UNIVERSIDADE FEDERAL DA BAHIA
ESCOLA DE ADMINISTRAÇÃO
NÚCLEO DE PÓS-GRADUAÇÃO DE ADMINISTRAÇÃO
MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO

REGINA SÁ MENEZES

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO IMPLEMENTADAS EM DUAS ORGANIZAÇÕES BAIANAS.

REGINA SÁ MENEZES

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO IMPLEMENTADAS EM DUAS ORGANIZAÇÕES BAIANAS.

Dissertação apresentada ao Núcleo de Pós-Graduação em Administração da Escola de Administração da Universidade Federal da Bahia, como parte dos requisitos para a obtenção de título de Mestre em Administração.

Orientador: Prof. Dr. Francisco Teixeira

Salvador, 2005

REGINA SÁ MENEZES

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO IMPLEMENTADAS EM DUAS ORGANIZAÇÕES BAIANAS.

Dissertação para obtenção do grau de Mestre em Administração

Salvador, 08 de março de 2005

Banca Examinadora:

Prof. Dr. Francisco Teixeira _____
Universidade Federal da Bahia

Prof. Dr. Cláudio Cardoso_____
Universidade Federal da Bahia

Prof. João Gualberto Rizzo Araújo_____
Faculdade Ruy Barbosa

Aos meus pais e meu irmão, companheiros em todos os momentos. Em especial, a minha mãe.

AGRADECIMENTOS

A meu orientador, Prof. Dr. Francisco Teixeira, pela atenção e acompanhamento desta pesquisa.

A João Gualberto Rizzo Araújo, por todo apoio recebido.

As organizações que permitiram a realização dos estudos de caso.

A Nildo Leite, meu eterno mestre, pelos incentivos para atuar na área acadêmica e continuar aprimorando meus conhecimentos.

Aos professores, em especial Maria do Carmo e Célio Andrade por toda dedicação, e aos funcionários do Mestrado Profissional.

A todos os meus colegas que proporcionaram momentos de aprendizagem, em especial, Frederico Albuquerque, Graziela Arakawa, José Barata, Lila Lopes, Marcelo Oliveira e Sandro Pasini.

Na impossibilidade de citar todas as pessoas, agradeço a todos aqueles que contribuíram para esta pesquisa.

“A vitória mais bela que se pode alcançar é vencer a si mesmo”
Santo Ignácio de Loyola

Resumo

As organizações públicas e privadas têm demonstrado carência com relação à proteção de informações organizacionais. Por tradição, elas direcionam uma atenção maior a segurança de bens patrimoniais e financeiros.

Na presente pesquisa foram investigadas as práticas de segurança da informação implementadas em duas organizações baianas, se elas são aderentes aos padrões de segurança existentes e as conseqüências da não implementação de controles adequados para a redução dos riscos presentes em seu ambiente.

Foi feita uma revisão da literatura sobre o tema e foram realizados estudos de caso em duas organizações baianas. Percebe-se que não há uma gestão da segurança da informação. Nessas organizações existem apenas medidas pontuais de segurança. Conclui-se que nas organizações estudadas, nem sempre são adotadas as práticas de segurança da informação necessárias para a redução dos riscos presentes em seu ambiente. Isso as deixa mais vulneráveis à ocorrência de incidentes de segurança, possibilitando a perda de confidencialidade, integridade e disponibilidade da informação.

Palavras-chave: práticas de segurança da informação; segurança da informação; tecnologia da informação.

Abstract

The public and private organizations have been demonstrating a lack of company´s information protection. By tradition, they give more attention to the security of patrimonial and financial goods.

In this research were investigated the information security practices implemented in two organizations of the state of Bahia-Brazil, if they were adherent to security existenting default and the consequences of not implementing the adequate controls to reduce the present risks in their enviroment.

Bibliographical review about the theme and cases studies were made in two organizations of the state of Bahia-Brazil. It can be perceived the lack of management of information security. In these organizations there are only some isolated security measures implemented. The conclusion drawn is that in the studied orgaizations, the information security practices not frequently are adopted to reduce present risks in their enviroment. This let them to be more vulnerable to occur security breaches, facilitating loss of confidenciality, integrity and availability of information.

Keywords: information security practices; information security; information technology.

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

ABNT – Associação Brasileira de Normas Técnicas

BS – British Standard

BSI – British Standard Institution

COBIT – Control Objectives for Information and Related Technology

EDI – Eletronic Data Interchange

E-Mail – Eletronic Mail

ISACA - Information System Audit and Control Association

ITIL - Information Technology Infrastructure Library

NBR – Norma Brasileira

NIST - National Institute of Standards and Technology

ISO – International Organization for Standardization

IEC – International Electro-technical Commission

PDCA – Plan-Do-Check-Act

TI – Tecnologia da Informação

Sumário

1. Introdução

Ao longo dos anos, os seres humanos sempre procuraram ter o controle das informações. As formas de registro e armazenamento passaram por grandes evoluções. No início dos tempos, os registros eram feitos em paredes e o armazenamento era feito na memória humana. Depois de muitos anos, passaram a ser feitos em papel (CARUSO & STEFFEN, 1999).

O mundo moderno exigiu das empresas agilidade e eficiência nos negócios para que elas continuassem em um mercado cada vez mais competitivo. Por este motivo, elas começaram a realizar investimentos tecnológicos e computacionais que facilitavam a obtenção de resultados mais precisos e em menor tempo. Neste período, os registros feitos em papel foram gradativamente substituídos por registros em meios digitais.

Com o crescimento da utilização de computadores e das redes, em especial a Internet, permitindo o compartilhamento de dados e a comunicação entre pessoas de qualquer parte do mundo, aumentou o fluxo de informações, e estas passaram a ser percebidas como um bem valioso e ao mesmo tempo vulnerável nas empresas. Junto com esta facilidade de comunicação, surgiram também novas ameaças como vírus de computador e *hackers* a sistemas, gerando a preocupação com segurança dos ativos de informação. Segundo a norma ISO/IEC 17799-1:2001, são considerados ativos de informação: base de dados, arquivos, documentação de sistema, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação e informações armazenadas.

A informação é um recurso essencial para as empresas e, por isso, os gestores estão cada vez mais preocupados com as conseqüências que teriam para a sua competitividade, em caso de incidentes que causassem danos a seus sistemas de informação, deixando vulneráveis um dos três princípios básicos da segurança da informação: confidencialidade, integridade e disponibilidade.

A ameaça do uso incorreto das informações e possível fraude, compromete a confiança de clientes e fornecedores, além da imagem da organização.

Diante de um cenário de dependência perante sistemas informatizados e de maior exposição das informações empresariais, a necessidade de proteger estas informações contra qualquer tipo de uso indevido passou a ser um requisito indispensável ao ambiente corporativo, independente da sua natureza e porte. Para que os princípios básicos da segurança da informação não fossem comprometidos, as organizações começaram a definir mecanismos a fim de avaliar e minimizar as vulnerabilidades.

No Reino Unido, foi feita uma pesquisa pelo Departamento de Indústria e Comércio em 2002 com mil organizações e o resultado divulgado informou que o número de negócios que sofreram incidentes de segurança da informação intencionais, como por exemplo, vírus, acesso não autorizado e fraude, aumentou de 18% em 1998 para 78% em 2002. Outro dado relevante desta pesquisa foi referente ao custo aproximado do pior incidente ocorrido, incluindo perda de negócios e custo do tempo da equipe para restabelecer a normalidade da situação. A maioria das organizações teve pequenos custos, algumas chegaram a ter prejuízos de pouco menos de dez mil libras esterlinas.

No Brasil, a nona pesquisa de segurança da informação realizada pela Módulo Security Solutions (2003) também mostra que empresas de diversos setores estão se preocupando mais com a proteção de suas informações e como conseqüência, adotando controles de segurança, em função de problemas ocorridos anteriormente. Em entrevistas realizadas em diversas empresas, totalizando 682 questionários, concluiu-se que 77% delas já sofreram ataques e invasões aos sistemas e 35% tiveram perdas financeiras. 60% dos profissionais entrevistados informaram que suas empresas pretendiam aumentar os investimentos em segurança em 2003.

Aparentemente, a preocupação com a segurança da informação e a continuidade dos negócios aumentou após o atentado ao *World Trade Center* (WTC) e do Pentágono em setembro de 2001, quando algumas empresas perderam além de seus funcionários, bens patrimoniais e informações sobre seus negócios. Poucas delas conseguiram recuperar essas informações (PEIXOTO, 2004).

Criada pela ABNT (Associação Brasileira de Normas Técnicas), a norma NBR ISO/IEC 17799 – Tecnologia da informação – código de prática para a gestão da segurança da informação, versão brasileira da norma BS7799-1, foi publicada com o objetivo de assegurar a continuidade dos negócios e minimizar o risco de incidentes de segurança, através da implementação e avaliação de práticas de gestão da segurança da informação. Vale ressaltar que a norma trata não só de aspectos técnicos de processamento e tecnologia da informação, mas também de todos os aspectos que envolvem a segurança da informação, como por exemplo, ambiente computacional, treinamento em segurança e conformidade legal.

Observa-se que esta norma passou a ser utilizada em empresas de diversos países como diretriz para implementação da segurança da informação, por ser considerada aquela que reúne as melhores práticas nesta área.

A relevância da presente pesquisa está na própria natureza do estudo, já que contribui para o aumento do nível de consciência das organizações a respeito da crescente importância da segurança da informação e investigar as práticas de segurança implementadas nas empresas é um desafio, pois normalmente este é um assunto sigiloso, portanto, de acesso restrito, pois expõe as vulnerabilidades da organização.

Diante do cenário de dependência das empresas com relação aos recursos tecnológicos e do crescente número de ocorrência de incidentes de segurança da informação, o presente trabalho tem como ponto de partida duas perguntas:

- As práticas de segurança da informação implementadas nas organizações que atuam no Estado da Bahia vêm atendendo às necessidades de segurança?
- Quais as conseqüências da não implementação de práticas adequadas para a redução dos riscos presentes em seu ambiente?

Pretende-se responder essas questões através da realização de estudos de caso em duas organizações baianas.

O objetivo geral deste trabalho é analisar as práticas de segurança da informação implementadas em organizações que atuam no Estado da Bahia, com

vistas a verificar em que medida estas são aderentes aos padrões de segurança existentes e as conseqüências da não implementação de controles adequados para a redução dos riscos presentes em seu ambiente.

Os objetivos específicos são:

- Descrever as práticas de segurança da informação implementadas nas organizações;
- Confrontar as necessidades de segurança existentes nas organizações estudadas com as práticas implementadas, a fim de analisar a gestão da segurança da informação;
- Identificar as razões da não implementação de algumas práticas de segurança recomendadas;
- Analisar quais as conseqüências da não implementação de controles adequados para a redução dos riscos presentes em seu ambiente.

Para realização da investigação empírica, foram consideradas as seguintes hipóteses:

- As práticas de segurança implementadas não vêm atendendo a todas as necessidades de segurança, o que vem ocasionando perdas de informação e financeiras, quebra de confidencialidade, integridade e disponibilidade da informação, possibilitando gerar uma imagem negativa para a organização;

- A não implementação de todas as práticas de segurança recomendadas ocorre em função da falta de consciência dos riscos envolvidos e da falta de recursos financeiros.

Este trabalho está estruturado em capítulos distribuídos da seguinte forma: capítulo 2 – Referencial teórico, cujo conteúdo foi formulado a partir da revisão da literatura sobre a segurança da informação, capítulo 3 – Estudos de caso, apresentando a metodologia de pesquisa e analisando o objeto de estudo em duas organizações baianas e capítulo 4 – Considerações finais.

2. Fundamentação Teórica

2.1 Informação e uso da TI

A informação e seu uso permeiam todos os aspectos da sociedade moderna (NIEKERK e SOLMS, 2004).

Rezende e Abreu (2000) definem informação como todo o dado trabalhado, útil, tratado, com valor significativo atribuído a ele. O dado é o elemento da informação, que isoladamente não transmite nenhum conhecimento.

> A informação nos dias de hoje tem um valor altamente significativo e pode representar grande poder para quem a possui, seja pessoa, seja instituição. Ela possui seu valor, pois está presente em todas as atividades que envolvem pessoas, processos, sistemas, recursos financeiros, tecnologias etc (REZENDE E ABREU, 2000 p.97).

No atual cenário competitivo, torna-se cada vez mais estratégico o papel que as informações exercem nas empresas (Dhillon, 2001). Informações sobre cliente, produto, serviço e sobre o negócio, circulam pelos diversos setores da empresa, auxiliando funcionários da área operacional e gestores na execução das atividades diárias. Para McGee e Prusak (1994), o sucesso de um gerente está associado à qualidade de suas decisões, que por sua vez, dependem da eficiência no uso das informações, da qualidade e precisão das mesmas.

O ambiente empresarial está se tornando cada vez mais dependente da informação para o gerenciamento de suas atividades, estejam elas no nível operacional, tático ou estratégico. Para Bio (1985), com o crescimento das

empresas, torna-se cada vez mais crítico o recurso da informação. A informação é a base e o resultado da ação executiva. Para Greewood, *apud* Cautela e Polloni (1982), a informação é a base da qual dependem todos os processos de decisão.

Uma forma de verificar o valor da informação para uma empresa é analisar o custo de não tê-la disponível e quanto isso pode representar de perda para a mesma.

Com o aumento do volume de negócios, surgiu a necessidade de buscar soluções que melhorassem o tratamento e a disponibilidade da informação e uma infra-estrutura tecnológica que suportasse o gerenciamento da mesma.

A influência dos sistemas de informação pode ser vista na maioria das áreas operacionais e gerenciais das empresas. As organizações têm se tornado cada vez mais dependentes da disponibilidade dos sistemas (DHILLON, 2001).

Segundo Prahalad e Hamel *apud* Rezende e Abreu (2000), existe uma crescente interdependência entre estratégias e procedimentos empresariais e sistemas de informação gerencial e telecomunicação, afetando produtos, mercados, fornecedores e clientes. Os sistemas de informação efetuam o processamento de dados em vários setores na empresa, agilizando o fluxo das informações, tornando a sua transmissão mais eficiente, controlando melhor as rotinas, a gestão das operações e melhorando o suporte a tomada de decisão.

Para a ABNT (2001), o compartilhamento de informações aumentou a necessidade de implantar controles para garantir a segurança das mesmas. A informação é um recurso que tem um valor para a organização e por isso, precisa ser protegida. Ela pode ser apresentada de várias formas: impressa em papel, armazenada eletronicamente, transmitida por correio ou por meios eletrônicos,

exibida em filmes ou falada durante uma conversação. Este ponto é enfatizado por Pinheiro.

> Informação é tradicionalmente relacionada a documentos impressos e a bibliotecas, quando de fato a informação de que trata a Ciência da Informação, tanto pode estar num diálogo entre cientistas, em comunicação informal, numa inovação para indústria, em patente, numa fotografia ou objeto, no registro magnético de uma base de dados ou em biblioteca virtual ou repositório, na Internet (PINHEIRO, 2004).

Como a nova conjuntura exige mudanças rápidas e informações precisas, o uso da Tecnologia da Informação (TI) é fator crítico de sucesso para a empresa se manter em um mercado tão competitivo.

A Tecnologia da Informação é definida como conjunto de recursos tecnológicos e computacionais para geração e uso da informação (REZENDE E ABREU, 2000).

