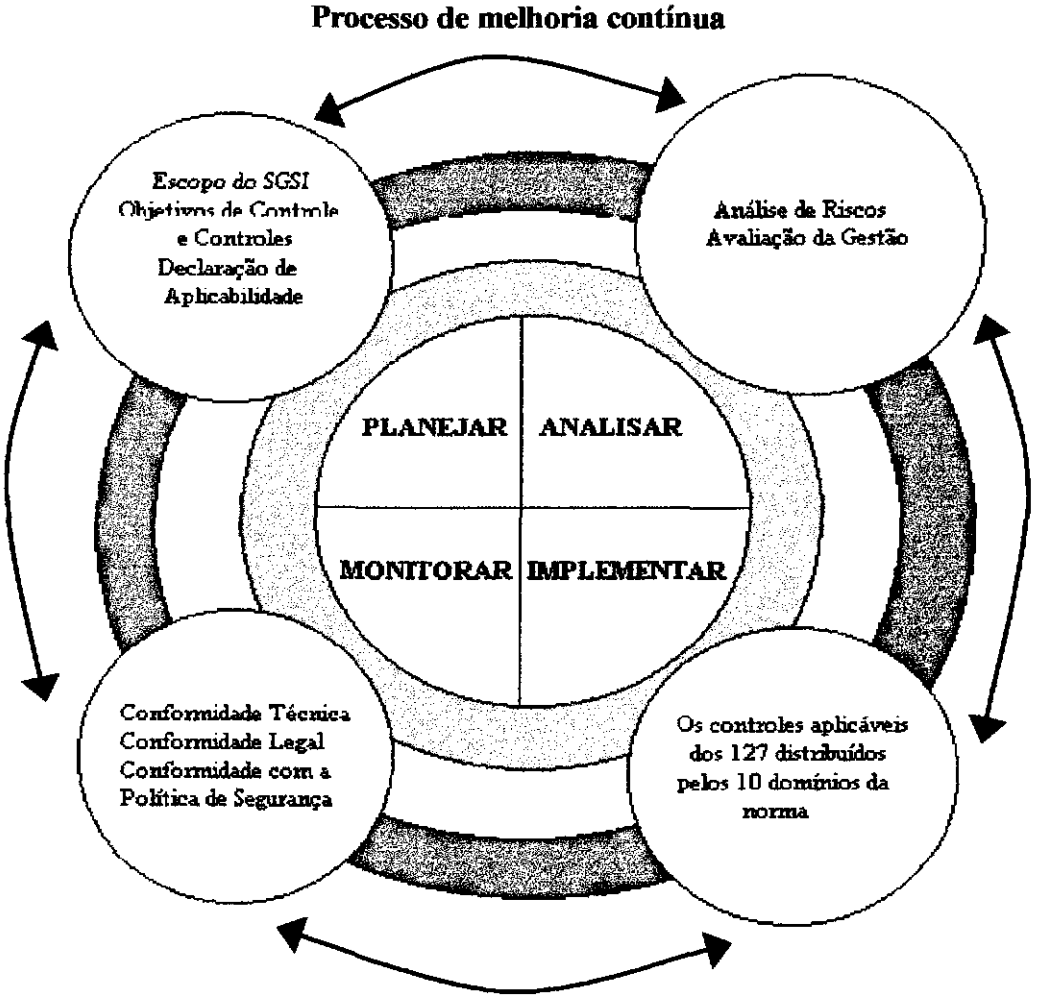


Figura 2.2 Modelo de *framework* SGSI – Sistema de Gestão de Segurança da Informação
Fonte: SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2003. p. 142

3 METODOLOGIA

Esta seção tem por objetivo apresentar os procedimentos metodológicos e operacionais utilizados para a realização desse trabalho monográfico.

3.1 Delineamento da pesquisa

Conforme apresentado na seção **1**, o objetivo geral dessa monografia é estabelecer um diagnóstico da situação em que se encontra a segurança da informação nas Secretarias de Estado de Minas Gerais, com o intuito de analisar como estas instituições têm lidado com a proteção de suas informações, recurso indispensável para o funcionamento adequado de qualquer organização, especialmente aquelas que prestam serviços essenciais para a população.

A pesquisa que será realizada para atender a questão levantada no parágrafo anterior será do tipo descritiva. Segundo Gil (1989, p. 46), "as pesquisas descritivas têm por objetivo primordial a descrição das características de determinada população ou fenômeno, ou então, estabelecimento de relações entre variáveis." No trabalho em questão, o fenômeno é a segurança da informação das Secretarias de Estado de Minas Gerais.

A primeira fase da pesquisa correspondeu a um momento exploratório. Segundo Batitucci (2003, p. 37), "na essência, toda pesquisa descritiva agrega uma fase ou momento exploratório". Os objetivos desse momento exploratório em uma pesquisa descritiva, ainda segundo autor, são aumentar a familiaridade com o assunto a ser pesquisado e estabelecer "regularidades descritivas", ou seja, descrever as características do assunto a ser pesquisado, estabelecendo relações entre variáveis.

Na seção **2**, por meio de uma pesquisa bibliográfica realizada em artigos, livros, monografias, dissertações, normas e sítios que versam sobre a segurança da informação, procurou-se atender aos objetivos do momento exploratório em uma pesquisa descritiva. A seleção das fontes consultadas foi baseada em indicações do orientador e no reconhecimento da relevância de tal fonte para a comunidade científica, como por exemplo, a norma NBR ISO/IEC 17 799, que orientam as organizações na gestão da segurança da informação. É importante frisar a dificuldade em encontrar trabalhos acadêmicos relacionados

à área de gestão da segurança da informação. A maioria dos trabalhos se restringe aos aspectos tecnológicos da segurança da informação.

As pesquisas descritivas geralmente assumem a forma de um levantamento[14], e envolvem o uso de técnicas padronizadas de coleta de dados, como questionários e formulários (GIL, 1989). Esse trabalho pode ser considerado como um levantamento, pois procurou obter informações nas Secretarias de Estado de Minas Gerais sobre a situação em que se encontra a segurança da informação nas organizações.

3.2 Coleta de dados

A técnica de pesquisa utilizada para realização do trabalho acadêmico foi a entrevista. A entrevista caracteriza-se pelo "encontro entre duas pessoas com o intuito de obter informações do entrevistado, sobre determinado assunto, mediante uma conversação de natureza profissional." (MARCONI; LAKATOS, 1986, p. 70). Segundo, as autoras, existem três tipos de entrevistas, que se alteram de acordo com o propósito do entrevistador: padronizada ou estruturada; despadronizada ou não estruturada; e painel.

O tipo de entrevista utilizada foi a estruturada no qual "[...] o entrevistador segue um roteiro previamente estabelecido; as perguntas feitas aos indivíduos são predeterminadas. Ela se realiza de acordo com um formulário elaborado e é efetuada de preferência com pessoas selecionadas de acordo com um plano." (MARCONI; LAKATOS, 1986, p. 71)

A entrevista estruturada foi escolhida como técnica a ser utilizada na coleta de dados devido principalmente a três fatores: o primeiro, se relaciona ao fato de existir maior flexibilidade, podendo o entrevistador explanar os objetivos da pesquisa, repetir ou esclarecer perguntas, e elucidar algum significado que o entrevistado não entenda (MARCONI; LAKATOS, 1986); o segundo se relaciona " [...] a obtenção de dados facilmente tabuláveis e quantificáveis" (GIL, 1989, p. 91); e por fim, a possibilidade de obter informações mais confiáveis em conseqüência do maior contato entre entrevistador e o entrevistado (MARCONI; LAKATOS, 1986).

---

[14] Levantamento corresponde a pesquisas em que "[...] procede-se à solicitação de informações a um grupo significativo de pessoas acerca do problema estudado para, em seguida, mediante análise quantitativa, obterem-se as conclusões correspondentes aos dados coletados." (GIL, 1989, p. 56)

3.2.1 Instrumento de coleta de dados

O instrumento de coleta de dados foi o formulário[15], que teve por objetivo investigar em qual situação real se encontra a segurança da informação nas Secretarias de *Estado de Minas Gerais.*

A elaboração do formulário teve como base a Pesquisa Nacional de Segurança da Informação realizada pela empresa Módulo Security Solutions, líder em consultoria na área de segurança da informação na América Latina e a NBR ISO/IEC 17 799. A Pesquisa Nacional de Segurança da Informação[16] é realizada anualmente, desde 1994, e é considerada pelos especialistas na área como um dos instrumentos norteadores do segmento no país, pois apresenta dados estatísticos atualizados sobre a segurança da informação nas organizações brasileiras. A 9ª Pesquisa Nacional de Segurança da Informação, realizada em 2003, contou com uma amostra de 682 organizações, sendo que a metade das 1 000 maiores organizações brasileiras participaram da pesquisa. As organizações do Governo correspondiam a 17% da amostra (MÓDULO SECURITY SOLUTIONS, 2003).

Do processo de elaboração do formulário participaram além do autor do trabalho, seu orientador. Esse processo constou com as seguintes fases:

a) criação de várias perguntas sobre a segurança da informação;

b) análise e seleção das perguntas mais relevantes ao objetivo do trabalho; e

c) agrupamento das perguntas em tópicos.

Seguindo as recomendações de Barros e Lehfeld (2003), assim como as de Marconi e Lakatos (1986), segundo a qual um formulário de pesquisa não deve ser longo demais para não cansar e desanimar quem está respondendo, foi elaborado um formulário constituído de 19 perguntas (apêndice A), com um tempo médio de 15 minutos para ser

---

[15] O formulário e o questionário diferenciam-se apenas no que se refere à forma de aplicação. O questionário é preenchido pelo próprio entrevistado sem a presença do entrevistador, já o formulário o entrevistador está presente e é ele quem registra as respostas. (GIL, 1989; BARROS; LEHFELD, 2003)

[16] As Pesquisas Nacionais de Segurança da Informação podem ser consultadas no Portal da Módulo Security Solutions no endereço eletrônico www.modulo.com.br.

respondido, que procurou abarcar as principais questões relacionadas à segurança da informação.

