Alexandre Renato Souza Tavares

GESTÃO DA SEGURANÇA DA INFORMAÇÃO E DO CONHECIMENTO CORPORATIVO:

MITIGANDO FRAUDES E RISCOS EMPRESARIAIS

Pedro Leopoldo

2006

Alexandre Renato Souza Tavares

GESTÃO DA SEGURANÇA DA INFORMAÇÃO E DO CONHECIMENTO CORPORATIVO:

MITIGANDO FRAUDES E RISCOS EMPRESARIAIS

Dissertação apresentada ao Curso de Mestrado Profissional em Administração da Fundação Cultural Dr. Pedro Leopoldo como requisito parcial para a obtenção do título de Mestre em Administração.

Orientadora: Prof. Dra. Maria Celeste Reis Lobo de Vasconcelos

Área de Concentração: Gestão da Inovação e Competitividade

Pedro Leopoldo

2006

FICHA CATALOGRÁFICA

6584038 TAVARES, Alexandre Renato Souza
T231g
2006

Gestão da Segurança da Informação e do Conhecimento Corporativo – Mitigando Fraudes e Riscos Empresariais/ Alexandre Renato Souza Tavares.
Pedro Leopoldo : FIPEL, 2006.

146 p.: il.

Dissertação (Mestrado – MPA/FPL, Ma – Área: Administração). FPL; Programa de Pós-graduação, 2006.

1. Gestão da Segurança da Informação. 2. Conhecimento Corporativo. 3. Risco. 4. Fraude 5. Tecnologia da Informação. I. Título. II. Vasconcelos, Celeste, orientadora.

FOLHA DE APROVAÇÃO

Título da Dissertação "GESTÃO DA SEGURANÇA DA INFORMAÇÃO E DO CONHECIMENTO CORPORATIVO: MITIGANDO FRAUDES E RISCOS EMPRESARIAIS."

CANDIDATO: ALEXANDRE RENATO SOUZA TAVARES

Dissertação de mestrado profissionalizante defendida junto ao Programa de Pós-Graduação em Administração das Faculdades Integradas de Pedro Leopoldo, aprovada pela banca examinadora, constituída pelos professores:

Profa. Dra. Maria Celeste Reis Lobo de Vasconcelos

Prof. Dr. Mauro Calixta Tavares

Profa. Dra. Juliana Teixeira do Carmo

Pedro Leopoldo (MG), 25 de agosto de 2006.

Dedico este trabalho a:

Meu pai, **Benedito Tavares**, minha mãe, **Maria Aurora Souza Tavares** (*in memoriam*)**,**

minha tia **Maria Madalena Tavares Jangola** que me criou como verdadeira mãe desde meu primeiro ano de vida,

minha **irmã Heloísa,** e meus primos-irmãos **Beth, Cléber** e **Welton**,

por me proporcionarem um lar e uma família que tinha por base a fé, a educação, a solidariedade, o amor, a humildade e a perseverança na busca de meus objetivos.

AGRADECIMENTOS

Agradeço a **DEUS** em primeiro lugar por me dotar das capacidades necessárias e colocar em meu caminho pessoas e eventos que direta ou indiretamente fizeram parte da construção dessa dissertação. E também:

Em especial à professora e orientadora **Dra. Celeste Vasconcelos** que, com o seu conhecimento sua objetividade e, sobretudo, sua tolerância e paciência, contribuiu indubitavelmente para a realização dessa dissertação.

Ao professor e co-orientador **Dr. Mauro Calixta Tavares**, cujas recomendações foram cruciais para a realização dessa dissertação.

Ao coordenador do curso de Ciência da Computação da Fundação Cultural Dr. Pedro Leopoldo, **Prof. Júlio César Lopes**, pela sua consideração pessoal e apoio ao desenvolvimento deste trabalho.

À Fundação Cultural Dr. Pedro Leopoldo e a todos os **professores** que colaboraram no aperfeiçoamento da educação nesse estabelecimento.

Àqueles que direta ou indiretamente contribuíram para este trabalho com idéias, sugestões, críticas e apoio moral.

Ao colega e amigo **Luís Rabelo**, pelo incentivo, aval e conselhos na realização deste trabalho; sem eles eu não ingressaria no Mestrado e esta dissertação não teria sido realizada.

Aos meus colegas e amigos de mestrado **Demian, Fábio, Gilberto, Matheus**, **Mosqueira** e **Vinícius** pelas discussões construtivas e sugestões proveitosas que me ajudaram a vencer os desafios deste Mestrado.

Ao meu amigo **Thiago Lopes** pela amizade sincera pelo apoio técnico, pelas dicas e incentivo sobretudo na reta final do trabalho.

Finalmente, gostaria de agradecer à **Companhia Vale do Rio Doce** e, em particular, à **Gerência de Segurança Empresarial**, nas pessoas de **Roger**, **Roberto** e **Oscar** e, em especial, ao **André** e ao **Melhado** do **Corporativo**, pelo importante suporte no fornecimento de documentos e referências para a análise documental.

“Senhor, eu não sou digno que entreis em minha morada, mas dizei uma só palavra e serei salvo”. Bíblia – Mateus, 8:8.

Tudo que somos está baseado em nossos pensamentos e é formado por eles. Tudo que somos é resultado daquilo que pensamos. Pessoas especiais são as que percebem que a força espiritual é infinitamente mais poderosa que qualquer força material, pois os pensamentos governam a vida.
ALEXANDRE RENATO SOUZA TAVARES (2006)

RESUMO

Este estudo teve por objetivo identificar e analisar a situação das fraudes e da segurança da informação e dos conhecimentos corporativos no Brasil, identificar metodologias e modelos de gestão e verificar se o emprego destes contribui para a mitigação das fraudes empresariais. Para isso, a pesquisa em pauta caracteriza-se como, aplicada e qualitativa. A perspectiva da pesquisa constitui categorias de análise e foram investigadas ao longo dos últimos três anos. Os dados foram coletados por meio de análise documental, pesquisa bibliográfica, observação livre e participante. O tratamento dos dados é predominantemente qualitativo. Para análise do fenômeno, objeto do trabalho, foram utilizadas duas pesquisas: A primeira foi a pesquisa 2004 KPMG sobre A Fraude no Brasil que com base em entrevistas com diretores e presidentes de empresas no Brasil, fornece uma visão abrangente acerca das percepções, das verdades e dos impactos das fraudes no mundo dos negócios. A fraude - desde o simples furto de ativos até manipulações financeiras e contábeis complexas - continua a ser uma questão relevante e tem se tornado cada vez mais importante aos olhos de investidores, administradores de empresas, órgãos reguladores e outros participantes do mercado. A segunda foi a Pesquisa Nacional de Segurança da Informação em sua 9ª edição. Neste estudo, considerado um dos importantes norteadores do segmento no Brasil, é apresentado um panorama da segurança da informação atualizado contendo as principais tendências do mercado nacional, indicadores e melhores práticas. O estudo revelou, após a análise e interpretação dos dados coletados, que os resultados obtidos reforçam a importância dos fatores de capacitação e conscientização como pontos fundamentais para proteção das informações corporativas. Para tornar essa constatação realidade é necessária a contínua adoção de controles para mitigar ameaças, riscos e vulnerabilidades que rondam o ambiente corporativo. Diante desse cenário, pôde-se concluir, nitidamente, que a análise dos resultados obtidos nas pesquisas sobre segurança da informação e fraudes empresariais no Brasil. O envolvimento de toda a organização neste processo é muito importante e deve ser um esforço corporativo no qual o elemento humano é fator crítico e peça fundamental. A resposta para tornar essas constatações realidade pode estar na contínua adoção de controles e medidas de gestão da segurança da informação e dos conhecimentos corporativos para mitigar ameaças, riscos e vulnerabilidades que rondam as organizações num mundo rápido e globalizado como o de hoje. Para amenizar ou mudar essa situação, o estudo sugere algumas das melhores práticas de gestão da segurança da informação e dos conhecimentos corporativos, com base no referencial teórico, na análise documental e nas observações do autor desta dissertação.

ABSTRACT

The objective of this study was to identify and to analyze the situation of the frauds and the information security and the corporative knowledge in Brazil, to identify methodologies and models of management and to verify if the application of these contribute for the mitigating of the enterprise frauds. For this, the research in guideline is characterized as, applied and qualitative. The perspective of the research constitutes categories of analysis and had been investigated during the last three years. The data had been collected by means of documentary analysis, bibliographical research, free and participant comment. The treatment of the data is predominantly qualitative. For analysis of the phenomenon, object of the work, had been used two research: The first was the research 2004 KPMG about Frauds in Brazil that with base in interviews with directors and presidents of companies in Brazil, supplies an including vision concerning the perceptions, of the truths and of the impacts of the frauds in the businesses world. The fraud - from the simple theft of assets to complex financial and accounting manipulations - continues to be a relevant subject and turned more and more important to the investors' eyes, companies managers, regulators organs and other market participants. Laws and regulations, national and international, more and more demanding are forcing the companies to prioritize the governance with the objective of to generate credibility and to encourage investments in stock markets. The penalties for the transgression of the rules are severe and, therefore, to identify and to answer the fraud cases keep as continuous challenges even for the most sophisticated companies. However, as that research demonstrates, frauds can be mitigated by the implementation of effective controls and information security and corporate knowledge management. The second one was the National Research of Information Security in its 9th edition. In this study, considered one of the most important guidelines of the segment in Brazil, is presented the updated status of the information security containing the main tendencies of the national market, indicators and best practices. The study revealed, after the analysis and interpretation of the collected data, that the obtained results reinforce the importance of the training factors and understanding as fundamental points for protection of the corporate information. To turn that verification reality is necessary the continuous adoption of controls to mitigate threats, risks and vulnerabilities that involve the corporate atmosphere. In front of that scenery, it could be ended, sharply, that the analysis of the obtained results in the researches about information security and business frauds in Brazil. The involvement of full organization in this process is very important and it should be a corporate effort in which the human element is critical factor and fundamental piece. The answer to turn those verifications reality could be in the continuous adoption of controls and measures of management of the information security and corporate knowledge to mitigate threats, risks and vulnerabilities that patrol the organizations in a fast and global world as today. To easy or to change that situation, the study suggests some of the best practical about management information security and corporate knowledge, with base in the reference theoretical, in the documental analysis and in the author's of this dissertation observations.

LISTA DE ABREVIATURAS E SIGLAS

ABNT	- Associação Brasileira de Normas Técnicas
BS	- British Standard
BIOS	- Basic Input Output System
BSC	- Balanced Scorecard
CIO	- Chief Information Officer
COBIT	- Control Objectives for Information and Related Technology
ERP	- Enterprise Resource Planning
ITGI	- Information Technology Governance Institute
ITIL	- Information Technology Infrastructure Library
ISACA	- Information System Audit and Control Association
ISO	- International Organization for Standardization
JIT	- Just-in-time
MRP	- Engineering Materials Requirements Planning
PKI	- Primary Key Infrastructure
PSD	- Personal Secure Drive
NIST	- National Institute of Standards and Technology
TI	- Tecnologia da Informação
TPM	- Trusted Platform Module

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

Nas últimas duas décadas, especialmente nos últimos anos, presenciou-se grandes evoluções no mundo dos negócios, as quais afetaram profundamente a vida das organizações e o modo como funcionam. A hostilidade ambiental decorrente dos níveis crescentes de dinamismo e incerteza vem provocando, de forma contínua, profundas transformações na conduta administrativa, especialmente a velocidade da evolução tecnológica, que gera a rápida obsolescência de produtos e serviços. É a sociedade da informação substituindo a sociedade industrial e criando novas estruturas sociais; é a valorização do capital humano e do conhecimento como principal ativo das empresas; é a tecnologia da informação desmantelando a burocracia de anos; são as novas relações de trabalho; é a organização de especialistas baseada em informações (Caldas e Hernandez, 2001).

> O *modus operandi* da sociedade pós-industrial identifica-se com o da sociedade da informação. Trata-se de um modo de desenvolvimento social e econômico em que a aquisição, armazenamento, processamento, valorização, transmissão, distribuição e disseminação da informação conducente à criação de conhecimentos e à satisfação das necessidades dos cidadãos e das organizações desempenham um papel central na atividade econômica, na criação de riqueza, na definição da qualidade de vida dos cidadãos e das suas práticas culturais (Livro Verde para a Sociedade da Informação em Portugal: http://www.missao-si.mct.pt/livroverde/lvfinal.zip)

O emprego destas técnicas como práticas de gestão é um forte fator que promove mudanças na forma de planejar, usar e extrair benefícios da informação, colocando em risco os conhecimentos corporativos, que são a única fonte capaz de gerar vantagem competitiva sustentável (DAVENPORT e PRUSAK, 1998, p. 20).

Uma vez que a sobrevivência da organização está diretamente relacionada à sua capacidade de manutenção da competitividade, a busca incessante de informações sobre as variáveis do ambiente externo que podem influenciar o rumo dos negócios tornou-se uma atividade fundamental. É nesse cenário que a gestão da segurança da informação firma-se como um processo indispensável à mitigação dos riscos empresariais e a conseqüente sobrevivência e manutenção de competitividade da organização.

A gestão da segurança da informação e dos conhecimentos corporativos é um processo que ganha importância cada vez maior dentro das empresas, tornando-se ferramenta de apoio indispensável em diversos níveis organizacionais, como planejamento estratégico, marketing, programas de gestão do conhecimento, entre outros.

Segredos de negócio, análise de mercado e da concorrência, dados operacionais históricos e pesquisas são informações fundamentais e se revelam como um importante diferencial competitivo ligado ao crescimento e à continuidade do negócio. (SÊMOLA, 2003).

Permitindo proteger todos esses conhecimentos e evitando que “caiam” em mãos erradas, os conceitos de gestão de segurança da informação e conhecimentos corporativos, e suas técnicas respectivas, ocupam um lugar essencial. Hoje é necessário dominar estes conceitos e técnicas de modo a adotar o que há de melhor nas práticas internacionalmente aceitas. As transformações ocorridas no ambiente globalizado de negócios e a emergência do modelo empresarial competitivo, enfatizando a importância do planejamento estratégico e a

necessidade permanente de reunir e processar informações culminaram na construção de um padrão atual que adota sempre uma visão por análise de risco empresarial.

As tendências e desafios impostos pela economia da informação, associados ao panorama tecnológico atual, avalizam a realização deste trabalho de pesquisa, visando compreender o caráter estratégico da gestão da segurança da informação e da proteção dos conhecimentos corporativos na mitigação de fraudes e riscos empresarias que, segundo Moreira (2001), são a base para dar às empresas a possibilidade e a liberdade necessárias para a criação de novas oportunidades de negócio. Diante deste cenário, o tema de estudo desta dissertação é oportuno e atual.

1.2 Problema de Pesquisa

Com o advento da globalização e a instauração de intensa competição internacional, e com vistas a garantir a continuidade no mundo dos negócios, é condição essencial decidir com acerto e precisão. No mundo globalizado, essa assertiva ainda é mais contundente, pois as tecnologias avançam em velocidade surpreendente e as mudanças e quebras de paradigma ocorrem com maior freqüência, gerando novos desafios, que estão relacionados com:

- Disposição para adotar novas tecnologias e mudar os procedimentos de trabalho;
- Habilidade para converter conhecimentos corporativos em ações e produtos lucrativos;
- Capacidade de mudar rapidamente, em função dos diversos atores do mercado como novos produtos, nova legislação, pressão de organizações não-governamentais, perdas econômicas, etc.

De acordo com Oliveira (2001, p.9), “a segurança da informação é um item complexo e pode abranger várias situações, como erro, displicência, ignorância do valor da informação, acesso indevido, roubo, fraude, sabotagem, causas da natureza, etc.”. Oliveira (2001, p.9) “ainda define Segurança das Informações como o processo de proteção de informações e ativos digitais armazenados em computadores e redes de processamento de dados.”

Levando-se em consideração as informações e os conhecimentos corporativos, atualmente é notório e consensual que o ativo mais valioso e estratégico para as empresas são as informações e os conhecimentos corporativos que seus colaboradores possuem e criam em favor dos objetivos empresariais. Por si só, esta premissa reforça a importância da avaliação dos riscos e da conscientização dos colaboradores como pontos fundamentais para proteção das informações e conhecimentos corporativos como forma de garantir a permanência e o sucesso no mundo dos negócios em um ambiente de elevada competição e incertezas.

As informações e o conhecimento produzidos pelas organizações são ativos estratégicos que têm muito valor de mercado. Por conseguinte, necessitam ser adequadamente protegidos. A segurança destes ativos contra diversos tipos de ameaças é condição imprescindível para o sucesso empresarial. A análise dessas variáveis remete à problemática dessa pesquisa, que pode ser definida com o seguinte questionamento: COMO A GESTÃO DA SEGURANÇA DAS INFORMAÇÕES E DOS CONHECIMENTOS CORPORATIVOS PODE MITIGAR AS FRAUDES E OS RISCOS EMPRESARIAIS?

1.3 Objetivo Geral

O objetivo geral deste presente trabalho de pesquisa foi determinar como a gestão da segurança das informações e conhecimentos corporativos proporciona mitigação das fraudes e dos riscos empresariais.

1.4 Objetivos Específicos

Foram considerados como objetivos específicos deste estudo os seguintes:

- Pesquisar os conceitos associados à segurança da informação e dos conhecimentos;

- Identificar os controles presentes na norma de segurança da informação NBR ISO/IEC1779 necessários para a redução dos riscos a um nível aceitável;

- Identificar o que é e o que não é fraude computacional.

1.5 Justificativa

Cada vez mais a informação e o conhecimento vêm se tornando o ativo mais importante das organizações e, para protegê-las, medidas estritamente técnicas não são suficientes. Por essa razão, este trabalho visa esclarecer e ajudar no entendimento da importância da segurança da informação dentro de um contexto corporativo de risco. Esta dissertação pretende determinar como a gestão da segurança da informação e do conhecimento corporativo proporcionam meios para mitigar os riscos empresariais.

A tecnologia continuamente impõe maiores demandas às empresas para manter o processo e comunicar a informação. A segurança desta informação, com relação à confidencialidade, integridade e disponibilidade, é de vital importância para estas empresas. No entanto, é difícil para as mesmas mensurar o valor da informação em termos financeiros e, por conseguinte quanto investir em segurança da informação.

Nos últimos 50 anos, as organizações de um modo geral passaram por um processo generalizado de transformação do foco das atividades, passando de um cenário tipicamente centrado na produção para um competitivo cenário onde predomina a prestação de serviços. Embora muitos elementos tenham contribuído para essa transformação, dois objetos tecnológicos aparecem como determinantes do seu desenvolvimento: telecomunicação e computação. Apoiados nestes objetos tecnológicos, a informação e o conhecimento que sempre foram elementos determinantes do crescimento econômico e da capacidade produtiva. Desencadearam uma verdadeira revolução impondo novos paradigmas, novas possibilidades e novos problemas para muitas atividades.

No novo milênio, uma nova economia surgiu em escala global. No passado, o diferencial competitivo das empresas estava centrado no estabelecimento de funções bem desenvolvidas e administradas, criando um padrão de excelência operacional. Hoje, a informação e o conhecimento fazem a diferença, e não adianta apenas detê-los; é preciso saber gerenciá-los e protegê-los.

Nesse contexto, a proteção dos conhecimentos corporativos e a segurança da informação trazem os conceitos e a metodologia necessários para que as empresas não apenas sobrevivam às turbulências dos mercados e da competição mas também adquiram vantagens competitivas que permitam a sua evolução.

A gestão da informação para Tarapanoff (2001) tem como objetivo identificar e potencializar os recursos informacionais de uma organização. A criação da informação,

aquisição, armazenamento, análise e difusão constitui a estrutura para suportar o crescimento e o desenvolvimento da organização inteligente, devidamente adaptada às exigências do ambiente em que se encontra.

A noção de segurança da informação foi derivada de um contexto militar e governamental, definida como o esforço organizado e sistemático para coletar informações, avaliar cuidadosamente e juntar até formar uma idéia clara das coisas que estão para acontecer (KELLEY, 1968).

A segurança da informação é a resposta aos desafios da globalização. Em face disso, é oportuno conhecer os conceitos intrínsecos a ela, bem como a avaliação de riscos empresariais, suas potencialidades e possíveis formas de mitigação de seus efeitos através da implantação e estruturação de uma política de segurança da informação em uma organização empresarial que ofereça condições dessa organização manter e ampliar a sua competitividade.

O cumprimento dos objetivos desta dissertação deverá representar uma contribuição para o tema e o meio profissional. Com o conhecimento das técnicas e estratégias de segurança da informação, pode-se determinar quais de suas características e procedimentos contribuem na mitigação dos riscos e conseqüentemente proporcionam a superação de ameaças além da manutenção da vantagem competitiva na Era da Informação.

Após conclusão dessa dissertação, a divulgação dos resultados em congressos, revistas, jornais, e sítios na internet, poderá contribuir para o empresariado brasileiro, sinalizando que quando se pratica a gestão da segurança da informação e dos conhecimentos corporativos adotando medidas que objetivem a proteção destes importantes ativos corporativos, as fraudes e o risco empresarial tendem a diminuir, oferecendo, assim, melhores condições para as organizações manterem e ampliarem a sua competitividade.

1.6 Estrutura da Dissertação

A dissertação está estruturada e subdividida em capítulos, como se apresenta:

Capítulo I Introdução: Contextualização, Problema da Pesquisa e Estrutura do Trabalho, Objetivo Geral, Objetivos Específicos e Justificativa.

Capítulo II Referencial Teórico: Aborda os seguintes assuntos: A importância da informação, fraude computacional, análise de riscos, o ITIL (*Information Technology Infrastructure Library*), o COBIT (*Control Objectives for Information and related Technology*), a norma ISO/IEC 17799 e a Segurança da Informação.

Capítulo III Procedimento Metodológico: Composto de três etapas, assim denominadas: Caracterização, Universo (Unidade de Análise) e Procedimentos de Obtenção de Dados.

Capítulo IV Análise Documental: Consiste na análise sobre duas pesquisas de âmbito nacional realizadas junto às maiores empresas no ambiente corporativo brasileiro, sendo a primeira sobre a fraude e a segunda sobre a segurança da informação.

Capítulo V Sugestões de Melhores Práticas: São sugeridas as melhores práticas para a implantação da gestão da segurança das informações e dos conhecimentos corporativos.

Capítulo VI Conclusões: são apresentadas as conclusões desse estudo.

Referências: São listadas todas as referências utilizadas.

Anexos: Anexo 1: Detalhamento dos objetivos e dos controles das onze seções de controle da norma ABNT NBR ISO/ IEC 17799:2005 (Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação).

2 REFERENCIAL TEÓRICO

2.1 A Importância da Informação e do Conhecimento

A informação é a base para dar às empresas a possibilidade e a liberdade necessárias para a criação de novas oportunidades de negócio. As novas tecnologias tornam os negócios cada vez mais dependentes destas que, por sua vez, necessitam imprescindivelmente inovar sempre além de proporcionar confidencialidade, integridade e disponibilidade às suas informações e conhecimentos corporativos.

Para Vasconcelos (2000),

> "...a conversão de novos conhecimentos em novos produtos é um processo extremamente complexo e que o processo de inovação exige conhecimentos de várias fontes, tanto internas como externas às empresas, toda inovação significativa é feita através de um longo caminho de contribuições técnicas e científicas provenientes de usuários, empresas, universidades e instituições de pesquisa, sendo quase impossível considerar que a inovação possa depender de apenas um indivíduo ou organização..."

A informação é um ativo, entre outros ativos, de extrema importância nos negócios. A informação deve ser protegida, de maneira que não ocorra a possibilidade de acessos não autorizados, alterações indevidas ou sua indisponibilidade.

Quando a alta gestão empresarial desperta para a importância e a relevância da informação para os negócios, medidas concretas são tomadas para estender esta consciência

aos processos, produtos e funcionários. Estes por sua vez, serão os responsáveis por gerar conhecimento a partir dessas informações.

O conhecimento será cada vez mais um fator de competitividade importante, mas o conhecimento é diferente de qualquer outro tipo de recurso, pois ele se torna constantemente obsoleto, e o conhecimento avançado de hoje poderá não ter importância amanhã (DRUCKER, 1997).

Para Nonaka e Takeuchi (1997), conhecimento é também um processo que se cria e que se renova, e a TI tem contribuído para agilizar esta renovação, de forma cada vez mais dinâmica. Este conhecimento, estruturado, atualizado e corretamente protegido com uma política de segurança da informação, é uma grande vantagem competitiva em um mundo globalizado e rápido como o de hoje.

Segundo Castells (2001), a produtividade e a competitividade dos agentes na nova economia dependem de sua capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos. A base material para essa nova economia é fornecida pela revolução da tecnologia da informação, estabelecendo um novo paradigma organizado em torno de tecnologias mais flexíveis e poderosas, possibilitando que a própria informação se torne o produto do processo produtivo.

Informação e conhecimento sempre foram elementos determinantes do crescimento econômico e da capacidade produtiva. Os padrões de vida alcançados nos vários estágios de desenvolvimento foram frutos da evolução tecnológica. Nas últimas duas décadas, uma nova economia surgiu em escala global.

A produtividade e a competitividade dos agentes na nova economia dependem de sua capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos. A base material para essa nova economia é fornecida pela revolução da tecnologia da informação, estabelecendo um novo paradigma organizado em torno de

tecnologias mais flexíveis e poderosas, possibilitando que a própria informação se torne o produto do processo produtivo. (CASTELLS, 2001).

A informação e o conhecimento são patrimônio para as empresas, hoje estes verdadeiros ativos são cobiçados pelos concorrentes que muitas vezes através de meios não éticos como fraudes tentam obter essas informações e conhecimentos estratégicos com vistas a conquistar ou neutralizar a vantagem competitiva.