A valorização das informações que circulam nas empresas refletiu no crescimento de investimentos e uso da Tecnologia da Informação. Inicialmente, a tecnologia era usada somente para otimizar os processos operacionais, mas pouco a pouco ela passou a contribuir em todos os processos empresariais. Atualmente, é difícil imaginar a quantidade de serviços e negócios que dependem da presença da TI para se viabilizarem.

A Tecnologia da Informação desempenha um papel estratégico promovendo vantagem competitiva. Ela precisa estar alinhada ao planejamento empresarial (REZENDE E ABREU, 2000).

A utilização da Tecnologia da Informação nas organizações proporciona o aumento da capacidade de tratamento de informações, rapidez na obtenção das mesmas, confiabilidade dos resultados e maior controle sobre a organização. Os efeitos da disseminação da TI permitem que a empresa atue de forma integrada e facilita a comunicação entre corporação, fornecedores e clientes (GRAEML, 2000).

A administração da Tecnologia da Informação permite que processos e recursos de TI sejam direcionados para facilitar o acesso a informações empresariais.

O conceito de governança de TI envolve a forma como a empresa estrutura e organiza o conjunto de processos de direção, de gestão, de controle e administrativos para oferecer bens e serviços ao mercado, de acordo com as estratégias traçadas e com os posicionamentos e escopos definidos para cada um dos produtos ofertados (FERNANDES, 2003). Seu objetivo é a obtenção de melhorias mensuráveis nos processos da empresa, já que ela é baseada em indicadores quantitativos e qualitativos, permitindo direcionar ações para alcançar os objetivos organizacionais. A excelência operacional e o efetivo alinhamento entre TI e negócios são os benefícios esperados pela adoção da governança de TI.

O COBIT (*Control Objectives for Information and Related Tecnology*) e o ITIL (*Information Technology Infrastructure Library*) são metodologias criadas com o objetivo de facilitar a implantação da governança de TI.

Em 1998, o *IT Governance Institute* (ITGI), fundado pela *Information System Audit and Control Association* (ISACA), desenvolveu um guia de governança de TI com intuito de aumentar a consciência dos benefícios de controles efetivos de

tecnologia da informação. O COBIT integra as melhores práticas de planejamento e organização, aquisição e implementação, entrega e suporte, e monitoramento do desempenho da Tecnologia da Informação para garantir que as informações essenciais para a empresa e a tecnologia utilizada na mesma suportem os objetivos de negócio (COBIT STEERING COMMITTEE e IT GOVERNANCE INSTITUTE, 2000). Através do COBIT, é possível perceber, de forma clara, a contribuição das estratégias de TI para as estratégias de negócio.

O ITIL foi desenvolvido no final da década de 80 pelo órgão do comércio britânico, com objetivo de gerenciar serviços de Tecnologia da Informação na central de governo do Reino Unido. Ele aborda as melhores práticas de gestão de infra-estrutura de TI (hardware, software, procedimentos, comunicação relacionada com computadores, documentação e habilidades necessárias para dar suporte a serviços de TI) (PINK ELEPHANT, 2004).

Metodologias para governança em Tecnologia da Informação como o COBIT e o ITIL adotam medidas para organizar e proteger as informações empresariais, além de direcionar os investimentos tecnológicos em benefício do negócio. Uma empresa baseada em métodos modernos de gestão também precisa acompanhar a evolução das necessidades de segurança das informações.

2.2. Definição de segurança da informação

A definição de segurança relatada no guia do *Information Security Governance* está relacionada à proteção do ativo de valor contra perda, uso indevido, falta de confidencialidade ou dano. Nesse contexto, ativos de valor são as informações

gravadas, processadas, armazenadas, compartilhadas e transmitidas ou acessadas de uma mídia eletrônica (ITGI, 2003).

A segurança da informação é caracterizada pela preservação da confidencialidade, integridade e disponibilidade (ABNT, 2001; COBIT STEERING COMMITTEE e IT GOVERNANCE INSTITUTE, 2000; CZEMIER, OVERBEEK e PETERS, 1999). Entende-se por confidencialidade a garantia de que a informação só será acessível a pessoas autorizadas. A integridade, está relacionada à "exatidão" e "completeza" da informação. A disponibilidade é a garantia de que os usuários autorizados terão acesso a informação e aos ativos correspondentes sempre que necessário.

Há um consenso entre os autores ao relatar a importância da proteção da informação nas organizações. Qualquer ocorrência de falha pode causar impacto na performance das mesmas e no valor de seus produtos no mercado (CZEMIER, OVERBEEK e PETERS, 1999; CARUSO & STEFFEN, 1999; PELTIER, 2001).

O *National Institute of Standards and Technology (*NIST*)* menciona, além desses, outros componentes que caracterizam a segurança da informação como a autenticidade, relacionado com a fidedignidade da fonte das informações e o não repúdio que visa assegurar que os remetentes não possam negar ter emitido a informação e os receptores não podem negar ter recebido, como componentes importantes na proteção da informação (NIST, 1995).

Dhillon e Backhouse *apud* Dhillon (2001) argumenta que princípios tradicionais da segurança da informação como confidencialidade, integridade e disponibilidade, são restritos. Princípios como responsabilidade, integridade, confiança e ética devem ser usados em resposta a um contexto de mudanças

organizacionais. Estes, estão ligados aos profissionais que vão manusear a informação. O sigilo das informações depende muito das pessoas que as utilizam.

2.3. Padrões e metodologias que abordam a segurança da informação

O início do processo oficial de criação de regras para segurança de computadores ocorreu em outubro 1967, quando foi criada uma "força tarefa", que gerou o documento chamado "*Security Control for Computer System: Report of Defense Science Boad Task Force on Computer Security*". Em 1977, o Departamento de Defesa dos Estados Unidos (DoD) formulou um plano para tratar dos problemas de segurança. A partir disso, surgiu o "*DoD Computer Security Initiative*" que desenvolveu um centro para avaliar a segurança das soluções disponibilizadas. Para que esta avaliação fosse feita, precisava-se definir regras e o conjunto destas, gerou o manual de segurança conhecido como "The Orange Book". Apesar do processo de desenvolvimento deste manual ter começado em 1978, somente em 1985, foi publicada a versão final deste documento (GONÇALVES, 2003). Este foi o marco inicial para elaboração de normas que permitem que um ambiente possa ser considerado seguro. Atualmente, o "*The Orange Book*" é considerado pelo mercado, um documento ultrapassado.

Solms *apud* Casanas e Machado (2002), relatam que em 1987, o Departamento de Comércio e Indústria do Reino Unido (DTI) criou um centro de segurança de informações, o CCSC (*Commercial Computer Security Centre*) que entre suas atribuições, deveria criar uma norma de segurança da informação para companhias britânicas que comercializavam produtos para segurança de

Tecnologia da Informação. Além deste objetivo, o CCSC deveria criar um código de segurança para os usuários das informações. A partir deste objetivo, foram feitas algumas publicações até surgir a norma BS7799-1:1999. Em 1998, a lei britânica, denominada 'Ato de Proteção de Dados', recomendou a aplicação da norma na Inglaterra, o que viria a ser efetivado em 01 de março de 2000.

Criada pela ABNT, a norma NBR ISO/IEC 17799-1 é a versão brasileira da norma BS7799-1. Ela aborda 10 áreas de controle da segurança da informação que podem ser vistas na figura abaixo (ABNT, 2001).

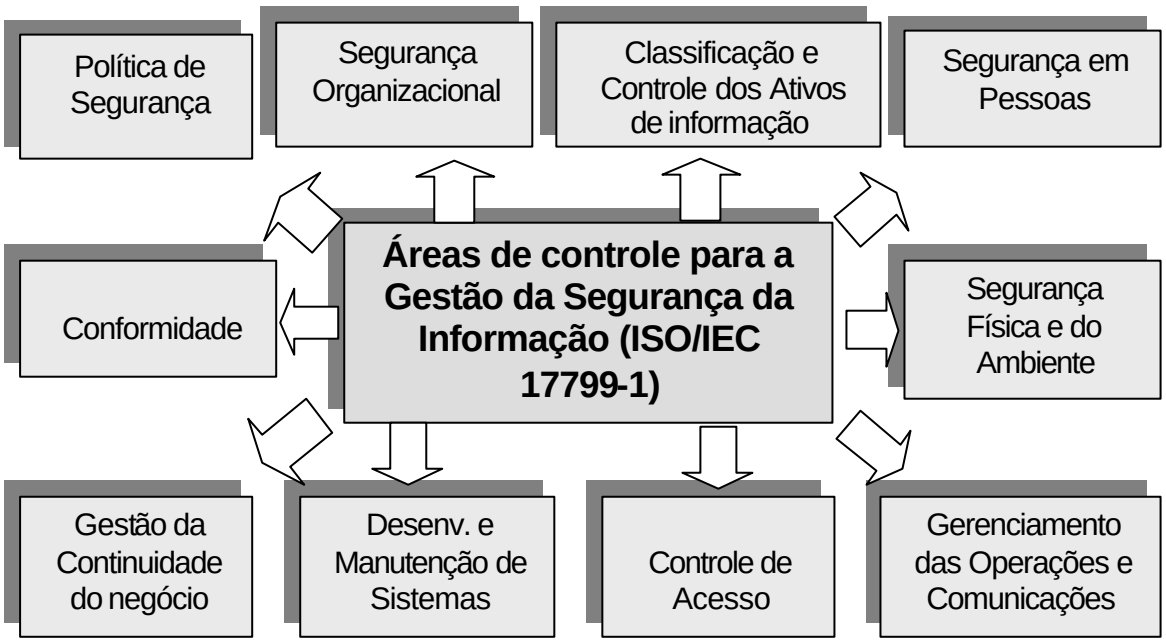

Figura 1: Áreas de controle da gestão da segurança da informação. Fonte: Código de prática para a gestão da segurança da informação – norma NBR ISO/IEC 17799-1:2001.

O NIST (1996), agência vinculada ao Departamento de Comércio Americano, recomenda controles de segurança para os sistemas de informação federal divididos nas seguintes áreas:

Figura 2: Áreas de controle da segurança da informação. Fonte: Adaptação das áreas de controle do NIST (1996).

Para Czemier, Overbeek e Peters (1999), a gestão de TI e a segurança da informação são inseparáveis.

O modelo de segurança da informação do ITIL sob a perspectiva do negócio é apresentado na figura abaixo.

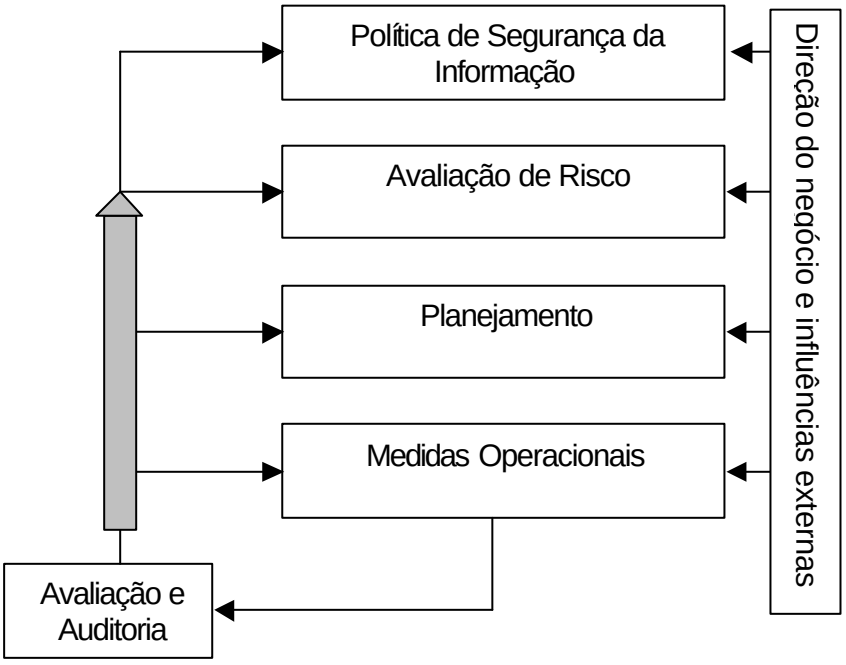

Figura 3: Modelo de segurança da informação Fonte: Czemier, Overbeek e Peters (1999).

Segundo Czemier, Overbeek e Peters (1999), os objetivos do gerenciamento de segurança são :

- Atender às necessidades externas de segurança, como por exemplo, contratos, legislação e qualquer política de segurança de outra organização que tenha que ser seguida pela empresa.
- Atender as necessidades internas de segurança, a fim de garantir a continuidade dos serviços de TI.

O documento do COBIT Steering Committee e IT Governance Institute (2000), estabelece controles para melhoria da proteção dos recursos de TI. Segundo esta metodologia, a segurança da Tecnologia da Informação precisa ser gerenciada através de medidas que estejam alinhadas as necessidades do negócio.

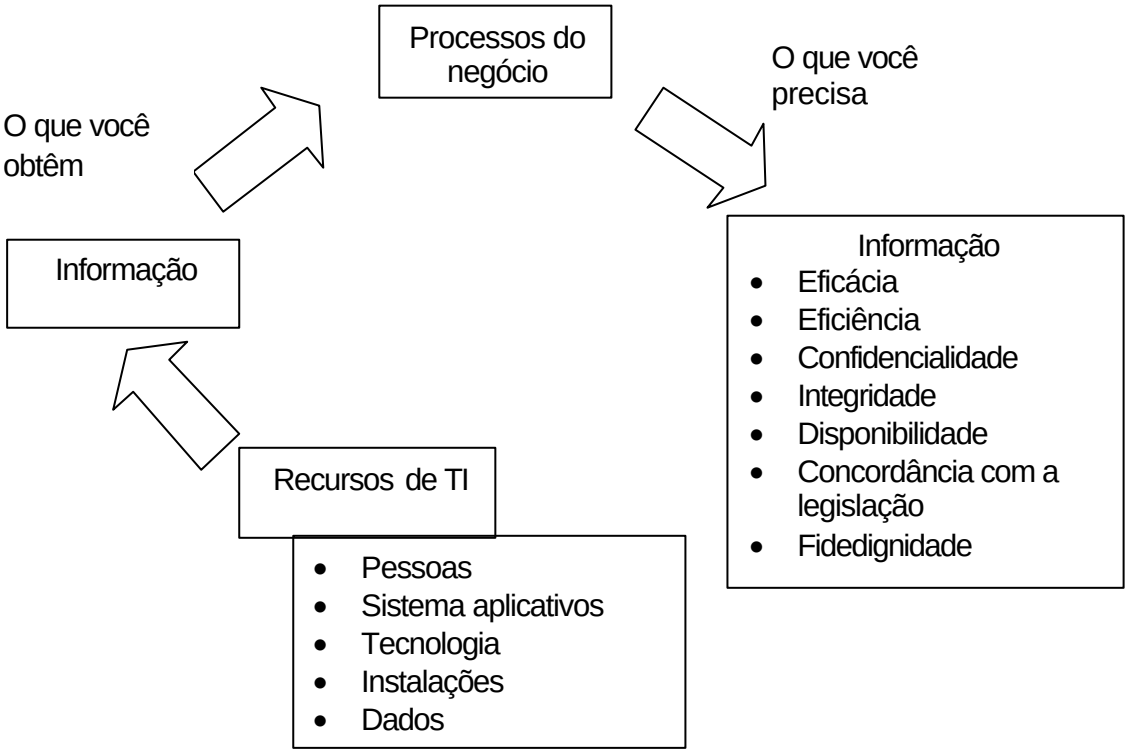

Figura 4: Objetivos de controle de TI. Fonte: COBIT Steering Committee e IT Governance Institute (2000)

Diversos processos do ITIL e do COBIT se referem às práticas de segurança da informação, e estas são baseadas na norma ISO/IEC 17799, por ser adotada como referencial das melhores práticas de segurança da informação (COBIT STEERING COMMITTEE e IT GOVERNANCE INSTITUTE, 2000; CZEMIER, OVERBEEK e PETERS, 1999).