As perguntas do formulário foram agrupadas em cinco tópicos:

1°) perfil da organização: procurou-se verificar tamanho das organizações pesquisadas através do número de funcionários e do número de computadores (estações de trabalho);

2°) responsáveis pela segurança da informação na organização: objetivou-se verificar qual a área responsável, o número de funcionários que trabalham com a segurança da informação na organização e a existência de um fórum, liderado pela direção, responsável pela gestão da segurança da informação;

3°) problemas com segurança da informação: nesse tópico, procurou-se verificar quais são as principais ameaças à segurança da informação, qual é a incidência dos problemas com a segurança, os principais responsáveis por provocar incidentes de segurança e os obstáculos para a implementação das técnicas e procedimentos que asseguram a segurança da informação nas organizações;

4°) melhores práticas em segurança da informação: procurou investigar se as Secretarias de Estado de Minas Gerais estão implementando as melhores práticas de segurança da informação segundo a NBR ISO/IEC 17 799, como Ánálise de Riscos, Política de Segurança da Informação, definição das responsabilidades em segurança da informação, treinamento e conscientização em segurança da informação, relatório de incidentes de segurança e o Plano de Contingência;

5°) relação das organizações com as normas NBR ISO/IEC 17 799 ou a BS 7 799: procurou-se verificar qual é o grau de conhecimento do entrevistado e qual é o envolvimento da organização com as normas de segurança da informação mencionadas acima.

As 19 questões do formulário são de múltiplas escolhas, a fim de facilitar as respostas e a tabulação das mesmas. No final do formulário foi reservado um espaço

denominado "Comentários Adicionais" para relatar algumas observações pertinentes que fossem percebidas ao longo da entrevista, possibilitando mais informações sobre a situação da segurança da informação nos órgãos pesquisados.

Apesar do formulário ser baseado em uma pesquisa reconhecida nacionalmente, foi realizada uma entrevista em uma Secretaria de Estado para validação do instrumento de coleta de dados, com o objetivo de detectar algumas questões que não fossem compreendidas claramente pelo entrevistado. Outro objetivo do pré-teste era avaliar o tempo que seria necessário para realizar as entrevistas. Depois de realizado o pré-teste, pequenas correções foram realizadas, dando-se concluída a fase de elaboração do questionário.

3.2.2 Método de escolha das organizações e da realização das entrevistas

Foram definidas que as organizações entrevistadas seriam todas as Secretarias de Estado de Minas Gerais. O motivo da escolha por tais órgãos está relacionado ao fato deles serem responsáveis pela execução das funções essenciais do Governo Estadual. Ao todo, são 15 Secretarias de Estado que formam o Poder Executivo mineiro em 2004. As Secretarias de Estado são:

a) Secretaria de Estado de Agricultura, Pecuária e Abastecimento (SEAPA);

b) Secretaria de Estado de Cultura (SEC);

c) Secretaria de Estado de Ciência, Tecnologia e Ensino Superior (SECTES);

d) Secretaria de Estado de Desenvolvimento Econômico (SEDE);

e) Secretaria de Estado de Desenvolvimento Social e Esportes (SEDESE);

f) Secretaria de Estado de Desenvolvimento Regional e Política Urbana (SEDRU);

g) Secretaria de Estado de Defesa Social (SEDS);

h) Secretaria de Estado de Educação (SEE);

i) Secretaria de Estado de Fazenda (SEF);

j) Secretaria de Estado de Governo (SEGOV);

l) Secretaria de Estado de Meio Ambiente e Desenvolvimento Sustentável (SEMAD);

m) Secretaria de Estado de Planejamento e Gestão (SEPLAG);

n) Secretaria de Estado de Saúde (SES);

o) Secretaria de Estado de Transportes e Obras Públicas (SETOP);

p) Secretaria de Estado de Turismo (SETUR).

Os contatos com as Secretarias de Estado foram feitos por uma funcionária da Superintendência Central de Governança Eletrônica (SCGE) da Secretaria de Estado de Planejamento e Gestão (SEPLAG), onde o autor realizou o estágio supervisionado, por meio de telefone. Os contatos foram realizados primeiramente com o responsável pela área de tecnologia de cada Secretaria, uma vez que esses profissionais, devido à natureza de suas atividades, normalmente têm conhecimento das questões envolvendo segurança da informação em suas organizações. Através desses contatos, foi divulgado o objetivo do trabalho e identificado o profissional mais indicado para responder sobre segurança da informação na organização. Depois desses contatos, que foram realizados previamente, foram marcadas as entrevistas para o preenchimento do formulário. O motivo da marcação das entrevistas ser realizada pela SCGE foi dar maior credibilidade à pesquisa e facilitar o acesso às organizações.

As entrevistas foram realizadas pelo próprio autor do trabalho, no período de 29 de setembro de 2004 a 20 de outubro de 2004. Todas as Secretarias de Estado se dispuseram a participar da pesquisa, dessa forma, a pesquisa abrangeu a análise de 15 formulários. No início de cada entrevista foi reafirmado o objetivo do trabalho e salientado que não seriam apresentados dados individuais sobre cada organização, nem a identidade do entrevistado no trabalho monográfico.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS DA PESQUISA

Este capítulo tem por objetivo apresentar e analisar os dados obtidos por meio do levantamento descrito na seção 3. Conforme já mencionado, a pesquisa contou com a participação de todas as 15 Secretarias de Estado de Minas Gerais.

A análise dos dados caracteriza-se como uma análise estatística dos resultados obtidos, e foram utilizados recursos, como gráficos e tabelas, para facilitar a visualização dos dados.[17] Para facilitar a compreensão dos aspectos dessa investigação, os resultados são descritos seqüencialmente, divididos em cinco blocos, conforme se apresentam no formulário de pesquisa utilizado (apêndice A).

Ao longo da análise dos resultados, também são apresentados dados de outras pesquisas, especialmente da Pesquisa Nacional de Segurança da Informação (PNSI), realizada pela Módulo Security Solutions, para perceber como está a situação da segurança da informação das Secretarias de Estado em relação ao contexto nacional.

4.1 Perfil das organizações

As Secretarias de Estado de Minas Gerais são organizações que possuem um grande número de funcionários sendo que nenhuma apresenta menos de 100 trabalhadores. 40% destas Secretarias de Estado possuem entre 101 e 300 funcionários, 33% possuem de 301 a 1 000 funcionários e 27% possuem mais de 1 000 funcionários (tab. 4.1).

[17] Optou-se por trabalhar com nenhuma casa decimal nos dados referentes a porcentagem (%).

Tabela 4.1: Número de funcionários das Secretarias de Estado de Minas Gerais – set./out. 2004

Número de funcionários	Secretarias	
	Absoluto	%
Até 50	-	-
De 51 a 100	-	-
De 101 a 300	6	40
De 301 a 1000	5	33
Mais de 1000	4	27
Total	15	100

Notas:
(a) O levantamento do número de funcionários de cada Secretaria de Estado foi baseado na resposta dos entrevistados.
(b) Os dados são referentes aos funcionários que trabalham nos prédios principais das organizações localizadas em Belo Horizonte.
(c) Sinal convencional utilizado:
- Dado numérico igual a zero não resultante de arredondamento

Os dados da pesquisa demonstram que existe uma concentração das Secretarias de Estado que possuem entre 51 a 200 computadores (40%), e entre 201 a 500 computadores (33%), totalizando essas duas faixas 73% das organizações pesquisadas (tab. 4.2).

Tabela 4.2: Número de computadores (estações de trabalho) das Secretarias de Estado de Minas Gerais – set./out. 2004

Número de computadores	Secretarias	
	Absoluto	%
Até 50	1	7
De 51 a 200	6	40
De 201 a 500	5	33
De 501 a 1000	1	7
Acima de 1000	2	13
Total	15	100

A partir da análise dos dados desta seção, podemos constatar que as organizações que fazem parte deste estudo possuem características que tornam mais difícil a implementação da segurança da informação, como o grande contingente de funcionários das Secretarias, já que o ser humano é considerado por diversos autores como o elo mais fraco na implementação da segurança da informação, e o grande número de computadores, sendo que

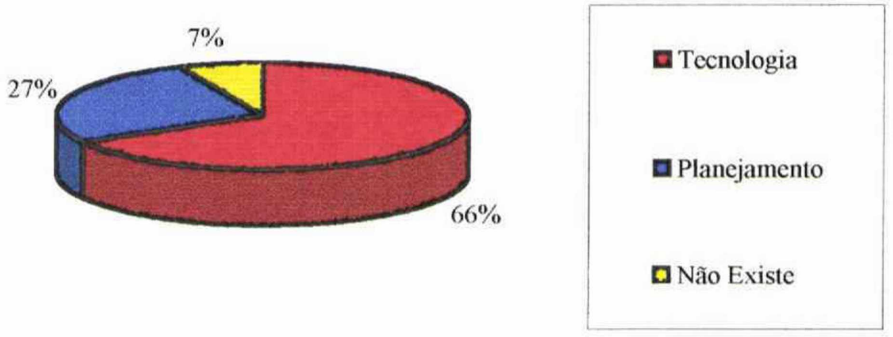
maioria das Secretarias, cerca de 93%, possuem mais de 50 estações de trabalho, sendo que duas organizações possuem mais de 1 000 computadores.

4.2 Responsáveis pela segurança da informação nas organizações

A área de Tecnologia tem sido a responsável pelas ações de segurança da informação na maioria das Secretarias de Estado (66%), sendo que em 27%, a área responsável é a de Planejamento. Em uma organização (7%), ainda não existe uma área responsável pela segurança da informação. Nenhuma Secretaria de Estado possui um *Security Office*, termo utilizado para denominar áreas exclusivas de segurança da informação (gráf. 4.1).

A 9ª PNSI também aponta a área de Tecnologia (49,5%) como a principal responsável pela segurança da informação nas organizações pesquisadas. Entretanto, 25,5% das organizações pesquisadas já apresentam um *Security Office* (MÓDULO SECURITY SOLUTIONS, 2003).

Gráfico 4.1: Área responsável pela segurança da informação nas Secretarias de Estado de Minas Gerais – set./out. 2004



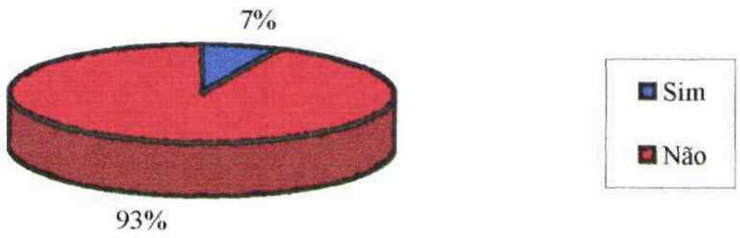
Com relação à quantidade de funcionários que dedicam a maior parte do seu trabalho à segurança da informação, 87% das Secretarias de Estado possuem pelo menos um profissional, sendo que a grande maioria, cerca de 53%, possuem de 2 a 4 funcionários trabalhando com a segurança da informação. Duas Secretarias, ou seja, 13%, ainda não possuem nenhum funcionário que dedicam a maior parte do seu trabalho à segurança da informação (tab. 4.3).