2.2 Segurança da Informação

De acordo com Oliveira (2001 p.9), “a segurança da informação é um item complexo e pode abranger várias situações, como erro, displicência, ignorância do valor da informação, acesso indevido, roubo, fraude, sabotagem, causas da natureza, etc.”. Oliveira (2001, p.9) ainda define Segurança das Informações como “o processo de proteção de informações e ativos digitais armazenados em computadores e redes de processamento de dados”.

Após os acontecimentos de 11 de setembro de 2001 no *Word Trade Center*, o assunto segurança tem ganhado cada vez mais popularidade. É como se todos estivessem envolvidos de um jeito ou de outro. A segurança transformou-se em área interdisciplinar e em uma necessidade absoluta através dos tempos. Até bem pouco tempo atrás, somente técnicos especializados tratavam da segurança em todos os níveis.

No entanto, hoje em dia, mesmo pessoas que não desempenham atividades técnicas trabalham em assuntos ligados à segurança, fazendo com que a segurança deixe de ser uma área especializada e minoritária. Sua natureza agnóstica foi perdida. Uma de suas evoluções

mais importantes é o envolvimento de várias ciências que devem trabalhar juntas e cooperar umas com as outras.

Para Oliveira (2003, p.9), a segurança não é uma questão técnica, mas uma questão gerencial e humana. Não adianta adquirir uma série de dispositivos de hardware e software sem treinar e conscientizar o nível gerencial da empresa e todos os seus funcionários.

É importante destacar que há várias definições sobre segurança da informação, e há conflitos de conceitos na literatura com relação aos pontos básicos para sua garantia.

Há diversas metodologias e ferramentas que, aliados aos conceitos apresentados, permitem uma definição e um estudo muito amplo de riscos e da segurança da informação. A seguir, serão detalhados alguns destes conceitos.

A segurança da informação deve ser implantada em todas as áreas da organização, uma vez que as informações são encontradas em diversos meios como: impresso ou escrito em papel, armazenado eletronicamente, enviado pelo correio ou através de meios eletrônicos.

A segurança da informação, conforme mostrado na FIG. 1, tem como objetivo a preservação de três princípios básicos, pelos quais se norteia a implementação desta prática:

CONFIABILIDADE – Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas. (SÊMOLA, 2003, p.45).

INTEGRIDADE – Toda a informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais. (SÊMOLA, 2003, p.45).

DISPONIBILIDADE – Toda a informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade. (SÊMOLA, 2003, p.45).

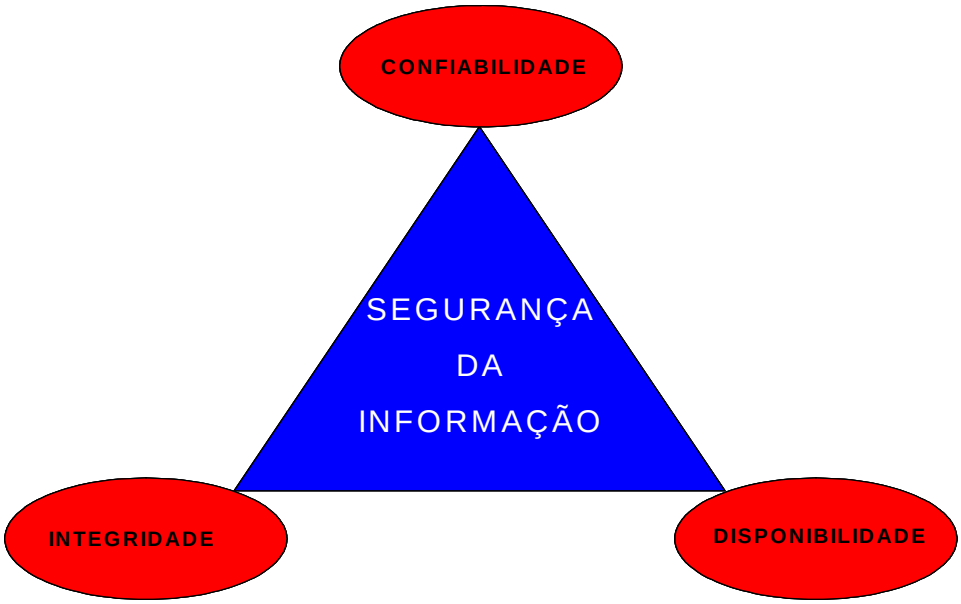

Figura 5: Conceitos Básicos da Segurança da Informação
Fonte: Adaptado pelo autor deste trabalho a partir de Oliveira, 2001, p. 9-10.

O processo de gestão da segurança da informação e dos conhecimentos corporativos deve contemplar todos os processos críticos do negócio. Como resultado, espera-se que um trabalho dessa natureza possibilite que os investimentos efetuados consigam:

- Reduzir a probabilidade de ocorrências de incidentes de segurança;
- Reduzir danos e perdas ocasionados por incidentes de segurança;
- Viabilizar a continuidade dos negócios em casos de desastre e/ ou incidente;
- Recuperar o negócio em casos de desastre e/ou incidente.

Nos tópicos seguintes serão apresentados vários conceitos diretamente relacionados ao objeto de pesquisa.

2.2.1 Ativo

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente precisa ser protegido de forma adequada. Segundo Dias (2000), a informação é o principal patrimônio da empresa e está em constante risco. A informação pode ser tão vital que o custo de sua integridade, qualquer que seja, pode ser menor que o custo de não dispor dela adequadamente.

O termo “ativo” possui esta denominação oriunda da área financeira, por ser considerado um elemento de valor para o indivíduo ou organização, e que, por esse motivo, necessita de proteção adequada.

Todo elemento que compõe os processos, incluindo o próprio processo, que manipula e processa a informação, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.

A gestão da informação tem como objetivo identificar e potencializar os recursos informacionais de uma organização. A criação da informação, aquisição, armazenamento, análise e difusão constituem a estrutura para suportar o crescimento e o desenvolvimento da organização inteligente, devidamente adaptada às exigências do ambiente em que se encontra (TARAPANOFF, 2001).

Existem muitas formas de dividir e agrupar os ativos para facilitar seu tratamento. Uma delas é: equipamentos, aplicações, usuários, ambientes, informações e processos. Desta forma, torna-se possível identificar melhor as fronteiras de cada grupo, tratando-os com especificidade e aumentando qualitativamente as atividades de segurança. (SÊMOLA, 2003, p. 45 e 46).

Porém, no que se refere à segurança da informação, as ações das empresas ainda são controversas e, muitas vezes, ainda deixam a desejar, tendo em vista todas as possibilidades de riscos aos quais estes ativos estão submetidos.

2.2.2 Certificação Digital

A Certificação Digital está se proliferando devido à necessidade da implantação de serviços on-line que possibilitem opções ágeis e confiáveis quando de uma transação efetuada pela Internet, envolvendo questões de extrema importância e sigilo (MÓDULO SECURITY MAGAZINE, 2002). Ela nos garantirá que as operações possam ser efetuadas de modo que a integridade e a autenticidade das informações permaneçam intactas.

A Certificação Digital pode ser definida como um processo eletrônico que visa garantir a integridade e a autenticidade de um determinado processo ou documento. Tecnicamente, o Certificado Digital é um arquivo de computador que faz a identificação de uma pessoa. Ele é um documento emitido por uma Autoridade Certificadora e serve para garantir a autenticidade e a inviolabilidade de mensagens trafegadas pela Internet. Ainda permite enviar e-mails assinados digitalmente e/ou criptografados.

O certificado consiste de um par de senhas, uma de conhecimento público (chave pública) e outra de conhecimento exclusivo da pessoa a ser certificada (chave privada). O Certificado Digital realiza 4 itens básicos: a identificação das partes envolvidas em uma transação, garantia da integridade, o sigilo e a impossibilidade de repúdio.

2.2.3 Criptografia

A criptografia é o ato da transformação de informação numa forma aparentemente ilegível, com o propósito de garantir a privacidade, ocultando informação de pessoas não-autorizadas.

Através da criptografia, os dados são codificados e decodificados, para que os mesmos sejam transmitidos e armazenados sem que haja alterações realizadas por terceiros não-autorizados. Como a Certificação Digital, o principal objetivo da criptografia é prover uma comunicação segura, garantindo confidencialidade, autenticidade, integridade e a não-repudiação (NAKAMURA, 2002).

Existem duas possibilidades de encriptação de mensagens por códigos ou cifras. Por códigos, o conteúdo das mensagens é escondido através de códigos predefinidos entre duas partes. Este tipo de solução tem dois grandes problemas: a facilidade de deciframento devido ao intenso uso dos códigos e o envio de apenas mensagens predefinidas.

Existe um outro método, a cifra, em que o conteúdo da mensagem é cifrado através da mistura e/ou substituição das letras da mensagem original. A mensagem é decifrada, fazendo-se o processo inverso ao ciframento. As cifras consistem na implementação de longas seqüências de números e/ou letras que determinarão o formato do texto cifrado através de algoritmos associados a chaves.

Este tipo de criptografia se baseia na classificação quanto ao número de chaves utilizadas, simétrica e assimétrica. Na criptografia simétrica (GRAFF, 2000), o poder da cifra é medido pelo tamanho da chave; geralmente as chaves de 40 bits são consideradas fracas e as de 128 bits ou mais, as mais fortes. Exemplos de algoritmos: DES, Triple DES, RC4 e IDEA.

Neste caso, é utilizada uma única chave secreta, que é compartilhada pelo emissor e pelo receptor.

Na criptografia assimétrica, são utilizados dois tipos de chaves, chave pública e chave privada, em que a criptografia da mensagem é feita utilizando a chave pública e a decriptografia é realizada com a chave privada, ou vice-versa. Os algoritmos utilizam métodos baseados na fatoração de números primos, como, por exemplo, o RSA.

2.2.4 Engenharia Social

Engenharia Social de acordo com Oliveira (2001, p. 6) é o termo que designa a prática de obtenção de informações por intermédio da exploração de relações humanas de confiança, ou outros métodos que enganem usuários e administradores de sistemas.

Para Vargas (2002), engenharia social é o ato de forjar, enganar pessoas e sociedades a respeito de algum assunto, a fim de se aproveitar, lucrar ou apropriar de direitos alheios. Serve para a obtenção de informações importantes de uma empresa, através de seus usuários e colaboradores por meio da ingenuidade ou confiança. Estes ataques geralmente são realizados através de telefonemas, correio eletrônico, salas de bate-papo e até mesmo pessoalmente (GARVEY, 2002).

Os ataques de engenharia social são realizados tipicamente, fazendo-se passar por um usuário autorizado para tentar ganhar o acesso ilícito aos sistemas. Também são feitos iludindo os responsáveis por liberação de acesso baseada na confiança. Indivíduos de má-fé se aproximam de certas pessoas e começam a vasculhar assuntos a fim de que, através de suas

próprias palavras, o invasor recolha requisitos necessários para a prática de algo não legal sem a permissão da vítima.

Muitas invasões de sistemas de grande porte já foram ocasionadas por meio de vítimas desta técnica, que consiste em apenas uma ligação a um usuário comum se passando por suporte técnico, relatando que estão com problemas de senhas e que o usuário terá que testar a sua senha em algum lugar já pré-configurado para recolher o *login* e a senha do usuário. A partir daí, o invasor irá se desfrutar do sistema como um usuário autenticado.

Este tipo de ataque se apega a fatores emocionais e amorosos, confundindo assuntos profissionais e pessoais e se aproveitando da atração afetiva. Outra técnica bastante difundida é a realizada pelo vasculhamento e análise de lixos convencionais e digitais. Como se trata de ataques que utilizam técnicas psicológicas, a solução acaba sendo um pouco desgastante e de difícil manipulação, de forma psicológica, oferecendo palestras aos funcionários, alertando-os e conscientizando-os do assunto.

A maioria dos *hackers* utiliza heurísticas de manipulação aliadas com seu conhecimento técnico para a invasão de grandes sistemas. Segundo noticiou o jornal *THE NEW YORK TIMES* do dia 10 de junho de 2006, um *hacker* de computador roubou informação sensível sobre 1.500 pessoas que estavam trabalhando para a unidade de armas nucleares do Departamento de Energia dos Estados Unidos. Mas nem as vítimas do roubo nem os altos oficiais foram notificados por nove meses. A revelação da falha e o fato de que o Secretário de Energia e seus maiores auxiliares não souberam do ocorrido por meses causou indignação em uma audiência do sub-comitê de fiscalização e investigação do Comitê de Comércio e Energia do congresso.

2.2.5 *Hackers*

A definição correta de "hackers" é: Indivíduos que criam e modificam software e hardware de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas. Originário do inglês, o termo é usado em português sem modificação. Freqüentemente, utilizadores maliciosos têm sido designados *hackers* pela imprensa, quando na realidade estes seriam mais corretamente classificados entre *crackers*. (WIKIPEDIA, 2006).

Outra definição de "*hacker*" é: uma pessoa que, por fins próprios, se interessa exageradamente por assuntos relacionados à informática (sistemas operacionais, redes e afins). Utiliza seu conhecimento avançado para descobrir falhas e vulnerabilidades de segurança. Erroneamente, o termo "*hacker*" passou a ser usado para qualquer pessoa que efetuasse algum tipo de crime cibernético. (OTILIO, 2000).

O termo "*cracker*" é o correto nome para alguém que utiliza seus conhecimentos para quebrar a segurança, ganhar acesso a sistemas de outras pessoas, sem a devida permissão, e cometer estragos nos mesmos. Ou seja, o "*cracker*" é um "*hacker*" atuando negativamente.

Com a evolução das tecnologias, ocorreu uma mudança no perfil dos "*crackers*" e dos "*hackers*". Antes, eles eram pessoas com alto grau de conhecimento em informática (sistemas operacionais, redes e tecnologia em geral).

> Etimologicamente relacionado com o verbo cortar das línguas germânicas, o termo desenvolveu-se vindo a ser associado ao ato de modificar algo para realizar funcionalidades que não as originais. As atividades de um inventor ou mecânico seriam o equivalente de *hacking* ("*hackear*") na língua portuguesa.
>
> A utilização moderna, relacionada com a informática, terá surgido na década de 60 entre os estudantes do MIT, que a usavam para designar sucessos em determinadas áreas, fosse como uma solução não particularmente elegante para um problema, uma partida inteligente pregada a alguém, ou o ligar os sistemas informáticos e telefônicos para fazer chamadas grátis. Eventualmente, o termo passou a ser utilizado exclusivamente nas áreas da programação ou eletrônica, em que passou a ser usado para designar indivíduos que demonstravam capacidades excepcionais nestes campos, efetivamente expandindo-os com atividades práticas.
>
> Fora do contexto especializado, o termo encontra-se geralmente associado à prática de atividades maliciosas e criminosas, como invasão de computadores, furto de informações, depredação de *sites*, entre outros. Esta associação é frequentemente criticada por várias comunidades (notavelmente pelos grupos produtores de software livre), que usam o termo para distinguir os seus principais programadores. Não estando estes ligados a atividades ilícitas, impõe-se uma distinção.
>
> Equivocadamente o termo *hacker* é usado referindo-se a pessoas relativamente sem habilidade em programação e sem ética, que quebram a segurança de sistemas, agindo ilegalmente e fora da ética *hacker*. O problema quando os *crackers* e *script kiddies* são referidos como *hackers* pela imprensa, por falta de conhecimento, e com isto gerando uma discussão sem fim. (WIKIPEDIA, 2006).

Devido à grande facilidade de troca de informações pela Internet, qualquer pessoa passou a ter acesso a informações sobre segurança. Outro fator muito importante foram as ferramentas (de console ou gráficas) criadas por "*hackers*" mais experientes, que trouxeram aos usuários comuns a possibilidade de invasão a sistemas particulares. Os motivos de pessoas infringirem leis invadindo sistemas e computadores são os mais variados possíveis. A seguir, são mencionados alguns deles:

- Lazer;
- Supremacia de grupos rivais;
- Roubo de informações;
- Protestos;
- Desafios propostos por *sites* e empresas de informática.

Nesta dissertação, o termo *hacker* será utilizado como sendo aquela pessoa que consegue infiltrar-se em sistemas sem a permissão dos responsáveis para qualquer fim, seja ele positivo ou negativo.

2.2.6 *Firewall*

Os *firewalls* são mecanismos de proteção de redes de computadores, que formam uma barreira interposta entre uma rede privada de qualquer organização e uma rede externa (por exemplo: Internet). Existem na forma de *hardware*, ou *software*, ou uma combinação de ambos (NAKAMURA, 2002).

Sua principal função é analisar o tráfego entre a rede interna e a rede externa em tempo real, permitindo ou bloqueando o tráfego de acordo com regras pré-definidas. Atualmente, é o principal instrumento de defesa de redes corporativas, controlando e monitorando o acesso aos sistemas e aos *hosts* da organização e a filtragem de tráfego entre duas redes.

Com ele, pode-se dispensar a instalação de *softwares* adicionais nos *hosts*, centralizando a administração e a configuração de toda a rede. Algumas funções dos *firewalls*:

- **Filtragem de serviços** – consiste em filtrar serviços que não são considerados seguros, aumentado a segurança da rede e dos *hosts*, podendo rejeitar pacotes de uma determinada origem.
- **Controle de acesso a serviços e *hosts*** – consiste na definição de regras de acesso externo para *hosts* da rede interna e para serviços específicos, fixando permissões de acessos a serviços e *hosts*, evitando assim invasões externas.

- **Bloqueio de serviços** – permite bloquear serviços considerados inseguros e serviços que forneçam informações utilizadas em intrusões.
- **Registro e estatísticas de utilização da rede** – permitem monitorar todo o sistema, registrando os acessos e permitem também fornecer estatísticas do sistema através de *logs* de utilização, sendo possível fornecer detalhes que identifiquem possíveis tentativas de ataque à rede.
- **Imposição da política de acesso à Internet** – a filtragem e a permissão a qualquer tipo de acesso à Internet é monitorada através do *firewall*. Com isso, é possível forçar o cumprimento de uma política de acessos, sem ter que depender da cooperação dos usuários.

O *firewall* é uma das principais soluções de segurança disponível em ambientes corporativos, mas não resolve todos os problemas e também não é a única solução disponível. É necessário incrementar a segurança com alguns dos sistemas complementares descritos nos próximos tópicos.

Abaixo são listadas algumas das vulnerabilidades dos *firewalls*:

- Ataques internos e usuários mal-intencionados;
- *Backdoors* ou portas abertas;
- *Bugs* e falhas no equipamento;
- Colisões da rede interna e externa;
- Proteção antivírus.

2.2.7 Política de Segurança

A política de segurança é a normalização dos procedimentos e regras relacionados à segurança em um determinado ambiente. Os procedimentos de instalação, administração, monitoramento, controle e manutenção dos recursos tecnológicos da organização devem ser descritos detalhadamente de forma sucinta e objetiva.

A principal finalidade da política de segurança é informar as obrigações para a proteção da tecnologia e do acesso à informação. Nela devem estar especificados os mecanismos através dos quais estes requisitos podem ser alcançados. Ela serve como ponto de referência para que se possa adquirir, configurar e auditar sistemas computacionais e redes, para que sejam adequados aos requisitos propostos. Alguns de seus princípios básicos são:

- Confidencialidade;
- Disponibilidade;
- Integridade;
- Legalidade.

De acordo com o grau de importância, as informações da empresa devem ser classificadas em:

- Públicas;
- Corporativas;
- Confidenciais.

A política de segurança dita as regras, expressando o que os usuários devem e não devem fazer em relação aos diversos componentes do sistema, incluindo o tipo de tráfego

permitido nas redes. Ela deve ser tão explícita quanto possível para evitar ambigüidades ou más interpretações (NAKAMURA, 2002).

Para que uma política de segurança se torne apropriada e efetiva, ela deve ter a aceitação e o suporte de todos os níveis de empregados dentro da organização. É especialmente importante que a gerência corporativa suporte de forma completa o processo da política de segurança, caso contrário haverá pouca chance de que ela tenha o impacto desejado. (PELISSARI, 2002). Abaixo segue um exemplo de etapas que um processo de elaboração de uma política de segurança deve conter:

- Definição da equipe responsável pela implantação e manutenção da segurança;
- Análise das necessidades e procedimentos utilizados pela empresa;
- Identificação dos processos críticos;
- Classificação da informação;
- Elaboração de normas e procedimentos para técnicos e usuários;
- Definição de um plano de recuperação a desastres ou plano de contingência;
- Definição de sanções ou penalidades pelo não cumprimento da política;
- Elaboração de um termo de compromisso;
- Comunicado da diretoria/ presidência aos funcionários;
- Divulgação da política;
- Implantação;
- Revisão da política.

2.2.8 Ameaças Virtuais

Com a constante evolução tecnológica, atualmente existem muitos tipos de pragas virtuais que ameaçam as informações e conhecimentos corporativos das empresas. Em se tratando de usuários leigos, qualquer código que acarrete problemas aos sistemas e computadores é chamado vírus. Porém existem diferenças entre estas pragas virtuais. Abaixo segue breve descrição dessas pragas mais comumente encontradas.

2.2.8.1 Cavalos de Tróia (*Trojan Horses*)

Conforme a *Microsoft Corporation* (2006), Cavalo de Tróia é um programa de computador que aparenta ser útil, mas na verdade causa danos. O termo "Cavalo de Tróia" vem de uma lenda antiga em que os gregos deram aos troianos um grande cavalo de madeira como sinal de que estavam desistindo da guerra, desejando a paz. Tal cavalo escondia no seu interior um grupo de soldados gregos, que abririam os portões da cidade para o exército grego, depois que os troianos levassem o cavalo para dentro da cidadela.

Esse tipo de programa parece fazer algo útil, ou pelo menos divertido, como ativar um protetor de tela atraente. Entretanto, como seu homônimo legendário, um programa Cavalo de Tróia oculta um propósito destrutivo: ao ser executado, pode destruir arquivos ou criar uma entrada pela "porta dos fundos" que permita ao intruso acessar seu sistema. (GALVÃO, 2002).

Ele não se propaga sozinho de um computador para outro. Os *Trojan horses* propagam-se quando as pessoas abrem inadvertidamente um programa, porque pensam que a mensagem é proveniente de uma fonte legítima.

De acordo com a definição da RFC 2828 (*Request for Coments* nº. 2828), é um "programa que aparenta ter uma função útil, mas possui alguma função maliciosa que burla os mecanismos de segurança. Não possui a capacidade de se auto-replicar. Como exemplo, pode-se citar um jogo puxado pela Internet, que, na verdade, ao ser executado, tira a atenção do usuário enquanto executa algum dano ao computador em segundo plano".

Este tipo de programa está sendo muito utilizado como forma de ataques. Por meio de qualquer disfarce, ele se instala na máquina hospedeira. A partir daí, o computador hospedeiro passa a ser controlado por outra pessoa. Com isso, o hacker poderá monitorar e realizar qualquer operação que estará sendo feita neste computador. A destruição de arquivos, bem como o roubo de senhas, é tarefa simples de se executar através desta técnica de invasão.

2.2.8.2 Vírus

Segundo Moreira (2001, p. 50), os vírus são programas que se inserem dentro de outros programas, fazendo com que, quando estes sejam executados, o vírus também o seja. Por conseguinte, vírus é um programa malicioso que possui a habilidade de auto-replicar e infectar partes do sistema operacional ou de programas de aplicação, com o intuito de causar a perda ou dano nos dados.

O nome, vírus, se dá devido à semelhança das ações e proliferações que o mesmo efetua, como um vírus real que domina o mecanismo de células normais. Ele normalmente se

disfarça em outros arquivos de programa. A infecção acontece quando o programa infectado é executado; juntamente o código do vírus também é executado. A ação do trecho de programa procura e infecta novos arquivos de programas. A proliferação é realizada quando o vírus, utilizando a lista de endereços do próprio usuário infectado, envia mensagens contendo o código do vírus ou um arquivo contaminado a outros usuários.

De acordo com Moreira (2001, p. 51), existem três tipos básicos de vírus: de macros, de programas e de sistema. No entanto, existem várias classificações sobre os tipos de vírus, as quais causam divergência entre autores. A título de ilustração, segue um quadro contendo a tipificação de vírus elaborada pelo autor desta pesquisa, em 2006:

Tipos	**Descrição e exemplos**
Vírus de arquivos ou programas	Vírus que normalmente ficam alojados em arquivos com extensões: .COM, .EXE, .DLL, .SYS, .BIN e .BAT. Exemplos de vírus de programa conhecidos são Jerusalém e *Cascade*;
Vírus de setor de *boot*	Vírus que ficam armazenados na inicialização do sistema. Exemplos de vírus de setor de boot são: *Form, Disk Killer, Michelangelo* e *Stoned*;
Vírus de macro	Vírus que infectam arquivos dos programas *Microsoft Office* (*Word, Excel, PowerPoint e Access*);
Vírus *Multipartite*	Vírus que infectam setores de boot, disquetes e arquivos executáveis. Exemplo: *Dead.Boot.488, Pieck.4444.A, Delwin.1759*;
Vírus Polimórficos	Vírus que se automodificam a cada nova disseminação, de forma que um único vírus pode ter inúmeras formas diferentes. Exemplo: *Satan Bug, Spanska.4250, W95/HPS*.
Vírus *Stealth*	Vírus que utiliza técnicas para ocultar as alterações executadas e enganar o antivírus. Exemplo: *AntiCNTE Boot, Natas.4988, Bleah*;

Quadro 1. Tipificação de Vírus.
Fonte: Adaptado pelo autor deste trabalho a partir de Oliveira, 2001, p. 105-110).