2.4. Gestão da Segurança da Informação

A gestão pode ser definida como um ato de gerenciar uma empresa ou uma unidade departamental. Ela envolve recursos humanos, atividades e funções e outros recursos pertinentes (REZENDE E ABREU, 2000). Como um subconjunto deste conceito, a gestão da segurança da informação envolve o gerenciamento da implementação de políticas e práticas de segurança, alinhadas às necessidades e estratégias do negócio.

> Segurança, mais do que estrutura hierárquica, homens e equipamentos, envolve uma postura gerencial, o que ultrapassa a tradicional abordagem da maioria das empresas (CARUSO & STEFFEN, 1999, p. 24).

Os principais benefícios da gestão da segurança da informação são:

- Identificação de medidas necessárias para proteção das informações, possibilitando a priorização das ações;
- Realização de planejamento e desenvolvimento de um documento contendo uma política de segurança;

- Definição de prazos e orçamentos para implementação da segurança na organização.

> O modelo e implementação do sistema de segurança da informação de uma empresa são influenciados por necessidades e objetivos do negócio, resultando em requisitos de segurança, pelo processo empregado e o tamanho e estrutura da organização (BSI, 2002) [tradução nossa].

O modelo adotado pela norma BS 7799-2:2002 é conhecido por PDCA (*Plan-Do-Check-Act* ou planejar-executar-verificar-agir).

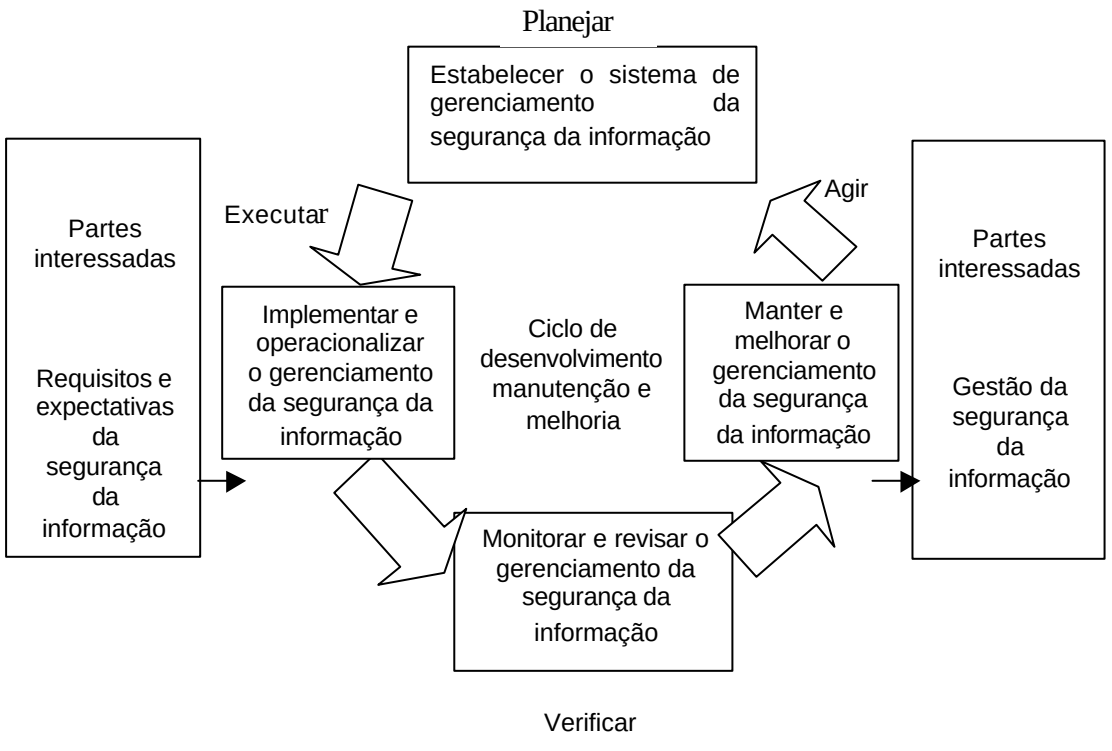

Figura 5: Modelo PDCA aplicado ao processo do sistema de gerenciamento da segurança da informação. Fonte: BSI (2002).

O conceito do ciclo PDCA foi originalmente desenvolvido por Walter Shewhart durante a década de 30. Ele era referenciado como ciclo de Shewhart. O PDCA foi amplamente divulgado a partir de 1950 por W. Edwards Deming através do gerenciamento de qualidade (HCI, 2004).

Na fase de planejamento são estabelecidos políticas, objetivos, processos e procedimentos relevantes para controlar riscos e melhorar a segurança da informação. A segunda fase está relacionada com a implementação e operacionalização da política de segurança, controles, processos e procedimentos. Na fase seguinte, são feitas as verificações, e quando aplicável, avaliação da performance com relação à política. Na última fase são tomadas ações corretivas e preventivas para alcançar uma melhoria contínua do sistema de gerenciamento da segurança da informação (BSI, 2002).

Não há um modelo engessado para a gestão da segurança da informação. As informações organizacionais devem ser protegidas partindo da análise do grau de importância da informação para a organização e da necessidade e viabilidade do investimento no projeto de segurança.

2.4.1. Planejamento

2.4.1.1. Avaliação de Risco

A base para a elaboração do planejamento da segurança da informação em uma empresa é a avaliação dos riscos presentes em seu ambiente (BERNSTEIN, BHIMANI, SCHULTZ E SIEGEL, 1996).

A avaliação de risco, processo de interpretar e analisar o risco, é composta de três atividades: determinar o escopo e metodologia, coletar e analisar informações e interpretar o resultado da analise dos riscos (NIST, 1995). Ela pode ser aplicada em toda a organização ou apenas em uma parte dela.

É necessário verificar o nível de exposição ao perigo e determinar qual é o limite aceitável, ou seja, que riscos as empresas estão dispostas a conviver para minimizar suas perdas e conseqüentemente, não prejudicar os seus negócios (COBIT STEERING COMMITTEE e IT GOVERNANCE INSTITUTE, 2000).

Os riscos relacionados à segurança da informação são traduzidos pelos gerentes em perdas financeiras, de negócios, de dados, redução de produtividade e divulgação de segredos corporativos (STEFANEK, 2002).

O risco é a possibilidade de alguma coisa adversa acontecer. Para avaliar os riscos, deve ser analisado: ativos, ameaças, vulnerabilidades, salvaguardas, conseqüências e probabilidades (NIST, 1995). Ameaças são causas potencias de incidentes que podem resultar em danos para os ativos da organização. A vulnerabilidade é quando um ativo está suscetível a um ataque.

Para o BSI (2002), a avaliação de risco envolve a conseqüência que uma falha de segurança vai gerar para a empresa e a probabilidade de ocorrência da mesma.

Podem ocorrer problemas de segurança da informação intencionais, como por exemplo, ataques de *hackers*, não intencionais, como erros humanos ou de *hardware*, e desastres da natureza, como inundações e incêndios.

Em uma organização podem existir ameaças que exploram vulnerabilidades dos sistemas ou serviços de TI usados pela a organização e estas podem causar algum dano ao ativo (BSI, 2002).

As conseqüências dos incidentes de segurança são medidas de acordo com o valor das informações para as organizações.

Cada risco tem um grau de criticidade de acordo com a importância da informação para a empresa. A tabela abaixo é uma adaptação dos níveis de risco apresentados por Caruso & Steffen (1999).

Tabela1: Níveis de risco

Grau de Criticidade	Riscos
0	Alto risco, pode levar a paralisação das atividades da empresa.
1	Médio risco, pode gerar uma dificuldade na execução das atividades da empresa.
2	Baixo risco, não prejudica o andamento das atividades da empresa.

Fonte: Adaptação Caruso & Steffen (1999).

STEFANEK (2002) argumenta que uma avaliação de risco deve ser realizada construindo uma matriz de conseqüência versus probabilidade.

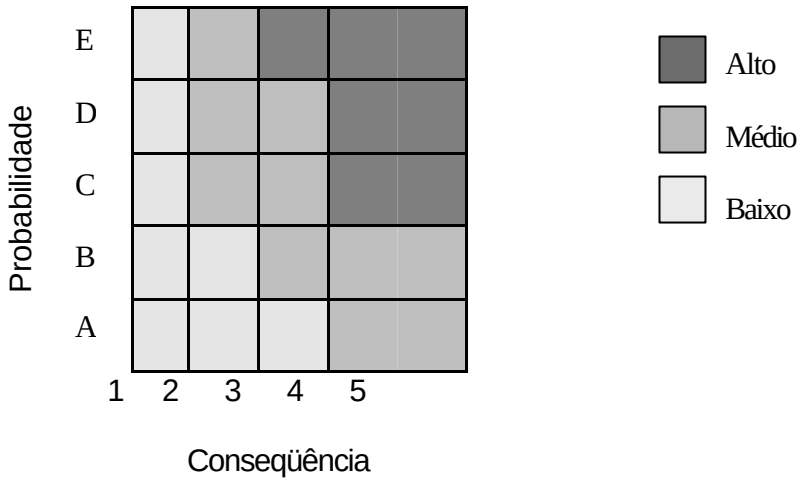

Figura 6: Matriz de classificação de risco. Fonte: Stefanek (2002).

A partir da avaliação de risco, pode-se ter um referencial para a implementação de ações de segurança, já que através dela, é possível estabelecer o tratamento apropriado para o risco (BSI, 2002). Além disso, pode-se definir os investimentos a serem realizados, pois será possível conhecer os recursos que precisam de proteção, que riscos eles estão expostos e que medidas devem ser adotadas para minimizá-los.

Quase sempre em organizações comerciais, a idéia de realização de uma avaliação de risco formal é rejeitada. Isso ocorre devido ao seu alto custo (WONG e WATT, 1990).

A avaliação de risco está presente na literatura de referencial da área. Ela precisa ser revista constantemente porque computadores e os ambientes em que

eles atuam são dinâmicos, e portanto, novas ameaças e vulnerabilidades podem surgir (SWANSON e GUTTMAN, 1996).

2.4.1.2. Política de segurança

Uma política de segurança é definida como uma declaração de crenças, metas e objetivos, e condições gerais para alcançá-las com relação à proteção dos ativos organizacionais (PELTIER, 2001). Para o NIST (1995), a política de segurança é a documentação das decisões sobre a segurança referente aos computadores. Na visão de Steinke *apud* Dhillon (2001) cada empresa precisa definir sua política de acordo com o valor da informação a ser protegida e através de uma análise das possíveis conseqüências que podem ocorrer quando houver algum dano, modificação ou exposição de informações relevantes ao negócio.

Segundo COUTANCHE (2001), as informações precisam ser protegidas por controles construídos a partir de uma política de segurança.

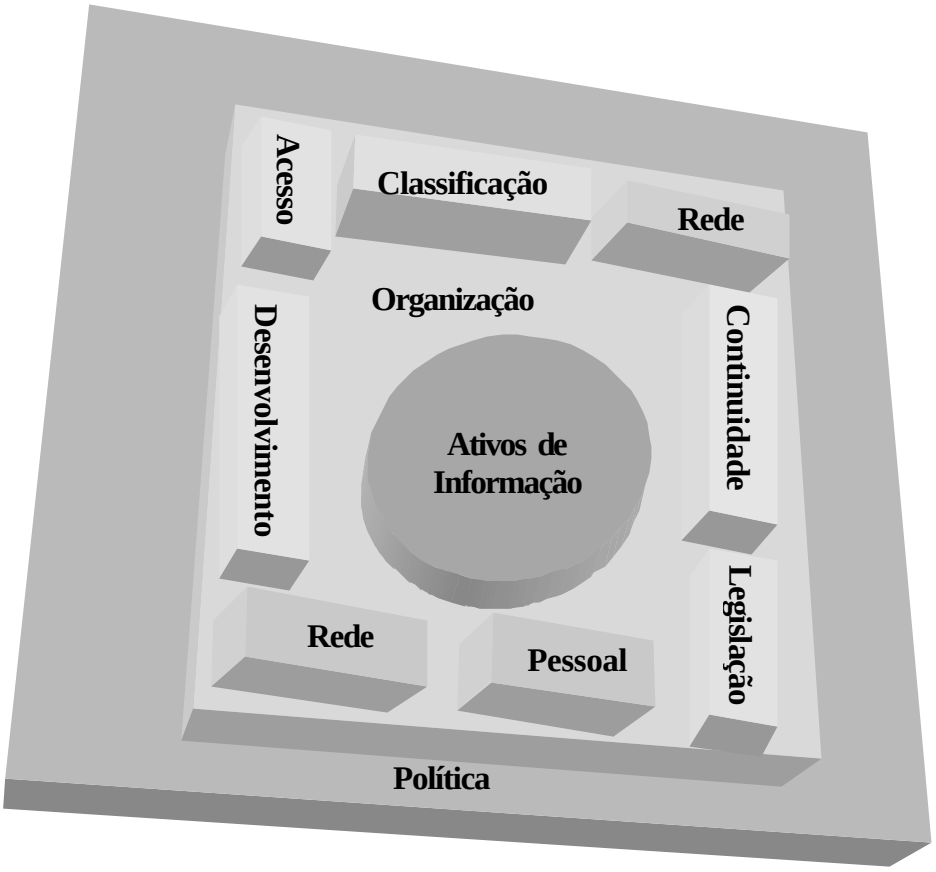

Figura 7: Componentes da política de segurança Fonte: Coutanche (2001)

Os componentes básicos de uma política de segurança são: seu propósito, escopo, requisitos de conformidade legal e definição das responsabilidades de segurança. Procedimentos, padrões e guias são usados para descrever como as políticas serão implementadas na empresa (NIST, 1995).

Uma política de segurança é um dos principais documentos da gestão da segurança. Ela precisa ser de fácil compreensão, coerente com ações da empresa, aprovada pela direção da empresa e divulgada entre todos os funcionários, a fim de orientar e conscientizar sobre a segurança na organização. Além disso, ela precisa ter um gestor que seja responsável pela sua manutenção e revisão periódica, visando a melhoria contínua (DHILLON, 2001).

A falta de uma política de segurança e de um documento guia é uma das maiores vulnerabilidades de segurança na maioria das empresas (STEFANEK, 2002).

Segundo pesquisa nacional realizada pela Módulo Security Solutions (2003), houve um crescimento de empresas que possuem uma política de segurança formalizada de 2002 para 2003.

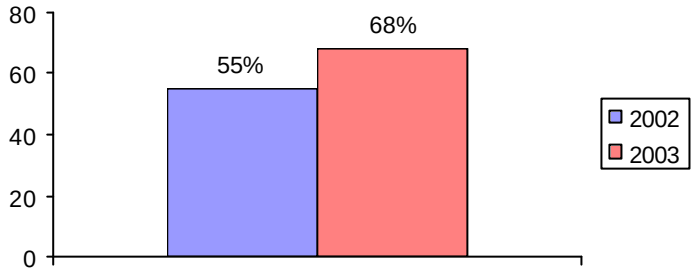

Figura 8: Política de segurança formalizada. Fonte: Módulo Security Solutions, 2003

2.4.2. Execução

Apesar de alguns autores apresentarem modelos de gestão da segurança da informação com estruturas diferentes, existem algumas práticas de segurança em comum.