Tabela 4.3: Quantidade de funcionários que dedicam a maior parte do seu trabalho à segurança da informação nas Secretarias de Estado de Minas Gerais – set./out. 2004

Número de funcionários	Secretarias	
	Absoluto	%
De 2 a 4	8	53
De 5 a 10	3	20
Nenhum funcionário	2	13
1	1	7
Mais de 10	1	7
Total	15	100

Apesar da maioria das Secretarias de Estado contarem com profissionais que trabalham com a segurança da informação, 93% delas não possuem um fórum de gestão de segurança da informação (gráf. 4.2). A NBR ISO/IEC 17 799 relata a importância de que "[...] fóruns apropriados de gerenciamento com liderança da direção sejam estabelecidos para aprovar a política de segurança da informação, atribuir as funções de segurança e coordenar a implementação da segurança através da organização." (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2003, p. 5). Ainda segundo a NBR ISO/IEC 17 799, a criação desse fórum de segurança busca "[...] garantir um direcionamento claro e um suporte de gestão visível dos envolvidos para as iniciativas de segurança." (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, p. 5)

Gráfico 4.2: Existência de um fórum de gestão da segurança da informação nas Secretarias de Estado de Minas Gerais – set./out. 2004



Diante da importância que possui o fórum de gestão da segurança da informação para as organizações, cabe aqui relatar a importante iniciativa do Governo Federal. Através do Decreto nº 3.505, de 13 de junho de 2000, foi criado o Comitê Gestor da

Segurança da Informação (CGSI) e a Política de Segurança da Informação dos órgãos e entidades da Administração Pública Federal (ROCHA, 2004a).

O art. 6° do Decreto n° 3.505 relata que a função do CGSI é "[...] assessorar a Secretaria Executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise."

O Tenente Coronel João Rufino de Sales, chefe do grupo de Assessoramento Técnico e membro do CGSI, relata em entrevista concedida a Módulo Security Magazine, em 9 fevereiro de 2004, que além de colaborar na implantação e execução da Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, o CGSI realiza atividades como: a criação de normas de segurança da informação no Governo Federal, como por exemplo, para sítios da Internet e classificação de ativos, além de apoio a aprovação de diversas modificações na legislação para dar melhor amparo ao tema; estudos para criação de um centro de resposta a incidentes; estudos sobre criptografia comercial e normas técnicas; estudos sobre legislação de interesse do setor; e realização de uma pesquisa de Segurança da Informação no setor público, que está em andamento (ROCHA, 2004a).

4.3 Problemas com a segurança da informação

Lixo eletrônico (73%), divulgação de senhas (67%), funcionários insatisfeitos (67%) e pragas virtuais (67%) foram consideradas as principais ameaças à segurança da informação nas Secretarias de Estado de Minas Gerais (tab. 4.4).

Em relação à principal ameaça à segurança da informação constatada nas Secretarias de Estado, Henrique Faulhaber relata em artigo, publicado em 13 de setembro de 2004 na Módulo Security Magazine, baseado em um estudo da Message Labs[18], que a prática de spam já é responsável por 80% do tráfego de e-mails que circulam atualmente na Internet e que isto já causa um prejuízo de US$ 25 bilhões em todo mundo anualmente (FAULHABER, 2004). Essa prática assumiu proporções de crescimento tão alarmantes que existem autores que acreditam na perda de credibilidade do e-mail como meio de comunicação nos próximos anos, se nenhuma providência for tomada.

[18] Message Labs é uma empresa britânica de filtragem de correspondência eletrônica

Tabela 4.4: Principais ameaças à segurança da informação nas Secretarias de Estado de Minas Gerais – set./out. 2004

Ameaças	Secretarias	
	Absoluto	%
Lixo eletrônico (spam,.hoax)	11	73
Divulgação de senhas	10	67
Funcionários insatisfeitos	10	67
Pragas Virtuais (vírus, *trojan horse, worm*)	10	67
Acessos locais indevidos	6	40
Alteração indevida de configurações	6	40
Erros e acidentes humanos	6	40
Falhas na segurança física	6	40
Vazamento de informações	5	33
Fraudes em e-mails	4	27
Pirataria	4	27
Acessos remotos indevidos	3	20
Incêndio/Desastre	3	20
Invasores Externos (*Hacker, Cracker*)	3	20
Super poderes de acesso	3	20
Engenharia Social	2	13
Roubo/Furto	2	13
Uso de indevido de *notebooks*	2	13
Roubo de senhas	1	7
Outras	-	-
Sabotagens	-	-

Nota:
(a) O total de citações é superior a 15 na coluna "Absoluto" e 100 na coluna "%" devido ao fato de a questão aceitar múltiplas respostas.
(b) Sinal convencional utilizado:
- Dado numérico igual a zero não resultante de arredondamento

As três ameaças apontadas por 67% das Secretarias de Estados de Minas Gerais como uma das principais à segurança da informação, também são grandes preocupações das organizações no cenário nacional. Segundo a 9ª PNSI, o vírus (66%), os funcionários insatisfeitos (53%) e a divulgação de senhas (51%) foram apontadas como as principais ameaças à segurança da informação nas organizações pesquisadas (MÓDULO SECURITY SOLUTIONS, 2003).

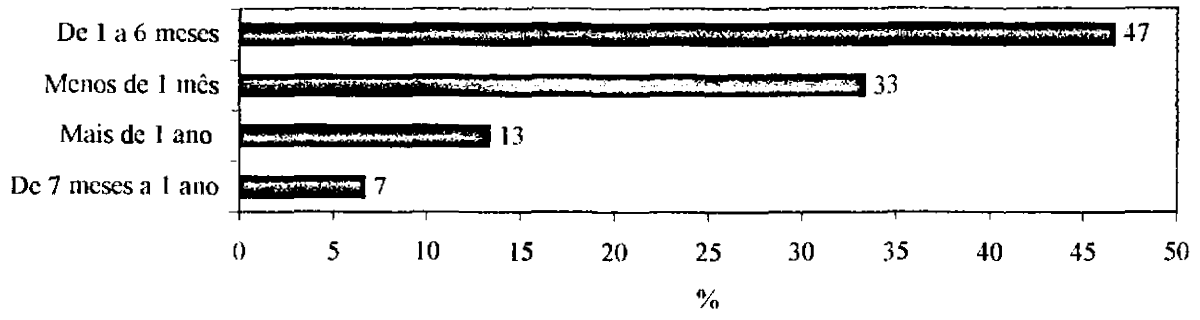
A pesquisa revela um índice bastante preocupante: 80% das organizações tiveram problemas com a segurança da informação nos últimos seis meses, sendo que 33% das Secretarias afirmaram ter tido problemas a menos de um mês da realização da pesquisa.

Nenhuma organização afirmou nunca ter sofrido algum tipo de problema com a segurança da informação (gráf. 4.3).

Dados das duas últimas PNSI demonstram que os problemas com segurança da informação estão cada vez mais constantes. Em 2002, 23% das organizações pesquisadas afirmaram ter tido algum tipo de problema com a segurança da informação nos últimos seis meses em relação à realização da pesquisa; em 2003, esse percentual quase que duplicou, aumentando para 43% (MÓDULO SECURITY SOLUTIONS, 2002; 2003).

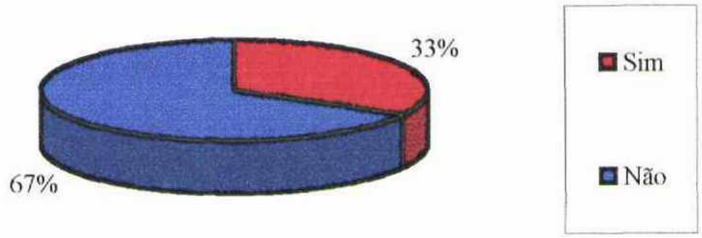
A partir da análise do gráfico 4.3, podemos constatar que as Secretarias de Estado de Minas Gerais tem que implementar medidas de segurança mais eficazes para lidarem com a constante evolução dos problemas com segurança da informação.

Gráfico 4.3: Período do último problema com a segurança da informação nas Secretarias de Estado de Minas Gerais – set./out. 2004



Em 2004, 33% dos entrevistados afirmaram que as organizações tiveram descontinuidade dos seus serviços em decorrência dos incidentes de segurança da informação (gráf. 4.4). Um dos incidentes de segurança que foi mencionado como causador da descontinuidade dos serviços nas cinco Secretarias foi a falta de energia elétrica. Este incidente causa grande impacto nas atividades da organização, tendo em vista a grande dependência das Secretarias de Estado em relação aos ativos tecnológicos, afetando principalmente a disponibilidade da informação, um dos princípios da segurança da informação.

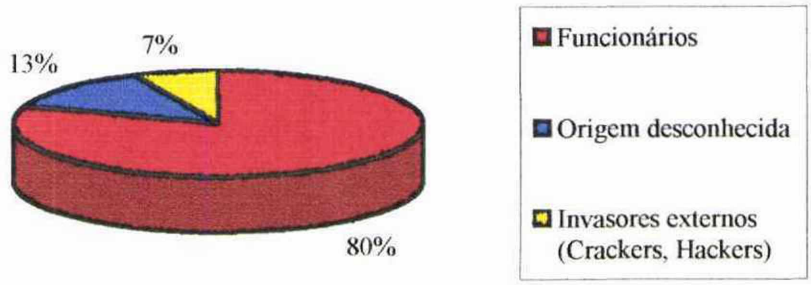
Gráfico 4.4: Ocorrência de descontinuidade dos serviços provocados por incidentes de segurança da informação nas Secretarias de Estado de Minas Gerais - 2004



Os funcionários foram apontados como os principais responsáveis pelos problemas de segurança da informação ocasionados nas organizações: de cada cinco entrevistados, quatro apontavam eles como os principais responsáveis. Dois entrevistados (13%) não conseguiram identificar quem são os principais responsáveis pelos problemas de segurança da informação (origem desconhecida) na organização, sendo que apenas um (7%) apontou os invasores externos como os principais responsáveis por este tipo de problema (gráf. 4.5). Podemos constatar que a maioria dos problemas com segurança da informação nas Secretarias de Estado de Minas Gerais são de origem interna, sendo que os funcionários insatisfeitos são apontados por 66% dos entrevistados (tab. 4.4) como uma das principais ameaças à segurança da informação nas organizações.