Alguns vírus são desenvolvidos para danificar o computador, corrompendo programas, excluindo arquivos ou reformatando o disco rígido. Outros não cometem estragos, simplesmente se reproduzem e chamam a atenção sobre a sua presença com mensagens de texto, vídeo e áudio. De acordo com a empresa britânica de segurança *Sophos*, os dez vírus mais perigosos em abril de 2006 seguem na tabela abaixo:

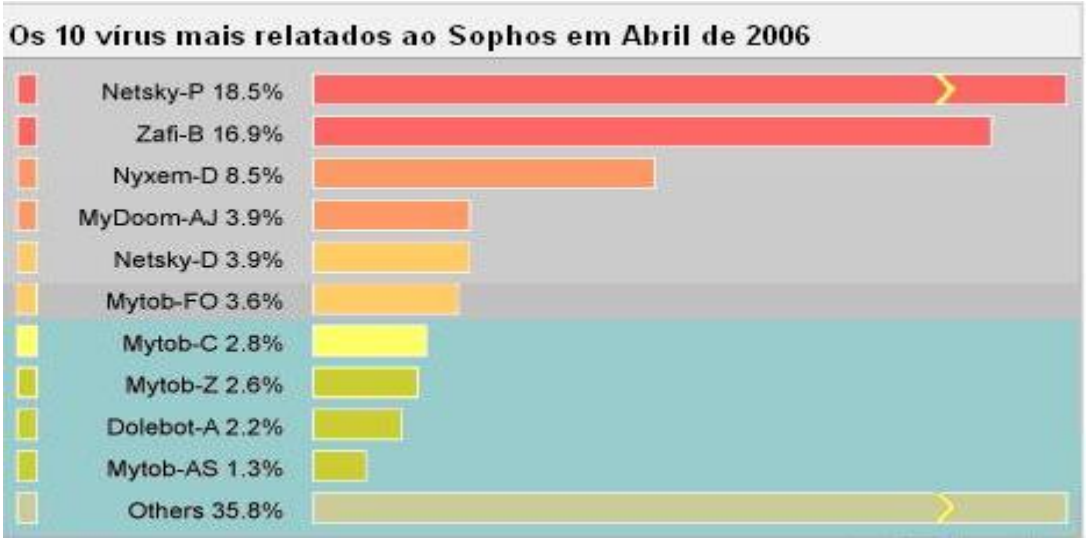

Figura 6: Top Ten Vírus
Fonte: http://www.sophos.com/virusinfo/topten/

2.2.8.3 *Worm* (Verme)

De acordo com CERT (2006), *worm* é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá

através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores. (CERT, 2006).

Geralmente o *worm* não tem como conseqüência os mesmos danos gerados por um vírus, como, por exemplo, a infecção de programas e arquivos ou a destruição de informações. Isto não quer dizer que não represente uma ameaça à segurança de um computador ou que não cause qualquer tipo de dano. (CERT, 2006).

Worms são notadamente responsáveis por consumir muitos recursos. Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar. Além disso, podem gerar grandes transtornos para aqueles que estão recebendo tais cópias. (CERT, 2006).

Detectar a presença de um *worm* em um computador não é uma tarefa fácil. Muitas vezes, os *worms* realizam uma série de atividades, incluindo sua propagação, sem que o usuário tenha conhecimento. (CERT, 2006).

Embora alguns programas antivírus permitam detectar a presença de *worms* e até mesmo evitar que eles se propaguem, isto nem sempre é possível. (CERT, 2006).

De acordo com Oliveira (2001, p. 105), os *worms* são programas servidores muitas vezes chamados de Cavalo de Tróia, também são parecidos com os vírus, porém se diferenciam na forma de infecção. Eles somente fazem cópias deles próprios e as propagam. Exemplos são: *LittleDavinia, Navidad*.

2.2.9 Rede Virtual Privada – RVP (*Virtual Private Network – VPN*)

Atualmente, a troca eletrônica de informações é um bem comum entre os indivíduos. A comunicação e a troca de dados entre os ambientes corporativos ocorrem constantemente, sendo necessário um meio de comunicação seguro e confiável. Os meios de comunicações dedicados são bastante utilizados, porém com alto valor de aquisição e manutenção. A solução encontrada para diminuir o custo da comunicação foi utilizar uma rede pública (Internet) como meio de comunicação.

No entanto, para Pelissari (2002), a segurança, a confiabilidade e a integridade neste tipo de comunicação são pontos que comprometem o serviço, devido ao conteúdo trafegado por ela ser acessível a todos, podendo ser interceptado e capturado. A VPN utiliza exatamente este conceito de comunicação, todavia com os quesitos mínimos de segurança, integridade e confiabilidade nos seus serviços (NAKAMURA, 2002).

Além disso, a Internet, sendo de alcance mundial, facilita a comunicação em lugares onde a situação é irregular, possibilitando assim uma total abrangência de comunicação. Para que a abordagem de VPN se torne efetiva, ela deve prover um conjunto de funções que garanta confidencialidade, integridade e autenticidade.

Assim como a Rede Virtual Privada é uma solução, existem muitas técnicas, ou modos, que podem ser usadas na sua implementação. No quadro a seguir são listadas algumas:

Modo	Características
Modo Transmissão	Somente os dados são criptografados, não havendo mudança no tamanho dos pacotes;
Modo Transporte	Somente os dados são criptografados, podendo haver mudança no tamanho dos pacotes;
Modo Túnel Criptografado	Os dados e o cabeçalho dos pacotes são criptografados, sendo empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e de destino.
Modo Túnel Não-Criptografado	Tanto os dados quanto o cabeçalho são empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e destino.

Quadro 2. Modos de Implementação para Redes Virtuais Privadas
Fonte: http://www.gpr.com.br/download/vpn

2.2.10 Sistema de Detecção de Intrusos – SDI (*Intrusions Detection System – SDI*)

Os sistemas de detecção de intrusos (SDI) são sistemas de monitoramento de tráfego de redes de computadores a procura de situações ilegais. Eles funcionam analisando tráfego ou eventos suspeitos. Caso encontre algo estranho aos padrões estabelecidos, é enviado um aviso ou é gerada uma rotina de correção. (NAKAMURA, 2002).

A detecção de intrusos pode ser realizada de dois modos: sensores procuram por “assinaturas” de ataques, que são os métodos utilizados por invasores e catalogados no SDI; sensores detectam alguma atividade suspeita, seja por eventos não esperados ou diferentes do perfil normal de um usuário ou aplicação.

Os SDI de rede têm a vantagem de proteger todo um segmento de rede, embora sejam limitados por não poderem “ver” o que acontece “dentro” dos servidores. Os SDI de rede

examinam os tipos e o conteúdo dos pacotes trafegados. SDI baseados em servidores examinam as trilhas de auditoria e *log* de atividades. Uma implementação completa de SDI deverá utilizar ambos os tipos de SDI.

De acordo com Pelissari (2002), para a perfeita monitoração do sistema, um SDI deve seguir alguns aspectos básicos:

- Base de dados não pode ser perdida em caso de falhas do sistema operacional;
- Detecção de alterações no funcionamento normal;
- Detecção de poucos falsos positivos;
- Dificuldade de ser enganado;
- Funcionamento constante em segundo plano sem interação;
- Funcionamento imperceptível no sistema;
- Monitoração de si próprio;
- Não-detecção de falsos negativos;
- Não permissão de subversão.

As duas principais funções de um SDI são:

I) Alarmar o administrador de rede ou do sistema, em tempo real, sobre uma possível invasão;

II) Disparar automaticamente mecanismos de segurança contra essa suspeita.

2.2.11 Tendências Tecnológicas Futuras

Hoje em dia, a segurança continua a ser uma das maiores preocupações das empresas, especialmente no que diz respeito à utilização de computadores portáteis. Riscos como ataques maliciosos, vírus, acesso não-autorizado aos sistemas, interceptação de informação confidencial, *hackers* e fraca encriptação podem transformar a informação privada em pública, levando a conseqüências como perdas de produtividade, de dados e roubo de informação e ainda a custos de TI adicionais.

Além das tecnologias de segurança da informação anteriormente descritas, existem algumas que estão em fase de experimentação e testes. Abaixo são descritas três delas, que já vêm sendo implantadas com sucesso e têm se mostrado bastante eficientes.

2.2.11.1 Biometria

A biometria tem se tornado uma forma de segurança bastante efetiva na autenticação de usuário. Pode-se definir biometria como sendo uma forma de verificação de identidade das pessoas por meio de característica física e única. Dentre muitas formas de biometria, pode-se destacar a impressão digital, scanner de íris e projeção facial.

Mesmo com o pequeno avanço, a biometria já obtém sucesso, baixando o índice de fraudes. O funcionamento do sistema consiste em verificar uma certa identificação em algum registro. Para isso, cada usuário configura uma característica física, biológica ou

comportamental junto ao sistema, a fim de que seja utilizada na verificação da identidade do usuário.

A verificação consiste na captura da característica do usuário através de sensores e comparação desta com o modelo biométrico armazenado no banco de dados do sistema. A seguir estão relacionados alguns tipos de sistemas que empregam a biometria:

- Identificação de íris;
- Impressão digital;
- Reconhecimento de voz;
- Reconhecimento da dinâmica da digitação;
- Reconhecimento da face;
- Identificação da retina;
- Geometria da mão;
- Reconhecimento da assinatura.

A contínua diminuição dos custos dessas soluções tende a facilitar a aquisição e o uso de algum tipo de sistemas biométricos pelas empresas em um curto espaço de tempo.

2.2.11.2 Cartão Inteligente (*Smartcard*)

Um dispositivo do tamanho de um cartão de crédito com um microprocessador embutido e uma pequena quantidade de armazenamento que é usada, com um código de acesso, para permitir a autenticação baseada em certificados. Os *smartcards* armazenam certificados, chaves privadas, chaves públicas, senhas e outros tipos de informações pessoais.

O termo inglês "*Smartcard*" significa cartão inteligente. Ele tem formato e tamanho de um cartão convencional, como, por exemplo, o cartão de crédito. A diferença fica por conta de um chip embutido, que pode processar e armazenar dados eletrônicos protegidos por características avançadas de segurança. Geralmente, ele pode existir em três versões diferentes:

- Cartão de memória – armazena dados e necessita de um processador externo para acessar e manipular os dados;

- Cartão processador – processa e armazena dados independentemente através de um microprocessador embutido com sistema operacional;

- Cartão de encriptação – obtém características adicionais de segurança através de um co-processador de encriptação.

Os *smartcards* são usados com diferentes propósitos, cada qual com seu mecanismo de segurança. Alguns são menos sofisticados, os cartões de memória, e outros mais sofisticados, os cartões processadores. Os *smartcards* podem ser usados como cartões comuns, onde somente o proprietário tem acesso às informações (por exemplo: cartões de crédito), ou como cartão de identificação, em que qualquer um pode ter acesso às informações (por exemplo: identificação de nome, RG, tipo sangüíneo, endereço).

Muitos testes já foram realizados com esta tecnologia, sendo esta aprovada e causando grande expectativa na área de segurança para o futuro. Algumas vantagens são descritas abaixo em relação a este novo conceito de cartão: a flexibilidade e a capacidade para armazenar grandes quantidades de dados e potencial de acomodar várias aplicações tarifárias fazem com que seja visto como um dos grandes benefícios da tecnologia.

Cartões inteligentes não são muito caros. A relação custo/benefício dos *smartcards* prova que esta tecnologia em breve estará no mercado, sendo usada como uma das principais

formas de armazenagem de dados pessoais. Testes estão sendo elaborados e executados em grande escala. As padronizações dos cartões ainda estão sendo desenvolvidas, preocupando-se em assegurar a interoperacionalidade do seu funcionamento.

2.2.11.3 Módulo de Plataforma Confiável (*Trusted Platform Module* - TPM)

Atualmente o *Trusted Platform Module* (TPM) representa a mais inovadora tecnologia de segurança. O TPM funciona como uma caixa de depósito de segurança que está fechada dentro de um cofre. A identidade e o acesso ao cofre precisam ser confirmados antes de se conseguir acessar o que está fechado lá dentro. Isto significa que a informação guardada numa plataforma TPM, mesmo que o equipamento seja roubado, permanece segura. O TPM é uma combinação única de tecnologias de *hardware* e de *software* em um só módulo; isto é o que faz dele o melhor em termos de segurança da informação. Além disso, este módulo proporciona uma autenticação forte e disponibiliza capacidades criptográficas.

O TPM proporciona a base da segurança – também chamada de raiz principal de confiança. A informação armazenada no chip pode ser utilizada para processos de verificação: processos de medição, gravação e relatórios de forma a assegurar que não são realizadas alterações nem acessos não-autorizados. Como base, o TPM proporciona um sólido alicerce de proteção que pode ser complementado com medidas de segurança adicionais.

- Características
    - O TPM pode ser utilizado para armazenar certificados importantes ou digitais como parte do sistema PKI (Primary Key Infrastructure), de forma simplificada, em uma PKI, os certificados digitais são emitidos por uma Autoridade

Certificadora para cada usuário ou equipamento envolvido. Com estes certificados, são gerados pares de chaves constituídos por uma chave pública e uma privada. Os algoritmos utilizados permitem que aquilo que foi criptografado com a chave pública só possa ser aberto pela chave privada, e vice-versa. Desta forma, tudo que é público é colocado à disposição num diretório onde se tenham acesso às informações de todos, e tudo que é privado é mantido em segredo pelo usuário, quer seja criptografado no disco de seu computador, dentro de um smartcard ou em um servidor na rede. Também pode ser utilizado para armazenar passwords;

- O TPM possui um controlador separado para armazenar a informação confidencial. Suporta a utilização do PKI, que permite ao utilizador a identificação através de uma terceira parte;
- O TPM suporta o reconhecimento automático para que os utilizadores não necessitem de digitar múltiplas senhas para efetuarem o acesso;
- O TPM pode ser utilizado para criar uma *Personal Secure Drive* (PSD).

- Benefícios
  - Maior segurança da rede, particularmente útil para transações comerciais on-line em que é necessária a assinatura digital;
  - O TPM está a salvo de vírus ou vermes que atacam arquivos executáveis ou o sistema operacional;
  - As identidades digitais e a autenticação também são protegidas;
  - Simplicidade;
  - Mesmo quando um portátil é roubado, a informação continua protegida.

Apesar das avançadas características de segurança, só o TPM não é suficiente para garantir um sistema de proteção de alto nível – é conveniente a utilização de um modelo de segurança complementar, para uma computação de segurança.

Um *hardware* inviolável significa que a memória está selada e é utilizada para gerar e armazenar chaves de forma segura, e as funções criptográficas utilizam essas chaves para desbloquear o resto do sistema. O Grupo da Computação de Confiança e o TPM asseguram este sistema, o que faz do TPM uma base fundamental para a plataforma de segurança. A plataforma de confiança utiliza as funções criptográficas para verificar a confiabilidade da mesma e para autenticar a identidade. A informação sobre o estado do *software* que corre na plataforma é armazenada no TPM e pode ser utilizada para verificar se o sistema foi ou não afetado. O TPM pode também ser utilizado para controlar o nível de acesso à *BIOS* do sistema.

Por estas razões, o *Gartner Group* propõe, de acordo com Hirst & Heidarson (2004), uma abordagem de três níveis, chamada de Computação de Confiança. A Computação de Confiança assegura um *hardware* inviolável, uma plataforma e execução do sistema de confiança.

Depois de abordados os principais conceitos e tecnologias relativos à segurança da informação e proteção dos conhecimentos corporativos armazenados em computadores, sejam em casa ou em ambientes corporativos. Serão apresentados os conceitos referentes a fraude computacional, sua definição, características e formas. O ato fraudulento constitui-se em ameaça e risco constante na atual era da informação, sendo responsável por muitos prejuízos às empresas e as pessoas.

2.3 Fraude Computacional

2.3.1 Considerações Iniciais

Fraudes computacionais, embora menos dramáticas que crimes de violência, podem infringir significativos prejuízos aos indivíduos e à comunidade. No entanto, para as organizações do mundo corporativo, elas podem ser letais, uma vez que, devido ao atual estágio de maturidade tecnológica, todas as informações vitais das corporações estão armazenadas em computadores. Com a finalidade de apropriadamente quantificar e mitigar os riscos inerentes, este assunto necessita ser estudado e bem compreendido para possibilitar a descoberta de métodos de prevenção e divulgação destas ocorrências.

O princípio fundamental de criminologia é que o crime precisa de oportunidades, e oportunidades abundam no mundo computacional de hoje. De acordo com Shover (2001), oportunidades criminais são arranjos ou situações que os indivíduos encontram e que oferecem atrativo potencial de recompensa para o criminoso, em grande parte porque eles são acompanhados por muito baixa percepção de risco, de detecção ou policiamento.

Segundo Lanham (1987), os computadores criaram muitas oportunidades para fraudadores e os habilitaram a assaltar através de controle remoto. Ele argumenta ainda que os computadores aumentaram o problema de fraude, uma vez que muitos usuários de locais remotos podem acessá-los. Dessa forma eles não podem ser vistos como um objeto passivo, como uma cadeira ou um arquivo de escritório.

Complementando, Smedinghoff (1996) observa que a habilidade para manipular dados de computador traz grandes benefícios, porém deriva dela o aumento significativo das oportunidades de fraude.

De modo a quantificar corretamente e mitigar o risco, o tema fraude de computador precisa ser bem entendido. Devido à grande complexidade e interdisciplinaridade do tema, ainda há um pouco de confusão sobre o que é ou não fraude de computador.

Fraudes de computador são altamente destrutivas para o livre-comércio e o capitalismo e, mais amplamente, para o bem-estar da sociedade, de acordo com Greenspan (1997). Para Dhillon e Moores (2001), fraudes de computador podem causar instabilidade e incerteza em um sistema, e podem impor um custo muito significante para a sociedade. Então, fraude de computador deve ser bem entendida por aqueles encarregados de combatê-la.

Sem uma definição clara de fraude de computador, não será possível compartilhar a informação que tem o mesmo significado para todo o mundo, não será possível concordar em como medir o problema e que recursos precisam ser alocados para mitigar o risco empresarial.

Entender melhor da natureza da fraude de computador pode ser muito útil para encontrar meios de prevenção, e pode ser uma ferramenta muito útil para educação e divulgação destas práticas nocivas ao desenvolvimento empresarial.

2.3.2 Arcabouço Teórico da Fraude

Como Albrecht (1984) argumenta, só pode ser alcançada uma compreensão completa de fraude por um estudo inclusivo executado por um time interdisciplinar de investigadores. Em consonância com o propósito principal deste trabalho, já que fraude de computador é um

dos tipos de ataques de computador, a fundamentação teórica decorre principalmente da área de segurança contra ataques a computadores.

Vários autores têm se dedicado ao estudo da fraude de computador. Parker (1998) apresenta um modelo de ataques a computadores baseado nos seguintes fatores: Habilidades; Conhecimento; Recursos; Autoridade e Motivos.

Howard (1997) apresenta uma taxonomia com respeito a tipos de atacantes, ferramentas usadas, informação de acesso, resultado do ataque e objetivos do ataque. Landwehr (1994) propõe uma taxonomia de ataques através de modo (como), tempo de introdução (quando) e local (onde), enquanto Perry (1984, p. 34-45) apresenta uma matriz de ataques.

Uma taxonomia de ameaças de segurança para redes é apresentada por Jayaram (1997). Lough (2001) apresenta uma taxonomia de ataques de computador com aplicações para redes sem fios. Uma taxonomia de ataques via *WEB,* que são ataques que usam o protocolo de HTTP/ HTTPS exclusivamente, é proposta por Álvarez (2003, p. 435-449).

Knight (2000) introduz uma taxonomia com respeito aos tipos de vulnerabilidade de computadores. Krsul (1998) apresenta uma classificação de vulnerabilidades de software, enquanto Smendinghoff (1996) discute sete classes de falhas de integridade.

Anderson (1980) desenvolve uma matriz que cobre os tipos de atacantes, baseada em quando eles são autorizados ou não a usar o computador e os programas ou dados desse computador.

Krauss (1979) discute a natureza do problema da fraude de computador em um ambiente de computador típico, a execução de fraudes de computador, controles preventivos e proteções. Stevenson (2000, p. 13-15) chama atenção para a detecção e prevenção de fraudes de computador. Uma taxonomia de fraude de computador é proposta por Bologna (1996),

porém, esta taxonomia não fornece nenhuma explicação de como e por que foi selecionada, e nem de como ela pode ser usada.

Todos estes autores supracitados e seus respectivos modelos não foram detalhados por não constituírem o objetivo dessa dissertação. Além disso, pode-se constatar que, embora todas estas tentativas sejam valiosas contribuições, o assunto é controverso e falta uma taxonomia definitiva que possa ser usada na função de prevenção.

2.3.3 Preliminares sobre a Fraude Computacional

Para entender fraude de computador, é muito útil em geral observar primeiro os elementos de uma ofensa e o ato de fraude. Logo, pode se definir o que não é e o que é fraude de computador.

De acordo com o que Gillies (1993) explica, um crime consiste, na maioria dos casos, de conduta pela qual o acusado é responsável, especificado pela definição daquele crime. Esta conduta tem componentes mentais (exceto em certos casos, quando o acusado é incriminado em virtude de uma relação ou outra implicação em uma situação estática) e físicos.

Fraude, como outros conceitos familiares, é um termo que parece ter um significado perfeitamente óbvio até que se tente defini-lo. Além disso, fraude é um conceito legal profundo, e poucos realmente entendem o que seja fraude ou usam uma definição comum. Sempre houve uma grande relutância entre advogados para tentar definir fraude, e isto só é natural quando se leva em consideração o número de tipos diferentes de conduta para a qual esta palavra é aplicada.

O termo "fraude" está definido no dicionário eletrônico Aurélio como:

1 V. logro (2).

2 Abuso de confiança; ação praticada de má-fé.

3 Contrabando, clandestinidade.

4 Falsificação, adulteração.

A fraude sempre é intencional, seja intencional através de aparecimento, seja intencional por conclusão do ato. Intenção não deveria ser confundida com o motivo que impulsiona uma pessoa a agir. Intenção refere-se somente ao estado de mente com que o ato é praticado. Porém, não há nenhum meio científico ou método para medir a intenção de uma pessoa.

O elemento da intenção para defraudar conota a intenção para produzir uma conseqüência que está em algum senso prejudicial para um direito legal, interesse, oportunidade, ou vantagem de a pessoa ser defraudada, e é uma intenção distinta e adicional à intenção de usar meios proibidos. Se não há nenhuma evidência de que a vítima foi defraudada, então não se pode falar em fraude de computador.

2.3.4 O que não é Fraude de Computador?

Fraude de computador às vezes se confunde com outras ofensas como, por exemplo:

- Acessar um computador intencionalmente, sem autorização ou excedendo acesso autorizado, e obtendo informações;

- Causar dano a um computador protegido. Seja através da transmissão de um programa, informação, código ou comando conscientemente, e como resultado de tal conduta, o dano é causado intencionalmente, sem autorização, para um computador protegido;
- Traficar senhas, ou seja, negociar senhas e informações semelhantes que teriam permitido a outros ganharem acesso sem autorização à rede de computador de uma organização.

Enquanto estas ofensas podem ser executadas em conexão com a fraude de computador, elas deveriam ser consideradas como distintas uma vez que não reúnem os requisitos necessários para serem consideradas fraudes de computador segundo Vasiu (2003).

2.3.5 O que é Fraude de Computador?

Para este conceito, foi escolhida como guia a definição dada pelo Ato de Criminalização da Fraude de Computador do *US Computer Fraud and Abuse* (18 U.S.C. § 1030 (a) (4)):

> Conscientemente e com a intenção de fraudar, acessar com ou sem autorização um computador protegido ou exceder a autorização de acesso e por meio dessa conduta promover a fraude e obter alguma coisa de valor, amenos que esse objeto da fraude e a coisa obtida consista somente no uso do computador e o valor desse uso não seja maior que $5,000 em qualquer período de 1 ano. .[1]

[1]Original em inglês (tradução nossa).

De acordo com esta definição, os elementos legais da fraude de computador consistem em:

- Agir propositadamente e com intenção para defraudar;
- Acessar um computador protegido sem autorização, ou excedendo autorização;
- Avançar na fraude e obter qualquer coisa de valor (diferentemente de tempo mínimo de acesso ao computador).

Com relação ao primeiro elemento, segundo Doyle (2002), a frase quer dizer que o ofensor está consciente das conseqüências naturais de seus atos, ou seja, alguém será fraudado. Já o segundo e terceiro elementos deveriam ser discutidos juntos, porque, como eles mostram que mais que mero acesso não-autorizado, é necessário, para qualificar a ofensa como fraude de computador, descrever a “coisa obtida” e não somente o uso do acesso não-autorizado. Ou seja, demonstrar algum fim adicional para o qual o acesso não-autorizado é um meio requerido. Somente ver a informação não pode ser julgado do mesmo jeito que obter algo de valor.