Os principais fatores que compõem a segurança de informática segundo LEES *apud* CARUSO & STEFFEN (1999) é apresentada na figura abaixo:

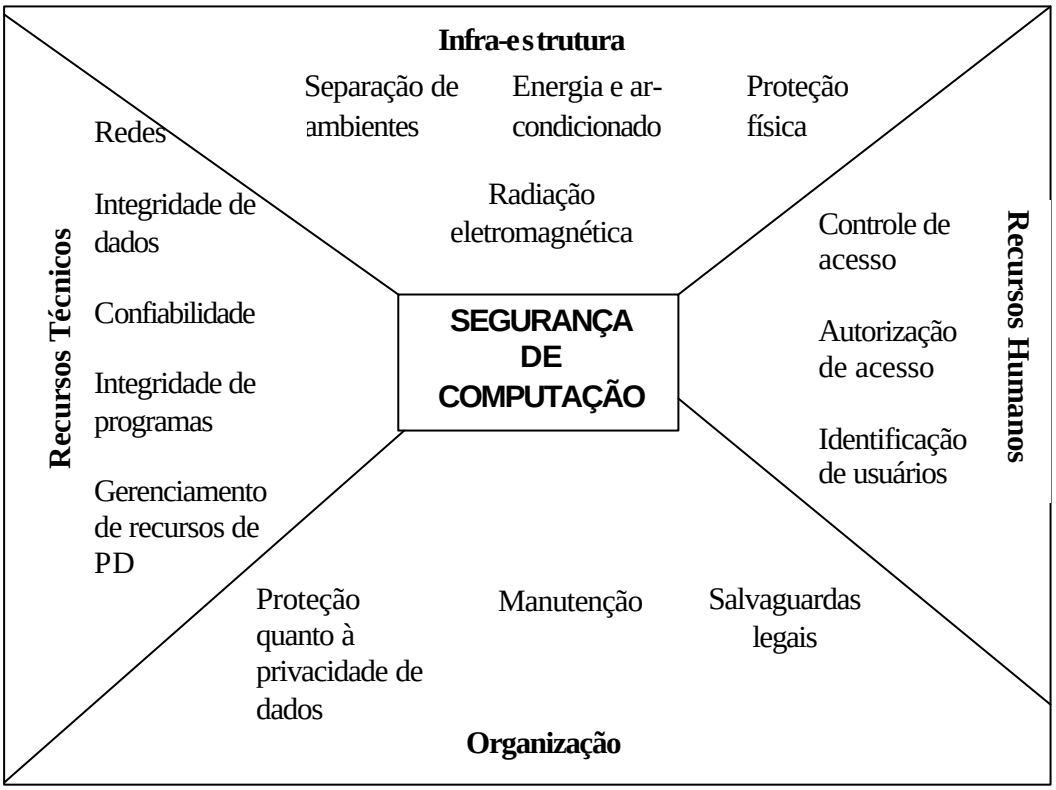

Figura 9: Os fatores principais na segurança de informática Fonte: Caruso & Steffen (1999)

Na visão de WONG E WATT (1990), a estrutura de segurança compreende os seguintes aspectos: controles organizacionais e de centro de processamento, gerenciamento da rede, segurança de acesso, controles operacionais e aplicação, segurança de mensagem, confidencialidade de dados, responsabilidade e custódia do usuário final, obrigações e questões legais.

A norma ISO/IEC 17799:2000 trata de forma integrada os aspectos relacionados à Tecnologia da informação, pessoas, políticas e conformidades, a fim de garantir a continuidade de TI.

Para maior detalhamento das práticas de segurança, objeto da gestão da segurança da informação, será utilizada a abordagem mais amplamente adotada, a da norma ISO/IEC 17799-1, a seguir.

2.4.2.1. Segurança Organizacional

Como a segurança da informação é algo que abrange toda a empresa, é muito importante que haja uma estrutura de gerenciamento para implantar e controlar a segurança. Para essa estrutura, recomenda-se que seja formado um fórum de segurança da informação para analisar e aprovar a política de segurança e responsabilidades envolvidas, monitorar mudanças na exposição dos ativos das informações às principais ameaças, analisar e monitorar incidentes de segurança e aprovar iniciativas para incrementar o nível de segurança (ABNT, 2001; CZEMIER, OVERBEEK e PETERS, 1999).

Todos os novos recursos de processamento da informação, sejam eles de *hardware* ou *software*, devem ter uma autorização para instalação e uso por parte da administração de usuários e do gestor responsável pela segurança da informação para garantir que estes atendam os requisitos de segurança estabelecidos pela empresa (ABNT, 2001).

Os recursos de processamento de informação e ativos de informação organizacionais acessados por prestadores de serviço devem ser analisados, a fim de identificar possíveis implicações na segurança dos mesmos. Devem ser considerados os acessos físico e lógico (ABNT, 2001).

O acesso de prestadores de serviço aos recursos organizacionais deve ser baseado em contratos formais que estejam de acordo com os requisitos de segurança estabelecidos pela empresa. Quando o processamento da informação é terceirizado, é necessário um contrato entre as partes para deixar claro as suas responsabilidades de segurança (ABNT, 2001; CZEMIER, OVERBEEK e PETERS, 1999).

2.4.2.2. Classificação e Controle dos Ativos de Informação

O processo de classificação da informação é uma decisão gerencial. São os gestores quem determinam o valor da informação para seu negócio (PELTIER, 2001).

Todos os principais ativos de informação precisam ser inventariados e cada um deles deve ter um proprietário responsável, atribuindo a ele a tarefa de manutenção de controles. Identificando seus ativos e seus respectivos valores e importância para a empresa, pode-se determinar o grau de proteção adequada para cada um deles (ABNT, 2001; COBIT STEERING COMMITTEE e IT GOVERNANCE INSTITUTE, 2000).

Os ativos associados a sistemas de informação podem ser de informação, como base de dados e arquivos, de *software*, físicos, como equipamentos computacionais, de comunicação e mídia magnética, e de serviços (ABNT, 2001).

Para determinar a importância e sensibilidade da informação para o negócio, e o nível de proteção que deverá ser destinado a cada ativo de informação, é necessário que ele seja classificado (CARUSO & STEFFEN, 1999). Esta

responsabilidade cabe ao proprietário da informação. A tabela abaixo é uma adaptação de classificação de informações quanto à proteção contra revelação, apresentada por Caruso & Steffen (1999).

Tabela 2: Classificação de informações

Classificação de informações	Definição
Crítico ou sensível	Refere-se a uma informação muito importante tecnicamente ou financeiramente para a organização.
Uso restrito	Informação referente ao negócio, destinada apenas ao uso de pessoas autorizadas.
Público	Informação que qualquer pessoa pode acessar.

Fonte: Adaptação Caruso & Steffen (1999).

Sob a ótica de Peltier (2001), existem quatro aspectos principais para classificação da informação: classificação sob o ponto de vista legal, responsabilidade pelo cuidado e controle da informação, integridade da informação e a criticidade da informação e dos sistemas de processamento da mesma.

2.4.2.3. Segurança em pessoas

Um dos principais problemas envolvendo a segurança do ambiente corporativo é o fator humano. Grande parte dos incidentes ocorre devido a pouca

preocupação com a interação dos usuários com os diversos ambientes e sistemas da empresa. Isso aumenta os riscos relacionados a segurança, podendo gerar perda financeira, de dados, indisponibilidade dos sistemas e impacto negativo para a imagem da organização (STEFANEK, 2002).

Um bom começo para estabelecer a segurança é no processo de contratação de pessoal, verificando as referências do futuro funcionário (CIO MAGAZINE, 2002). A norma ISO/IEC 17799-1 e o COBIT Steering Committee e IT Governance Institute (2000) concordam com a afirmação anterior e acrescentam que as responsabilidades de segurança devem ser atribuídas desde a fase de recrutamento, incluídas em contratos, e monitoradas constantemente. No caso de trabalhos que envolvem informações sigilosas, é conveniente que os funcionários e prestadores de serviço assinem acordos de confidencialidade (ABNT, 2001).

Solms *apud* Niekerk e Solms (2004) relatam que estudos recentes demonstram que para uma efetiva segurança da informação é necessário estabelecer uma cultura na empresa.

Segundo a matéria da *CIO Magazine* (2002), na Universidade George Washington, o gerente de informática e o responsável pela segurança da universidade determinaram que a segurança de informações iria fazer parte do código de conduta da mesma e, estudantes, professores e equipe de funcionários teriam que ler e assinar concordando com o mesmo.

Recomenda-se que os usuários sejam treinados para ampliar a consciência da necessidade de proteger os ativos, desenvolver habilidades e conhecimentos para que possam executar seu trabalho de forma mais segura e saber implementar e operar programas de segurança nas empresas (NIST, 1995; COBIT STEERING

COMMITTEE e IT GOVERNANCE INSTITUTE, 2000). Um processo disciplinar formal pode ser aplicado quando as políticas e procedimentos de segurança organizacional forem violados (ABNT, 2001; CZEMIER, OVERBEEK e PETERS, 1999).

Ao ocorrer algum incidente de segurança da informação ou surgir alguma ameaça, é necessário notificar imediatamente aos superiores através de um procedimento formal, junto a um procedimento de resposta ao incidente, definindo a ação a ser tomada ao recebê-lo. Não é aconselhável o funcionário ou prestador de serviço tentar solucionar o problema sozinho ou deixar de notificar o ocorrido ao seu superior, pois esses registros deverão ser analisados para implantações de controles preventivos. Todos os funcionários e prestadores de serviço precisam conhecer esses procedimentos (ABNT, 2001).

Incidente e mau funcionamento de equipamentos ou *softwares*, deve ser quantificado e monitorado para que se estabeleçam melhorias nos controles existentes ou controles adicionais para minimizar a freqüência, danos e custos de ocorrências futuras (CZEMIER, OVERBEEK e PETERS, 1999).

2.4.2.4. Segurança física e do ambiente

Segurança física envolve a limitação de acesso a computadores, dispositivos de rede e instalação elétrica (STEFANEK, 2002).

As áreas de segurança devem ser protegidas por controles de entrada. Esse controle pode ser feito de forma simples, através do reconhecimento das pessoas

que transitam pelo ambiente ou de forma mais sofisticada, através da impressão digital, uso de cartões magnéticos, entre outros.

Alguns sistemas com informações sensíveis necessitam de um dispositivo como a biometria para o processo de autenticação. A biometria usa um atributo físico para provar a identidade do usuário (STEFANEK, 2002).

É recomendado que os recursos e instalações de processamento de informações críticas sejam mantidos em áreas seguras para prevenir não só acessos não autorizados, mas também danos, interferências e exposição das informações.

Para Swanson e Guttman (1996), a seleção da área de segurança deve levar em conta a possibilidade de ocorrência de incêndio, inundação, explosões, roubos, falhas de energia e outras formas de desastres naturais ou causados por seres humanos.

> Um ambiente de informação deve ter sua estrutura de segurança pensada em termos da filosofia de camadas concêntricas de segurança em que cada área é projetada em função do grau de sensibilidade das atividades ali exercidas para a organização (CARUSO & STEFFEN, 1999 p.228).

Caruso & Steffen (1999, p.237) afirmam que "Centros de processamento de informação são dependentes de instalação de climatização em função direta de seu tamanho e complexidade". Os computadores, especialmente os servidores, precisam ficar em ambientes climatizados para evitar falhas (STEFANEK, 2002).

Quando houver necessidade de utilizar algum equipamento para processar a informação fora das instalações da organização ou algum *software* ou informação, é preciso obter autorização da direção. Esses equipamentos devem ter a mesma segurança recebida dentro da organização (ABNT, 2001).

2.4.2.5. Gerenciamento das operações e comunicações

Para Caruso & Steffen (1999), o ambiente de comunicação de dados é a parte mais frágil do ambiente de informações, pois grande parte dos equipamentos e linhas de comunicação está fora de controle das organizações.

Segundo a ABNT (2001), os procedimentos e responsabilidades pela gestão e operação das informações devem ser definidos e estar sempre atualizados pelos gestores. Vale destacar a importância da definição dos procedimentos de gerenciamento de incidentes para garantir uma resposta rápida aos incidentes de segurança. Para qualquer tipo de falha precisam ser tomadas ações corretivas e estas devem ser registradas.

As modificações nos sistemas e recursos de processamento da informação devem ser controladas para evitar falhas na segurança ou de sistemas. O planejamento é necessário para garantir a disponibilidade adequada de capacidade e recursos. Isso inclui também que seja feita uma avaliação da capacidade das máquinas e que requisitos operacionais dos novos sistemas sejam definidos, documentados e testados antes do seu uso para reduzir o risco de falhas (ABNT, 2001).

Para reduzir o risco de mau uso dos sistemas, é necessário que seja realizada a segregação de funções. As atividades chave que precisam de cumplicidade para a concretização de uma fraude devem ser de responsabilidade de mais de uma pessoa (WONG E WATT, 1990; ABNT, 2001; COBIT STEERING COMMITTEE e IT GOVERNANCE INSTITUTE, 2000). O relatório do COBIT Steering Committee e IT Governance Institute (2000) relata que a segregação de função deve abranger além do uso de sistemas de informação, a entrada de dados, operação com computadores, gerenciamento da rede, administração de sistema, desenvolvimento e manutenção de sistema, gerenciamento de mudanças, administração de segurança e auditoria de segurança.

Os ambientes de desenvolvimento, teste e produção devem ser separados, a fim de evitar modificações não autorizadas de arquivos ou do sistema ou até mesmo, indisponibilidade dos sistemas (ABNT, 2001; CZEMIER, OVERBEEK e PETERS, 1999).

Todas as empresas precisam adotar precauções para prevenir e detectar a introdução de *software* malicioso, tais como vírus e cavalo de tróia[1] (COBIT STEERING COMMITTEE e IT GOVERNANCE INSTITUTE, 2000).

A contaminação eletrônica ocorre com a execução de programas ou uso de arquivos que estejam infectados. O número de computadores infectados no mundo cresce assustadoramente, causando enormes prejuízos, sejam pela paralisação dos computadores ou destruição dos arquivos. Muitas horas são perdidas na tentativa de corrigir os problemas. Uma forma de proteção é

disseminar a cultura de prevenção, instalando antivírus em todos os computadores e mantendo-o atualizado (STEFANEK, 2002).

Por mais que se criem vacinas, não se consegue acompanhar e prevenir, na mesma proporção que essas pragas se proliferam, causando muitas vezes a paralisação e sobrecarga nos sistemas.

Todas as atividades realizadas pelo pessoal de operação precisam ser registradas. Assim será possível identificar os horários e os responsáveis pelas ações executadas (ABNT, 2001).

Para a ABNT (2001), são necessários procedimentos operacionais para proteger documentos, mídias magnéticas de computadores e documentação dos sistemas contra roubo, acesso não autorizado e danos em geral. A documentação dos sistemas deve ser guardada em um ambiente seguro e somente pessoas autorizadas devem ter acesso à mesma.