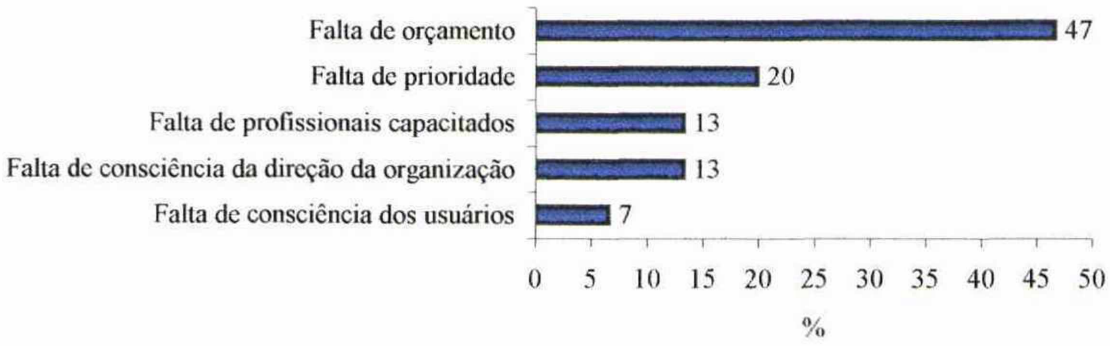
Um dado que chama atenção é a baixa representatividade que os invasores externos, como o *hacker* e o *cracker*, têm em relação aos problemas com segurança da informação nas Secretarias de Estado de Minas Gerais. Apenas três entrevistados (20%) apontaram estes invasores como principais ameaças à segurança da informação (tab. 4.4), sendo que apenas um apontou os como principais responsáveis por provocar incidentes de segurança nas Secretarias de Estado. Entretanto, por três anos consecutivos (2001, 2002, 2003), as PNSI revelaram que as organizações entrevistadas apontaram os *hackers* como os principais responsáveis por incidentes de segurança na organização, sendo que na 9ª PNSI eles são apontados por 32% das organizações e os funcionários por 23% (MÓDULO SECURITY SOLUTIONS, 2001; 2002; 2003).

Gráfico 4.5: Principal responsável por provocar incidentes de segurança da informação nas Secretarias de Estado de Minas Gerais – set./out 2004



O principal obstáculo apontado para a implementação da segurança da informação nas Secretarias de Estado de Minas Gerais foi a falta de orçamento, representando quase a metade das entrevistas (47%). Outros obstáculos apontados, em menor escala, foram a falta de prioridade (20%), a falta de profissionais capacitados e de consciência da direção da organização, ambos citados por 13% dos entrevistados, e a falta de consciência dos usuários, apontada por um entrevistado (7%) (gráf. 4.6).

Gráfico 4.6: Principal obstáculo para a implementação da segurança da informação nas Secretarias de Estado de Minas Gerais – set./out. 2004



A falta de orçamento é sempre apontada como um dos grandes empecilhos para a realização de determinadas ações nas instituições públicas. No caso da segurança da informação, além da falta de recursos, que são essenciais para sempre manter a segurança atualizada dos ativos, a falta de consciência das pessoas da organização em relação à importância da segurança da informação é outra grande barreira para a sua implementação. As PNSIs de 2002 e 2003 revelam que o principal obstáculo apontado para a implementação da

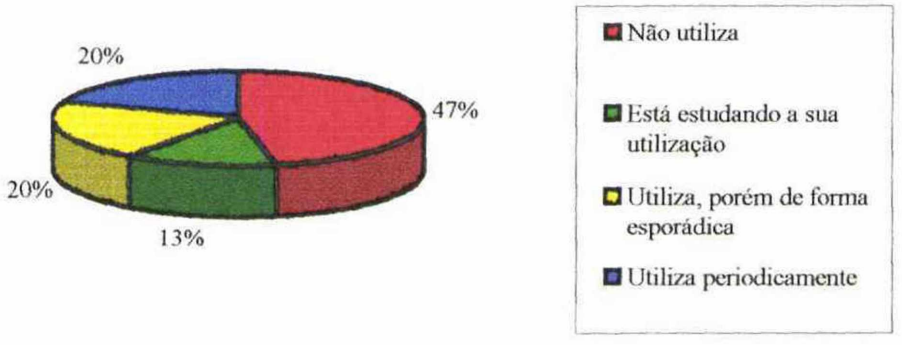
segurança da informação nas organizações pesquisadas foi a falta de consciência da direção da organização, ator fundamental para legitimar a importância da segurança na instituição. Isso foi verificado em 33% das organizações pesquisadas no ano 2002 e em 23% no ano de 2003 (MÓDULO SECURITY SOLUTIONS, 2002; 2003).

4.4 Melhores práticas em segurança da informação

A NBR ISO/IEC 17 799, assim como diversos outros autores, entre eles Moreira (2001) e Sêmola (2003), destacam a importância da Análise de Riscos como instrumento que possibilita conhecer melhor os problemas que envolvem a segurança da informação na organização, com intuito de subsidiar a seleção das medidas de segurança mais eficazes a serem implementadas no ambiente organizacional.

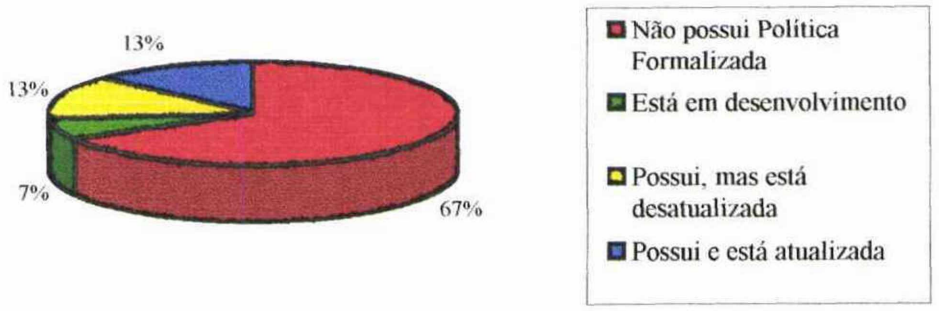
Apesar da importância da Análise de Riscos, 60% das Secretarias de Estado de Minas Gerais não utilizam esse instrumento antes da implementação das suas medidas de segurança. A não utilização da Análise de Riscos pode acarretar a adoção de medidas de segurança ineficazes, como a proteção inadequada de ativos essenciais da organização, ou excesso de medidas de segurança para proteger ativos menos relevantes para os processos organizacionais. Das organizações que afirmaram utilizar a Análise de Riscos, apenas três Secretarias (20%), usam freqüentemente esta ferramenta (gráf. 4.7).

Gráfico 4.7: Utilização da Análise de Riscos pelas Secretarias de Estado de Minas Gerais para identificação dos problemas de segurança da informação – set./out. 2004



Um dado que chama bastante atenção pelo seu caráter negativo é a baixa porcentagem de Secretarias de Estado de Minas Gerais que possuem uma Política de Segurança Formalizada. Apenas 26% das Secretarias afirmaram possuir uma Política de Segurança, sendo que apenas duas (13%) relataram que as suas Políticas estão atualizadas (gráf. 4.8).

Gráfico 4.8: Existência de Política de Segurança da Informação nas Secretarias de Estado de Minas Gerais – set./out. 2004



Os dados da 9ª PNSI revelam um cenário bastante diferente do cenário das Secretarias de Estado de Minas Gerais, quando o assunto é Política de Segurança. 68% das organizações pesquisadas na 9ª PNSI afirmaram possuir uma Política de Segurança da Informação formalizada, sendo que 50% relataram que elas estão atualizadas (MÓDULO SECURITY SOLUTIONS, 2003).

A baixa porcentagem de Secretarias de Estado que possuem uma Política de Segurança da Informação indica que tais organizações não possuem uma base sólida que oriente a gestão da segurança da informação, prejudicando a proteção dos seus ativos e, conseqüentemente, a preservação da integridade, disponibilidade e confidencialidade de suas informações.

No que tange ao controle relacionado à definição de responsabilidades de segurança da informação, 67% dos entrevistados afirmaram que existe uma definição dos responsáveis pela proteção de cada ativo na Secretaria. Quatro entrevistados (27%) relataram que apenas uma parte dos ativos da Secretaria possui responsáveis pela sua proteção e um entrevistado (7%) relatou que não utiliza este tipo de controle na Secretaria (tab 4.5).

Tabela 4.5: Existência de uma definição das responsabilidades de segurança da informação nas Secretarias de Estado de Minas Gerais – set./out. 2004

Definição das responsabilidades de segurança da informação.	Secretarias	
	Absoluto	%
Existe uma definição dos responsáveis pela proteção de cada ativo da organização	10	67
Apenas uma parte dos ativos da organização possui responsáveis pela a sua proteção.	4	27
Não existe.	1	7
Total	15	100

A alta porcentagem de entrevistados que relataram que as Secretarias de Estado de Minas Gerais possuem uma definição dos responsáveis pela proteção dos ativos da organização esta relacionada ao Decreto nº 43 053, de 28 de novembro de 2002, que em seu art. 39 estabelece que "nenhum material permanente poderá ser distribuído à unidade requisitante sem a respectiva carga patrimonial, que se efetiva com o Termo de Responsabilidade, devidamente assinado." O art. 42 menciona que " a carga patrimonial corresponde à relação dos materiais permanentes lotados em determinada unidade administrativa, cujo objetivo é atribuir a responsabilidade pela guarda e conservação dos mesmos" a um servidor da unidade, que deverá assinar o Termo de Responsabilidade, assumindo total responsabilidade sobre os mesmos, sob pena de ser responsabilizado, caso aconteça algum dano ou desaparecimento do bem por sua culpa, negligência ou dolo, conforme exposto no art. 62.

É importante destacar que a definição das responsabilidades de segurança não pode se limitar apenas aos bens patrimoniais, ou seja, aos ativos físicos, que é o foco do Decreto nº 43 053. A definição das responsabilidades de segurança deve englobar todos os tipos de ativos da organização, como softwares e sistemas de informação. Um instrumento indicado para a definição de tais responsabilidades é a Política de Segurança da Informação, medida de segurança pouco adotada nas Secretarias de Estado de Minas Gerais como podemos perceber no gráfico 4.8.

Com relação às práticas de segurança que estão diretamente relacionadas ao fator humano, 60% das Secretarias de Estado de Minas Gerais não realizam nenhum tipo de treinamento em segurança da informação para os seus funcionários, sendo que 80% não

realizaram nenhuma palestra ou campanha de conscientização sobre a segurança da informação nos últimos doze meses (gráf. 4.9 e gráf. 4.10).