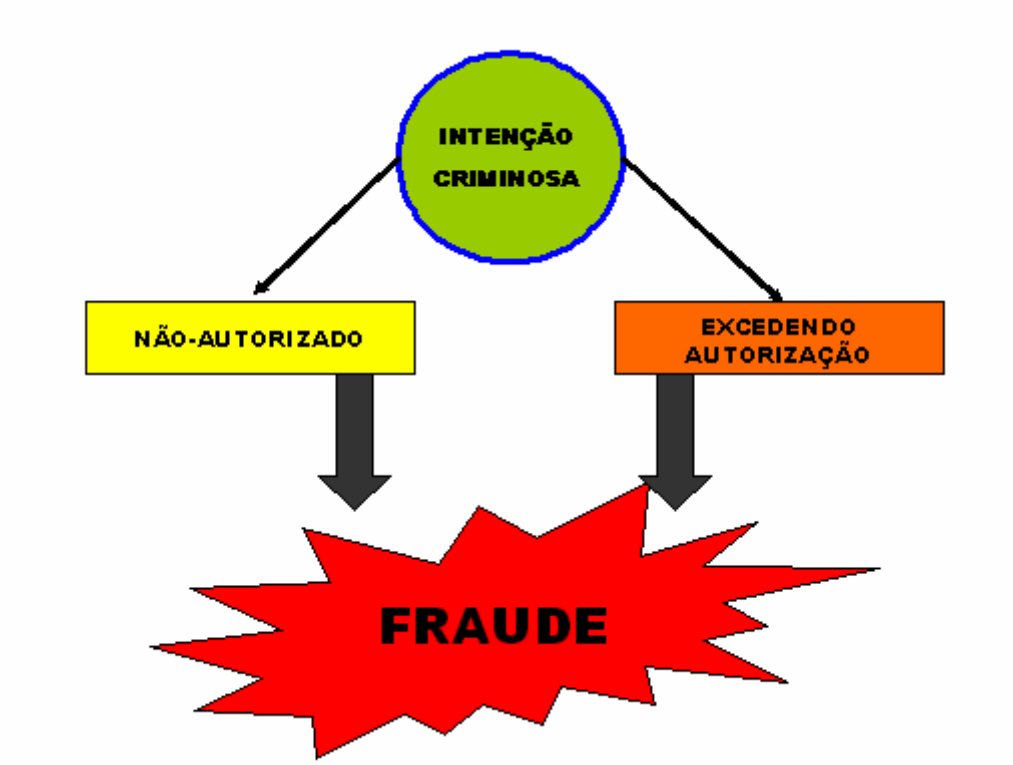

Figura 1. Os elementos legais de fraude de computador.
Fonte: Adaptado pelo autor deste trabalho a partir de Vasiu, 2004, p. 4.

De acordo com a definição do Conselho Europeu (1989), fraude de computador é causar a perda de propriedade a outro por:

A. Qualquer contribuição, alteração, apagamento ou supressão de dados de computador,

B. Qualquer interferência com o funcionamento de sistema de um computador, com intenção fraudulenta ou desonesta de obter, sem direito, um benefício econômico para si mesmo ou para outro.

Quando oportunidades abundam e há uma provisão potencial de ofensores incentivados que percebem que as chances de serem detectados e processados são muito baixas, o risco de fraudes de computadores deve ser considerado como sendo muito alto. Quanto mais cuidado com as possibilidades de fraudes de computadores, menos problemas

são encontrados. Porém, para Dhillon e Moores (2001, p.715-723), as conseqüências de ataques de alto-grau, como fraudes financeiras ou roubo de informação proprietária, podem ser muito altas e de longo alcance. Estas possibilidades não devem ser negligenciadas no planejamento de segurança.

Nenhum ramo de negócio informatizado está livre deste crescente e rápido fenômeno. Os aspectos técnicos de sistemas eletrônicos são projetados para serem à prova de fraude, porém, a natureza humana é tal que é provável que a fraude seja um problema perene, segundo Kreltszheim (1999, p. 223-231).

Embora o risco de fraude de computador não possa ser eliminado, medidas proativas podem reduzi-lo consideravelmente. O risco de perda é mais alto com estratégias de detecção quando o crime está em curso ou aconteceu há pouco tempo; conseqüentemente a habilidade para parar ou recuperar a perda está limitada. Entretanto, medidas proativas deveriam prevalecer, deveriam ser apropriadas ao nível de risco e também deveriam ser reavaliadas regularmente.

A luta contra a fraude é um esforço constante e contínuo. A despeito da tendência no aumento no número de fraudes detectadas e da eficiência dos sistemas antifraude em desenvolvimento, sempre existirão indivíduos e grupos de indivíduos com incentivo, oportunidade e habilidade para racionalizar a perpetração da fraude.

Com base no crescente aumento do risco de fraude, a análise de risco passa a ser uma atividade de importância vital para as organizações. Estas por sua vez, devem constantemente desenvolver controles e investir em mecanismos de análise de riscos para assegurar que, mesmo que seja impossível erradicar totalmente as fraudes, elas não contribuirão para a formação de um ambiente em que o risco empresarial possa prosperar.

2.4 Análise de Riscos

Os meios pelos quais uma fraude é detectada podem ser divididos em duas grandes categorias: detecção por acaso e detecção pelos controles e sistemas de análise e administração de riscos adotados pelas empresas. À medida que as organizações forem encarando mais seriamente não apenas os danos financeiros e intangíveis causados pelas fraudes, mas também a ameaça crescente de penalidades pelos órgãos reguladores, um número significativamente maior de níveis de controles internos e sistemas de análise e administração de riscos há de ser implementado.

2.4.1 Administração de Riscos

Segundo a norma australiana *Standard* AZ/NZS 4360-1999, o termo administração de riscos pode ser definido como: "a cultura, os processos e a estrutura que são direcionados ao efetivo gerenciamento de potenciais oportunidades e efeitos adversos".

Isto significa que o gerenciamento de riscos é planejado para propiciar o acesso integrado à gestão de riscos em uma organização, objetivando melhores resultados através da identificação de oportunidades e diminuição das perdas. Significa, também, que os riscos devem ser gerenciados em toda a organização, desde os níveis estratégicos até os operacionais, passando por todas as áreas de atividades e funções. O gerenciamento de riscos auxilia os gestores e demais servidores a tomar decisões oportunas e adequadas que garantam o uso mais efetivo dos recursos dentro de um nível de risco aceitável. No contexto corporativo, pode-se definir o gerenciamento de riscos como um método organizado que

identifica, conhece e seleciona os fatores de riscos, buscando minimizá-los, controlá-los ou eliminá-los.

Esta seção dá uma avaliação da administração de risco com a finalidade de realçar onde capacidades de tecnologia são melhores aplicadas na mitigação do risco. Para iniciar, serão usadas as seguintes:

- Vulnerabilidade: Uma fraqueza no sistema de segurança, em termos de procedimentos, projeto, implementação, controles internos e etc., que pode ser acidentalmente disparada ou intencionalmente explorada e resultar em uma violação da política de segurança do sistema.
- Fonte de Ameaça: Qualquer intenção e método deflagrado para exploração intencional de uma vulnerabilidade ou a situação e método que podem ativar uma vulnerabilidade acidentalmente.
- Ameaça: O potencial para uma "fonte de ameaça" explorar (intencionalmente) ou ativar (acidentalmente) uma vulnerabilidade específica.
- Risco: É a probabilidade de uma ocorrência combinada com o impacto de uma particular fonte de ameaça explorar ou ativar uma vulnerabilidade particular de Tecnologia da Informação. Riscos relacionados com Tecnologia da Informação surgem de responsabilidade legal ou perda da missão empresarial devido a:

    I. Revelação não-autorizada (maliciosa, não-maliciosa, ou acidental), revelação, modificação ou destruição de informação.
    II. Erros não-maliciosos e omissões.
    III. Falhas na Tecnologia da Informação devido a desastres naturais ou artificiais.
    IV. Fracasso no cuidado e diligência devidos na implementação e operação de sistemas de Tecnologia da Informação.

Ainda segundo a norma australiana *Standard AZ/NZS 4360-1999*, risco é: "a chance de acontecer algo que causará impacto nos objetivos, e que é mensurado em termos de conseqüências e probabilidade". Os riscos podem se apresentar como problemas ou desafios que necessitam ser encarados, como, por exemplo, os obstáculos que nos impedem de cumprir as tarefas diárias, desenvolver e implementar projetos ou atingir os objetivos e as metas da organização ou, então, como oportunidades a serem aproveitadas.

A tarefa de administração de riscos não pode ser vista como uma atividade limitada à alta cúpula de uma organização, mas deve ser implementada por todas as partes envolvidas nos processos, ou seja, deve ser implementada em todos os níveis da organização. Ao mesmo tempo em que todos os gestores de uma organização têm a responsabilidade pelo gerenciamento de riscos, esta responsabilidade varia de acordo com a posição de cada um dentro da estrutura organizacional.

Políticas, orientações normativas e o estabelecimento formal dos deveres de cada gestor são maneiras de garantir que haja um claro entendimento da extensão da responsabilidade atinente a cada cargo ou função. É preciso que os gestores, além de estarem cientes de seus deveres e responsabilidades, tenham a habilidade e o conhecimento necessários para desempenharem satisfatoriamente suas obrigações como tomadores de decisões no processo de Administração de Riscos.

É fundamental que as pessoas-chave sejam envolvidas em todas as etapas do processo de gerenciamento de riscos, a fim de garantir que todos os riscos que permeiam a organização sejam identificados e avaliados, principalmente os relativos a informação e ao conhecimento corporativos. Assim, as avaliações serão mais completas, bem como o processo será compreendido por toda organização, e os *stakeholders* (pessoal envolvido) se sentirão parte integrante do processo e responsáveis por seus resultados.

A avaliação do risco nada mais é do que saber qual a chance do risco vir a acontecer. Quando a empresa possui um histórico, ou seja, possui dados anteriores, pode-se trabalhar com dados objetivos, através da estatística, levantando a média, desvio padrão e coeficiente de variação. Neste caso, a probabilidade fica embasada com dados reais e objetivos.

Entretanto, como, na maioria das vezes, as empresas não possuem histórico de ocorrências, pode-se estimar, de forma subjetiva, a probabilidade de risco, ou seja, a materialização de uma ameaça. Para isso, pode-se aplicar uma tabela progressiva para mensurar, através de critérios subjetivos, tais como:

I. O nível de conscientização dos atores;
II. A cultura empresarial;
III. Política de segurança existente;
IV. Características da concorrência para realizar indução ou intrusão.

A FIG. 2 mostra onde a mitigação de riscos é realizada em face de ataques intencionais. O termo "ataque" é colocado em aspas porque o assunto é “intencional”, e não malicioso. É relativamente comum para a segurança, às vezes, ser atacado intencionalmente por propósitos não-maliciosos com a finalidade de teste.

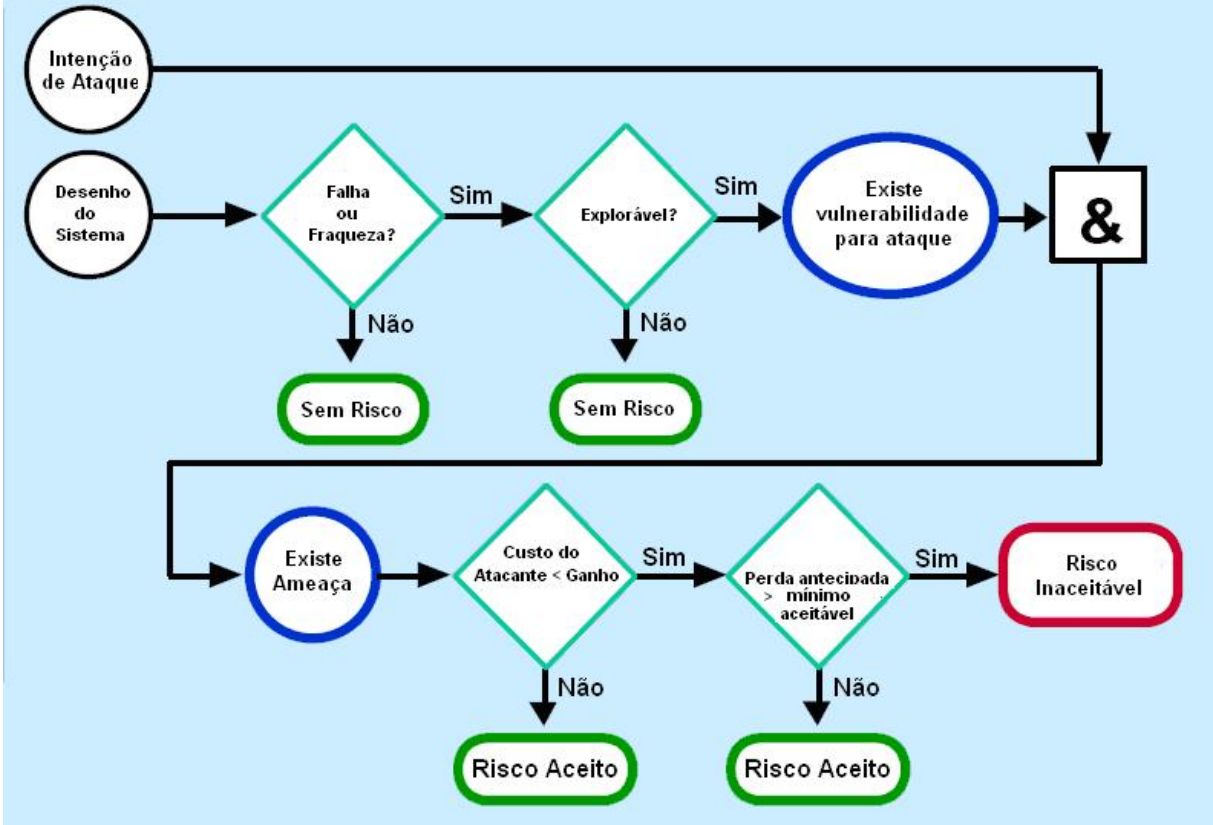

Figura 2: Fundamentos de mitigação de risco - "ataques"
Fonte: *C O M P U T E R S E C U R I T Y: Underlying Technical Models for Information Technology Security Recommendations of the National Institute of Standards and Technology, Page* 18. [2]

A mitigação de riscos de ataque através de meios técnicos pode ser realizada nos seguintes pontos:

I. Falha existente. Solução: Implementar técnicas que garantam a redução da probabilidade de uma falha.

II. Falha explorável. Solução: Aplicar proteções estendidas em camadas e projetos de arquitetura para prevenir a exploração.

III. O custo do ataque é menor que o ganho. Solução: Aplicar proteções para aumentar o custo de atacante (nota-se que escolhas não-técnicas como limitar o que é processado pode reduzir significativamente o ganho do atacante).

[2]Original em inglês (tradução nossa).

IV. Perda significativa. Solução: Aplicar princípios de projeto, projetos de arquitetura e proteções técnicas para limitar a extensão de ataque, reduzindo assim a perda. (Novamente, pode-se perceber que escolhas não-técnicas como limitar o que é processado pode prover a mitigação de riscos mais efetiva.).

A FIG. 3 mostra como a mitigação do risco é aplicada para riscos que surgem de erros de sistemas e de ações de usuário que não pretenderam violar a política de segurança. Para estas situações, a mitigação de riscos é muito similar.

I. Falha existente. Solução: Implementar técnicas que garantam a redução da probabilidade da falha.

II. Falha explorável. Solução: Aplicar proteções estendidas em camadas e projetar arquiteturas para prevenir a exploração.

III. Considerando que a brecha de segurança não é o resultado de uma decisão explícita, não há nenhuma consideração de custo para um atacante.

IV. Perda significativa. Solução: Aplicar princípios de projeto, princípios de arquitetura e proteções técnicas para limitar a extensão de uma brecha de segurança, reduzindo assim a perda.

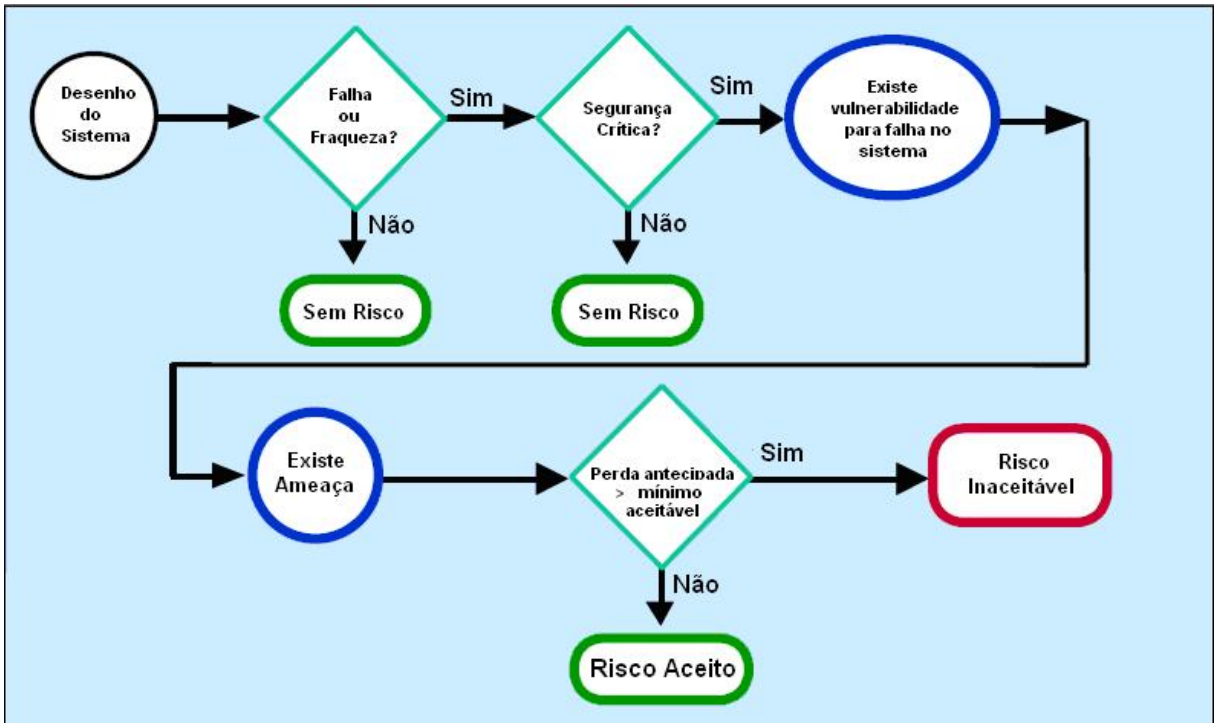

Figura 3: Fundamentos de mitigação de risco - "erros e enganos"
Fonte: *C O M P U T E R S E C U R I T Y: Underlying Technical Models for Information Technology Security Recommendations of the National Institute of Standards and Technology, Page* 19.[3]

A seguir serão descritas três metodologias contendo modelos, controles, práticas e normas internacionalmente aceitos que podem ajudar na gestão da segurança da informação e dos conhecimentos corporativos possibilitando assim a detecção e mitigação de fraudes com vistas a reduzir os riscos empresariais.

[3]Original em inglês (tradução nossa).

2.5 Metodologias e Modelos de Gestão de Segurança da Informação

A segurança da informação tem assumido um papel crucial nas organizações, mudando a cultura de trabalho e a interação entre as empresas. Recentemente as ameaças à segurança dos sistemas de informação têm se tornado freqüentes, principalmente nos ambientes conectados a Internet. Cientes destas ameaças, hardware e software que compõem os ativos de Tecnologia da Informação (TI) representam investimentos que devem ser protegidos estes por sua vez armazenam e suportam todas as informações e conhecimentos corporativos da organização. Estabelecer os padrões e recomendações para a correta utilização e proteção destes recursos por meio da elaboração de políticas de segurança, passou a ser crítico dentro das empresas. Os padrões a seguir, são adotados e reconhecidos como referência mundial, fornecem recomendações para a elaboração e implantação de tais políticas.

2.5.1 O ITIL (Information Technology Infrastructure Library)

O ITIL *(Information Technology Infraestructure Library*) foi desenvolvido pelo governo britânico no final da década de 1980 e tem como foco principal a operação e a gestão da infra-estrutura de TIC (Tecnologia da Informação e Comunicação) na organização, incluindo todos os pontos importantes no fornecimento e manutenção dos serviços de TIC (OGC, 2000).

O ITIL, composto por um conjunto das melhores práticas para auxiliar a Governança de TIC, vem sendo um dos modelos mais amplamente utilizados atualmente (RUDD, 2004).

O princípio básico do ITIL é o objeto de seu gerenciamento: a infra-estrutura de TIC. O ITIL descreve os processos que são necessários para dar suporte à utilização e ao gerenciamento da infra-estrutura de TIC.

Outro princípio fundamental do ITIL é o fornecimento de qualidade de serviço aos clientes de TIC a custos justificáveis, isto é, relacionar os custos dos serviços de tecnologia de forma que se possa perceber como estes trazem valor estratégico ao negócio.

Através de processos padronizados de Gerenciamento do Ambiente de TIC, é possível obter uma relação adequada entre custos e níveis de serviço prestados pela área de TIC.

O ITIL consiste em um conjunto de melhores práticas que são inter-relacionadas para minimizar o custo, ao mesmo tempo em que aumenta a qualidade dos serviços de TIC entregue aos usuários. O ITIL é organizado em 5 módulos principais:

I. Perspectiva de Negócios;
II. Gerenciamento de Aplicações;
III. Entrega de Serviços;
IV. Suporte a Serviços;
V. Gerenciamento de Infra-estrutura.

Embora o modelo ITIL não tenha um módulo dedicado ao Gerenciamento de Segurança Computacional, ele faz referência a este tema apontando em um documento como o mesmo poderia ser incorporado através dos processos descritos nos módulos de Suporte a Serviços e Entrega de Serviços.

Dentre os 5 módulos citados, os mais populares são o Suporte a Serviços e Entrega de Serviços. Apesar de o modelo ITIL possuir processos bem definidos para auxiliar na Governança da Tecnologia da Informação e Comunicação, esta dissertação identifica a

necessidade de algumas adaptações ou adoção de algumas outras práticas complementares para que ele possa ser utilizado para implementar todos os requisitos de um modelo de gestão de segurança da informação e proteção dos conhecimentos corporativos. Essas necessidades estão relacionadas principalmente à forma como tratar incidentes de segurança da informação e proteção aos conhecimentos corporativos.

2.5.2 O COBIT (Control Objectives for Information and Related Technology)

O COBIT - *Control Objectives for Information and Related Technology* (COBIT, 2000) – é um modelo internacionalmente reconhecido e recomendado pelo ISACF (*Information Systems Audit and Control Foundation*, disponível em: <www.isaca.org>) como instrumento de fomento da Governança de Tecnologia da Informação e consiste em um conjunto de padrões e coleções de melhores práticas, que prescrevem como melhor governar a função de tecnologia da informação em uma organização.

O COBIT (COBIT, 2000) estrutura toda a função de TI em 34 grandes processos de gestão, subdivididos em 318 sub-processos. A fim de assegurar que a Governança de TI atenda aos objetivos de negócio, o COBIT (COBIT, 2000) fornece a capacidade de analisar o nível de maturidade dos processos de TI contra as melhores práticas da indústria e padrões de organismos internacionais.

Para conseguir isto, ela habilita a Área de TI a: identificar as atividades mais importantes a serem executadas; medir o progresso de suas execuções em direção aos objetivos a serem alcançados; e determinar quão bem os processos de TI estão executando. Além disso, o COBIT (COBIT, 2000) orienta o direcionamento e a gerência das atividades de

TI para aumentar o seu valor agregado e atingir um balanceamento efetivo entre o gerenciamento de riscos e o alcance de metas e objetivos.

O COBIT inclui ainda recursos, tais como um sumário executivo, um *framework*, controle de objetivos, mapas de auditoria, um conjunto de ferramentas de implementação e um guia com técnicas de gerenciamento. As práticas de gestão do COBIT são recomendadas pelos peritos em gestão de TI que ajudam a aperfeiçoar os investimentos de TI e fornecem métricas para avaliação dos resultados. O COBIT independe das plataformas de TI adotadas nas empresas.

O COBIT é orientado ao negócio. Fornece informações detalhadas para gerenciar processos baseados em objetivos de negócios. O COBIT é projetado para auxiliar três audiências distintas:

I. Gerentes que necessitam avaliar o risco e controlar os investimentos de TI em uma organização.
II. Usuários que precisam ter garantias de que os serviços de TI que dependem dos seus produtos e serviços para os clientes internos e externos estão sendo bem gerenciados.
III. Auditores que podem se apoiar nas recomendações do COBIT para avaliar o nível da gestão de TI e aconselhar o controle interno da organização.

De acordo com COBIT (2000, p. 4), por meio de políticas, processos e procedimentos, este modelo tem como orientação o negócio em si. Através de uma maneira abrangente, este modelo proporciona o envolvimento e a participação de diversos profissionais de fora da TI como os supracitados.

O COBIT (COBIT, 2000) está dividido em quatro grandes domínios que, por sua vez, englobam um grupo de 34 objetivos gerais de alto nível que abrangem todos os aspectos das informações e da TI.

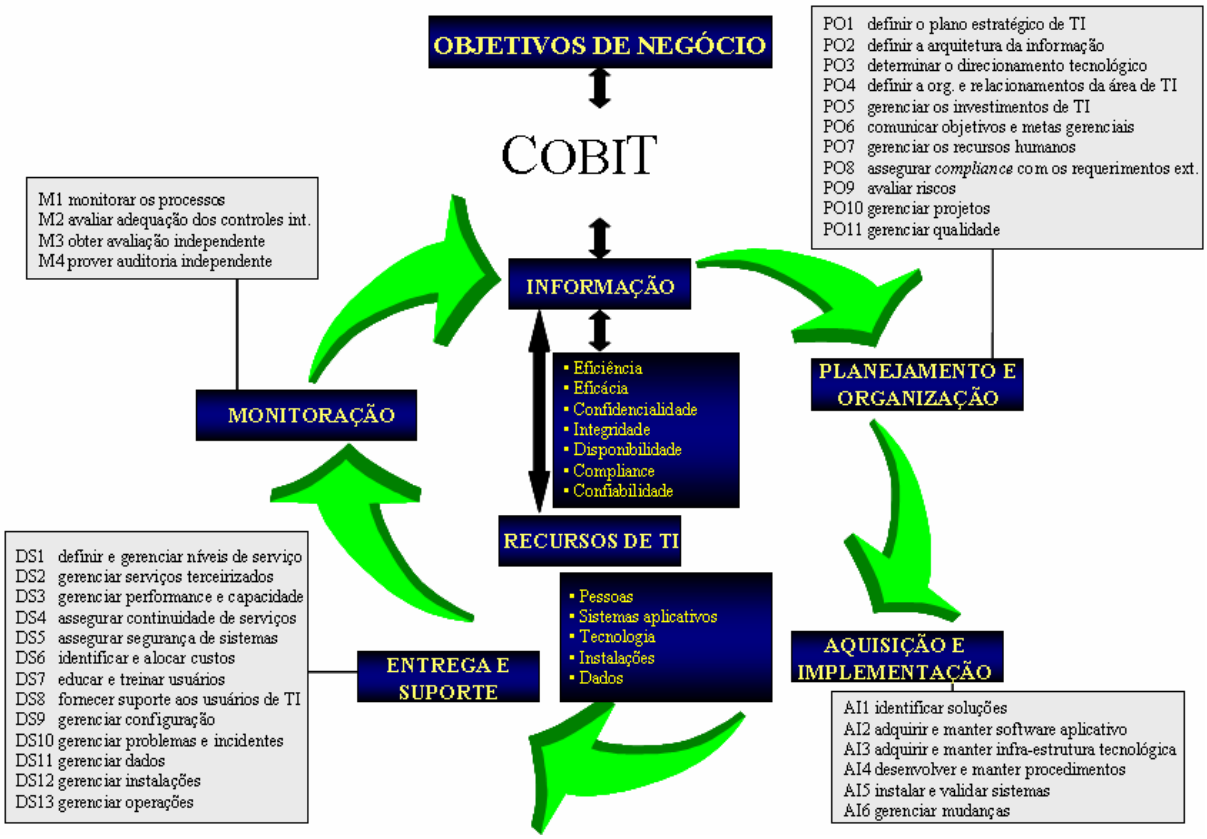

Figura 4. Processos de TI definidos nos quatro domínios do COBIT.
Fonte: COBIT, 2000, p. 5.