Com relação às mídias removíveis, é preciso de um cuidado especial para não expor as informações contidas nelas. O descarte das diversas mídias deve ser feito de forma segura, inutilizando-as quando necessário. O controle das mídias deve ser feito para prevenir contra perda de confidencialidade, integridade e disponibilidade da informação, de dado e *software* (NIST, 1995).

As trocas de informações e *softwares* entre organizações devem ser feitas com contratos formalizados, definindo responsabilidades pelo controle e danos que venham a ocorrer, comunicação de transmissão, recepções, entre outros (ABNT, 2001).

Programa de computador com função aparentemente ou realmente útil, que contém as funções (escondidas) adicionais e que explora secretamente as autorizações legítimas do processo,

A implementação de controles deve abranger também as informações que trafegam nas redes de computadores para garantir sua proteção (ABNT, 2001; CZEMIER, OVERBEEK e PETERS, 1999).

As redes de computadores, especificamente a internet, rede pública que conecta diversos computadores ao redor do mundo, surgiram para democratizar o acesso às informações, devido à facilidade de troca das mesmas entre qualquer pessoa conectada. Com o uso da internet criou-se um mundo sem fronteiras. Ela passou a ser utilizada com diversas finalidades como meio de promover e fechar negócios, realização de pesquisas e meio de comunicação entre pessoas de qualquer parte do mundo. Para Dhillon (2001), a maior força da internet, é também sua maior fraqueza: qualquer pessoa com um computador e um modem pode ter acesso a internet, deixando-a vulnerável a invasão de um *hacker*.

Como inicialmente não se previa que a internet seria aberta ao público, sua finalidade era somente para uso militar, não houve muita preocupação com ferramenta de segurança e privacidade dentro dela (CARUSO & STEFFEN, 1999).

As atividades realizadas no espaço virtual têm exigido mudanças na forma de atuação específica à nova economia digital. Para que as empresas atuem nesta nova realidade, é necessária a implantação de uma infra-estrutura tecnológica adequada, sistemas integrados, disponibilidade de acesso a qualquer hora, um serviço de entrega do produto eficiente e a garantia de sigilo das informações que tramitam pela rede.

O comércio realizado pela internet é considerado um marco de uma nova era nos negócios, porém, há uma grande preocupação por parte dos

---

provocando perda de segurança. (ABNT, 2001)

consumidores com relação à confiança nesta modalidade de negócio porque um de seus pontos críticos e a possível redução da privacidade (DHILLON, 2001). Nas transações eletrônicas, muitas vezes o consumidor precisa informar os dados de sua conta corrente ou o número do seu cartão de crédito, e por isso, se não houver uma segurança adequada neste processo, passa a existir a possibilidade de pessoas não autorizadas fazerem mau uso dessas informações. Dhillon (2001) acrescenta que se não foi agregado conceitos éticos e definidos modelos de segurança aos negócios realizados pela internet, haverá uma dificuldade maior para o público fechar negócios virtuais.

Pesquisa nacional feita pela Módulo Security Solutions (2003) confirma que 58% dos entrevistados sentem-se inseguros para comprar em *sites* de comércio eletrônico por causa da sensação de falta de segurança. A segurança na troca de informações, sejam estas realizadas entre empresas, consumidores, ou ambos, principalmente no requisito forma de pagamento, ainda é um fator limitante do crescimento desta modalidade de negócio. Há uma constante preocupação com a exposição de informações confidenciais. Cada vez mais, a proteção da privacidade dos consumidores é considerada, por si só, uma vantagem estratégica, uma oportunidade para conquistar a confiança dos mesmos e consolidar a boa imagem da organização.

O comércio eletrônico pode envolver troca eletrônica de dados (EDI), de correio eletrônico e de transações *on-line*. Todas essas atividades estão sujeitas a um risco relativo a segurança, e por isso, devem ser estabelecidos controles para

proteção das informações, tais como: autenticação, autorização, criptografia[2], entre outros (ABNT, 2001).

Com relação ao uso do correio eletrônico, é importante a definição de uma política de uso que estabeleça a proteção dos anexos de correio, orientação sobre uso, responsabilidades dos funcionários e armazenamento de mensagens na caixa de entrada. Todas as informações disponíveis publicamente precisam ser protegidas contra modificação para não prejudicar a reputação da organização. Estas devem estar de acordo com a legislação e devem ser autorizadas formalmente antes de serem divulgadas (ABNT, 2001).

Outra vantagem obtida através da internet é o uso do *e-mail*. Ele ganhou popularidade entre corporações, escolas e pessoas comuns (STEFANEK, 2002). O correio eletrônico passou a ser um instrumento de trabalho, de divulgação de notícias, anúncios, de diversão e uma forma mais rápida para transportar arquivos. Segundo matéria publicada no jornal Folha de São Paulo *On line*, um estudo divulgado em setembro de 2001 pelo IDC informou que no mundo são trocados mais de 10 bilhões de *e-mails* por dia. A previsão para 2005 deve ser de 36 bilhões.

Todas as pessoas que usam o *e-mail* desejam que sua mensagem seja confidencial e que apenas o receptor a receba (STEFANEK, 2002).

Apesar de todos os benefícios que o correio eletrônico trouxe, ele pode permitir falhas de segurança. Quem recebe os correios fica vulnerável a contaminação por vírus. Com os *e-mails*, muitas vezes são encaminhados os vírus encontrados em mensagens anexadas. Muitos vírus se auto-enviam para lista de

[2] Os dados são codificados e decodificados para garantir a privacidade.

endereços da máquina infectada. A Confederação de Diretores Lojistas (CDL) foi vítima de um falso *e-mail*, solicitando ao usuário que clicasse em link para verificar pendências financeiras, e caso este procedimento fosse realizado, o usuário seria automaticamente contaminado por um vírus.

Os fraudadores da internet vão diversificando os temas utilizados e as empresas em suas ações na tentativa de obter algum êxito com relação à quebra de segurança. Outra prática fraudulenta é o envio de falsos *e-mails* solicitando a confirmação dos dados cadastrais dos clientes, com o objetivo de obter essas informações confidenciais.

O termo Engenharia social é usado quando alguém obtém uma informação importante de pessoas ou empresas, através de telefonemas, envio de mensagens eletrônicas, sala de bate-papo ou até mesmo pessoalmente, somente perguntando. “Engenheiro social é qualquer indivíduo que utiliza as facilidades de uma sociedade ‘ingênua’ e orientada por regras para alcançar objetivos pessoais” (BARBOSA E COELHO 2004).

Empresas como Citibank, Banco do Brasil, Serasa e Receita Federal já foram vítimas do uso de suas marcas para enganar os usuários. Circularam pela internet mensagens fraudulentas usando o nome dessas empresas. Os fraudadores desejavam que a pessoa que recebesse o e-mail, clicasse em um link para que automaticamente instalasse no computador do destinatário, sem a permissão do mesmo, um programa que lhes permitissem capturar senhas bancárias.

O envio de correio eletrônico para divulgação de um produto ou serviço é permitido, mas o excesso de *e-mails* recebidos por empresas ou consumidores é visto como uma prática ruim. O *spam,* envio de *e-mails* por fonte identificada ou

não, de forma não maliciosa, consiste em mandar correios para muitas contas, podendo ocorrer muitas vezes ao dia. De forma maliciosa, consiste em encaminhar *e-mails* até o servidor ficar sem espaço em disco. Isso pode ocasionar o aumento do tráfego de dados, podendo comprometer a rede (STEFANEK,2002).

No Brasil, há grupos anti-*spam* formado por associações, sociedades simples ou empresárias ou qualquer outro tipo de entidades, nacionais ou estrangeiras, pessoas físicas, entre outras, com o objetivo de estabelecer regras para as práticas de comunicação comercial através de mensagens eletrônicas e no combate ao *spam*.

2.4.2.6. Controle de Acesso

Segundo a ABNT (2001), o acesso às informações e a processos do negócio deve ser controlado levando em consideração as políticas de autorização e disseminação das informações. Os procedimentos referentes ao acesso aos sistemas de informação devem abranger o registro inicial de um novo usuário, a suspensão de acesso, quando necessário e a sua exclusão. A exclusão dos direitos de acesso a informação ou recurso de um funcionário que se desligou da empresa deve ser imediata.

O usuário deve receber um documento informando sobre seus direitos de acesso e assiná-lo para garantir que está ciente das condições estabelecidas. O acesso interno e externo aos serviços de rede deve ser controlado. As senhas são uma das principais formas de validar o acesso (ABNT, 2001).

A política de segurança corporativa deve especificar o período que a senha deve expirar para que ela seja modificada, para aumentar a segurança no acesso a sistemas. O ponto mais fraco da segurança no acesso a sistemas é a senha. Usuários escolhem senhas curtas, fáceis para lembrar e não as trocam com freqüência. As senhas devem ser compostas por uma mistura de caracteres e números (STEFANEK, 2002).

Ao se afastar do computador, é recomendado o uso de bloqueios para evitar o acesso não autorizado (STEFANEK, 2002).

Freqüentemente os gerentes ficam surpresos com certas fraudes cometidas por funcionários aparentemente honestos, ou pessoas relacionadas a eles (WONG e WATT, 1990). Segundo pesquisa nacional da Módulo Security Solutions (2003) sobre segurança da informação, funcionários e ex-funcionários são referenciados como responsáveis por fraudes.

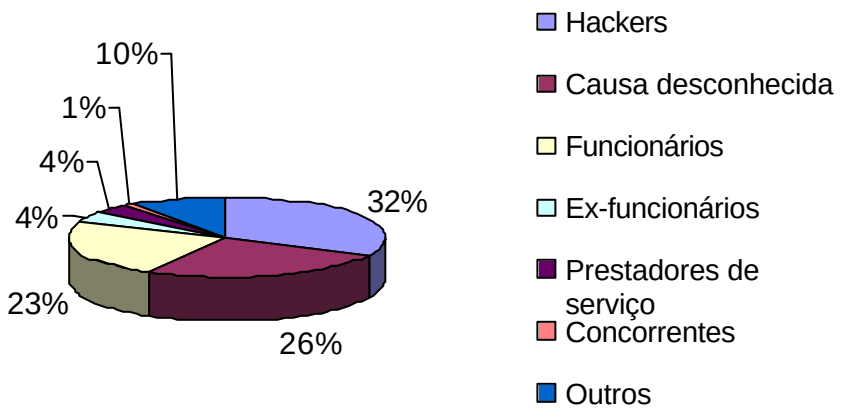

Figura 10: Responsáveis por fraudes. Fonte: Módulo Security Solutions (2003)

Um dos maiores fatores de vulnerabilidade de sistemas é o uso inadequado de privilégios dos funcionários. Por isso, eles devem ser controlados através de um processo de autorização formal. Wong e Watt (1990), citam um exemplo de uma fraude ocorrida em um banco, por causa ao excesso de privilégios disponibilizados a uma funcionária, devido à confiança que os patrões depositavam nela.

Ao permitir que funcionários não autorizados acessem recursos ou sistemas que não conhecem, estes podem ocasionar indisponibilidade do sistema e alterar ou remover informações, mesmo sem intenção.

Os sistemas devem ser monitorados para detectar divergências entre o que foi determinado nos controles de acesso e os registros de acesso (*logs*). Os *logs* devem identificar o usuário, a data e o horário de entrada e saída do sistema e tentativas de acesso bem e mal sucedidas a sistemas e recursos. Os resultados das atividades de monitoração devem ser analisados regularmente (ABNT, 2001; STEFANEK, 2002).

Ao utilizar recursos como *notebooks* e *palmtops*, é preciso ter cuidados especiais para proteção das informações contidas nesses equipamentos, já que eles podem ser transportados para qualquer ambiente. Há também o perigo de roubo ou esquecimento desses equipamentos em algum local, pelo proprietário (ABNT, 2001). Uma matéria publicada no *site* da Módulo Security Solutions (2001) informou que um oficial do Ministério de Defesa Britânico esqueceu um *notebook* em um táxi e não conseguiu mais recuperá-lo. No *notebook*, havia segredos de segurança nacional, que foram perdidos.

2.4.2.7. Desenvolvimento e manutenção de sistemas

Os requisitos de segurança devem ser identificados e acordados antes do desenvolvimento dos sistemas de informação. Ao definir os requisitos e controles de segurança, eles devem refletir o valor dos ativos de informação e os potenciais riscos ao negócio (ABNT, 2001).

Controles para evitar modificação ou uso inadequado de dados e registros devem ser previstos para os sistemas. Os dados de entrada desses sistemas devem ser validados para garantir que estão corretos e que são apropriados. Além disso, a verificação de validação deve ser incorporada aos sistemas para detectar possíveis corrupções de dados causadas por erros de processamento ou ações intencionais (WONG E WATT, 1990; ABNT, 2001).

A criptografia é conhecida desde a antiguidade quando era usada para comunicações militares, mas foi recentemente que ela passou a ser mais utilizada, devido a intensificação do uso de transações comercias. “A criptografia serve para tornar ininteligíveis as informações constantes dos meios de armazenamento e em linhas de comunicação de dados” (CARUSO & STEFFEN, 1999 p. 151). Wong e Watt (1990) compartilham com a visão de Caruso & Steffen (1999) citada anteriormente, de que a criptografia protege as informações, dificultando as fraudes.

Existem várias áreas relacionadas a segurança no processo de desenvolvimento de sistema que devem ser consideradas, tais como: documentação de sistema, controle e gerenciamento de mudança e teste de intruso (WONG E WATT, 1990). Para Caruso & Steffen (1999), os programas

devem ter a documentação atualizada e esta deve ser copiada e guardada em uma sala de segurança.

Os ambientes de desenvolvimento e suporte devem ser controlados para que não ocorram falhas que possam comprometer a segurança. Os novos *softwares* devem ser testados em ambientes diferentes dos de desenvolvimento e produção. Procedimentos formais devem garantir que os programadores e pessoas de suporte tenham acesso somente às áreas necessárias ao seu trabalho (ABNT, 2001).

2.4.2.8. Gestão da continuidade do negócio

A gestão da continuidade do negócio, visa restaurar os processos críticos empresariais em menor tempo possível, em caso de falhas ou desastres. O primeiro passo é identificar os processos críticos da empresa, analisar os riscos aos quais a empresa está exposta, avaliando a probabilidade de ocorrência e o impacto que poderão causar. Após esta etapa, elabora-se um plano de contingência ou continuidade do negócio, detalhando o que deve ser feito, contemplando recursos técnicos e humanos, e quem irá executar as ações planejadas (ABNT, 2001; NIST, 1995).

Dados e *software* representam um investimento e recursos dos quais a organização depende, mas eles não são vistos como ativos. Entretanto, a perda de dados pode causar uma interrupção nos negócios e o seu custo pode ser significativo. Para muitas empresas, o valor dos dados pode exceder o valor do *hardware* que os processam (WONG e WATT, 1990).

Problemas de *hardware* e *software* podem ocorrer inesperadamente e por este motivo, as empresas devem estar preparadas para lhe dar com panes, falhas, queda de energia ou desastres que leve a destruição de todos os equipamentos e informações, como no caso do *World Trade Center*. Mesmo sabendo que este cenário pode ser parte de qualquer empresa, Adam e Haslam *apud* Dhillon (2001) relatam que em suas pesquisas, o plano de contingência ainda não é valorizado adequadamente pela gerência. Os gerentes preferem concentrar seus esforços em projetos que gerem lucros.

Ao acontecer algum desastre ou falha gerando um impacto na rotina da empresa, há uma tendência pela procura de outra empresa que ofereça serviços ou produtos similares. Desastres sempre causam prejuízo a credibilidade da empresa (DHILLON, 2001).