Em seis Secretarias de Estado (40%) um quadro de funcionários específicos, ligados geralmente à área de tecnologia, recebem treinamento em segurança da informação. Duas Secretarias (13%) realizaram uma palestra ou campanha de conscientização nos últimos doze meses, sendo que apenas uma (7%) realizou de 2 a 3 vezes. Nenhuma Secretaria realizou mais de 4 palestras ou realiza treinamento em segurança para a maior parte dos seus funcionários (gráf. 4.9 e gráf. 4.10).

Gráfico 4.9: Realização de treinamento em segurança da informação para os funcionários das Secretarias de Estado de Minas Gerais – set./out. - 2004

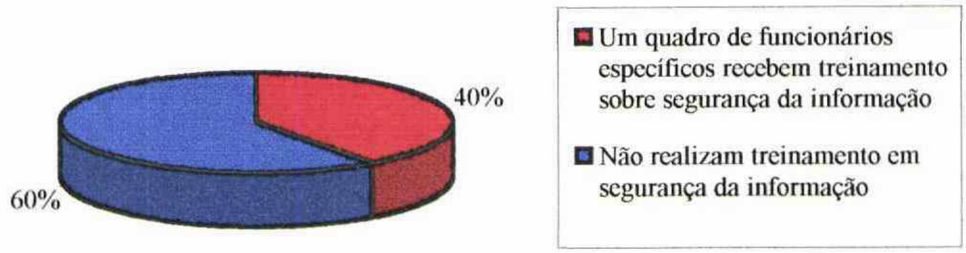
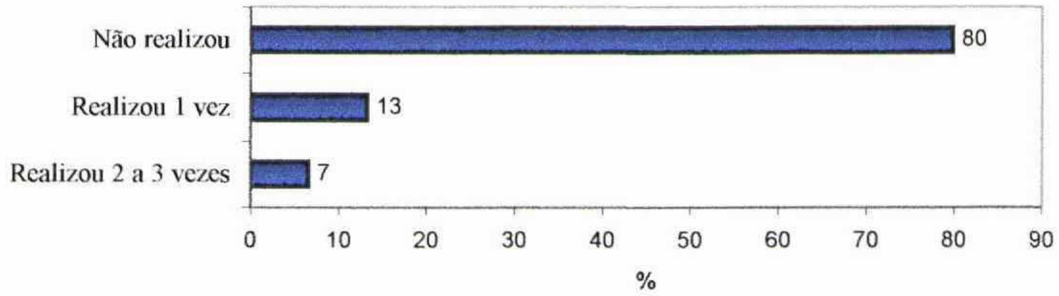


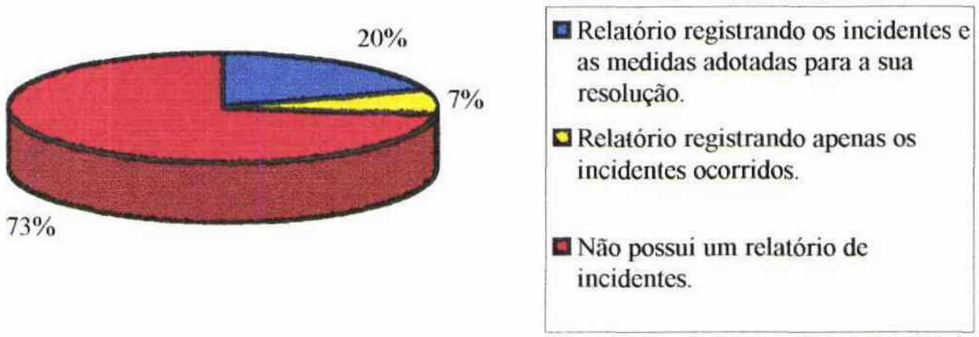
Gráfico 4.10: Freqüência de palestras e campanhas de conscientização sobre a segurança da informação, nos últimos doze meses, nas Secretarias de Estado de Minas Gerais – set./out. 2004



Podemos constatar a partir dos dados apresentados nos gráficos 4.10 e 4.11 que a grande maioria das Secretarias de Estado de Minas Gerais não realizam ações essenciais para se criar uma cultura de segurança da informação na organização, o que dificulta a implementação da segurança da informação, já que o ser humano é apontado por vários autores, entre eles Moreira (2001), Sêmola (2003), Ramos (2004) e Teófilo (2002), como o elo mais fraco desse processo.

Em relação à existência de um relatório de incidentes de segurança da informação na organização, 73% das organizações não possuem nenhum tipo de relatório, uma Secretaria de Estado (7%) possui um relatório registrando apenas os incidentes ocorridos e 20%, ou seja, três Secretarias de Estado, possuem um relatório registrando os incidentes ocorridos e as medidas adotadas para a sua resolução (gráf. 4.11).

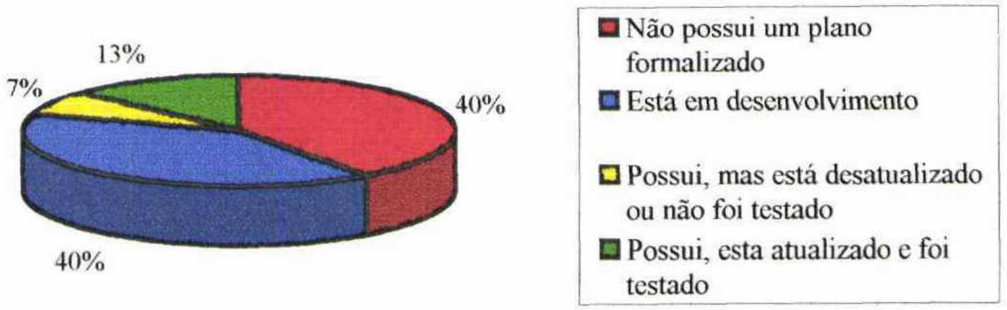
Gráfico 4.11: Existência de relatório de incidentes de segurança nas Secretarias de Estado de Minas Gerais – set./out. 2004



A falta de um documento como o relatório de incidentes, constatada em quase 75% das Secretarias de Estado de Minas Gerais, demonstra que tais organizações não têm realizado uma administração e monitoração efetiva da segurança da informação, pois este instrumento possui "[...] ótimas fontes de informação para medir o grau de aderência dos funcionários, o índice de eficiência dos controles e, ainda, para perceber falhas de segurança que permaneceram mesmo depois dos controles implementados" (SÊMOLA, 2003, p. 133), sendo considerado pela NBR ISO/IEC 17 799, como uma das melhores práticas em segurança da informação.

Apenas 13% das Secretarias de Estado de Minas Gerais, ou seja, duas organizações, possuem um Plano de Contingência atualizado e testado. Entretanto, em 40% das Secretarias o Plano de Contingência está em desenvolvimento, indicando um cenário mais promissor (gráf. 4.12). Os dados da 9ª PNSI demonstram também uma baixa porcentagem (21%) das organizações que possuem um Plano de Continuidade de Negócios ou Plano de Contingências (MÓDULO SECURITY SOLUTIONS, 2003).

Gráfico 4.12: Existência de Plano de Contingência nas Secretarias de Estado de Minas Gerais - set/out. 2004



Pelos dados apresentados pelas duas pesquisas, podemos perceber que a maioria das organizações não estão preparadas para lidarem com situações inesperadas que comprometam o andamento normal dos processos e a conseqüente prestação dos seus serviços. Outros dados que chamam a atenção para a necessidade de um Plano de Contingência são o alto percentual (80%) de Secretarias de Estado que tiveram problemas com a segurança das suas informações nos últimos seis meses (gráf. 4.3), sendo que 33% das organizações afirmaram ter tido descontinuidade dos seus serviços provocados por incidentes de segurança (gráf. 4.4).

Realizando uma seleção dos principais resultados constatados na pesquisa em relação a utilização das melhores práticas em segurança da informação pelas Secretarias de Estado de Minas Gerais e relacionando-os com as quatro etapas do Sistema de Gestão da Segurança da Informação, apresentado na seção **2.4**, obtemos as seguintes conclusões:

a) em relação aos instrumentos característicos de uma etapa de planejamento em segurança da informação, somente 13% das organizações possuem uma Política de Segurança atualizada e um Plano de Contingência atualizado e testado;

b) em relação à Análise de Riscos, técnica utilizada para estabelecer um diagnóstico da situação em que esta a segurança da informação na organização, apenas 20% das Secretarias de Estado a utilizam periodicamente para direcionar a escolha de seus controles de segurança;

c) em relação à implementação das medidas de segurança, item que é bastante influenciado pelo fator humano, 60% das organizações não realizam treinamento em segurança da informação para os seus funcionários, sendo que 80% das Secretarias de Estado

não realizaram nenhuma palestra ou campanha de conscientização sobre segurança da informação nos últimos doze meses;

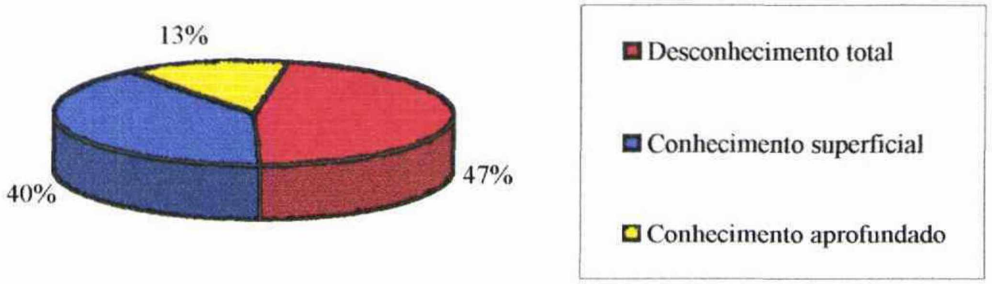
d) em relação à existência de um relatório de incidentes, documento que auxilia na administração e monitoração da segurança da informação, 73% das Secretarias de Estado não possuem nenhum tipo deste documento.

Em suma, os dados apresentados acima indicam que há ainda uma longa trajetória a ser traçada pelas Secretarias de Estado de Minas Gerais para alcançar um nível satisfatório de implementação de sistemas de gestão de segurança da informação, fornecendo uma proteção adequada aos ativos da organização ao preservar a confidencialidade, integridade e disponibilidade das informações, princípios básicos da segurança da informação.