A FIG. 4 ilustra a estrutura do COBIT com os quatro domínios ligados claramente aos processos de negócio da organização. Os mapas de controle fornecidos pelo COBIT auxiliam os auditores e gerentes a manter controles suficientes para garantir o acompanhamento das iniciativas de TI e recomendar a implementação de novas práticas, se necessário.

O ponto central é o gerenciamento da informação através dos recursos de TI para garantir o negócio da organização. Para garantir a completa gestão de TI, cada domínio cobre um conjunto dos processos descritos a seguir:

PLANEJAMENTO E ORGANIZAÇÃO

- Define o plano estratégico de TI
- Define a arquitetura da informação
- Determina a direção tecnológica
- Define a organização de TI e seus relacionamentos
- Gerencia os investimentos de TI
- Gerencia a comunicação das direções de TI
- Gerencia os recursos humanos
- Assegura o alinhamento de TI com os requerimentos externos
- Avalia os riscos
- Gerencia os projetos
- Gerencia a qualidade

AQUISIÇÃO E IMPLEMENTAÇÃO

- Identifica as soluções de automação
- Adquire e mantém os softwares
- Adquire e mantém a infra-estrutura tecnológica
- Desenvolve e mantém os procedimentos
- Instala e certifica softwares
- Gerencia as mudanças

ENTREGA E SUPORTE

- Define e mantém os acordos de níveis de serviços (SLA)
- Gerencia os serviços de terceiros
- Gerencia a performance e capacidade do ambiente

- Assegura a continuidade dos serviços
- Assegura a segurança dos serviços
- Identifica e aloca custos
- Treina os usuários
- Assiste e aconselha os usuários
- Gerencia a configuração
- Gerencia os problemas e incidentes
- Gerencia os dados
- Gerencia a infra-estrutura
- Gerencia as operações

MONITORAÇÃO

- Monitora os processos
- Analisa a adequação dos controles internos
- Promove auditorias independentes
- Proporciona segurança independente

2.5.2.1 Desenvolvimento do COBIT

A primeira publicação foi em 1996, enfocando o controle e análise dos sistemas de informação. Sua segunda edição, em 1998, ampliou a base de recursos, adicionando o guia prático de implementação e execução. A edição atual, já coordenada pelo *IT Governance*

*Institut*e, introduz as recomendações de gerenciamento de ambientes de TI dentro do modelo de maturidade de governança.

O COBIT recebe um conjunto de contribuições de várias empresas e organismos internacionais, entre eles:

- Padrões técnicos da ISO, EDIFACT, etc.
- Os códigos de conduta emitidos pelo Conselho de Europa, OECD, ISACA, etc.
- Critérios de qualificação para TI e processos: ITSEC, TCSEC, ISO 9000, SPICE etc.
- Padrões profissionais para controles internos e auditoria: COSO, IFAC, AICPA, CICA, ISACA, IIA, PCIE, GAO, etc.
- Práticas e exigências dos fóruns da indústria (ESF, I4) e das plataformas recomendadas pelos governos (IBAG, NIST, DTI), etc.
- Exigências das indústrias emergentes como operação bancária, comércio eletrônico e engenharia de software.

2.5.2.2 Benefícios do COBIT

Na era da dependência eletrônica dos negócios e da tecnologia, as organizações devem demonstrar controles crescentes em segurança. Cada organização deve compreender seu próprio desempenho e deve medir seu progresso. O *benchmarking* com outras organizações deve fazer parte da estratégia da empresa para conseguir a melhor competitividade em TI. As recomendações de gerenciamento do COBIT com orientação no modelo de maturidade em

governança auxiliam os gerentes de TI no cumprimento de seus objetivos alinhados com os objetivos da organização.

Os *guidelines* de gerenciamento do COBIT focam na gerência por desempenho usando os princípios do BSC (*Balanced Scorecard).* Seus indicadores-chave identificam e medem os resultados dos processos, avaliando seu desempenho e alinhamento com os objetivos dos negócios da organização.

2.5.2.3 Ferramentas de Gerenciamento do COBIT

Os modelos de maturidade de governança são usados para o controle dos processos de TI e fornecem um método eficiente para classificar o estágio da organização de TI. A governança de TI e seus processos, com o objetivo de adicionar valor ao negócio através do balanceamento do risco e retorno do investimento, podem ser classificados da seguinte forma:

0. Inexistente
1. Inicial/ *Ad Hoc*
2. Repetitivo, mas intuitivo
3. Processos definidos
4. Processos gerenciáveis e medidos
5. Processos otimizados

Essa abordagem é derivada do modelo de maturidade para desenvolvimento de software, SW-CMM *(Capability Maturity Model for Software)*, proposto pelo SEI *(Software Engineering Institute*). A partir desses níveis, foi desenvolvido para cada um dos 34 processos do COBIT um roteiro para diagnóstico, conforme etapas a seguir:

I. Onde a organização está hoje

II. O atual estágio de desenvolvimento da indústria (*best-in-class*)

III. O atual estágio dos padrões internacionais

IV. Aonde a organização quer chegar

Os fatores críticos de sucesso definem os desafios mais importantes ou ações de gerenciamento que devem ser adotadas para colocar sobre controle a gestão de TI. São definidas as ações mais importantes do ponto de vista do que fazer a nível estratégico, técnico, organizacional e de processo.

Os indicadores de objetivos definem como serão mensurados os progressos das ações para atingir os objetivos da organização, usualmente expressos nos seguintes termos:

- Disponibilidade das informações necessárias para suportar as necessidades de negócios;
- Riscos de falta de integridade e confidencialidade das informações;
- Eficiência nos custos dos processos e operações;
- Confirmação de confiabilidade, efetividade e conformidade das informações;
- Indicadores de desempenho definem medidas para determinar como os processos de TI estão sendo executados e se eles permitem atingir os objetivos planejados; são os indicadores que definem se os objetivos serão atingidos ou não; são os indicadores que avaliam as boas práticas e habilidades de TI.

Como a maioria dos gestores de TI não possuem habilidade para demonstrar os riscos associados ao negócio e nem mesmo os corretos procedimentos relativos à TI, este modelo contribui para melhorar o processo de análise de riscos e tomada de decisão através de um processo estruturado para gerenciar e controlar as iniciativas de TI nas empresas, além de garantir o retorno de investimentos e adição de melhorias nos processos empresariais.

2.5.3 A Norma NBR ISO/IEC 17799

A Norma Brasileira ISO/IEC 17799 – Tecnologia da Informação/ Código de prática para a gestão da segurança da informação – tem sua origem na primeira parte da Norma Britânica BS7799, desenvolvida pela *British Standards Institute* (BSI), iniciada em 1995, contendo uma introdução, definição de extensão e condições principais de uso da norma. Disponibilizava ainda 148 controles divididos em dez partes distintas. Esta norma foi planejada como um documento de referência para implementar "boas práticas" de segurança nas empresas. Posteriormente, foi padronizada pela *International Organization for Standardization* (ISO) em 2000 como ISO/IEC 17799.

O objetivo desta norma é fornecer recomendações para a gestão da segurança da informação para uso dos departamentos responsáveis pela introdução, implementação ou manutenção da segurança em suas organizações, proporcionando uma base comum para o desenvolvimento das normas de segurança organizacional e das práticas efetivas de gestão da segurança, e prover confiança nos relacionamentos entre as organizações. É importante observar que essas recomendações descritas na norma estejam de acordo com a legislação e regulamentação vigente.

A NBR ISO/IEC 17799 abrange ao todo 10 domínios, reunidos em 36 grupos que se totalizam em 127 controles, sendo seus domínios a Política de Segurança, a Segurança Organizacional, a Classificação e Controle dos Ativos de Informação, a Segurança de Pessoas, a Segurança Física e do Ambiente, o Gerenciamento das Operações e Comunicações, o Controle de Acesso, o Desenvolvimento e Manutenção de Sistemas, a Gestão da Continuidade do Negócio e a Conformidade.

Atualmente esta norma está entre as ferramentas mais utilizadas em todo o mundo, uma compilação de recomendações para melhores práticas de segurança, que podem ser aplicadas por empresas, independentemente do seu porte ou setor. Ela foi criada com a intenção de ser um padrão flexível, nunca guiando seus usuários a seguirem uma solução de segurança específica em detrimento de outra. As recomendações da ISO 17799 são neutras com relação à tecnologia e não fornecem nenhuma ajuda na avaliação ou entendimento de medidas de segurança já existentes.

A flexibilidade e imprecisão da ISO 17799 são intencionais, pois é muito difícil criar um padrão que funcione para todos os diversos ambientes de TI. Ela simplesmente fornece um conjunto de regras, em uma indústria onde elas não existiam.

As onze seções de controle da norma da Associação Brasileira de Normas Técnicas (ABNT), NBR ISO/ IEC 17799:2005 (Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação) são:

Seção 5 - Política de Segurança da Informação;

Seção 6 - Organizando a Segurança da Informação;

Seção 7 - Gestão de Ativos;

Seção 8 - Segurança em Recursos Humanos;

Seção 9 - Segurança Física e do Ambiente;

Seção 10 - Gestão das Operações e Comunicações;

Seção 11 - Controle de Acesso;

Seção 12 - Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;

Seção 13 - Gestão de Incidentes e Segurança da Informação;

Seção 14 - Gestão da Continuidade do Negócio;

Seção 15 - Conformidade;

Vale ressaltar que a ordem das seções não significa o seu grau de importância ou criticidade. Dependendo das circunstâncias, todas as seções podem ser importantes e críticas. Como mencionado anteriormente, a norma ISO 17799 é intencionalmente flexível e genérica e, como pode ser observado pelos diversos controles, é complexa. Por este motivo e para a obtenção de melhores resultados, requer ferramentas complementares.

O próximo capítulo apresenta a metodologia utilizada nesta dissertação.

3 PROCEDIMENTO METODOLÓGICO

Este capítulo apresenta a metodologia que foi utilizada para a realização desta dissertação, tal como: Método adotado de pesquisa, tipo de pesquisa, unidade de análise, unidade de observação, coleta de dados, análise e tratamento dos dados e as limitações do método.

3.1 Caracterização

Na presente pesquisa, buscou-se conhecimento a respeito do assunto, com vistas a aplicá-lo na construção de uma proposta de solução para um problema associado à realidade empresarial da atualidade. Assim, quanto à sua natureza, classifica-se como pesquisa aplicada, conforme Silva e Menezes (2001).

Quanto à forma de abordagem do problema, a presente pesquisa caracteriza-se como uma pesquisa qualitativa que, segundo Yin (1984), tem a sua essência no uso da observação detalhada do mundo natural, feita pelo pesquisador, e ressaltando que esta observação é, necessariamente, baseada em um modelo teórico.

Para Liebscher (1988), esta abordagem justifica-se quando o fenômeno em estudo é complexo, de natureza social e não tende à quantificação. É o caso da aplicação da Segurança da Informação e Proteção dos Conhecimentos Corporativos visando a mitigação dos riscos empresariais no Brasil.

- Bogdan & Biklen (1994) indicam as principais características da pesquisa qualitativa que servirão de base para este trabalho. São elas:
- A pesquisa qualitativa tem como fonte direta dos dados o ambiente natural e o pesquisador como instrumento-chave;
- Os dados coletados, em sua maioria, são descritivos;
- Os pesquisadores qualitativos preocupam-se com o processo e não simplesmente com os resultados e o produto;
- A análise dos dados tende a ser um processo indutivo;
- O “significado” é a preocupação essencial da abordagem qualitativa.

Quanto aos seus objetivos, a presente pesquisa caracteriza-se como exploratória descritiva. Segundo Gil (1996), a pesquisa exploratória busca tornar o problema mais explícito, enquanto que a pesquisa descritiva tem como objetivo descrever características de uma determinada população, fenômeno ou o estabelecimento de relações entre variáveis. Para Rudio (1986), o pesquisador deve procurar conhecer e interpretar a realidade, sem nela interferir para modificá-la.

Segundo Ruiz (1979, p.57),

> O processo de leitura exploratória, seletiva, reflexiva e interpretativa favorece a construção dos argumentos por progressão ou por oposição. Para, este tipo de trabalho é denominado pesquisa bibliográfica, já que, para o autor, "qualquer espécie de pesquisa, independente da área, supõe e exige pesquisa bibliográfica prévia, quer com atividade exploratória, ou para estabelecer o s*tatus quaestions* ou ainda para justificar os objetivos e contribuições da própria pesquisa".

Quanto aos procedimentos técnicos, a presente caracteriza-se como uma pesquisa bibliográfica e pesquisa documental. Segundo Gil (1996, p.51), a pesquisa bibliográfica é elaborada a partir de material já publicado em livros, artigos, revistas, jornais e Internet.

Já a pesquisa documental, assemelha-se muito à pesquisa bibliográfica. A diferença essencial entre ambas está na natureza das fontes. Enquanto a pesquisa bibliográfica se utiliza fundamentalmente das contribuições dos diversos autores sobre determinado assunto, a pesquisa documental vale-se de materiais que não receberam ainda tratamento analítico, ou que ainda podem ser re-elaborados de acordo com os objetos da pesquisa.

Na análise documental, foram pesquisadas as fontes e a bibliografia. As fontes são os textos originais ou textos de primeira mão, sobre determinado assunto. A bibliografia é o conjunto das produções escritas para esclarecer as fontes, divulgá-las, analisá-las, refutá-las ou para estabelecê-las; é toda a literatura originária de determinada fonte.

A análise documental pode ser definida também como uma série de operações que visam a estudar e a analisar um ou vários documentos, para descobrir as circunstâncias com as quais podem estar relacionadas. Ela pode proporcionar dados suficientemente ricos para evitar a perda de tempo com levantamento de campo, a partir da análise de documentos do tipo registros estatísticos, arquivos históricos, planilhas e outros disponíveis na organização.

Esta pesquisa também se classifica como pesquisa participante pelo fato do autor trabalhar na área de Segurança da Informação de uma grande empresa brasileira do setor de mineração e suas observações terem sido compiladas nas proposições das melhores práticas para a implantação da gestão da segurança da informação e dos conhecimentos corporativos. Para Thiollent (2000, p. 72),

> "...Pesquisa participante é um tipo de pesquisa social com base empírica que é concebida e realizada em estreita associação com uma ação ou com a resolução de um problema coletivo e no qual os pesquisadores e os participantes representativos da situação ou do problema estão envolvidos de modo cooperativo ou participativo.".

3.2 Universo

O universo de análise desta pesquisa foi o mercado corporativo brasileiro, não sendo enfocado um setor específico. Devido à riqueza e potencialidade da Segurança da Informação e Proteção dos Conhecimentos Corporativos, a abrangência estende-se a todas as organizações que estejam inseridas num ambiente de competição ou concorrência, sejam elas indústrias que produzam determinados produtos, empresas ligadas a atividades comerciais ou fornecedores de serviços em geral.

3.3 Procedimento de Obtenção de Dados

No levantamento dos dados da pesquisa para a presente dissertação, foram utilizadas primordialmente as técnicas da análise documental e pesquisa bibliográfica, as quais abrangeram a busca de informações relacionadas ao assunto em livros, brochuras, artigos publicados em conferências sobre o tema, relatórios, artigos de periódicos, informações disponibilizadas na Internet e, sobretudo, as duas pesquisas supracitadas que foram realizadas por entidades reconhecidas internacionalmente.

Quanto aos meios de investigação, trata-se de uma análise documental de duas pesquisas realizadas no mercado corporativo brasileiro, a primeira sobre as fraudes e a segunda sobre a segurança da informação. Além disso, foi realizada pesquisa bibliográfica, baseada nos temas que norteiam o objetivo do trabalho.

Esta etapa da coleta de dados teve a finalidade de levantar, principalmente, os conceitos sobre informação, conhecimento, segurança da informação e proteção dos conhecimentos corporativos além das forças que governam a avaliação de riscos, contidos na literatura. Para essa revisão bibliográfica, foi utilizada a literatura disponível sobre o assunto, nacional e estrangeira.

No próximo capítulo será apresentada através da análise documental como as empresas têm gerenciado a segurança da informação e como está a questão das fraudes que tanto ameaçam os negócios colocando em risco a própria sobrevivência das empresas.

4 ANÁLISE DOCUMENTAL E DISCUSSÃO DOS RESULTADOS

Esta etapa do desenvolvimento dessa dissertação abrangeu a realização de uma análise documental que teve a finalidade de avaliar, principalmente, a situação das fraudes e atos correlatos e também a segurança da informação no ambiente corporativo brasileiro. Nesta análise documental foram utilizadas duas pesquisas, a saber:

A primeira foi a pesquisa 2004 KPMG sobre A Fraude no Brasil que com base em entrevistas com diretores e presidentes de empresas no Brasil, fornece uma visão abrangente acerca das percepções, das verdades e dos impactos das fraudes no mundo dos negócios. A fraude - desde o simples furto de ativos até manipulações financeiras e contábeis complexas - continua a ser uma questão relevante e tem se tornado cada vez mais importante aos olhos de investidores, administradores de empresas, órgãos reguladores e outros participantes do mercado.

Leis e regulamentos, nacionais e internacionais, cada vez mais exigentes estão forçando as empresas a priorizar a governança com o objetivo de gerar credibilidade e encorajar investimentos nos mercados de capitais. As penalidades pela transgressão das regras são severas e, portanto, identificar e responder aos casos de fraude permanecem como desafios contínuos mesmo para as empresas mais sofisticadas. Entretanto, como essa pesquisa demonstra, as fraudes podem ser mitigadas pela implementação de controles efetivos e da gestão da segurança da informação e dos conhecimentos corporativos.

A segunda foi a Pesquisa Nacional de Segurança da Informação em sua 9ª edição. Neste estudo, considerado um dos importantes norteadores do segmento no Brasil, é

apresentado um panorama da segurança da informação atualizado contendo as principais tendências do mercado nacional, indicadores e melhores práticas.

Os resultados encontrados nesta pesquisa reforçam a importância dos fatores de capacitação e conscientização como pontos fundamentais para proteção das informações corporativas. Para tornar essa constatação realidade é necessária a contínua adoção de controles para mitigar ameaças, riscos e vulnerabilidades que rondam o ambiente corporativo.

4.1 Pesquisa sobre Fraudes

Para ilustrar o *status* da fraude no Brasil, seguem dados obtidos na terceira edição da pesquisa "A Fraude no Brasil", de 2004, da KPMG *Transaction and Forensic Services* S/C Ltda, realizada junto aos executivos-chefes das principais empresas brasileiras e cujo objetivo é disponibilizar informações importantes, voltadas ao assunto de fraudes no Brasil.

Em agosto de 2004, a área de *Forensic* da KPMG enviou a aproximadamente 1.000 empresas um novo questionário sobre a fraude empresarial. O objetivo foi espelhar o pensamento dos executivos-chefes acerca da questão, bem como atualizar, analisar e comparar os resultados ora obtidos com aqueles oriundos das pesquisas de 2000 e 2002. A maioria dos respondentes pertence ao ramo industrial (57%), com faturamento anual concentrado nas faixas de R$ 250 milhões a R$ 3 bilhões (71%), ocupando, em geral, posições nas Diretorias Financeira, Administrativa ou de Revisão/Auditoria Interna (49%).

Nesta terceira edição bienal, novamente foram abordados aspectos fundamentais relativos ao ato fraudulento nas organizações: suas características, suas formas, o perfil do fraudador, o comércio eletrônico, a espionagem corporativa, as conseqüentes medidas e os procedimentos adotados para dificultar e mitigar sua ocorrência.

De acordo com o GRAF. 1, mais da metade das empresas participantes da pesquisa descobriu a fraude por meio de seus Controles Internos (52%). A Auditoria e a Revisão Interna também foram formas de constatar um grande número de atos fraudulentos (39%). Quase 30% receberam informações de seus próprios funcionários.

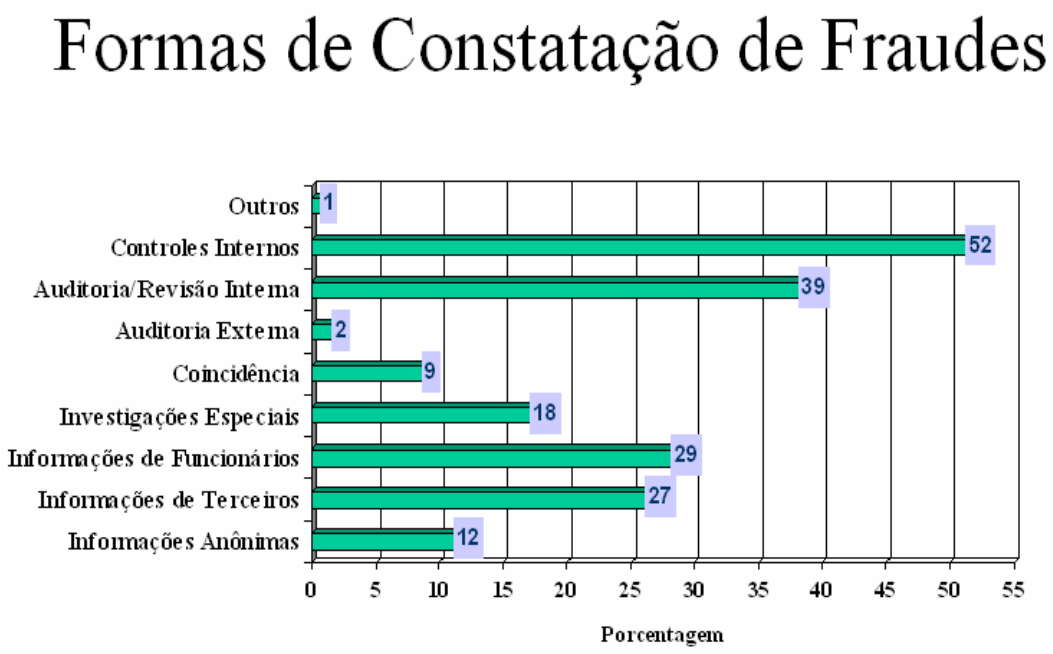

Gráfico 1. Formas de Constatação de Fraude.
Fonte: Elaborado pelo autor deste trabalho a partir de 2004 KPMG *Transaction and Forensic Services Ltda*.

A precariedade do sistema de Controles Internos é simultaneamente indicada como uma circunstância facilitadora de fraudes (71%) e 26% dos respondentes alocaram o problema de *management override*, ou seja, controles internos burlados. Assim, como mostra o GRAF. 1, um forte e estruturado sistema de controles internos previne, detecta e evita a ocorrência de atos fraudulentos. A seguir são destacados os principais resultados encontrados na pesquisa.

O índice de respondentes que vivenciaram fraudes em suas organizações foi de 69%. Todavia, no universo empresarial, pela relutância em responder ou pela impossibilidade de algumas empresas em quantificarem suas experiências ou, ainda, considerando as numerosas

fraudes que podem passar despercebidas, é possível presumir que tal número não representa a totalidade real de perdas.

Para 74% de todos os respondentes, a fraude é ou pode tornar-se um grande problema para sua empresa;

Para 55% dos respondentes, a fraude aumentará no futuro; apenas 18% acreditam que ela diminuirá. As razões citadas para essa expectativa de aumento futuro são, principalmente, o enfraquecimento dos valores na sociedade, falhas no sistema de controle, impunidade e pressões econômicas.