A estratégia de um plano de contingência consiste em três partes: resposta a emergências, recuperação e recomeço. A primeira se refere a ações iniciais para limitar o perigo. Recuperação é a manutenção que é dada para a continuidade de funções críticas e o recomeço é a normalização das operações (NIST, 1995).

Um dos elementos chave de um plano de continuidade do negócio é a organização e disponibilidade das pessoas em recuperar os procedimentos. As pessoas individualmente ou equipes, precisam ser identificadas e estas devem ter suas responsabilidades determinadas não só para executar o plano de ação, mas também para mantê-lo (WONG e WATT, 1990).

O plano de continuidade do negócio precisa ser documentado, testado, atualizado (ABNT, 2001; NIST, 1995).

O plano de contingência deve contemplar uma política de *back-up,* essencial para a continuidade dos negócios da empresa. A cópia de segurança deve ser efetuada diariamente, e após cada *back-up*, deve ser feita uma verificação para confirmar o sucesso do mesmo.

Para garantir a segurança da mídia, o armazenamento do *back-up* deve ser feito em um local com o mesmo nível de segurança que a sala dos servidores, e em um local externo a empresa (STEFANEK, 2002; WONG E WATT, 1990).

Para minimizar a interrupção do trabalho devido a falta de energia elétrica, algumas empresas possuem um gerador de energia. Para as empresas que não contam com este recurso, é recomendado o uso de *no-breaks*, a fim de proporcionar a utilização de computadores durante algum tempo, mesmo sem luz elétrica (WONG E WATT, 1990).

2.4.2.9. Conformidade

> Convém que procedimentos apropriados sejam implementados para garantir a conformidade com as restrições legais no uso de material de acordo com leis de propriedade intelectual, como as de direitos autorais, patentes ou marcas registradas. A violação do direito autoral pode levar a uma ação legal envolvendo processos criminais (ABNT, 2001, p. 48).

Os *softwares* sem licença de uso são chamados de piratas. É ilegal o uso desses *softwares,* e portanto, as empresas que os utilizam estão sujeitas a serem multadas. Existe uma dificuldade em legalizar os programas devido ao alto valor das licenças (Dhillon, 2001). Além disso, alguns funcionários instalam *softwares*

ilegais sem autorização. Portanto, é muito importante que haja um procedimento para controle de licença de *software*.

Antigamente, o dever de proteger o ambiente tecnológico era responsabilidade apenas dos especialistas de informática e somente as pessoas jurídicas respondiam pelas indenizações em caso de incidentes de TI.

Peixoto (2003) relata que a partir da Legislação Federal Americana "*The U.S. Public Company Accounting Reform and Investor Protection Act of 2002*", conhecida como Sabanes-Oxley, rígidos parâmetros legais foram impostos às companhias de capital aberto e suas subsidiárias no âmbito de governança corporativa e ética nos negócios.

> Ao regular as atividades de contabilidade e auditoria das empresas de capital aberto, a Sarbanes-Oxley reflete diretamente seus dispositivos nos sistemas de Tecnologia da Informação. Impossível separar processos de negócios e tecnologia no panorama corporativo atual (Peixoto, 2003).

A Sarbanes-Oxley gera novas responsabilidades e sanções aos administradores, com o objetivo de coibir práticas que possam expor as empresas a elevados níveis de risco.

Ameaças à segurança da informação podem implicar responsabilidade direta dos administradores, gerando possibilidades concretas de sanções civis e penais, se não houver prova suficiente de adoção de medidas coordenadas com os parâmetros do artigo 404 da legislação brasileira. Segundo Negrão (2003), este artigo trata de controle de processos internos e sistemas contábeis. Cada vez mais, os controles de segurança fazem parte de sistemas eficientes de controle

interno. Os sistemas financeiros precisam estar seguros para garantir a veracidade dos dados e a integridade de seus controles internos.

As iniciativas legais brasileiras de disciplinar a segurança da informação já estão em vigor no novo código civil. A lei n° 10.406, de 10 de janeiro de 2002 instituiu o novo código civil, e em seus artigos 43, 186, 187, 927 e 1.011, os administradores passam ser responsáveis pelos riscos referentes ao negócio e criados por ele. O administrador deverá gerenciar os riscos organizacionais a níveis aceitáveis, pois caso contrário, ele poderá ser considerado negligente por aceitar e conhecer as conseqüências que estes podem causar a terceiros. A responsabilidade não é restrita a alta administração. Respondem também os gerentes e especialistas por serem condescendentes com qualquer tipo de risco, porém com menor grau de culpa (OLIVEIRA, 2004).

Ao direito, cabe regular as relações de forma geral e nem sempre a ciência jurídica acompanha a evolução tecnológica. Apesar da determinação de zelar pelas responsabilidades da organização, ainda não há uma legislação específica para a área de Tecnologia da Informação, gerando uma persistente defasagem entre a estática do código e a dinâmica dos fatos.

2.5. Verificação e ação

Para o BSI (2002), a fase de verificação inclui uma nova avaliação de risco para constatar se os controles implementados estão reduzindo os riscos, e a fase de ação corresponde ao tratamento dos riscos.

Czemier, Overbeek e Peters (1999) destacam a importância de supervisionar e verificar se os padrões e normas implementadas estão de acordo com a política de segurança da organização. Para isso, são necessárias auditorias regulares da segurança técnica e de sistemas de TI.

As trilhas de auditoria são um meio de acompanhar vários objetivos de segurança, inclusive responsabilidades individuais e detecção de intrusos (NIST, 1996).

Todas as práticas de segurança implementadas em uma empresa precisam ser monitoradas para verificação da sua eficiência e eficácia e para que elas sejam atualizadas, no mesmo ritmo em que evoluem as empresas e suas relações.

3. Estudos de Caso

3.1 Metodologia de Pesquisa

Para verificar as hipóteses de que as práticas de segurança implementadas não vêm atendendo a todas as necessidades de segurança, o que vem ocasionando perdas de informação e financeiras, quebra de confidencialidade, integridade e disponibilidade da informação, possibilitando gerar uma imagem negativa para a organização e que a não implementação de todas as práticas de segurança recomendadas ocorre em função da falta de consciência dos riscos envolvidos ou da falta de recursos financeiros, foram realizados dois estudos de caso.

Enfrentou-se uma enorme dificuldade para conseguir a adesão de empresas para a realização dos estudos de caso. Inicialmente, foram contatadas três empresas, que não concordaram em participar da pesquisa, sob a alegação de que o assunto, de alguma forma, poderia expor informações sensíveis a organização.

Este estudo caracteriza-se como uma pesquisa exploratória, ilustrado com a descrição de dois estudos de caso, cuja amostragem foi feita por conveniência. O assunto segurança da informação ainda precisa ser explorado empiricamente, principalmente em organizações locais.

Como muitas empresas não registram algumas ocorrências referentes à segurança da informação, apesar de ser uma conduta altamente recomendável, nesta pesquisa serão avaliados indicadores predominantemente qualitativos.

A pesquisadora assinou um acordo de confidencialidade com as organizações participantes para assegurar a guarda de sigilo de todas as informações que serão obtidas a partir da realização das entrevistas e não expor as vulnerabilidades das mesmas (apêndice A). Portanto, seus nomes não serão publicados e o resultado da pesquisa não distinguirá a qual organização se refere os determinados conjuntos de dados e análises.

3.2. Instrumentos de Coleta de Dados

As principais técnicas de coleta de dados utilizadas durante esta pesquisa foram: roteiro de entrevistas e observações. As entrevistas foram semi-estruturadas, com roteiro elaborado a partir do referencial teórico, modelo de análise e da experiência da pesquisadora (apêndice B). A entrevista foi realizada junto a uma amostra de gestores e de pessoas que atuam na área operacional, com duração, em média, de uma hora cada. Os entrevistados foram solicitados a falar sobre a segurança da informação na organização em que trabalham.

Foram feitas algumas observações para verificar como eram implementadas algumas práticas de segurança.

3.2.1. Pré-teste do instrumento de coleta de dados

Para validação do roteiro da entrevista, foi feito um pré-teste do instrumento de coleta de dados com três analistas de sistemas, um gerente do CPD e um diretor de TI, em uma instituição de ensino superior que atua no Estado da Bahia. Durante a aplicação do pré-teste, e após as análises preliminares dos dados

levantados, evidenciaram-se algumas falhas, como por exemplo, necessidade de um maior esclarecimento em algumas perguntas e definição de conceitos com os entrevistados, sendo necessário ajustes. Após esta fase, o roteiro foi aplicado definitivamente nas organizações selecionadas para realização dos estudos de caso.

3.2.2 Unidade de Análise

O foco do trabalho é a segurança de informações disponibilizadas em meios digitais, por isso não serão investigados outros aspectos de segurança da informação, tais como: impressa em papel, exibida em filmes ou falada durante uma conversação.

O corte temporal para a investigação das práticas de segurança e das conseqüências do não atendimento de algumas necessidades de segurança compreenderá o período correspondente aos três últimos anos.

3.3. Limitação da pesquisa

Como só foram feitos dois estudos de caso, as informações obtidas não podem servir de parâmetro para o universo de organizações locais, apesar de representarem segmentos importantes.

Este estudo não pretende aprofundar as práticas de segurança utilizadas em instituições financeiras e nem organizações que utilizam comércio eletrônico, por possuírem características peculiares ao negócio.

3.4. Modelo de Análise

O modelo de análise envolve etapas que levam à definição de dimensões e variáveis referentes à gestão da segurança da informação, levantados pela pesquisadora, em que as dimensões são materializadas através das variáveis. As dimensões e variáveis, bem como os conceitos referentes aos princípios básicos da segurança da informação (confidencialidade, integridade e disponibilidade) são derivados do referencial teórico e da norma ISO/IEC 17799-1:2001.

Confidencialidade é a garantia de que a informação só será acessível a pessoas autorizadas, integridade está relacionada à exatidão da informação e disponibilidade é a garantia de que os usuários autorizados terão acesso a informação e aos ativos correspondentes sempre que necessário. As variáveis foram construídas a partir de alguns controles de segurança da informação. O modelo de análise é apresentado na tabela 3.

Tabela 3: Modelo de análise

	Etapas	Dimensões	Variáveis
Segurança da informação (caracterizada pela preservação da confidencialidade, disponibilidade e integridade da informação)	Planejamento da segurança	Avaliação de risco	- Orçamento destinado à segurança da informação.
		Política de segurança da informação	- Responsabilidade da segurança da informação; - Política de segurança formalizada.
	Administração da segurança da informação	Confidencialidade	- Acesso controlado a sistemas e a ambientes computacionais; - Classificação de informações; - Uso de criptografia; - A não ocorrência de vírus; - Projetos de segurança previstos para serem realizados durante o ano de 2004; - Cultura de segurança da informação; - Procedimentos para registro de Falhas.
		Integridade	- Não alteração de dados através de fraude, erro ou acidente; - Uso de criptografia; - Ocorrência de segregação de funções; - A não ocorrência de vírus; - Projetos de segurança previstos para serem realizados durante o ano de 2004; - Cultura de segurança da informação; - Procedimentos para registro de Falhas.
		Disponibilidade	- Existência de um plano de continuidade do

			de continuidade do negócio, evitando a paralisação de atividades e equipamentos em caso de acidentes; - Planejamento da capacidade de recurso e sistema; - Ocorrência de separação dos ambientes de desenvolvimento, teste e produção; - A não ocorrência de vírus; - Correto armazenamento e restauração do *back-up*; - Instalações adequadas evitando danos físicos; - Manutenção do ar condicionado na sala dos servidores; - Manutenção da energia elétrica na organização; - Projetos de segurança previstos para serem realizados durante o ano de 2004; - Cultura de segurança da informação; - Procedimentos para registro de Falhas.
	Avaliação da segurança da informação	Resultados	- Auditorias; - Incidentes de segurança da informação; - Perdas de informação; - Perdas financeiras.

Fonte: Elaborado pela autora.

Para levantar as variáveis, as fontes foram os gestores e pessoas do setor operacional e os meios de verificação foram entrevistas (apêndice B) e observações.

3.5. Análise dos dados

Como já foi mencionado anteriormente, optou-se por não identificar ou caracterizar completamente as organizações estudadas. Na análise dos dados, elas serão denominadas organização A e B.

As duas organizações estudadas atuam em áreas de negócio diferentes, ambas no Estado da Bahia. A organização A atua no varejo, no ramo de supermercado, possui entre 300 a 500 funcionários e o seu parque de informática é composto por uma faixa entre 100 e 500 computadores. A organização B atua no setor de educação, é uma instituição de ensino superior, possui mais de 500 funcionários e mais de 500 computadores.

Ambas organizações possuem diversas unidades funcionais e setores e todos são informatizados. Na organização A, a pesquisa foi feita na matriz e em uma das filiais, cujo número de funcionários é de 180 pessoas. Sua estrutura é composta por uma matriz e 4 filiais. Na organização B, a pesquisa foi aplicada apenas na área de TI, com uma estrutura composta por uma diretoria, divisões de planejamento, projeto, suporte e produção, com um total de 85 pessoas entre funcionários e prestadores de serviço, por onde circulam as informações mais sensíveis ao negócio.

Nas duas organizações, a responsabilidade da segurança da informação pertence ao departamento de TI. Apenas na B existe um especialista em segurança, que está ligado ao departamento de TI.

> Numa analogia com o ditado de 'colocar a raposa para tomar conta do galinheiro', não se deve ligar a administração de segurança a nenhuma

> das funções de informática, - visto que elas também serão consideradas usuárias da segurança, - nem à área de auditoria, - pois cabe à mesma fiscalizar a área de segurança (CARUSO & STEFFEN, 1999, p.109).

Desta afirmação do autor, depreende-se que a área de administração de segurança precisa se relacionar diretamente à alta administração, para que fique isenta de qualquer tipo de pressão.

Nas duas organizações não há um percentual do orçamento total destinado ao orçamento da TI ou específico para segurança da informação. Com relação à organização A, os investimentos em TI e em segurança são feitos por demanda. Na organização B, há um planejamento para a área de TI e nele são definidos todas as ações e investimentos que irão ser realizados na área de segurança da informação.

A segurança da informação é uma preocupação em ambas organizações estudadas. Como confirmação, na tabela abaixo, são destacados os principais projetos de segurança previstos para serem realizados durante o ano de 2004.

Tabela 4: Projetos de segurança

Projetos	**Organização A**	**Organização B**
Controle de acesso físico	X	X
Controle de acesso lógico	X	X
Capacitação da equipe de TI	X	
Segurança em internet	X	X
Contratação de serviços de	X	

empresas especializadas		
Definição de uma política de segurança.		X

Fonte: Elaborado pela autora

Além desses projetos, a organização B relatou que pretende reestruturar o sistema de *back-up* e implantar um sistema de detecção de incêndio.

Pode-se notar que apesar das práticas de segurança da informação como avaliação de risco e plano de continuidade do negócio serem de cunho preventivo, elas não estão presentes nos projetos a serem realizados pelas organizações em 2004.

Nas duas organizações, os responsáveis pela área de TI foram unânimes em afirmar que há uma falta de consciência da importância da segurança da informação pelos funcionários e por alguns gerentes. Este fato é considerado um obstáculo para implementação de práticas de segurança. Neste caso, percebe-se uma necessidade de treinamento para devida conscientização, requisito que vem sendo mencionado por diversos autores, como por exemplo, Solms (2000) e NIST (1995).