4.5 Relação das organizações com as normas NBR ISO/IEC 17 799 ou a BS 7 799

Um total de 47% dos entrevistados informaram que ainda não conheciam nenhuma das normas de segurança da informação (NBR ISO/IEC 17 799 e BS 7 799) e 40% informaram já conhecê-las superficialmente. Apenas 13%, ou seja, dois entrevistados, informaram conhecer bem as normas (gráf. 4.13).

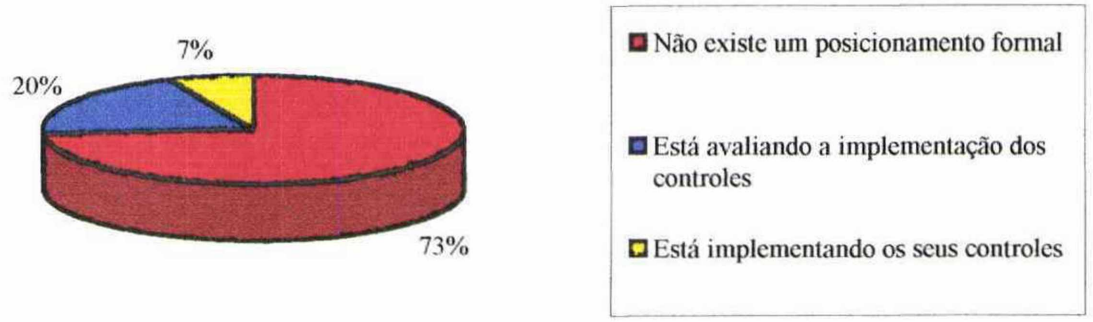
Gráfico 4.13: Grau de conhecimento dos entrevistados em relação à norma NBR ISO/IEC 17 799 (1) ou a BS 7 799 (2) – set./out. 2004



Notas: Siglas:
(1) NBR ISO/IEC 17 799: Tecnologia da informação – código de prática para a gestão da segurança da informação (Norma nacional)
(2) BS 7 799: Norma britânica sobre segurança da informação

Com relação às Secretarias de Estado, 73% delas não tomaram um posicionamento formal em relação à utilização das normas, 20% estão avaliando a implementação dos controles sugeridos por elas, e apenas uma Secretaria (7%) está implementando os controles sugeridos pelas normas. Nenhuma Secretaria afirmou ter concluído o processo de implementação dos controles das normas (gráf. 4.14).

Gráfico 4.14: Relação das Secretarias com as normas NBR ISO/IEC 17 799 (1) ou a BS 7 799 (2) – set./out. 2004



Notas: Siglas:
(1) NBR ISO/IEC 17 799: Tecnologia da informação – código de prática para a gestão da segurança da informação (Norma nacional)
(2) BS 7 799: Norma britânica sobre segurança da informação

A 9ª PNSI apresenta resultados bastante distintos dos encontrados nas Secretarias de Estado quando o assunto é adesão a norma NBR ISO/ IEC 17 799. 63,5% das organizações pesquisadas estão utilizando a NBR ISO/IEC 17 799 como referência técnica norteadora das suas ações de segurança da informação (MÓDULO SECURITY SOLUTIONS, 2003). Em relação às organizações mundiais que possuem a certificação BS 7 799, o número aumentou consideravelmente nos últimos 21 meses.

Apesar dessas normas (NBR ISO/IEC 17 799 e BS 7799) serem reconhecidas e utilizadas nacionalmente e internacionalmente pelos especialistas da área, como um conjunto de normas e padrões de gerenciamento para a implementação de boas práticas de segurança da informação nas organizações, sendo que a NBR ISO/IEC 17 799 foi homologada pela ABNT há três anos[19], apenas dois entrevistados afirmaram conhece-las bem, sendo que 73% das Secretarias não tomaram um posicionamento formal em relação à utilização das mesmas.

[19] A NBR ISO/IEC 17 799 foi homologada pela ABNT em setembro de 2001 (SÊMOLA, 2003).

5 CONCLUSÃO

A importância da informação no contexto organizacional atual, somada ao crescente número de ameaças aos ativos da organização, demonstram que a segurança da informação passa a ser um assunto estratégico, que interfere na capacidade das instituições de realizarem as suas atividades.

Entretanto, as questões que envolvem a implementação da segurança da informação não se limitam a ações isoladas, que abordem apenas aspectos tecnológicos, como a implementação de *firewall* ou antivírus nas organizações. A implementação de segurança da informação deve ser tratada na organização como um processo gerencial, em que os problemas de segurança devem ser tratados considerando os aspectos técnicos, organizacionais e, principalmente, humanos.

As organizações devem desenvolver um processo de gestão da segurança da informação, que envolva atividades e processos cíclicos que se integrem, a fim de garantir sempre o aperfeiçoamento do processo e, conseqüentemente, a preservação da confidencialidade, disponibilidade e integridade das informações. A preocupação com a gestão da segurança da informação nas instituições começa a estar cada vez mais em foco, graças à crescente adoção de normas como a NBR/ISO 17 799 e a BS 7 799 pelas organizações.

Tendo em vista o contexto relatado acima, esse trabalho monográfico realizou um diagnóstico da situação em que se encontra a segurança da informação nas Secretarias de Estado de Minas Gerais, órgãos responsáveis pela execução das funções essenciais do Governo Estadual, por meio de uma pesquisa realizada em todas essas instituições. Os principais resultados dessa pesquisa serão apresentados a seguir.

As Secretarias de Estado de Minas Gerais são organizações que possuem um grande contingente de funcionários e de computadores, sendo que 40% delas possuem entre 101 e 300 trabalhadores e de 51 a 200 estações de trabalho, características que tornam mais difícil a implementação da segurança da informação nestas instituições.

Com relação aos responsáveis pela segurança da informação foi constatado que essa atividade está a cargo do departamento de Tecnologia na maioria das Secretarias de Estado (66%), sendo que 53% delas possuem de 2 a 4 funcionários dedicando a maior parte do seu trabalho à segurança da informação. Apesar desse número relevante de funcionários que trabalham com a segurança da informação, 14 das 15 Secretarias de Estado de Minas Gerais não possuem um fórum de gestão da segurança da informação, estrutura responsável por garantir um direcionamento claro e um suporte às ações de segurança da informação na organização.

O lixo eletrônico (spam, hoax), a divulgação de senhas, os funcionários insatisfeitos e as pragas virtuais (vírus, *worm*, *trojan horse*) foram consideradas as principais ameaças à segurança da informação nas Secretarias, sendo apontadas por mais da metade destas organizações. Todos os entrevistados relataram que as organizações tiveram problemas com a segurança da informação, sendo que estes estão cada vez mais recentes, já que 80% das Secretarias de Estado afirmaram ter tido incidentes a menos de seis meses da realização dessa pesquisa.

Em decorrência dos incidentes ocorridos, um terço das Secretarias de Estado afirmaram ter tido descontinuidade dos seus serviços em 2004. Os principais responsáveis apontados por provocar incidentes de segurança foram os próprios funcionários da organização. A falta de orçamento é o principal obstáculo apontado pelos entrevistados para a implementação da segurança da informação na instituição.

Em relação à utilização das melhores práticas em segurança da informação, sugeridas pela NBR ISO/IEC 17 799, percebemos um cenário preocupante nas Secretarias de Estado de Minas Gerais. Mais de 60% delas não utilizam a Análise de Riscos para identificação dos problemas de segurança da informação, não possuem uma Política de Segurança Formalizada, não realizam treinamento para os seus funcionários em segurança da informação, não possuem um Plano de Contingência, não realizaram campanhas de conscientização em segurança da informação nos últimos doze meses e não possuem um relatório de incidentes de segurança.

As normas NBR ISO/IEC 17 799 e BS 7 799, apesar de serem reconhecidas nacionalmente e internacionalmente como padrões em gestão da segurança da informação,

são desconhecidas por 47% dos entrevistados e quase três quartos da Secretarias de Estado não tomaram um posicionamento formal em relação à utilização das mesmas.

Analisando os números apresentados nessa pesquisa, podemos constatar que existe uma longa trajetória a ser traçada pelas Secretarias de Estado de Minas Gerais para alcançar um nível satisfatório de proteção das suas informações. O alto índice de organizações que tiveram problemas com segurança da informação nos últimos seis meses, a falta de implementação das melhores práticas em segurança da informação indicada pela NBR ISO/IEC 17 799 e a inexistência de um fórum de gestão da segurança da informação, indicam uma situação crítica em relação à proteção da informação nestas instituições.

Tendo em vista o baixo grau de conhecimento dos entrevistados - profissionais que lidam com a segurança da informação nas organizações - em relação à NBR ISO/IEC 17 799 ou a BS 7 799 e o fato de que os funcionários foram considerados os principais responsáveis por provocar incidentes de segurança nas instituições, a realização de treinamento e palestras em segurança da informação para todos os trabalhadores (efetivos, terceirizados, direção), abordando assuntos relacionados à utilização correta dos instrumentos de trabalho, procedimentos de segurança e a importância de proteger os ativos da organização, quando bem implementada são medidas de segurança eficazes e eficientes. A implementação de tais medidas propicia a criação de uma cultura de segurança da informação na organização e, conseqüentemente, a redução dos riscos de incidentes de segurança afetarem a confidencialidade, disponibilidade e integridade das informações.

Outra ação essencial para a adequada proteção das informações nas Secretarias de Estado é a criação de um fórum ou comitê que fique responsável pela gestão da segurança da informação nas organizações. Seguindo o exemplo do Governo Federal, poderia se criar um Comitê Gestor de Segurança da Informação, englobando todas as Secretarias de Estado de Minas Gerais, com o objetivo de assessorar as organizações em suas ações de segurança.

Para finalizar, cabe destacar que episódios como as panes no sistema de processamento de dados do Instituto Nacional do Seguro Social (INSS), ocorridas no dias 09 e 10/11/04, provocando quase a paralisação total no atendimento aos aposentados de todo país e, conseqüentemente, enormes filas nos postos de atendimento, apenas reafirmam a necessidade das organizações públicas implementarem medidas de segurança eficazes para a

proteção da confidencialidade, integridade e disponibilidade das suas informações, e dessa forma, garantir as condições necessárias para uma adequada prestação de serviços para toda a sociedade.

6 REFERÊNCIAS

1 ABC NEWS. **Funcionários insatisfeitos representam perigo ao sistema das empresas.** 5 jun. 2002. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=7&objid=1137&pagecounter=0&idiom=0>. Acesso em: 16 set. 2004.