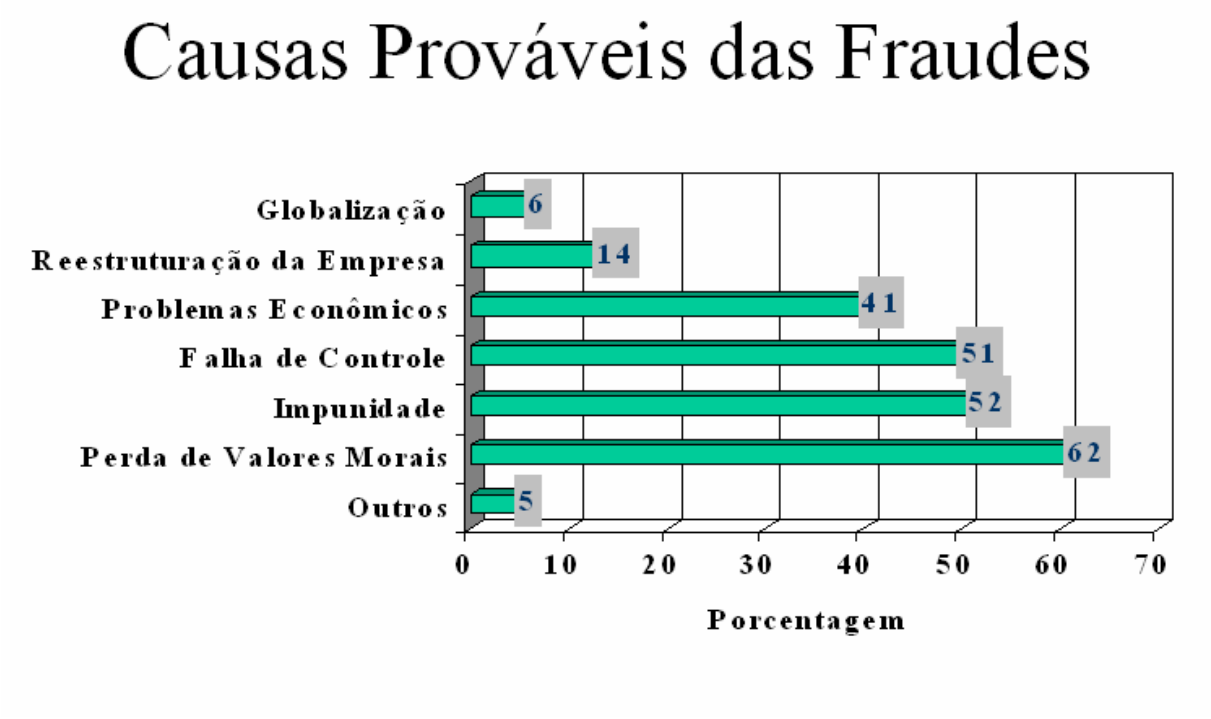

Gráfico 2. Causas Prováveis das Fraudes.
Fonte: Elaborado pelo autor deste trabalho a partir de 2004 KPMG *Transaction and Forensic Services Ltda*.

Assim como controles internos deficientes permitiram a ocorrência de fraudes (71%), bons controles internos foram citados como um dos métodos mais comuns de sua detecção (52%). Isso ressalta o papel central dos controles internos no combate à fraude conforme GRAF 1.

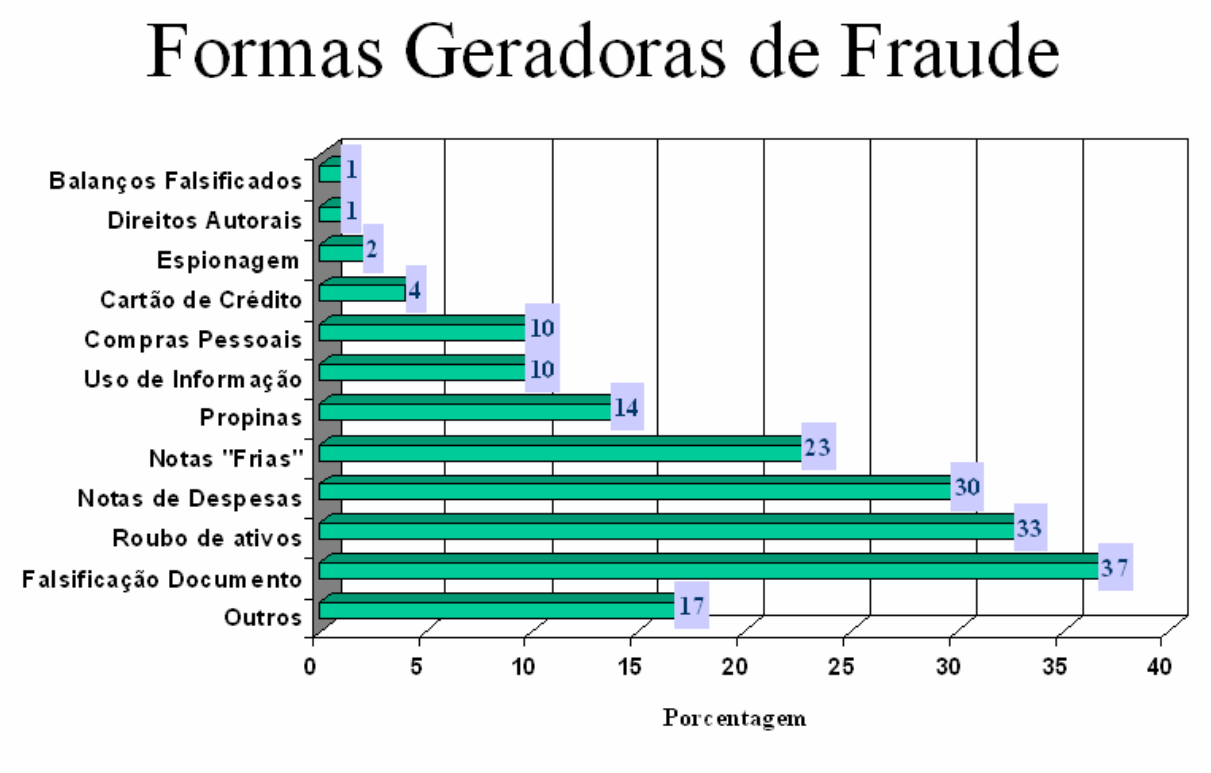

Gráfico 3. Formas Geradoras de Fraude.
Fonte: Elaborado pelo autor deste trabalho a partir de 2004 KPMG *Transaction and Forensic Services Ltda*.

Conforme GRAF. 3, os tipos de fraudes que resultaram nas maiores perdas foram falsificação de cheques ou documentos, roubo de ativos e notas de despesas e notas frias.

O resultado mostra que os participantes adquirem um maior conhecimento sobre como as fraudes podem ocorrer nas organizações: 93% têm conhecimento sobre o assunto. O Grau de Conhecimento da Diretoria sobre Fraudes, suas Formas e Práticas tem crescido significativamente.

Dentro das causas prováveis para o crescimento de atos fraudulentos, a exemplo das respostas das pesquisas passadas, atribuiu-se ao enfraquecimento dos valores sociais e morais (62%) a grande causa para o aumento na ocorrência de fraudes. São citadas em seguida a impunidade (52%), as falhas nos controles (51%) e as dificuldades econômicas (41%).

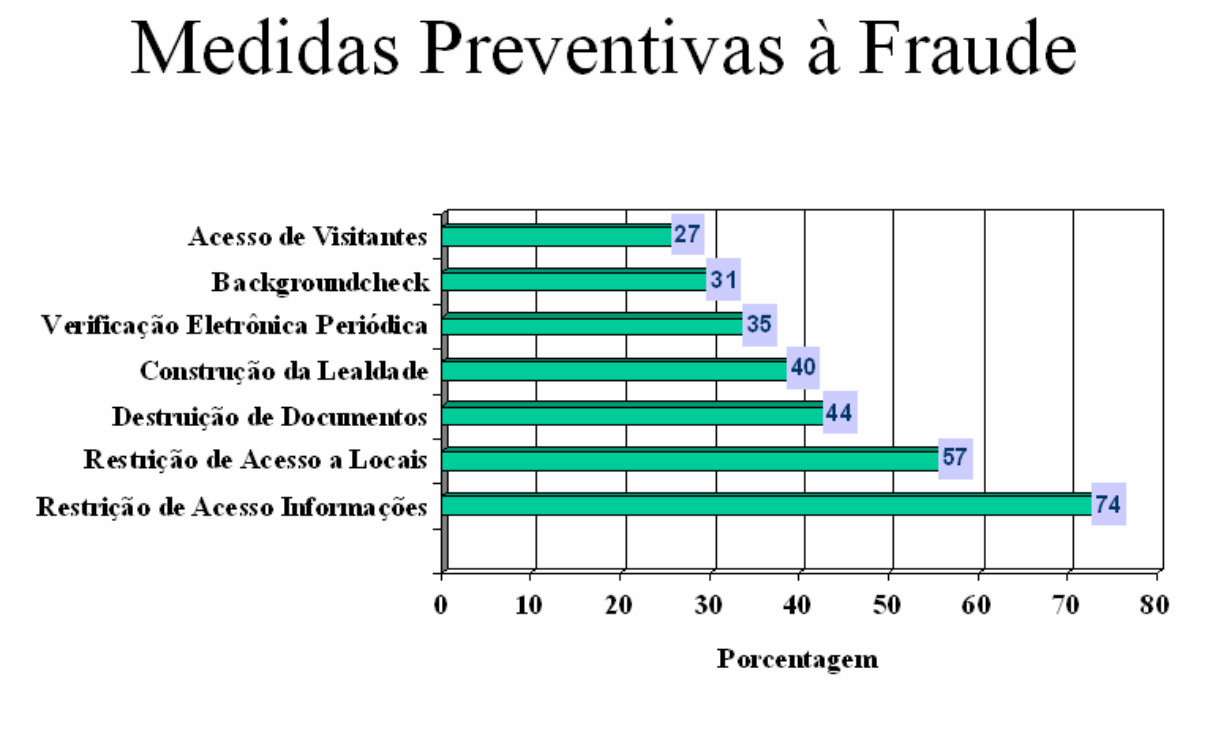

Gráfico 4. Medidas Preventivas à Fraude.
Fonte: Elaborado pelo autor deste trabalho a partir de 2004 KPMG *Transaction and Forensic Services Ltda*.

Para 83% dos respondentes, os montantes envolvidos em fraude foram inferiores a R$ 1 milhão; porém, em 49% dos casos, não se recuperou nenhuma parte do valor.

Como parte de seus planos para diminuir a possibilidade de fraudes, as organizações pretendem se concentrar em métodos internos de detecção, em treinamento de pessoal e no estabelecimento de um código de conduta ou de um manual de comportamento profissional.

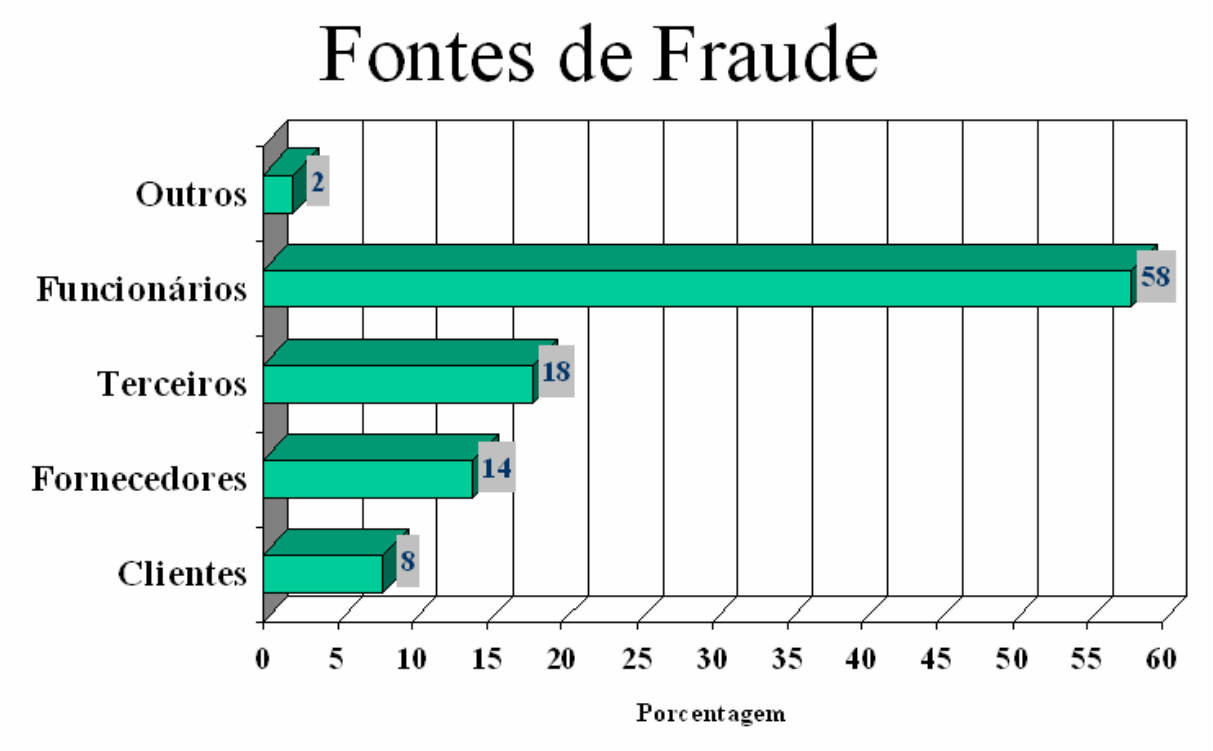

Gráfico 4. Fontes de Fraude.
Fonte: Elaborado pelo autor deste trabalho a partir de 2004 KPMG *Transaction and Forensic Services Ltda*.

O fraudador típico é homem (83%), situa-se na faixa etária de 26 a 40 anos (70%) e recebe, mensalmente, entre R$ 1.000,00 e R$ 4.500,00 (61%). A maioria das fraudes reportadas foi cometida por funcionários com mais de dois e menos de cinco anos na empresa.

Como uma constante, as respostas quanto à origem do fraudador deixam claro que o maior deles está dentro da empresa: é o funcionário (quase 60%). Houve um crescimento de 14,5% no índice do empregado fraudador.

Os respondentes acreditam que seus próprios funcionários (58%) são a maior fonte de ameaça, especialmente seu pessoal de suporte (57%), esse resultado sinaliza que o fraudador agiu propositadamente, conforme Doyle (2002).

Como de acordo com o GRAF. 4 a maior fonte de fraude nas empresas foram seus próprios funcionários, foi solicitado aos respondentes a caracterização dos fraudadores.

Segundo mostra o GRAF. 5, o pessoal de suporte (staff) gerou a maioria das perdas incorridas nas organizações (57%). Funcionários em posição de chefia e gerência foram também responsáveis por uma considerável parcela dos casos: 26% e 16%, respectivamente.

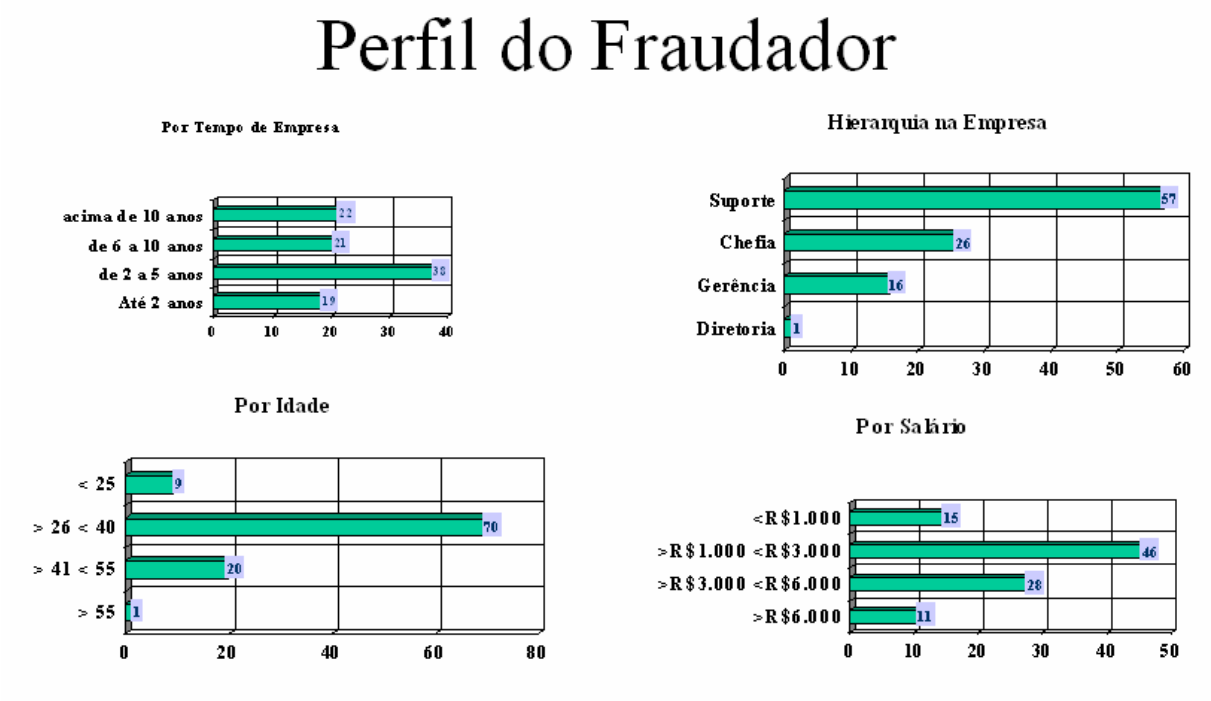

Gráfico 5. Perfil do Fraudador.
Fonte: Elaborado pelo autor deste trabalho a partir de 2004 KPMG *Transaction and Forensic Services Ltda*.

Os negócios por meio de comércio eletrônico foram realizados por 44% dos participantes. Destes, 51% atuam no B2B (*Business to Business*), 15% no B2C (*Business to Consumer*) e 34% em ambas as áreas.

Apenas 11% dos usuários do comércio eletrônico tiveram problemas de segurança em seus sistemas.

O crime organizado representa uma ameaça/perigo para a indústria ou a empresa, segundo 77% dos respondentes. As maiores preocupações são fraudes e roubos, bem como a utilização de informações privilegiadas, pois representam ativos estratégicos da organização (DAVENPORT, 1998).

A espionagem corporativa representa uma ameaça ou perigo para a área de atuação e/ou para a própria empresa de 66% dos respondentes.

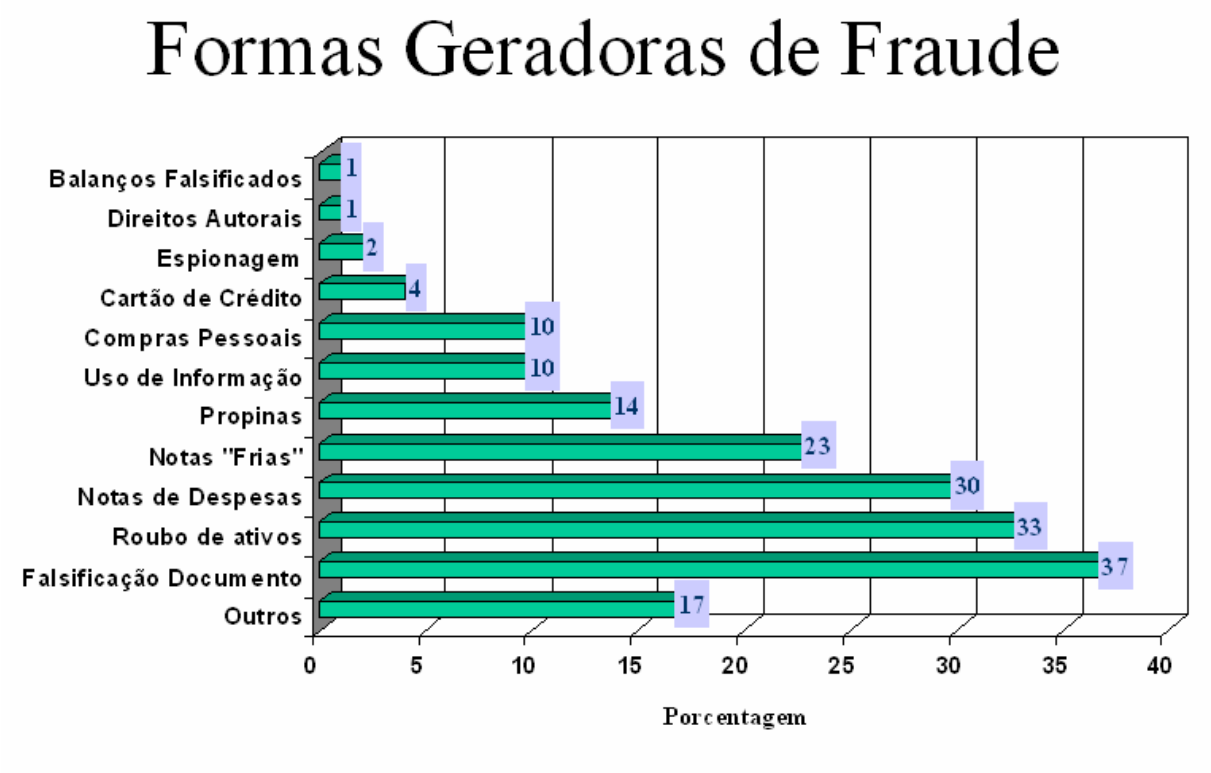

Gráfico 6. Formas Geradoras de Fraude.
Fonte: Elaborado pelo autor deste trabalho a partir de 2004 KPMG *Transaction and Forensic Services Ltda*.

Os tipos de formas geradoras de fraude classificados no item “Outros” incluem acesso não autorizado a computador (DOYLE, 2002), avaliação de crédito fraudulenta, cobranças falsas ou superfaturadas e não-conciliação de transações intra-escritórios. A rejeição por parte dos clientes e/ou fornecedores é o motivo que prevalece para aqueles que não estão realizando negócios por meio de comércio eletrônico, enquanto questões de segurança tendem a ser uma preocupação secundária.

Após a análise das respostas, fica visível a contínua preocupação do empresariado brasileiro em relação à fraude e atos correlatos. Através da mídia em geral, pode-se observar novos escândalos de fraudes e atos ilícitos praticados e suas graves conseqüências, o que faz lembrar que toda organização é vulnerável à fraude. (KRELTSZHEIM, 1999).

O tema torna-se mais complexo e interessante para os respondentes, enquanto seu resultado repete, ao mercado em geral, a posição das organizações no Brasil perante o assunto. O índice geral de respostas mostra uma evolução, denotando que, a cada dia, os executivos sentem a necessidade de discutir um problema sério, que gera graves perdas financeiras e éticas.

A maioria das empresas, ao longo das suas vidas corporativas, enfrentará o ato fraudulento, de uma forma ou de outra. Se as empresas sobreviverão às experiências ou emergirão mais fortes dependerá, em última análise, das atitudes e dos processos internos em vigor, para responder, controlar e prevenir a fraude. Assim como baixos índices de criminalidade não significam a aparente ausência de crimes, o desconhecimento de fraudes em sua organização não significa sua inexistência. Este fato é ressaltado por Kreltszheim (1999).

Os índices de atos fraudulentos têm incentivado pesquisas sobre segurança da informação. Cuja finalidade é mapear o *status* da situação e também conscientizar sobre a importância da segurança da informação.

4.2 Pesquisa sobre Segurança da Informação

Prosseguindo com análise documental, avaliou-se a 9ª edição da Pesquisa Nacional de Segurança da Informação. Neste estudo, considerado um dos importantes norteadores do segmento no Brasil, é apresentado um panorama atualizado das principais tendências do mercado nacional, indicadores, melhores práticas, além de uma análise comparativa entre as pesquisas de 2002 e 2003.

A pesquisa foi desenvolvida e coordenada pela Módulo Security Solutions S.A., empresa brasileira líder em segurança da informação na América Latina e a primeira empresa de segurança da informação do mundo a conquistar a certificação ISO 27001.

A ISO 27001 é a primeira norma mundial para certificação em segurança da informação e é a evolução do padrão britânico BS 7799, que será abordado nesta dissertação. Ela trata da definição de requisitos para implementação de um Sistema de Gestão de Segurança da Informação – SGSI. Em outubro de 2005, a norma foi incorporada pela "*The International Organization for Standardization* (*ISO*)", que cuida de padrões internacionais de certificação.

A publicação da ISO 27001 demonstra a importância conquistada pela Segurança da Informação, que passa a ser percebida como estratégica para o negócio de qualquer companhia. Um dos resultados do fortalecimento desta norma é o aumento do interesse das organizações em obter um certificado reconhecido mundialmente, a exemplo do que aconteceu com ISO 9001, para qualidade, e ISO 14001, para meio ambiente.

De acordo com a metodologia empregada, a coleta de dados contou com respostas presenciais e via on-line. Totalizando, a pesquisa quantitativa teve uma amostra de 682 questionários, coletados entre março e agosto de 2003, junto a profissionais ligados às áreas de Tecnologia e Segurança da Informação. Os questionários foram compostos por 40 questões objetivas, sendo algumas de respostas múltiplas. Foram computadas somente as perguntas efetivamente respondidas.

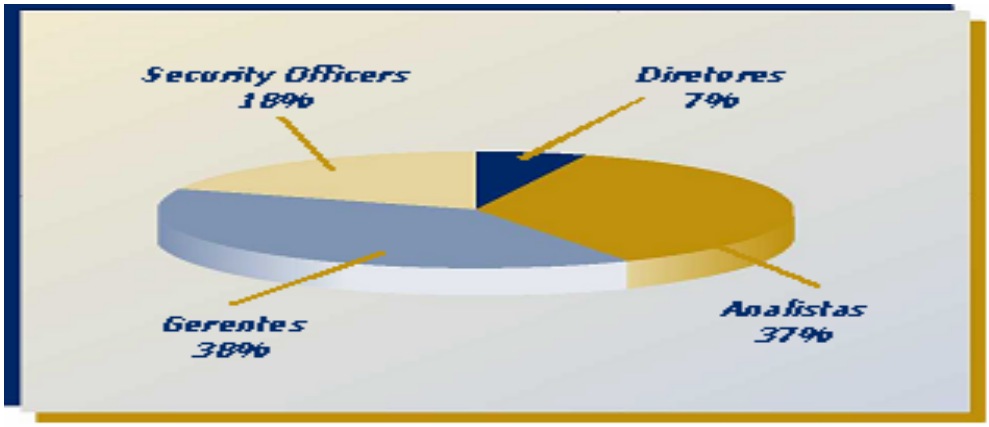

Gráfico 7: Perfil dos Entrevistados.
Fonte: 9ª edição da Pesquisa Nacional de Segurança da Informação de Outubro de 2003.