Somente a organização B considerou também como um obstáculo, o orçamento limitado.

Em nenhuma das duas organizações pesquisadas existe uma política de segurança formalizada. As atividades de segurança não estão sendo regidas por diretrizes formais, representando uma visão estratégica sobre a segurança da informação. Isso vai de encontro com as idéias de Coutanche (2001) e

informações do NIST (1995), na medida em que afirmam a necessidade de um documento formal da política de segurança da informação.

Os depoimentos colhidos em ambas organizações, evidenciaram possíveis ameaças que poderiam comprometer a segurança da informação. São consideradas ameaças para a organização A:

- Acessos e alterações indevidas;
- Fraudes, erros e acidentes. Esta ameaça foi resultante de erros de operação financeira que influenciaram negativamente a imagem da organização;
- Funcionários e prestadores de serviço insatisfeitos;
- *Hackers*;
- Falta de sigilo no uso de senhas;
- Uso indevido de recursos computacionais, como o acesso a programas para uso pessoal;
- Indisponibilidade do sistema e da rede;
- Vírus.

Para a organização B, são consideradas ameaças:

- Acessos e alterações indevidas;
- Erros e acidentes;
- *Hackers*;

- Incêndios e desastres;
- Falha no armazenamento, circulação e descarte de informações nas suas diversas mídias;
- Pirataria;
- Falta de sigilo no uso de senhas;
- Uso indevido de recursos computacionais;
- Vazamento de informações;
- Indisponibilidade do sistema e da rede;
- Vírus;
- Pequenos furtos, como por exemplo, *HD*, memória etc.

De acordo com Caruso e Steffen (1999), a climatização do ambiente computacional é muito importante para o bom funcionamento dos equipamentos. O não cumprimento deste requisito traz conseqüências, a exemplo do que ocorreu na organização B. A rede já teve problemas de indisponibilidade devido a defeito do ar condicionado na sala dos servidores. Os equipamentos precisaram ser desligados para que não ocorresse o aquecimento dos mesmos, evitando que fossem danificados.

Nem todos os funcionários da organização B têm o hábito de bloquear o acesso a seu computador quando não está usando, ou quando estão fora da sala. Por este motivo, já ocorreu acesso indevido a informações, afetando a confidencialidade, integridade e disponibilidade da informação. Stefanek (2002) recomenda o uso de bloqueios para evitar o acesso não autorizado.

Pela quantidade de ameaças listadas, aparentemente, os entrevistados percebem diversos problemas que podem comprometer a segurança da informação em suas organizações.

Ao serem questionados sobre incidentes de segurança, os gestores da área de tecnologia informaram que estes vêem ocorrendo em ambas organizações nos últimos três anos, período relativo ao corte temporal da pesquisa, e o principal deles é o vírus e *spam*. Na organização B, por exemplo, o servidor de *e-mail* já ficou fora do ar por algumas horas em função dos incidentes anteriormente citados, prejudicando o trabalho de vários funcionários que dependem deste meio de comunicação e demandando algumas horas do especialista de segurança da informação para que o servidor voltasse a funcionar normalmente.

Outro incidente relevante ocorrido na organização B, estava relacionado com direito autoral. A organização foi notificada pelo mau uso de arquivos, mas na verdade, isso foi objeto da ação de um cliente. Este fato compromete a reputação da organização, apesar de não ter sido ela quem utilizou esses arquivos ilegalmente. Daí a importância do envolvimento e do compromisso de todos os parceiros, sejam clientes ou fornecedores, na questão de segurança.

Na organização A, o último incidente de segurança ocorreu há cerca de seis meses da realização da pesquisa. Já na organização B, ocorreu há menos de um mês da realização da pesquisa.

Nas duas organizações já ocorreram quebra de confidencialidade, integridade e disponibilidade, como pode ser visto nas tabelas abaixo.

Tabela 5: Relação entre dimensões e variáveis da organização A

Dimensões	Variáveis
Quebra de confidencialidade	Invasão ao *site* da organização
	Ocorrência de vírus
Quebra de integridade	Alteração de dados através de fraude
	Ocorrência de vírus
Quebra de disponibilidade	Ocorrência de vírus
	Falta de teste do gerador de energia para verificar o seu funcionamento

Fonte: Elaborado pela autora

Tabela 6: Relação entre dimensões e variáveis da organização B

Dimensões	Variáveis
Quebra de confidencialidade	Acesso indevido a informações
	Ocorrência de vírus
Quebra de integridade	Alteração de dados através de erro
	Ocorrência de vírus
Quebra de disponibilidade	Falta de separação dos ambientes de desenvolvimento, teste e produção
	Ocorrência de vírus
	Ocorrência de defeito no ar condicionado na sala dos servidores.

Fonte: Elaborado pela autora

Apenas na organização A ocorreu perda financeira. Esta organização não tem registros dos incidentes de segurança ocorridos e portanto não sabe mensurar de quanto foi à perda. Ela estima o valor do prejuízo em torno de cinco mil reais. O problema foi causado por fraude de um funcionário cujos privilégios de acesso permitiam o manuseio de informações financeiras. Esta ocorrência atesta as estatísticas apresentadas no referencial teórico, de que muitas vezes os funcionários são envolvidos em fraudes.

Quando ocorre um incidente de segurança, as duas organizações estudadas tomam as seguintes providências: correção do problema e adoção de medidas preventivas para evitar nova ocorrência. Portanto, não há um procedimento para registro de falhas. Analisando este fato, percebe-se que não é possível gerar um histórico dos incidentes ocorridos. As organizações informaram também que não têm hábito de realizar auditorias, contrariando as recomendações de diversos autores, a exemplo de Czemier, Overbeek e Peters (1999), que destacam a importância de auditorias regulares das práticas de segurança da informação implementadas nas organizações.

As duas organizações possuem *site*. A organização A já teve seu *site* invadido por um *hacker*, mas em poucas horas voltou a disponibilizar seus serviços. Este incidente não gerou nenhum outro tipo de conseqüência mais grave.

As medidas de segurança implementadas na organização A são:

- Planejamento de recursos. A equipe de TI se preocupa em manter alguns equipamentos extras na organização em caso de necessidade, mas não há um planejamento de sistemas.

- Contratação de serviços de organizações especializadas;
- *Firewall*;
- Monitoração de *log*;
- Controle de conteúdo. A organização controla o conteúdo acessado relativo a *Web* e não permite o recebimento de arquivos executáveis por *e-mail*;
- Restrição de acesso físico em alguns ambientes da organização. Na matriz, há um controle de acesso maior do que nas filiais, a sala dos servidores fica trancada;
- Prevenção contra pirataria. Constantemente são feitas vistorias nos micros para evitar que programas piratas sejam instalados;
- Atualização constante do antivírus;
- Existem alguns procedimentos formalizados no setor de informática;
- Servidor *proxy*[3];
- Segurança de acesso remoto;
- Segurança em internet;
- Segurança de instalações e equipamentos;
- Controle de acesso. Os funcionários utilizam senhas para acesso a rede e sistemas. Quando um funcionário sai da organização, automaticamente recebe uma ordem do diretor para desativação da senha. Os direitos de acesso são revistos regularmente;
- Segregação de funções ao utilizar o sistema;
- Separação de ambiente de teste e produção;

[3] Uma empresa usa um servidor proxy para prevenir que seus funcionários acessem sites indesejados.

- Realização de *back-up*. A organização não possui um local adequado para armazenamento de *back-up*. Uma fita é guardada em um armário, que não é considerado um local seguro, e outra é encaminhada para um local fora da organização.

Os sistemas da organização A são terceirizados. Não há documentação dos sistemas.

As medidas de segurança implementadas na organização B são:

- Criptografia;
- *Firewall*;
- Controle de conteúdo. A organização controla o conteúdo da *Web* acessado pelos usuários;
- Restrição de acesso físico em alguns ambientes da organização;
- Atualização constante do antivírus;
- Existem alguns procedimentos formalizados;
- Servidor *proxy*;
- Segurança de acesso remoto;
- Segurança em internet;
- Segurança de instalações e equipamentos;
- Controle de acesso. Os funcionários utilizam senhas para acesso a rede e sistemas. Há uma troca regular de senha, porém, não há um procedimento disciplinando a desativação de senha quando um funcionário deixa a

organização ou troca de função. Os direitos de acesso não são revistos regularmente;

- Segregação de funções ao utilizar o sistema;
- Separação de ambiente de desenvolvimento e produção, porém, às vezes, são feitos testes em ambientes de produção;
- Realização de *back-up*. A organização não possui um local adequado para armazenamento de *back-up*. Uma fita é guardada em um armário.

A nona pesquisa nacional da Módulo Security Solution divulgou o ranking das dez medidas de segurança implementadas pelas empresas em 2003, como pode ser visto na tabela abaixo.

Tabela 7: Top 10 medidas de segurança já implementadas

Ranking	Medidas implementadas	Percentual
1	Antivírus	90
2	Sistema de *back-up*	76,5
3	*Firewall*	75,5
4	Política de segurança	72,5
5	Capacitação técnica	70
6	*Software* de controle de acesso	64
7	Segurança física na sala de servidores	63
8	*Proxy Server*	62

9	Criptografia	57
10	Análise de riscos	56

Fonte: Módulo Security Solutions (2003)

Nos casos estudados, verificou-se que algumas medidas de segurança da informação implementadas, coincidem com as mais adotadas nas empresas nacionais.

A organização B, desenvolve sistemas para o seu próprio uso. Esta organização não realiza um teste de carga do sistema para analisar sua performance. Isso gera uma vulnerabilidade, podendo tornar o sistema indisponível. Outro fator crítico relativo à área de desenvolvimento de sistema é que nem sempre a documentação dos sistemas é atualizada. Além disso, esta documentação não é guardada em um local seguro.

Relacionando os itens considerados como ameaças, para as duas organizações, com as medidas de segurança já implementadas nas mesmas, pode-se perceber que há uma fragilidade envolvendo o fator humano. É importante que todos os colaboradores estejam conscientes de suas responsabilidades de segurança da informação. Para isso, conforme visto na revisão da literatura, é necessário estabelecer uma cultura de segurança na organização, treinando todo o pessoal desde a sua contratação.

Algumas práticas de segurança da informação não implementadas nas duas organizações:

- Análise de risco;
- Política de segurança formalizada;

- Capacitação na área de segurança;
- Classificação das informações;
- Plano de continuidade do negócio;
- Registros em caso de incidentes de segurança;
- Segurança e tratamento de informações nas suas diversas mídias;
- Auditorias.

Pode-se notar que as duas organizações estudadas não adotam algumas estratégias pró-ativas para a preservação da segurança da informação. O modelo PDCA adotado pela norma BS 7799-2:2002, apresentado no referencial teórico, contempla a fase de planejamento, que abrange a etapa de avaliação de risco e política de segurança da informação e a fase de verificação da implementação de práticas de segurança da informação. Essas etapas representam uma forma de prevenção para alcançar a proteção adequada dos ativos de informação.

Conforme a ABNT (2001), recomenda-se que o plano de continuidade do negócio seja documentado, testado e constantemente atualizado.

Apesar de não existir um plano de continuidade do negócio formalizado nas duas organizações estudadas, existem medidas que demonstram uma preocupação em preservar os processos críticos do negócio em caso de alguma falha, como por exemplo, *no-break*, recursos reservas, como por exemplo, placas, micros e impressoras, gerador de energia, pessoal treinado para recuperação dos processos mais críticos e teste de recuperação de *back-up*. A organização A já ficou quatro horas sem energia e apesar de possuir um gerador, não pode contar

com este recurso porque no momento necessário, ele não funcionou. Isso demonstra que esta organização não vem testando adequadamente os equipamentos que são utilizados de forma eventual.

Nas duas organizações, o acesso à internet é feito através da rede interna. Atualmente, na organização A, apenas os diretores e analistas de sistemas tem disponibilidade de acesso à internet na organização para evitar o mau uso deste recurso. Esta foi a forma encontrada pela organização para evitar o acesso a *sites* indevidos e evitar que os usuários baixem programas da internet sem autorização da direção.

A migração das atividades convencionais para a forma eletrônica tem crescido muito. Com isso, as organizações agilizam suas tarefas ganhando tempo e aumentando sua produtividade. Uma dessas facilidades é a utilização da movimentação bancária pela internet. Nessa pesquisa, foi constatado que apenas a organização A usa este recurso, sem ter apresentado nenhum tipo de problema até o momento da realização da mesma.

Após a realização dos estudos de caso, utilizando o modelo de análise como referência, pode-se apresentar os seguintes resultados:

Tabela 8: Resultados com base no modelo de análise

	Etapas	Dimensões	Organização A	Organização B
Segurança da informação (caracterizada pela preservação da confidencialidade, disponibilidade e integridade da informação)	Planejamento	Avaliação de risco	- Não realiza avaliação de risco	- Não realiza avaliação de risco
		Política de segurança da informação	- Não possui política de segurança formalizada	- Não possui política de segurança formalizada
	Administração	Confidencialidade	- Apresenta controle no acesso a sistemas e ambientes computacionais - As informações não são classificadas - Não utiliza criptografia - Eventualmente a empresa é infectada por vírus - Há projetos de segurança previstos para serem realizados durante o ano de 2004 (tabela 4) - Não há disseminação de cultura de segurança adequada entre funcionários e com os prestadores de serviço - Não há procedimentos para registros de falhas	- Apresenta controle no acesso a sistemas e ambientes computacionais, mas os direitos de acesso não são revistos regularmente - As informações não são classificadas - Utiliza criptografia - Às vezes a empresa é infectada por vírus - Há projetos de segurança previstos para serem realizados durante o ano de 2004 (tabela 4) - Não há disseminação de cultura de segurança adequada entre funcionários e com os prestadores de serviço. - Não há procedimentos para registros de falhas

		Integridade	- Já ocorreu alteração de dados através de fraude, erro ou acidente - Não utiliza criptografia - Realiza a segregação de funções no uso do sistema - Eventualmente a empresa é infectada por vírus - Há projetos de segurança previstos para serem realizados durante o ano de 2004 (tabela 4) - Não há disseminação de cultura de segurança adequada entre funcionários e com os prestadores de serviço - Não há procedimentos para registros de falhas	- Já ocorreu alteração de dados através de erro ou acidente - Utiliza criptografia - Realiza a segregação de funções no uso do sistema - Às vezes a empresa é infectada por vírus - Há projetos de segurança previstos para serem realizados durante o ano de 2004 (tabela 4) - Não há disseminação de cultura de segurança adequada entre funcionários e com os prestadores de serviço. - Não há procedimentos para registros de falhas.

		Disponibilidade	- Não há um planejamento de continuidade do negócio formalizado - Há uma separação dos ambientes de teste e produção. - Eventualmente a empresa é infectada por vírus - A fita de back-up não é guardada em local adequado - Nem sempre esta organização testa adequadamente o gerador de energia. - Há projetos de segurança previstos para serem realizados durante o ano de 2004 (tabela 4) - Não há disseminação de cultura de segurança adequada entre funcionários e com os prestadores de serviço - Não há procedimentos para registros de falhas	- Não há um planejamento de continuidade do negócio formalizado - Falta teste de carga nos novos sistemas. - Nem sempre há uma separação dos ambientes de desenvolvimento, teste e produção - Às vezes a empresa é infectada por vírus - A fita de back-up não é guardada em local adequado - Há projetos de segurança previstos para serem realizados durante o ano de 2004 (tabela 4) - Não há disseminação de cultura de segurança adequada entre funcionários e com os prestadores de serviço. - Não há procedimentos para registros de falhas

	Avaliação	Resultados	- Não são realizadas auditorias - Há ocorrência de incidentes de segurança da informação - Já ocorreram perdas financeiras - Já houve quebra de confidencialidade, integridade e disponibilidade	- Não são realizadas auditorias - Há ocorrência de incidentes de segurança da informação - Já houve quebra de confidencialidade, integridade e disponibilidade

Fonte: Elaborado pela autora.