2 AKUTSU, Luiz; PINHO, José Antônio Gomes de. Sociedade da informação, accountability e democracia delegativa: investigação em portais de governo no Brasil. Revista de Administração Pública, Rio de Janeiro, v. 36, n. 5, p. 723-745, set/out. 2002.

3 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17 799** – Tecnologia da informação – código de prática para a gestão da segurança da informação. Rio de Janeiro, 2003. 56 p.

4 BARROS, Aidil de Jesus Paes de; LEHFELD, Neide Aparecida de Souza. **Projeto de pesquisa:** propostas metodológicas. 14.ed. Petrópolis: Vozes, 2003.

5 BASTOS, Alberto. Os novos rumos da gestão de segurança com as normas ISO 17 799 e BS 7 799. **Módulo Security Magazine,** São Paulo, 14 ago. 2002. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=297&pagecounter=0&idiom=0>. Acesso em: 2 maio. 2004.

6 BATITUCCI, Eduardo Cerqueira. **Apostila de metodologia científica do Programa de Especialização em Administração Pública**. Belo Horizonte: Fundação João Pinheiro, Escola de Governo, 2003. 38 p.

7 BRASIL. Constituição, 1988. **Constituição da República Federativa do Brasil.** Disponível em: <www.senado.gov.br/bdtextual/const88/Con1988br.pdf> Acesso em: 5 maio 2004.

8 BRASIL. Decreto nº 3.505 de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 13 jun. 2000. Disponível em: http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=16&objid=3&pagenumber=0&idiom=0 Acesso em: 10 nov. 2004.

9 BRASIL. Ministério do Planejamento, Orçamento e Gestão. **Fundamentos do modelo de segurança da informação.** Brasília: 2000. Disponível em: <http:// http://www.redegoverno.gov.br/eventos/arquivos/Mod_Seg_Inf.pdf>. Acesso em: 05 abr. 2004.

10 BRASIL. Tribunal de Contas da União. Secretaria Adjunta de Fiscalização. **Boas práticas em segurança da informação**. Brasília, 2003. 70 p. Disponível em: <http://www.tcu.gov.br/isc/sedip/pdf/Boas_Praticas_em_Seguranca_da_Informacao.pdf>. Acesso em: 20 jun. 2004.

11 CALHEIROS, Rosemberg Faria. **Segurança de informações nas empresas:** uma prioridade corporativa. 2002. 47 f. Trabalho de Conclusão de Curso (Graduação) – Escola de Biblioteconomia, Universidade do Rio de Janeiro, 2002. Disponível em: <http://www.modulo.com.br/pdf/rosemberg.pdf> Acesso em: 5 maio. 2004.

12 CANDÉA, Sérgio Luiz da Cunha. **Coletânea de recomendações básicas de segurança de sistemas, destinadas aos administradores de rede**. 2002. 56 f. Trabalho de Conclusão de Curso (Especialização) – Centro Técnico Espacial, Instituto de Tecnológico da Aeronáutica, 2002. Disponível em: <http://www.modulo.com.br/pdf/segurança_ti.pdf>. Acesso em: 8 maio 2004.

13 CASANAS, Alex Delgado Gonçalves; MACHADO, César de Souza. **O impacto da implementação da norma NBR ISO/IEC 17 799**: código de prática para a gestão da segurança da informação – nas empresas. Florianópolis, 2001. Disponível em: <http://www.modulo.com.br/pdf/NBR_ISO-IEC_17799_.pdf> Acesso em: 1 ago. 2004

14 CASTELLS, Manuel. **A sociedade em rede**. 7.ed. São Paulo: Paz e Terra, 2003. p.1 –118. (A era da informação: economia, sociedade e cultura, v.1)

15 CASTELO BRANCO, Henrique José. **Fundamentos e conceitos sobre Informação & Gestão da Informação**. Belo Horizonte: Fundação João Pinheiro, Escola de Governo, 2003. 31p. Apostila 01

16 CAUBIT, Rosângela. Qualidade com segurança ou segurança com qualidade?. **Módulo Security Magazine,** São Paulo, 21 nov. 2002. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=309&pagecounter=0&idiom=0>. Acesso em: 2 set. 2004.

17 FAULHABER, Henrique. O combate à praga do spam. **Módulo Security Magazine**, São Paulo, 13 set. 2004. *Disponível em:* <http://www.modulo.com.br/index.jsp>. Acesso em: 20 set. 2004

18 FREITAS, Marco Antônio Diniz. **Análise da segurança da informação em ambientes corporativos.** 2002. 116 f. Trabalho de Formatura (Graduação) – Faculdade de Engenharia de Sorocaba, Sorocaba, 2002. Disponível em: <http://www.modulo.com.br/pdf/ambiente-freitas.pdf>. Acesso em: 28 abr. 2004.

19 GALVÃO, Márcio. As principais dúvidas sobre malware: vírus, trojans & worms. **Módulo Security Magazine**, São Paulo, 20 maio. 2002. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=4&objid=19&pagecounter=0&idiom=0>. Acesso em: 15 ago. 2004.

20 GIL,Antônio Carlos. **Como elaborar projetos de pesquisa**. 2.ed. São Paulo: Atlas, 1989.

21 GONÇALVES, Júlio César. **O gerenciamento da informação e sua segurança contra ataques de vírus de computador recebidos por meio de correio eletrônico.** 2002. 339 p. Dissertação (Mestrado) - Faculdade de Economia, Contabilidade e Administração, Universidade de Taubaté, Taubaté, 2002. Disponível em: <http://www.unitau.br/prppg/cursos/ppga/mestrado/goncalves_julio_cesar.pdf>. Acesso em: 15 ago. 2004.

22 GONÇALVES, Luís Rodrigo de Oliveira. **O surgimento da norma nacional de segurança de informação**. [s.l] 19 mar. 2004. Lockabit - Portal de Segurança da Informação. Disponível em: < http://www.lockabit.coppe.ufrj.br/>. Acesso em: 20 ago. 2004

23 INFOCONOMY.COM; MÓDULO SECURITY MAGAZINE. **Mitnick alerta para os perigos da engenharia social.** [s.l] 06 set 2002. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=7&objid=1346&pagecounter=0&idiom=0>. Acesso em: 20 ago. 2004

24 ISMS International User Group. **International register of BS 7 799 accredited certificate.** [s.l] 15 nov. 2004. Disponível em: <http://www.xisec.com/register.htm> .Acesso em: 15 nov. 2004

25 MACHADO, César de Souza. **51 questões mais frequentemente formuladas sobre a BS 7 799 e ISO 17 799.** [s.l]. 3 mar. 2003 – atualizado em set. 2004. Disponível em: < http://www.cdigital.com.br/iso/faq.htm>. Acesso em: 13 nov. 2004.

26 _____. **Gerenciamento da segurança da informação em sistemas de teletrabalho.** 2002. 136 f. Dissertação (Mestrado) – Universidade Federal de Santa Catarina, Florianópolis, 2002. Disponível em: <http://teses.eps.ufsc.br/Resumo.asp?3240> Acesso em: 15 jul. 2004.

27 _____.. FAQ sobre as normas BS e ISO 17 799. **Módulo Security Magazine**, São Paulo, 24 abr. 2002. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=4&objid=17&pagenumber=0&idiom=0>. Acesso em: 12 maio. 2004.

28 MAIA, Marco Aurélio. Conceitos de segurança da informação. **Módulo Security Magazine**, São Paulo, 02 maio 2002. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=10&objid=160&pagecounter=0&idiom=0>. Acesso em 10 maio 2004.

29 _____. Métodos de engenharia social: confira as técnicas e saiba como se defender. **Módulo Security Magazine,** São Paulo, 10 maio 2001. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=173&pagecounter=0&idiom=0>. Acesso em: 1 ago. 2004.

30 MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Técnicas de pesquisa**: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados. São Paulo: Atlas, 1986.

31 MARINHO, Zilta Penna. Campanha de divulgação da Política de Segurança da Informação. **Módulo Security Magazine**, São Paulo, 26 set. 2000. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=349&pagecounter=0 &idiom=0>. Acesso em: 20 set. 2004.

32 MINAS GERAIS. Decreto n°. 43053, de 28 de novembro de 2002. Regulamenta, no âmbito da Administração Pública Direta, Autárquica e Fundacional do Poder Executivo, a aquisição, a incorporação, a armazenagem, a movimentação, o reaproveitamento, a alienação e outras formas de desfazimento na gestão de material. Disponível em: <http://www.planejamento.mg.gov.br/legisla/leg_mat/leg_est.asp> Acesso em: 12 nov. 2004.

33 MÓDULO SECURITY SOLUTIONS. 7a. Pesquisa Nacional de Segurança da Informação. **Módulo Security Magazine**, São Paulo, 30 jul. 2001. Disponível em: < http://www.modulo.com.br/pdf/pesq_seg_01.zip >. Acesso em 05 abr. 2004.

34 _____. 8a. Pesquisa Nacional de Segurança da Informação. **Módulo Security Magazine**, São Paulo, 31 out. 2002. Disponível em: <http://www.modulo.com.br/pdf/oitava-pesquisa-modulo.pdf>. Acesso em 05 abr. 2004.

35 _____. 9a. Pesquisa Nacional de Segurança da Informação. **Módulo Security Magazine,** São Paulo, 24 nov. 2003. Disponível em: <http://www.modulo.com.br/pdf/nona_pesquisa_modulo.pdf>. Acesso em: 05 abr. 2004.

36 MOREIRA, Nilton Stringasci. **Segurança mínima**: uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001. 240 p.

37 MORENO, Cláudio. **Aspectos de segurança da informação envolvidos na divulgação de informações via internet pelos órgão públicos.** 1997. 87 f. Dissertação (Mestrado) – Escola de Governo, Fundação João Pinheiro, Belo Horizonte, 1997.

38 NIC BR Security Office. **Cartilha de Segurança para Internet.** Glossário. Versão 2.0. [s.l]. 11 mar. 2003. Disponível em: <http://www.nbso.nic.br/docs/cartilha/>. Acesso em: 10 jul. 2004.

39 _____. **Cartilha de Segurança para Internet**, Parte I: Conceitos de Segurança. Versão 2.0. 11 mar. 2003. Disponível em: <http://www.nbso.nic.br/docs/cartilha/>. Acesso em: 10 jul. 2004.

40 _____. **Cartilha de Segurança para Internet**. Parte IV: SPAM. Versão 2.0. 11 mar. 2003. Disponível em: <http://www.nbso.nic.br/docs/cartilha/>. Acesso em: 10 jul. 2004.