Como mostra o GRAF. 8, os profissionais que participaram deste estudo estão distribuídos em diversos segmentos, como: Financeiro (21%), Governo (17%), Indústria e Comércio (14%), Tecnologia/Informática (14%), Prestação de Serviços (9%), Outros (8%), Telecomunicações (7%), Comércio/Varejo (4%), Energia Elétrica (2%), Educação (2%) e Saúde (2%), correspondendo a cerca de 50% das 1.000 maiores empresas brasileiras.

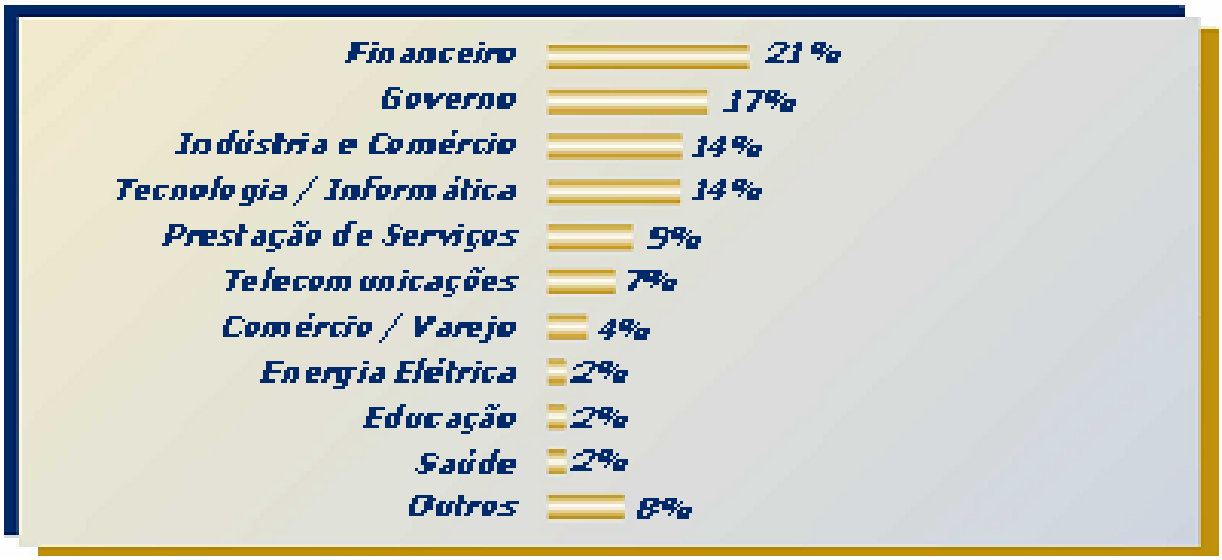

Gráfico 8: Ramo de Atividade das Empresas Pesquisadas
Fonte: 9ª edição da Pesquisa Nacional de Segurança da Informação de Outubro de 2003

Sobre as legislações, normas e regulamentações de segurança que norteiam suas organizações, 63,5% dos entrevistados apontaram a ISO 17799; 37%, as publicações do Governo Federal (decreto 4553 e outros); 30%, as publicações do Banco Central (resolução 2554 e outras); 27%, a Regulamentação da ICP-Brasil; 20%, o COBIT; e 20%, as Publicações da CVM (Resolução 358 e outras).

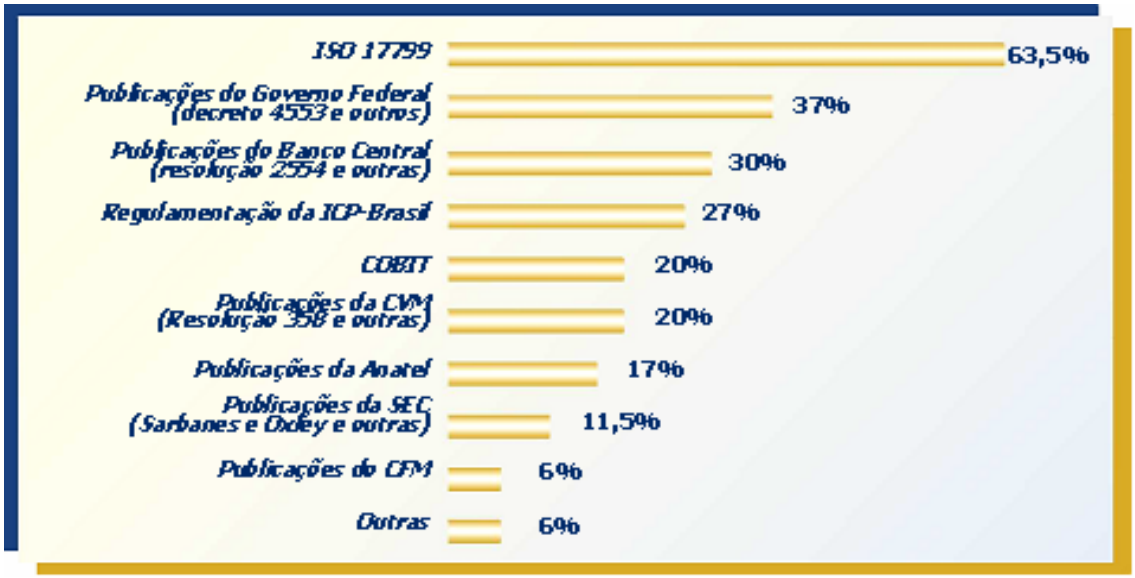

Gráfico 9: Legislações, Normas e Regulamentações de Segurança
Fonte: 9ª edição da Pesquisa Nacional de Segurança da Informação de Outubro de 2003

O ano de 2003 foi de grande importância para a Segurança da Informação, e pode-se dizer que ele marca o início da fase madura do setor. As equipes de segurança das empresas encontram-se estruturadas ou em fase avançada de estruturação. Conforme observado por Oliveira (2003) a questão da segurança da informação tem que ser abordada de forma multidisciplinar e tem que envolver todos os funcionários de todos os setores da organização. Observa-se ainda, a crescente relação com os outros departamentos, com os executivos, e a cada dia há a convergência entre legislação, regulamentações e normas do setor, conforme Nakamura (2002).

Um dos mais importantes resultados desta pesquisa é o que trata da adequação com legislação, regulamentação e normas. Este estudo mostra que, por um lado, a ISO 17799 tem sido adotada fortemente como referência técnica pelas equipes de Segurança da Informação, seguida pelo COBIT, muitas vezes em conjunto. Mas, por outro lado, cada segmento tem também adotado as regulamentações específicas como, por exemplo, resoluções do Banco Central e decretos do Governo Federal.

Esta tendência de uso de normas e regulamentos é fortalecida com o Novo Código Civil, que traz maior responsabilização para os administradores das empresas e autoridades do Governo (NAKAMURA, 2002). Tudo isso tem se destacado como uma grande oportunidade para os profissionais de Segurança da Informação nos próximos anos, uma vez que a matéria se aproxima a cada dia da sua atividade-fim e dos executivos da organização (SÊMOLA, 2002).

Outro aspecto importante da pesquisa mostra que o profissional está interagindo cada vez mais com os departamentos de sua organização e que, a cada dia, deixa de se relacionar apenas com Tecnologia da Informação e Auditoria, e passa a ser interlocutor de departamentos como Jurídico, Recursos Humanos e Comunicação Social. Com isso, a segurança está deixando de ser técnica para ser normativa, e os profissionais precisam estar alertas para este desafio. (OLIVEIRA, 2002).

As principais ameaças apontadas são: vírus, funcionário insatisfeito, divulgação de senhas, acessos indevidos e vazamento de informações. Todas essas ameaças corroboram com a questão do ato intencional conforme afirma Doyle (2002).

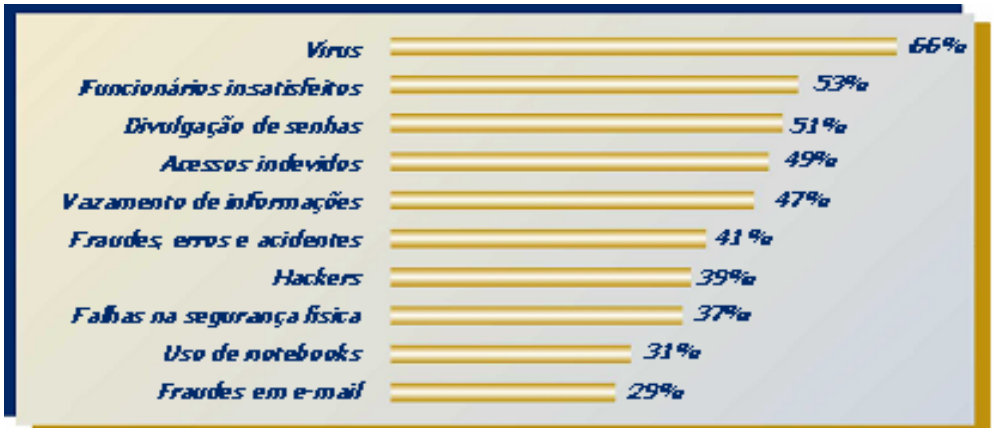

Gráfico 10: Principais Ameaças à Segurança da Informação
Fonte: 9ª edição da Pesquisa Nacional de Segurança da Informação de Outubro de 2003.

Com relação aos prejuízos contabilizados, 35% das empresas no Brasil tiveram perdas financeiras; 22% das empresas acima registraram perdas de até R$ 50 mil; 8%, entre R$ 50 mil e R$ 500 mil; 4%, de R$ 500 mil a R$ 1 milhão; e 65% não conseguem quantificar o valor dos prejuízos. À medida que os prejuízos crescem, aumentam os investimentos em segurança da informação (DIAS, 2000).

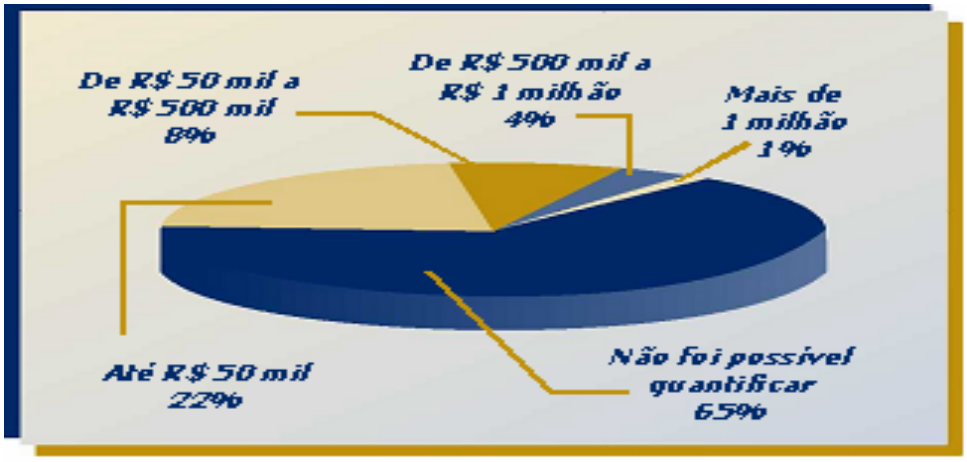

Gráfico 11: Prejuízos contabilizados com a falta de Segurança da Informação
Fonte: 9ª edição da Pesquisa Nacional de Segurança da Informação de Outubro de 2003

Dentre os principais problemas encontrados para implementação da segurança da informação, a falta de consciência dos executivos (23%), a dificuldade em demonstrar o

retorno (18%) e custo de implementação (16%) foram considerados os três principais obstáculos para implementação da segurança nas empresas.

Gráfico 12: Principais Ameaças à Segurança da Informação
Fonte: 9ª edição da Pesquisa Nacional de Segurança da Informação de Outubro de 2003

Em relação ao ano anterior, constatam-se duas mudanças significativas: a queda da falta de consciência dos usuários, que passou de 29% para 14%; e o aumento do custo de implementação, que passou de 1% para 16%.

A seguir, são destacados os principais resultados encontrados na pesquisa:

- Para 78% dos entrevistados, as ameaças, os riscos e os ataques deverão aumentar;
- 42% das empresas constantes da amostra tiveram problemas com a Segurança da Informação nos seis meses anteriores à pesquisa;
- 35% das empresas reconhecem que tiveram perdas financeiras. Já o percentual de empresas que não conseguiram quantificar essas perdas diminuiu de 72%, em 2002, para 65%, em 2003;
- Vírus (66%), funcionários insatisfeitos (53%), divulgação de senhas (51%), acessos indevidos (49%) e vazamento de informações (47%) foram apontados como as cinco principais ameaças à segurança das informações nas empresas;

- O percentual de empresas que afirmam ter sofrido ataques e invasões subiu de 43%, em 2002, para 77%, em 2003;
- 32% dos entrevistados apontam os *hackers* como os principais responsáveis por ataques e invasões de sistemas corporativos;
- 26% das empresas não conseguem sequer identificar os responsáveis pelos ataques;
- 48% não possuem nenhum plano de ação formalizado em caso de invasões e ataques;
- 60% indicam a internet como principal ponto de invasão em seus sistemas;
- 58% dos entrevistados sentem-se inseguros para comprar em sítios de comércio eletrônico por causa da sensação de falta de segurança;
- A falta de consciência dos executivos é apontada por 23% dos entrevistados como o principal obstáculo para implementação da segurança;
- 63,5% dos entrevistados adotam a ISO 17799 como a principal norma que norteia suas empresas;
- Política de Segurança formalizada já é realidade em 68% das organizações.
- Apenas 21% das empresas afirmaram possuir um Plano de Continuidade de Negócios (PCN) atualizado e testado;
- 60% das empresas fazem Planejamento de Segurança, sendo que 27% possuem Planejamento para até 1 ano;
- A área de Tecnologia (49,5%) continua sendo a principal responsável pelo gerenciamento da Segurança da Informação nas empresas, seguida pela área específica, *Security Office*, com 25,5%.
- Antivírus (90%), sistemas de backup (76,5%) e *firewall* (75,5%) foram apontados como as três medidas de segurança mais implementadas nas empresas;

- 60% afirmam que os investimentos de suas empresas em segurança para os próximos anos vão aumentar.

Estes dados reforçam a idéia de que a segurança das informações e conhecimentos corporativos deve ser alvo de grande interesse das empresas, principalmente aquelas que utilizam a Internet e estão totalmente conectadas. Ou seja, as empresas reconhecem a importância da segurança de suas informações e conhecimentos, porém muitas não estão preparadas para reagir caso venham a sofrer um ataque.

Em termos técnicos, a pesquisa ratificou como os desafios principais:

- A preocupação com vírus, funcionários insatisfeitos e senhas como principais ameaças;
- O aumento do uso da internet como meio de fraudes e vazamento de informação, acompanhando o desenvolvimento dos negócios eletrônicos;
- Conscientizar os executivos, motivar os usuários e capacitar a equipe técnica, assim como demonstrar o retorno sobre o investimento da segurança;
- A necessidade de realizar análise de riscos e revisar periodicamente a política de segurança;

A Segurança da Informação tornou-se fator prioritário na tomada de decisões e nos investimentos das organizações no país (SÊMOLA, 2003). Essa afirmação foi uma das principais conclusões apontadas pelos índices obtidos pela 9ª Pesquisa Nacional de Segurança da Informação.

Esses dados ficam evidentes quando se observa que 73% das empresas destinaram orçamento específico para área de Tecnologia da Informação e que, deste total, 28,5% alocaram mais de 5% para área de Segurança. Além disso, 60% dos entrevistados acreditavam que os investimentos de suas empresas aumentariam (DIAS, 2000).

A pesquisa trouxe ainda importantes avanços relacionados aos três principais aspectos dentro de um projeto de Segurança: Tecnologia (recursos físicos e lógicos), Pessoas (cultura, capacitação e conscientização) e Processos (metodologia, normas e procedimentos).

Em termos de Tecnologia, constatou-se a consolidação das soluções técnicas e pontuais (antivírus e *firewall*, por exemplo) como a principal medida de segurança implementada (PELISSARI, 2002). Além disso, os profissionais apontaram como satisfatória a oferta dessas ferramentas e soluções no mercado.

Em relação a Processos, é preciso ressaltar que as novas exigências legais como o novo Código Civil, a regulamentação da lei Sarbanes e Oxley (SARBOX), publicações do Banco Central entre outros, tornaram a segurança da informação prioridade entre os requisitos de negócios de executivos e empresas. Ainda nessa área, a pesquisa revela o fortalecimento da NBR ISO/IEC 17799 como a principal norma para implementação da gestão em segurança da informação, complementando outras normas, legislações e regulamentações que já vinham sendo utilizadas pelas organizações.

Analisando as principais ameaças (vírus, divulgação de senhas e vazamento de informações) e obstáculos para implementação da segurança da informação (falta de consciência de executivos e usuários) apontados na pesquisa, verificou-se a necessidade de um contínuo investimento em programas de formação, capacitação e conscientização. O fator positivo é que as organizações já vislumbraram a necessidade de reverter esse cenário: política de segurança e capacitação técnica estão entre as cinco principais medidas de segurança a serem implementadas.

Para alcançar o nível satisfatório de segurança das informações, é mister conhecer e dominar:

- Os requisitos básicos de segurança;
- Os riscos existentes, que colocam em xeque estes requisitos mínimos e os principais ataques conhecidos, que permitem perpetrar esta situação de risco;
- Os mecanismos de segurança, que existem para implementar estes requisitos básicos e eliminar os riscos existentes;
- As principais ferramentas desenvolvidas que permitem a implementação destes mecanismos.

Cada um destes itens é de vital importância. Os responsáveis pela segurança das informações e conhecimentos corporativos de cada empresa e os próprios usuários devem estar cientes desta responsabilidade e comprometidos com os resultados que devem ser alcançados (OLIVEIRA 2003).

Os resultados obtidos reforçam a importância dos fatores de capacitação e conscientização como pontos fundamentais para proteção das informações corporativas. Mas como tornar essa constatação realidade? A resposta pode estar na contínua adoção de controles para minimizar ameaças, riscos e vulnerabilidades que rondam os sistemas nos quais trafegam as informações e os conhecimentos corporativos das empresas.

O que se pode concluir é que, se muito já foi feito pela segurança das informações e conhecimentos corporativos, muito mais ainda há por se fazer para que estes ativos estratégicos possam ser totalmente seguros e livres de riscos.

Desta forma, nas próximas páginas desta dissertação, serão descritas e sugeridas algumas das melhores práticas de gestão da segurança da informação e dos conhecimentos corporativos, com base no referencial teórico, na análise documental e nas observações do autor desta dissertação.

5 SUGESTÕES DE MELHORES PRÁTICAS

5.1 Melhores Práticas para a Implantação da Gestão da Segurança da Informação e dos Conhecimentos Corporativos

O maior problema da segurança das informações é que os empregados pensam que proteger informações não é o seu trabalho ou que não faz parte do processo de trabalho. Já a segurança de informação e dos conhecimentos tradicionalmente nas empresas é focada em proteger o perímetro para manter as ameaças fora do ambiente corporativo. Entretanto como se pode observar, a quebra da segurança em grandes corporações é inevitável. *Hackers* poderão penetrar a rede, mas as ocorrências mais freqüentes são atribuídas aos inimigos internos que vão comprometer os dados de companhia e possivelmente seus clientes. Além disso, a concorrência, pode utilizar técnicas de indução junto aos empregados, visando tirar a informação de forma involuntária.

Com o avanço tecnológico emergiram ferramentas para ajudar na tarefa de proteger estes ativos. Porém, organizações que apenas implantam estas ferramentas achando que isso pode ser uma medida definitiva se enganam. Na verdade, é necessário um processo para responder imediatamente a esses incidentes para habilitar a sua administração, retenção e mitigação.

A gestão da segurança da informação e a sua conseqüente utilização para a produção dos conhecimentos corporativos se tornam elementos básicos para o desenvolvimento estratégico das organizações. Com a globalização, as organizações passaram a se preocupar

com a competitividade. Para que a organização possa manter a sua competitividade, precisa se posicionar no mercado com uma vantagem competitiva, atributo que decorre em grande parte da sua capacidade de gerir adequadamente a segurança da informação e dos conhecimentos corporativos.

O desafio para as organizações é lidar com a incerteza, a turbulência e a instabilidade de um mundo em transformação. Nesse contexto, é de fundamental importância para a sobrevivência da organização assegurar a proteção de suas informações e conhecimentos diante dos concorrentes, apesar das constantes mudanças no ambiente de negócios.

A organização deve se antecipar às mudanças, enxergar as oportunidades e observar com olhos críticos o panorama socioeconômico, visando identificar, antecipadamente, possíveis ameaças e oportunidades, o que permitirá à organização defender ou até ampliar a sua posição no mercado. Assim sendo, qualquer processo de segurança efetivo, seja ele segurança doméstica, segurança corporativa ou segurança nacional, precisa de ações que estejam em consonância com as melhores práticas internacionalmente aceitas. A seguir, são elencadas ações que vão ao encontro dessas melhores práticas:

1. A segurança da informação deve ser elaborada de forma ativa e preventiva, ou seja, o trabalho deve ser feito antecipadamente a uma perda de informação, os profissionais de segurança geralmente CSOs (*Chief Security Officers*), devem identificar padrões, vulnerabilidades e contramedidas para evitar a fuga e tornar eficaz o processo de gestão.

2. O modelo de segurança da informação proposto, deve ser alicerçado em medidas ativas. Estas são métodos para reduzir as vulnerabilidades no processo de produção, armazenamento e compartilhamento das informações. Devem ser vistas sob o prisma antecipatório, ou seja, preventivo. É por esta razão que a identificação da intrusão deve ser antes e não depois da perda de informação ou evento.

3. Os responsáveis pela proteção das informações e conhecimentos corporativos, CSOs, precisam adotar procedimentos para conduzir uma avaliação periódica sobre segurança, revisar os resultados com sua equipe e comunicar o resultado para a alta gestão;

4. Os CSOs precisam planejar, patrocinar e incentivar a adoção de boas práticas corporativas para segurança computacional, sendo municiados com indicadores objetivos que permitam avaliar as ameaças e vulnerabilidades;

5. As organizações devem conduzir periodicamente uma avaliação de riscos relacionada a informações e conhecimentos corporativos como parte do programa de gerenciamento de riscos empresariais;

6. As organizações precisam desenvolver e adotar políticas e procedimentos baseados na análise de riscos para garantir a segurança das informações e conhecimentos corporativos;

7. As organizações precisam estabelecer uma estrutura de gerenciamento da segurança empresarial para definir explicitamente o que se espera de cada indivíduo (papéis e responsabilidades);

8. As organizações precisam desenvolver um planejamento estratégico e tomar medidas efetivas para prover a segurança adequada para a sua rede de telecomunicações e seus sistemas computacionais por onde trafegam as informações e os conhecimentos corporativos;

9. As organizações precisam tratar a segurança empresarial como parte integral da gestão além de ser uma importante área de negócios, e não apenas uma área que evita perdas;

10. As organizações precisam divulgar as informações sobre segurança empresarial, treinando e educando os empregados;

11. As organizações precisam conduzir testes periódicos e avaliar a eficiência das políticas e procedimentos relacionados à segurança das informações e conhecimentos corporativos;

12. As organizações precisam definir e pôr em prática um plano para avaliar e mitigar vulnerabilidades ou deficiências que comprometam a segurança empresarial;

13. As organizações precisam desenvolver e colocar em prática ações e procedimentos de resposta imediata a incidentes;

14. As organizações precisam definir um plano de continuidade de negócios e testar sua funcionalidade, mantendo-o sempre atualizado;

15. As organizações precisam adotar *frameworks* com as melhores práticas relacionadas à segurança da informação, como o COBIT, o ITIL e a ISO 17799, para medir o nível de maturidade dos processos alcançado com relação à segurança da informação.

Para que estas práticas se tornem apropriadas e efetivas, elas devem ter a aceitação e o suporte de todos os níveis de empregados dentro da organização. É especialmente importante que a alta administração suporte de forma completa os processos propostos, caso contrário haverá pouca chance que ela tenha o impacto desejado (PELISSARI, 2002).

Uma grande mudança vem ocorrendo no mundo corporativo: a mudança de uma economia tipicamente industrial para uma economia globalizada, com um foco muito forte na informação e no conhecimento. Nessa nova economia, o processo de gestão da segurança das informações e conhecimentos corporativos entra como uma forma de manter uma vantagem competitiva sustentável, a qual se torna cada vez mais útil aos gestores no desenvolvimento do planejamento estratégico das organizações.

A segurança é a base para dar às empresas a possibilidade e a liberdade necessárias para a criação de novas oportunidades de negócio (MOREIRA, 2001). Segundo Tavares (2000), o ambiente apresenta um conjunto de demandas que se constituem, em grande parte, oportunidades de negócios para tipos específicos de organizações. Na verdade o conceito de segurança deve ser repensado, pois atualmente, o entendimento sobre tendências ganha muito

mais força, ao tratar de cenários futuros. Estes cenários devem ser elaborados e projetados com base em informações e conhecimentos profundos e minuciosos, evitando desta forma uma tomada de decisão pouco fundamentada. O processo de criação do conhecimento é que provoca inovações e gera competências organizacionais que ampliam o horizonte das escolhas possíveis no processo de tomada de decisão (CHOO, 1998).

Partindo desse pressuposto, e valendo-se da experiência profissional este autor identifica em ordem de importância e freqüência, como principais desafios do processo de gestão da segurança das informações e conhecimentos corporativos para as empresas:

1. Antecipar e monitorar as possibilidades de inovações em fraudes;
2. Acompanhar o avanço tecnológico;
3. Mostrar eficácia dos programas de segurança;
4. Reduzir custos;
5. Treinar os empregados com eficiência;
6. Recrutar e selecionar profissionais com precisão.