4. Considerações Finais

A partir do referencial teórico e da pesquisa apresentada, pode-se concluir que as práticas de segurança da informação implementadas nas organizações estudadas não vêem atendendo às necessidades de segurança. Esta afirmação é baseada nas análises feitas em ambas organizações, onde se constata que existem problemas de segurança, como por exemplo, a falta de cultura de segurança, classificação das informações e realização de auditorias, proporcionando um aumento da probabilidade de ocorrência de incidentes. Como conseqüência da não implementação de práticas adequadas para a redução dos riscos presentes em seu ambiente, pode ocorrer perda financeira, de confidencialidade, integridade e disponibilidade da informação. Portanto, as duas organizações estudadas precisam implementar práticas de segurança da informação recomendadas pelo mercado, para alcançar um nível satisfatório de proteção de seus ativos. Revelou-se ainda que um dos fatores preponderantes para proteger as informações organizacionais é a elevação do nível de conscientização geral sobre a importância do assunto nas organizações. Muitas vezes, os funcionários não sabem quanto podem prejudicar a organização deixando-a sujeita aos incidentes de segurança da informação e aos prejuízos decorrentes. Por este motivo, recomenda-se treinamento adequado para que os funcionários possam executar seus trabalhos de forma segura.

Diversas fontes de pesquisas foram utilizadas para a discussão teórica, mas para o detalhamento das práticas de segurança, foi utilizada a norma ISO/IEC

17799, por ser um referencial internacionalmente adotado como as melhores práticas de segurança da informação.

É indiscutível o papel da tecnologia na vida do cidadão e a profunda transformação que ela vem impondo a sociedade. Em contrapartida, junto com as facilidades que a economia digital trouxe ao cidadão, surgiram questões relativas a segurança da informação. Até que ponto pode-se confiar no sigilo das informações pessoais que circulam pelos meios digitais? Problemas como roubo de senhas de contas bancárias, desvios de dinheiro pela internet, vírus de computador são algumas das novas ameaças que surgiram com a economia digital. Portanto, para garantir a credibilidade e confiança das organizações que fazem parte desta nova economia, é necessário implementar rígidos padrões para proteção de informações.

Os estudos de caso foram realizados em organizações de natureza e porte diferentes, mas apesar disso, com relação à segurança da informação, elas possuem alguns problemas em comum. Elas utilizam soluções técnicas e pontuais de segurança da informação, mas não efetuam ações que possam antecipar os riscos dos quais o ambiente computacional está exposto, como a avaliação de risco para verificar as possíveis vulnerabilidades existentes na organização e melhorar seus controles, a fim de reduzir a probabilidade de ocorrência de um incidente de segurança da informação. As organizações estudadas reconhecem que não utilizam todas as práticas de segurança da informação necessárias para proteção dos seus ativos e que não adotam nenhum padrão de segurança existente no mercado.

As organizações A e B não apresentam uma gestão da segurança da informação adequada, visto que nem todos os aspectos necessários à redução de riscos de segurança da informação são abordados e não há diretrizes e procedimentos formalizados. A gestão da segurança da informação envolve aspectos técnicos, humanos, conformidade legal e o gerenciamento de implementação de políticas e práticas de segurança alinhadas às necessidades do negócio.

Nesta pesquisa, não foram identificadas críticas na literatura que considerassem as práticas de segurança da informação como obrigatórias. A implementação destas está associada às necessidades de proteção das informações empresariais, cuja abrangência é diferenciada de organização para organização. As abordagens teóricas configuram uma discussão sobre a caracterização da segurança da informação. A maior parte dos autores fala sobre a preservação da confidencialidade, integridade e disponibilidade da informação, enquanto alguns acrescentam a autenticidade e o não repúdio.

A segurança da informação é uma área de pesquisa em potencial, já que as organizações precisam proteger as informações para sua sobrevivência e a cada dia surgem novas ameaças. Para realização de trabalhos futuros, sugere-se uma pesquisa mais ampla cobrindo um número maior de organizações ou uma pesquisa setorial. Uma outra sugestão é a avaliação de risco para conhecer as ameaças e a probabilidade de ocorrência de incidentes de segurança da informação, nos quais o ambiente organizacional está exposto.

Esta área de pesquisa torna-se cada vez mais relevante, considerando que se as organizações não utilizarem a segurança da informação de forma mais intensa, pode aumentar as barreiras para que a sociedade se beneficie com os recursos que a TI oferece.

Referências

ABNT – Associação Brasileira de Normas Técnicas. **Tecnologia da Informação – Código de prática para gestão de segurança da informação**. NBR ISO/IEC 17799: 2001. Rio de Janeiro.

BARBOSA, Paulo; COELHO Moacir. **Engenharia Social. A maior das ameaças ao seu negócio**. Disponível em: <www.theprime.com.br/research/artigos/artigo_engsocial.htm>. Acesso em: 09 set. 2004.

BERNSTEIN, T.; BHIMANI, A.; SCHULTZ, E.; SIEGEL, C. **Internet Security for Business**. Ed. John Wiley & Sons, Inc, 1996.

BEUREN, Ilse Maria. **Gerenciamento da Informação: um recurso estratégico no processo de gestão empresarial.** São Paulo, Atlas 1998.

BIO, Sérgio Rodrigues. **Sistemas de Informação: um enfoque gerencial**. Atlas, 1985.

BSI. **Sistema de Gerenciamento da Segurança da Informação – Especificação com guia para uso.** BS 7799-2: 2002**.**

BSI. **Guide to BS7799 Risk Assessment.** Londres, 2002.

CARUSO & STEFFEN. **Segurança em informática e de informações**. Editora Senac, 1999. São Paulo.

CASANAS, Alex. D. G.; MACHADO, César de S. **O Impacto da Implementação da Norma NBR ISO/IEC 17799 – Código de Prática para Gestão da Segurança da Informação – nas Empresas**. 2002. Disponível em: < http://egov.alentejodigital.pt/Page10549/Seguranca/iso17799-1.pdf> Acesso em: 03 ago. 2003.

CAUTELA, A. L.; POLLONI, E. G. F. **Sistemas de informação na administração de empresas**. São Paulo, Atlas 1982.

CAZEMIER, Ing. Jacques A.; OVERBEEK, Ir. Paul L.; PETERS, Louk M. C. **ITIL: Best Practice for Security Management.** Editora: TSO, 1999.

ClO MAGAZINE. **Security. Dr. Crime´s terminal of Doom and other tales of betrayal, sabotage & skullduggery**. 2002. Disponível em: <http://www.cio.com/archive/060102/doom.html>. Acesso em: 23 nov. 2004.

COBIT STEERING COMMITTEE e IT GOVERNANCE INSTITUTE. **Relatório do comitê de Direção 2000.** Disponível em: < http://208.215.18.13/Default.aspx>. Acesso em: 03 abr. 2004

_____. **Control Objectives**. 3ª edição, 2000. Disponível em: <www.isaca. Org> Acesso em: 03 abr. 2004.

_____. **Framework**. 3ª edição, 2000. Disponível em: <www.isaca. Org> Acesso em: 03 abr. 2004

COUTANCHE, Brian J. **Securing Your Information Assets.** Disponível em: <www.coutanche.com/bs7799.html>. Acesso em: 4 Set. 2004

DHILLON, Gurpreet. **Information Security Management: Global Challenges in the New Millennium**. Editora: Idea Group Publishing, 2001.

DOMINGUES, Heron. **A Marcha ao Norte da Governança em TI**. Disponível em:< www.lucinski.com.br/artigos/governanca.pdf>. Acesso em: 03 abr. 2004.

DEPARTAMENT OF TRADE INDUSTRY (DTI). ***Information Security Breaches****. Survey* 2002. Disponível em: <http://www.dti.gov.uk>. Acesso em: 05 out. 2003.

FERNANDES, Jorge Monteiro. **Gestão da Tecnologia como parte da Estratégia Competitiva das Empresas.** Editora Brasília: IPDE, 2003.

Folha de São Paulo On Line. **Correspondência com @ vem da Arpanet.** In disponível em: < http://www1.folha.uol.com.br/folha/informatica/ult124u8217.shl>. Acesso em: 13 out. 2004.

GONÇALVES, Luís Rodrigues de Oliveira. 2003. **Instituições Padronizadoras e Normas de Segurança**. In disponível em: <www.modulo.com.br/index.jsp>. Acesso em: 30 ago. 2004.

GRAEML, Alexandre Reis. **Sistemas de informação: o alinhamento da estratégia de TI com a estratégia corporativa**. Atlas, 2000.

HCI. **Ciclo PDCA**. Disponível em: <www.hci.com.au/hcisite2/toolkit/pdcacycl.htm>. Acesso em: 10 nov. 2004.

ITGI. **Guia do Information Security Governance: Guindance for Boards of Directors and Executive Management**. In disponível em: http://www.itgi.org/template_itgi.cfm?section=Security,_Control_and_Assurance&T. Acesso em 03 jun.2003.

MACHADO, César de S. **Gerenciamento da segurança da Informação em Sistemas de Teletrabalho**. 136f. Dissertação (Mestrado em Engenharia de

Produção) – Programa de Pós-Graduação em Engenharia de Produção – UFSC, Florianópolis. 2002. Disponível em: <http://teses.eps.ufsc.br/defesa/pdf/7469.pdf>. Acesso em: 29 set. 2003.

MCGEE, James; PRUSAK, Laurence. **Gerenciamento Estratégico da Informação**. Editora Campus, 1994.

Módulo Security Solutions. **9ª Pesquisa Nacional de Segurança da Informação**. 2003. Disponível em:<www.modulosecurity.com.br>. Acesso em: 27 nov. 2003.

_____. **Laptop do Ministério de Defesa Britânico está desaparecido**. 2001. In disponível em: <www.modulo.com.br>. Acesso em 27 nov. 2004.

NEGRÂO, Theotonio; GOUVÊA, José Roberto Ferreira. **Código Civil e Legislação Civil em vigor**. São Paulo: Saraiva, 2003.

NIEKERK, Johan; SOLMS, Rossouw V. **Organizational Learning Models for Information Security**. 2004. Disponível em: <www.infosecsa.co.za/proceedings2004/043.pdf>. Acesso em: 21 nov. 2004.

NIST – National Institute of Standards and Technology. **An Introduction to Computer Security. Nist Handbook**. 1995 Disponível em:< http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>. Acesso em: 05 set. 2004.

OLIVEIRA, Salomão. **Segurança da Informação: quando decidir investir**. 2004. In disponível em:<www.modulo.com.br>. Acesso em: 30 ago. 2004.

PEIXOTO, Rodney de Castro. **Implicações da Lei Sarbanes-Oxley na Tecnologia da Informação.** 2003. Disponível em: <www.wirelessbrasil.org/wirelessbr/colaboradores/rodney_peixoto/sarbanes_oxley. html>. Acesso em: 19 set. 2004.

PEIXOTO, Rodney de Castro. **Marcos Divisórios na Segurança da Informação: 11 de Setembro de 2001 e Escândalos Contábeis nos Estados Unidos.** 2004. Disponível em: < http://www.issabrasil.org/artigos_0003.asp >. Acesso em: 25 set. 2004.

PELTIER, Thomas R. **Information Security Policies, Procedures, and Satandards**. Guidelines for Effective Information Security Management. Editora: CRC Press, Auerbach Publications, 2001.

PINHEIRO, Lena V. Ribeiro. **Informação - Esse Obscuro Objeto da Ciência da Informação**. Disponível em: < http://www.unirio.br/cead/morpheus/Numero04-2004/lpinheiro.htm>. Acesso em: 18 nov. 2004.

PINK ELEPHANT. **The ITIL Story White Paper**. 2004. Disponível em: <http://www.pinkelephant.com/aboutus/About_ITIL>. Acesso em 30 out. 2004.

REZENDE, Denis A.; ABREU, Aline F. **Tecnologia da Informação Aplicada a Sistemas de informações Empresariais**. São Paulo: Atlas, 2000.

SWANSON, Marianne; GUTTMAN, Bárbara. General **Accepted Principles and Practices for securiting Information Technology Systems**. US. NIST, 1996. Disponível em: <http://csrc.nist.gov/publications/nistpubs/index.html>. Acesso em: 05 nov. 2004.

WEBOPEDIA 2002. Disponível em: <http:://www.webopedia.com>. Acesso em: 06/09/2004.

WONG, Ken; WATT, Steve**. Managing Information Security. A Non-technical Management Guide.** Editora: Elsevier Science Publishers Ltda, 1990.

Apêndices

Apêndice A – Acordo de confidencialidade

O objetivo deste acordo é assegurar a guarda de sigilo para todas as informações que serão obtidas a partir da realização de uma pesquisa acadêmica sobre a Gestão da Segurança da Informação na empresa A/B.

Pelo presente instrumento, Regina Sá Menezes, Analista de Sistemas, residente à Av. Sete de Setembro 2592, Vitória, Cep: 40.080-001, identidade 4.991.934-23, mestranda em administração pela Universidade Federal da Bahia, responsável e única executora da citada pesquisa propõe, a seguir, os termos do referido acordo:

Da pesquisa:

A pesquisa realizar-se-á por intermédio de entrevistas junto aos quadros técnicos e diretivos da empresa A/B, segundo roteiro, conteúdo e agenda prévios a serem pactuados e, eventualmente, observação de algumas práticas implantadas, com a finalidade de levantar e analisar as práticas de gestão da segurança da informação utilizadas pela organização.

Da confidencialidade:

Comprometo-me a manter sob confidencialidade todas as informações acessadas por intermédio da pesquisa junto a empresa A/B. Adicionalmente, informo que a

mesma será simultaneamente aplicada em outra organização, que os nomes das organizações não serão publicados e que o resultado não distinguirá a qual organização se refere os determinados conjuntos de dados e análises.

Salvador, 28 de julho de 2004

_____

Regina Sá Menezes

Apêndice B – Roteiro para entrevista

Questões norteadoras:

1) Como é a distribuição da responsabilidade da segurança da informação na organização?
2) Qual o orçamento destinado à área de TI e à segurança da informação?
3) Quais são os projetos a serem realizados na área de segurança em 2004?
4) Quais são os obstáculos para implementação de práticas de segurança na sua organização?
5) Existe uma política de segurança? Ela é de conhecimentos de todos, inclusive os terceirizados?
6) O que você considera ameaças para a sua organização?
7) Ocorreram incidentes de segurança nos últimos três anos e quais foram as conseqüências destes para a organização?
8) Quando ocorreu o último incidente de segurança?
9) Quais os prejuízos com problemas de segurança da informação em 2003 (em mil reais)? Quais os responsáveis?
10) Que providências foram adotadas quando houve falha de segurança?
11) Quais são as medidas de segurança já implementadas na organização?
12) Há um plano de continuidade do negócio desenvolvido e implantado? Qual a sua composição?
13) O uso da internet na empresa é restrito ou é permitido para todos, inclusive os terceirizados?

14) Quais são as principais aplicações efetuadas na Internet?