41 OTILIO, C. Hackers – conceitos básicos. **Módulo Security Magazine**, São Paulo, 9 out. 2000. Disponível em <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=10&objid=3&pagecounter=0&idiom=0>. Acesso em: 25 ago. 2004.

42 RAMOS, Anderson. Conscientização de usuários e segurança da informação. **Módulo Security Magazine**, São Paulo, 1 out. 2004. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=406&pagenumber=0&idiom=0>. Acesso em: 10 out. 2004.

43 ROCHA, Luis Fernando. Aumenta o número de empresas certificadas BS 7 799 pelo mundo. **Módulo Security Magazine**, São Paulo, 20 fev. 2003. Disponível em: http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=7&objid=1732&pagecounter=0&idiom=0. Acesso em: 10 nov. 2004.

44 _____. Exclusivo: conheça a segurança da informação no Governo Federal brasileiro. **Módulo Security Magazine,** São Paulo, 9 fev. 2004. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=6&objid=51&pagecounter=0&idiom=0>. Acesso em: 10 out. 2004.

45 _____. Vamos combater o spam? - Parte 1. **Módulo Security Magazine,** São Paulo, 13 set. 2004. Disponível em: <http://www.modulo.com.br/index.jsp?page=3&catid=6&objid=64&pagecounter=0&idiom=0>. Acesso em 15 set. 2004.

46 SCHIRM, Helena. **Apresentação de referências, citações e notas de rodapé**. Belo Horizonte: Fundação João Pinheiro, 2003. 33 p.

47 SCHIRM, Helena. **Apresentação de trabalhos acadêmicos**. Belo Horizonte: Fundação João Pinheiro, 2003. 29 p.

48 SCUA Segurança da Informação. **Tipos de ameaças:** Ameaças Externas. [s.l] 2004. Disponível em: <http://www.scua.net>. Acesso em 10 set. 2004.

49 SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. Rio de Janeiro: Elsevier, 2003. 156 p.

50 SYMANTEC DO BRASIL. **O padrão de segurança global emergente:** ISO 17 799. São Paulo. 2 abr. 2002. Disponível em: <http://www.symantec.com/region/br/enterprisesecurity/content/framework/BR_1261.html>. Acesso em: 20 jun. 2004.

51 TEÓFILO, Álvaro. Treinamento e conscientização: fatores essenciais para o sucesso de uma política de segurança. **Módulo Security Magazine**, São Paulo, 15 out. 2002. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=304&pagecounter=0 &idiom=0>. Acesso em 8 out. 2004.

52 VARGAS, A. Ameaça além do Firewall. Por que as empresas devem se preparar contra a engenharia social? **Módulo Security Magazine,** São Paulo, 10 abr. 2002. Disponível em: <http://www.modulo.com.br/index.jsp>. Acesso em 14 jul. 2004.

53 VELOSO, Caio Julio Martins. **Segurança da informação:** um mapeamento teórico e a prática nas empresas de telecomunicações do Brasil. 2002. 286 f. Dissertação (Mestrado) – Escola de Governo, Fundação João Pinheiro, Belo Horizonte, 2002.

54 VUNET.COM. **Ataques virtuais motivados por questões ideológicas**. [s.l] 20 jun. 2002. Disponível em: <http://www.modulo.com.br/index.jsp>. Acesso em: 27 set. 2004.

APÊNDICE

APÊNDICE A – Formulário utilizado na pesquisa

PESQUISA SOBRE A SEGURANÇA DA INFORMAÇÃO NAS SECRETARIAS DE ESTADO DE MINAS GERAIS – SET/OUT DE 2004

PERFIL DA ORGANIZAÇÃO

1. Número de funcionários da organização:

( ) até 50
( ) de 51 a 100
( ) de 101 a 300
( ) de 301 a 1000
( ) mais de 1000

2. Quantos computadores (estações de trabalho) que a organização possui:

( ) Até 50
( ) De 51 a 200
( ) De 201 a 500
( ) De 501 a 1000
( ) Acima de 1000
( ) Não sabe informar

RESPONSÁVEIS PELA SEGURANÇA DA INFORMAÇÃO NA ORGANIZAÇÃO

3. Qual a área responsável pela segurança da informação na organização:

( ) Auditoria/Inspetoria
( ) Logística
( ) Planejamento
( ) Security Office (área específica para segurança)
( ) Tecnologia
( ) Outras. Quais? _____
( ) Não Existe

4. Qual o número de funcionários que dedicam a maior parte do seu trabalho à segurança da informação:

( ) 1
( ) De 2 a 4
( ) De 5 a 10
( ) Mais de 10
( ) Nenhum funcionário

5. Existe algum tipo de fórum na organização, com liderança da direção, responsável pela gestão da segurança da informação?

( ) Sim
( ) Sim, porém não está desempenhando esta função
( ) Não

PROBLEMAS COM SEGURANÇA DA INFORMAÇÃO

6. Quais são as principais ameaças à segurança da informação na organização:

( ) Acessos locais indevidos
( ) Acessos remotos indevidos
( ) Alteração indevida de configurações
( ) Pragas Virtuais (Trojan Horse, Vírus, Worm)
( ) Divulgação de senhas
( ) Engenharia Social
( ) Falhas na segurança física
( ) Fraudes em e-mails
( ) Erros e acidentes humanos
( ) Funcionários insatisfeitos
( ) Invasores Externos (Hacker, Cracker)
( ) Incêndio/Desastre
( ) Lixo informático (SPAM/HOAX)
( ) Pirataria
( ) Roubo de senhas
( ) Roubo/Furto
( ) Sabotagens
( ) Super poderes de acesso
( ) Uso de indevido de notebooks
( ) Vazamento de informações
( ) Outras. Quais? _____

7. A organização teve problemas com segurança da informação há:

( ) Menos de 1 mês
( ) De 1 a 6 meses
( ) De 7 meses a 1 ano
( ) Mais de 1 ano
( ) Nunca sofreu
( ) Não sabe informar

8. A organização já teve descontinuidade dos serviços com problemas de segurança da informação em 2004:

( ) Sim
( ) Não
( ) Não sabe informar

9. Qual o principal responsável por provocar incidentes de segurança da informação na organização:

( ) Ex-funcionários
( ) Funcionários
( ) Invasores externos (Crackers, Hackers)
( ) Origem desconhecida
( ) Prestadores de serviços
( ) Outros. Quais? _____

10. Qual o principal obstáculo para a implementação da segurança da informação na organização:

( ) Dificuldade em demonstrar o retorno
( ) Falta de consciência da direção da organização
( ) Falta de consciência dos usuários
( ) Falta de orçamento
( ) Falta de prioridade
( ) Falta de profissionais capacitados
( ) Outros. Quais? _____

MELHORES PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

11. Em relação à Análise de Riscos, a organização:

( ) Não utiliza este instrumento
( ) Está estudando a sua utilização
( ) Utiliza, porém de forma esporádica
( ) Costuma usar este instrumento para direcionar suas ações no gerenciamento da segurança da informação

12. Em relação a uma Política de Segurança da Informação Formalizada, a organização:

( ) Não possui
( ) Está em desenvolvimento
( ) Possui, mas está desatualizada
( ) Possui e está atualizada
( ) Não sabe informar

13. A organização possui uma definição das responsabilidades na segurança da informação?

( ) Sim, existe uma definição clara dos responsáveis pela proteção de cada ativo da organização
( ) Sim, entretanto apenas uma parte dos ativos da organização possuem responsáveis pela a sua proteção
( ) Não, a organização não possui definição das responsabilidades em segurança da informação.

14. Os funcionários da organização recebem treinamento em relação à segurança da informação?

( ) Sim, a maior parte dos funcionários são treinados nos procedimentos de segurança
( ) Sim, porém apenas um quadro de funcionários específicos recebem treinamento sobre segurança da informação
( ) Não

15. Em relação à realização de palestras e campanhas de conscientização sobre a segurança da informação nos últimos doze meses, a organização?

( ) Não realizou
( ) Realizou 1 vez
( ) Realizou 2 a 3 vezes
( ) Realizou mais de 4 vezes (inclusive)

16. Em relação a um relatório de incidentes de segurança?

( ) A organização possui um relatório registrando os incidentes e as medidas adotadas para a sua resolução.
( ) A organização possui um relatório registrando apenas os incidentes ocorridos.
( ) A organização não possui um relatório de incidentes.

17. Em relação a um Plano de Contingências formalizado, a organização:

( ) Não possui um plano formalizado
( ) Está em desenvolvimento
( ) Possui, mas está desatualizado ou não foi testado
( ) Possui, esta atualizado e foi testado
( ) Não sabe informar

RELAÇÃO DAS ORGANIZAÇÕES COM AS NORMAS NBR ISO/IEC 17 799 OU A BS 7 799

18. O entrevistado conhece as normas NBR ISO/IEC 17799 ou a BS 7799:

( ) Não sei do que se trata
( ) Conheço superficialmente
( ) Conheço bem

19. Qual a relação da organização com as normas citadas acima:

( ) Não existe um posicionamento formal por parte da organização em relação as essas normas
( ) Está avaliando a implementação dos controles sugeridos por elas
( ) Está implementando os seus controles
( ) Já implementou os seus controles

COMENTÁRIOS ADICIONAIS

Data da entrevista:

Duração da entrevista:

ANEXO

ANEXO A – Principais tecnologias em segurança da informação[20]

Antivírus - Programa ou software especificamente desenvolvido para detectar, anular e eliminar vírus de computador.

Assinatura Digital - Um código utilizado para verificar a integridade de um texto ou mensagem. Também pode ser utilizado para verificar se o remetente de uma mensagem é mesmo quem diz ser.

Criptografia - Criptografia é a ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

Firewall - Dispositivo constituído pela combinação de *software* e *hardware*, utilizado para dividir e controlar o acesso entre redes de computadores.

IDS - Do Inglês *Intrusion Detection System*. Um programa, ou um conjunto de programas, cuja função é detectar atividades incorretas, maliciosas ou anômalas.

Senha - Conjuntos de caracteres, de conhecimento único do usuário, utilizados no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser.

VPN - Do Inglês *Virtual Private Network*. Termo usado para se referir à construção de uma rede privada utilizando redes públicas, como a Internet, como infra-estrutura. Estes sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

---

[20] Este anexo foi extraído de NIC BR Security Office. **Cartilha de Segurança para Internet.** Glossário. Versão 2.0. 11 mar. 2003. Disponível em: <http://www.nbso.nic.br/docs/cartilha/>. Acesso em 10 jul. 2004.