A preservação da informação faz parte do escopo do departamento de segurança, ajudando desta forma a empresa a alcançar seus objetivos. No mercado atual, globalizado e altamente competitivo, só permanecerão as empresas rápidas, flexíveis e que tiverem a competência de proteger suas informações e conhecimentos corporativos (ativos estratégicos), visando conquistar nichos estratégicos e manter sua própria sobrevivência.

Segredos de negócio, análise de mercado e da concorrência, dados operacionais históricos e pesquisas, são informações fundamentais e se revelam como um importante diferencial competitivo ligado ao crescimento e à continuidade do negócio. (SÊMOLA, 2003).

Quanto maior o investimento em segurança, menor será a possibilidade de o prejuízo em caso de sinistro. Desta forma a responsabilidade pela segurança destes ativos, que se transformam em ferramentas para a correta tomada de decisão objetivando manter a empresa em condições competitividade. Dever ser compartilhada com a alta gestão, cabendo aos profissionais da segurança empresarial estarem sempre aptos a assessorar tecnicamente.

6 CONCLUSÕES

Este capítulo é a reunião objetiva dos resultados alcançados ao longo do trabalho. Essa dissertação teve como objetivo principal determinar como a gestão da segurança das informações e conhecimentos corporativos proporciona mitigação das fraudes e dos riscos empresariais. Esse pressuposto surge a partir das premissas que compõem um quadro contextual para a consideração da relação: Segurança – Risco – Fraude. Os pontos principais são:

- A informação e os conhecimentos corporativos são recursos estratégicos dentro do novo paradigma organizacional;
- A proteção desse recurso é um fator determinante desse paradigma. Neste sentido, a organização deve estar atenta aos riscos e ameaças do seu ambiente interno e externo. Esse processo de monitoramento é o que se entende por gestão da segurança da informação e dos conhecimentos corporativos;
- A fuga dessas informações e conhecimentos vem se apresentando como um fator incomensurável de risco empresarial, e de inimagináveis oportunidades. A sua exploração e a utilização pelos concorrentes vêm se constituindo em grave entrave para obtenção da vantagem competitiva para as organizações.

Através da pesquisa bibliográfica e da análise documental foi possível observar que em uma economia globalizada, na qual as informações e conhecimentos são os maiores ativos das organizações e estes uma vez explicitados, podem ser digitalizados e atravessar o mundo

em questão de nanosegundos, nunca foi tão forte a necessidade de se proteger esses ativos. Por isso, a gestão eficaz da segurança das informações e conhecimentos corporativos pode prover à organização as condições exigidas para se mitigar riscos e fraudes empresariais, de forma a assegurar uma posição de vantagem competitiva.

A união da segurança da informação e dos conhecimentos corporativos à gestão de riscos é uma prática que começa a ser desenhada no mercado para blindar as informações estratégicas nas corporações. Esta prática pode elevar significativamente o nível de proteção das corporações no cenário de competição global e concorrência on-line, mas ainda é uma configuração que exige avaliação cuidadosa, uma vez que, mesmo com tantas semelhanças, essas áreas têm escopos, objetivos e poderes bem distintos. Enquanto a primeira foca a proteção dos ativos da empresa, a gestão de riscos atua analisando e monitorando os imprevistos que podem impedir a organização de alcançar seus objetivos.

É impossível negar, contudo, que os pontos de contato entre as duas são tão variados quanto vitais para os setores e a corporação como um todo. Elas podem interagir e complementar estratégias para fortalecer ações, embora sejam em grande parte independentes. Não obstante as funções da segurança da informação e de análise de riscos estarem atuando de maneira isolada, uma corporação que busca proteção demanda uma parceria entre essas áreas, pois elas colaboram para a definição de políticas, que dizem respeito aos riscos, segurança e conformidade com as normas.

6.1 Principais contribuições

As principais contribuições, a partir do objetivo proposto, são agrupados quanto ao quadro conceitual e quanto à proposta da seguinte forma:

a) Quanto ao Quadro Conceitual

Houve um esforço no delineamento dos conceitos, que é a primeira contribuição que surge deste estudo, no entender deste autor, em termos teóricos.

Essa conceituação dá suporte e embasamento à elaboração da proposta. Ela é o resultado da análise e explicitação dos fundamentos teóricos, conforme descrito no capítulo Referencial Teórico (p.19), e considerou:

A importância da informação e do conhecimento organizacional dentro do novo paradigma organizacional: contextualiza o problema colocado no cenário atual, o que leva à necessidade de uma atuação preventiva com vista à manutenção da competitividade e sobrevivência empresarial. Isso justifica a adoção da prática da gestão da segurança. Os conceitos essenciais que devem ser considerados, então, pelas organizações são, no entender deste autor:

- Informação e conhecimentos corporativos: como recursos estratégicos e maiores ativos empresariais. Estes são conceitos básicos deste trabalho.
- Gestão da segurança da informação e dos conhecimentos corporativos: como o foco é a gestão, está se tratando de processos e não de técnicas;
- Fraude computacional ou não: o limite para as ações dos malfeitores é a imaginação. Enquanto o ser humano for dotado de uma imaginação e de uma capacidade criativa, haverá o perigo de perdas por roubo, fraude, desvio de recursos, etc.

- Análise de riscos: o gerenciamento de riscos é planejado para propiciar o acesso integrado à gestão de riscos em uma organização, objetivando melhores resultados através da identificação de oportunidades e diminuição das perdas.
- Metodologias e Modelos de Gestão de Segurança da Informação: estabelecer os padrões e recomendações para a correta utilização e proteção das informações e conhecimentos por meio da elaboração de políticas de segurança, passou a ser crítico dentro das empresas, assim como o de atendimento às normas regulatórias vigentes.

b) Quanto à Sugestão de Melhores Práticas

A sugestão apresentada: Melhores Práticas para a Implantação da Gestão da Segurança da Informação e dos Conhecimentos Corporativos, considerou:

1. O cenário e a estratégia de atuação da organização;
2. Os responsáveis pelo processo;
3. A definição das informações e conhecimentos estratégicos;
4. A identificação de fontes de ameaças e riscos;
5. A adoção de políticas e procedimentos.

Esta, no entender deste autor, é a principal contribuição desta dissertação, que aliou os conceitos adotados a modelos teóricos obtidos na fundamentação teórica. A sugestão apresentada resultou num guia operacionalizável por qualquer organização. Esse processo se baseia nos pontos fundamentais para a atuação das organizações no paradigma atual, como já colocado. Isto significa uma inter-relação de análises que vai, desde o autoconhecimento organizacional, até a administração de riscos e adoção de metodologias e modelos de segurança da informação e dos conhecimentos corporativos para mitigar fraudes e riscos empresariais.

6.2 Limitações e Sugestões

As limitações da dissertação levam a sugestões, e prendem-se aos seguintes aspectos: Quanto ao escopo:

Limitações:

- O estudo não abrangeu os processos de gestão do conhecimento e inteligência competitiva.

Sugestões para estudos que completem o processo:

- Estudos de técnicas de gestão do conhecimento e inteligência competitiva, uma vez que esses temas estão ligados diretamente ao tema dessa dissertação;
- Processos de treinamento e conscientização dos funcionários com relação a segurança das informações e conhecimentos corporativos;
- Processos de como introduzir e incorporar medidas de salvaguarda de informações e conhecimentos sensíveis, na cultura organizacional.

Essas limitações são, portanto, decorrência da apresentação de sugestões conceituais de melhores práticas de um processo de gestão da segurança das informações e conhecimentos corporativos que não contempla a implementação. O processo, apesar de genérico, deverá apresentar resultados de acordo com as características e necessidades de cada organização.

6.3 Considerações Finais

Numa economia global saturada de dados que atravessam o mundo em questão de nanosegundos, nunca foi tão forte a necessidade de se proteger as informações e os conhecimentos corporativos que trafegam pelas redes empresariais. A gestão desse processo de proteção deve prover à organização as ferramentas exigidas para se manter ágil, focada e flexível, de forma a evitar a fuga dessas informações e conhecimentos que asseguraram uma posição de vantagem competitiva.

Numa época de incertezas, de competição acirrada e de mudanças freqüentes no ambiente empresarial, a segurança da informação e dos conhecimentos corporativos tem um papel muito importante. A mitigação de riscos pode evitar fraudes e perdas significativas para o negócio.

A maioria das organizações, ao longo das suas vidas corporativas, enfrentará o ato fraudulento, de uma forma ou de outra. Se as corporações sucumbirão às experiências ou emergirão mais fortes, dependerá, em última análise, das atitudes e dos processos internos em vigor, para proteger informações e conhecimentos, responder a incidentes, controlar e prevenir a fraude.

A fraude, como qualquer outro risco do negócio, pode ser eficazmente gerenciada por meio de estratégias apropriadas para sua detecção e controle. Seu impacto não se limita a perdas financeiras. O ato fraudulento pode deteriorar o ambiente de trabalho, afetar a reputação de toda a corporação e corroer lentamente as bases organizacionais e administrativas.

Não é possível mitigar 100% das fraudes e riscos empresariais, porém quando se pratica uma gestão eficaz da segurança da informação e dos conhecimentos corporativos alinhada com uma avaliação e gerenciamento de riscos pode-se construir um ambiente onde as fraudes e riscos não ameacem a sobrevivência das empresas.

A análise dos resultados obtidos nas pesquisas sobre segurança da informação e fraudes empresariais no Brasil reforça a importância dos fatores de capacitação e conscientização como pontos fundamentais para proteção das informações e dos conhecimentos corporativos. O envolvimento de toda a organização neste processo é muito importante e deve ser um esforço corporativo no qual o elemento humano é fator crítico e peça fundamental. A resposta para tornar essas constatações realidade pode estar na contínua adoção de controles e medidas de gestão da segurança da informação e dos conhecimentos corporativos para mitigar ameaças, riscos e vulnerabilidades que rondam as organizações num mundo rápido e globalizado como o de hoje.

REFERÊNCIAS

ABC NEWS. **Funcionários insatisfeitos representam perigo ao sistema das empresas.** 5.jun.2002. Disponível em: <http://www.modulo.com.br/index.jsp>. Acesso em 31.jun.2005.

ABNT - Associação Brasileira de Normas Técnicas. **Tecnologia da Informação** – Código de prática para a gestão da segurança da informação. NBR ISO/IEC 17799. 30/09/2001.

ABNT. - Associação Brasileira de Normas Técnicas. NBR/ISO/IEC 17799. **Tecnologia da Informação** – Código de prática para a gestão da segurança da informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2001. 56p.

ABREU, D. **Política de Segurança**: Definir para implementar. 12.jun.2002. Disponível em: <http://www.modulo.com.br/index.jsp>. Acesso em: 16.jun.2002.

ALBRECHT, W. S.; HOWE, K. R.; ROMNEY, M. B. (1984) **Deterring Fraud:** The Internal Auditor's Perspective, The Institute of Internal Auditors Research Foundation, Almonte Springs, Florida.

ÁLVAREZ, G.; PETROVI, S. (2003). **A new taxonomy of Web attacks suitable for efficient encoding.** Computers & Security, Vol. 22, Nº. 5, pp. 435-449.

AMARAL, M. P. **Segurança da informação em ambientes computacionais complexos:** uma abordagem baseada na gestão de projetos. Belo Horizonte, 2001. Dissertação (Mestrado em Tecnologia), CEFET-MG: 2001. 171f. Disponível em: <http://www.modulo.com.br/index.jsp>. Acesso em: 19.jun.2002.

ANDERSON, J. P. (1980). **Computer security threat monitoring and surveillance**, Technical Report Contract 79F296400. Abril, 1980.

AusCERT (2002). **Australian computer crime and security survey**. Disponível em: <http://www.auscert.org/Information/Auscert_info/new.html>. Acesso em: 12.Jun.2002.

AusCERT (2003). **Australian computer crime & security survey**. Disponível em: <http://www.auscert.org.au/render.html?it=2001&cid=1920>. Acesso em: 18.mai.2003.

AUSTRALIAN NATIONAL AUDIT OFFICE (2000). **Australian taxation office internal fraud control arrangements,** Report Nº. 16.

BANNWART, Cláudio. **Empresa segura, capital garantido.** Infoguerra, 30.nov.2001. Entrevista. Disponível em: <http://www.infoguerra.com.br/infonews/arc10-2001.html>. Acesso em: 30.jun.2004.

BARBOSA, Antônio L. F. **Sobre a propriedade do trabalho intelectual:** uma perspectiva crítica. Rio de Janeiro: UFRJ, 1999.

BARRETO, Aldo. **A questão da informação.** São Paulo em Perspectiva, São Paulo, v. 8, n. 4, p. 3-8, 1994.

BOGDAN, Robert; BIKLEN, Sari. **Investigação qualitativa em educação:** uma introdução à teoria e aos métodos. Porto: Porto Ed., 1994.

BOLOGNA, J.; SHAW, P. (1996). **Corporate crime investigation**, Butterworth-Heinemann.

BRASIL. **Decreto n. 2910** – 29 de dezembro de 1998. Estabelece normas para a salvaguarda de documentos, materiais, áreas, comunicações e sistemas de informação de natureza sigilosa, e da outras providencias. Disponível em: <http://www.senado.gov.br/legislacao/>. Acesso em: 31.mar.2006.

BRASIL. **Decreto n. 4.553** – 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da administração pública federal, e dá outras providências. Disponível em: <http://www.senado.gov.br/legislacao/>. Acesso em: 31.mar.2006.

BRASIL. **Lei n. 9.279** – 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. Disponível em: <http://www.senado.gov.br/legislacao/>. Acesso em: 31.mar.2006.

BRASILIANO & ASSOCIADOS. **Métodos para análise de risco na segurança patrimonial.** Disponível em: <http://www.brasiliano.com.br/download/artigo_299.doc.> Acesso em: 07.out.2004.

BRENNER, S. W. (2001). **Is there such a thing as "virtual crime"?**, 4 Cal. Crim. Law Rev.1.

BSA-BUSINESS SOFTWARE ALLIANCE. **Information security governance:** toward a framework for action. 2003. Disponível em: <http://www.bsa.org>. Acesso em: 12.dez.2004.

BUCKLAND, Michael K. **Information as thing.** Journal of the American Society for Information Science, Silver Spring, EUA, v. 45, n. 5, p. 351-360, 1991.

CALDAS, M. P., HERNANDEZ, J. M. C. **Resistência à Mudança**: Uma Revisão Crítica. In: RAE. São Paulo: 2001, v. 41, n.2, p. 31

CARVALHO, Gilberto A. S. **A nova empresa na era da concorrência e da gestão do conhecimento.** Rio de Janeiro: FGV, 2003.

CASANAS, Alex Delgado Gonçalves; MACHADO, César de Souza. **O impacto da implementação da norma ISO/IEC 17799** – Código de prática para segurança da gestão da informação – nas empresas. In: PEREIRA, Luís Filipe Rosado. O e-Government no mundo. 2002. Disponível em: <http://egov.alentejodigital.pt/Page10549/Seguranca/iso17799-1.pdf>. Acesso em: 08.mai.2004.

CASTELLS, M. (2001). **The internet galaxy.** reflections on the internet, business and Society. Oxford University Press.

CEPIK, Marco A.C. **Espionagem e democracia.** Rio de Janeiro: FGV, 2003.

CERT.Br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de segurança para Internet.** Julho, 2005. Disponível em: <http://cartilha.cert.br/malware/sec6.html>. Acesso em: 31.jul.2006.

CGTFR-CORPORATE GOVERNANCE TASK FORCE REPORT. **Information security governance:** a call to action. Abril, 2004. Disponível em: <http://www.cyberpartnership.org/InfoSecGov4_04.pdf>. Acesso em: 02.fev.2005.

CHOO, C. W. **The Knowing Organization**. Oxford: Oxford University Press, 1998.

COBIT - Control Objectives for Information and Related Technology. 3rd Edition, Information Systems Audit and Control Foundation, July 2000.

COHEN, F. (2002). **Computer fraud scenarios: robbing the rich to feed the poor.** Computer Fraud & Security, Vol. 2002, Iss. 1, dezembro, pp. 5-6.

COLLIER, P. A.; DIXON, R.; MARSTON, C. L. (1990). **The prevention and detection of computer fraud**, The Chartered Institute of Management Accountants.

COMPUTER Fraud and Abuse Act, P.L. 98–473, Title II, Section 2102, 98 Stat. 2190, October 12, 1984, as amended by P.L. 99–474, 100 Stat. 1213, October 16, 1986; 18 U.S.C. Chapter 47, Section 1030.

COMPUTER Security Act of 1987, 40 U.S. Code 759, (Public Law 100-235), January 8, 1988.

CONHEÇA a segurança da informação no governo federal brasileiro. **Módulo Security Magazine**, São Paulo, n. 328, 09 fev. 2004. Disponível em: <http://www.modulo.com.br/arquivoboletins/2k4/msnews_no328.htm>. Acesso em: 29.jul.2004.

COUNCIL OF EUROPE (2001). **Final Draft Convention on Cyber-crime.** Disponível em: <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>. Acesso em: 1.ago.2002

COUNCIL OF EUROPE. **Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime,** adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies. Disponível em: <http://www.coe.fr/cm/ta/rec/1989/89r9.htm>. Acesso em: 21.dez.2005.

DAHAB, Ricardo. **INF712:** gerência de segurança da informação - controle de acesso. Campinas: Instituto de Computação/UNICAMP, 2002. Disponível em: <http://www.dcc.unicamp.br/~rdahab/cursos/inf712/materialdidatico/aula3 -1.pdf>. Acesso em: 03.abr.2004.

DAVENPORT, T; PRUSAK, L. **Conhecimento empresarial:** Como as organizações gerenciam o seu capital intelectual. Rio de Janeiro: Campus, 1998.

DE SORDI, J.O. **Tecnologia da informação aplicada aos negócios.** São Paulo: Atlas, 2003. 185p.

DEFENSE Authorization Act (P.L. 106-398) including Title X, Subtitle G. **Government Information Security Reform.** October 28, 2000.

DEPARTMENT of State, Draft Best Security Practices Checklist Appendix A. 22, Janeiro, 2001.

DEZ questões para avaliar a gestão da segurança na sua organização. In: FUJITSU. 2003. Disponível em: <http://pt.fujitsu.com/noticias/leituras/gseguranca/frecumenda/>. Acesso em: 29 jul.2004.

DHILLON, G. (1999). **Managing and controlling computer misuse.** Information Management & Computer Security, 7/4, pp. 171-175.

DHILLON, G.; MOORES, S. (2001). **Computer crimes:** theorizing about the enemy within. Computers & Security, Vol. 20, No. 8, pp. 715-723.

DIAS, C. **Segurança e auditoria da tecnologia da informação.** Rio de Janeiro: Axcel Books, 2000. 218p.

DINIZ, Davi M. **Propriedade industrial e segredo em comércio.** Belo Horizonte: Del Rey, 2003.

DOYLE, C. (2002). **Computer fraud and abuse laws:** an overview of federal criminal laws, Novinka, New York.

DRUCKER, P. **Sociedade pós-capitalista.** São Paulo: Pioneira, 1997.

ELLINGSON, J. F. (1998). **Devising an information based strategy for fighting fraud.** Journal of Internet Security, Vol. 1, Nº. 1, September.

ENTRUST. **Information security governance (ISG):** an essential element of corporate governance. Abril, 2004. Disponível em: <http://www.entrust.com/governance/>. Acesso em: 16.mar.2005.

ETTER, B. (2001). **The forensic challenges of e-crime.** 7th Indo-Pacific Congress on Legal Medicine and Forensic Sciences, Melbourne, Australia.

FERREIRA, Aurélio Buarque de Holanda. Dicionário Eletrônico Novo Aurélio Século XXI. Versão 3.0. Rio de Janeiro: Nova Fronteira, 1999.

FERREIRA, F. **Segurança da informação**. Rio de Janeiro: Ciência Moderna, 2003. 162p.

GAITHERSBURG, MD, National Institute of Standards and Technology, September 20, 1995.

GALVÃO, M. **Aspectos de segurança em redes voz sobre IP:** White Paper. Rio de Janeiro, 2003. Disponível em:<http://www.modulo.com.br/index.jsp>. Acesso em: 01.ago.2006.

GANDELMAN, Marisa. **Poder e conhecimento na economia global.** Rio de Janeiro: Civilização Brasileira, 2004.

GARVEY. **Companies exposed to "social engineers"**. Maio, 2002. Disponível em: <http://www.zone-h.org/em/news/read/id=809>. Acesso em 15.set.2005.

GENERAL ACCOUNTING OFFICE. **Federal information system control audit manual** (FISCAM), GOA/AIMD-12.19.6, Janeiro, 1999.

GENERAL ACCOUNTING OFFICE. **Information security risk assessment practices of leading organizations,** GAO/AIMD-99-139. Agosto, 1999.

GIL, A. C. **Como elaborar projetos de pesquisa.** São Paulo: Atlas S.A., 1996.

GILBERT (1997). **Law dictionary**. Harcourt Brace Legal and Professional Publications.

GILLIES, P. (1993). **Criminal law**, Law Book Co., North Ryde, N.S.W., Australia.

GOOD, J.; HATT, P.K. **Métodos em Pesquisa Social.** São Paulo: Nacional, 1977.

GRAYCAR, A.; SMITH, R. (2002) **Identifying and responding to corporate fraud in the 21st century.** Speech to the Australian Institute of Management. 20, Março, 2002.

GREENSPAN, A. (2002). **Monetary policy report to the congress.** 16, Julho, 2002.

GROUP, NIST Special Publication 800-18, **Guide for Developing Security Plans for Information Technology Systems**, Gaithersburg, MD, National Institute of Standards and Technology, December 1998.

HEITOR, Manuel; HORTA, Hugo; CONCEIÇÃO, Pedro. **Engenharia e conhecimento:** ensino técnico e investigação. In: INSTITUTO SUPERIOR TÉCNICO. Centro de estudos em inovação, tecnologia e políticas de desenvolvimento. 1999. Disponível em: <http://in3.dem.ist.utl.pt/laboratories/pdf/11_1.pdf>. Acesso em: 06.abr.2004.

HIRST, C.; HEIDARSON, C. **Beyond data security:** toward trustable computing means. October 6th, 2004). Disponível em: <http://eu.computers.toshiba-europe.com/Contents/Toshiba_teg/EU/WHITEPAPER/files/FEA-2005-11-Beyond-Data-Security-EN.pdf>. Acesso em: 1.ago.2005.

HOWARD, J. D. (1997). **An analysis of security incidents on the internet.** Ph.D. dissertation, Carnegie Mellon University, Pittsburgh, Pennsylvania.

HOWARD, J. D.; LONGSTAFF, T. A. (1998). **A Common Language for Computer Security Incidents**, Sandia Report SAND98-8667.

IIA-THE INSTITUTE OF INTERNAL AUDITORS. **Information Security Governance:** What Directors Need to Know. (2001). The Critical Infraestructure Assurance Project. Disponível em: <http://www.theiia.org/eSAC/pdf/ISG_1215.pdf>. Acesso em: 14.jan.2005.

INFORMATION WEEK. **Treinamento em segurança torna-se prioridade em grandes empresas.** 2 setembro, 2002. Disponível em:<http://www.modulo.com.br/index.jsp>. Acesso em: 26 set. 2004.

ISO - International Organization for Standardization/ International Eletrotechnical Committee. **Information technology** – Code of practice for information security management. Reference number ISO/IEC 17799:2000(E).

ISO 17799. **A code of practice for information security management** (British Standard 7799).

ITGI-THE IT GOVERNANCE INSTITUTE. **COBIT:** Control objectives for information and related technology. Printed in the United States of America, 2000.

ITGI-THE IT GOVERNANCE INSTITUTE. **Information security governance:** guidance for boards of directors and executive management. Printed in the USA, 2001. Disponível em: <http://www.itgi.org/template_ITGI.cfm?template /ContentManagement/ContentDisplaycfm&ContentID=6672>. Acesso em: 02.fev.2005.

JAYARAM, N. D.; MORSE, P. L. R. (1997). **Network security:** a taxonomic view, european conference on security and detection. School of Computer Science, University of Westmister, UK, 28-30. Abril, 1997.

KELLEY, W. **Marketing intelligence:** the management of marketing information. London: Staple Press, p.2, 1968

KERLINGER, F.N. **Metodologia da pesquisa em Ciências Sociais.** São Paulo: EPU/EDUSP, Brasília, INEP, 1980.

KNIGHT, E. (2000). **Computer vulnerabilities.** Disponível em: <http://www.securityparadigm.com>. Acesso em: 20.mar.2000.

KPMG. **A Fraude no Brasil:** Resultado da pesquisa 2004. Disponível em:<http://www.kpmg.com.br/publicacoes_forensic.asp?ft=5&fx=18>. Acesso em: 1.ago.2006.

KRAUSS, L. I.; MAC GAHAM, A. (1979). **Computer fraud and countermeasures**, Prentice-Hall, New Jersey.

KRELTSZHEIM, D. (1999). **Identifying the proceeds of electronic money fraud.** Information Management & Computer Security, 7/5, pp. 223-231.

KRSUL, I. V. (1998). **Software Vulnerability Analysis.** Ph.D. dissertation, Purdue University. Maio, 1998.

LANDWEHR, C. E. (1981). **Formal models for computer security.** Computing Surveys, Vol. 13, No. 3. Setembro.

LANDWEHR, C. E.; BULL, A. R.; MCDERMOTT, J. P.; CHOI, W. S. (1994). **A taxonomy of computer program security flaws, with examples.** ACM Computing Surveys 26, 3 setembro.

LANHAM, D.; WEINBERG, M.; BROWN, K. E.; RYAN, G. W. (1987). **Criminal fraud.** The Law Book Company Limited, Sydney.

LE COADIC, Yves-François. **A ciência da informação.** Brasília: Briquet de Lemos, 1996.

LIEBSCHER, P; ABELS, E.; DENMAN, D. "**Factors that influence the use of electronic networks by science and engineering faculty at small institutions.** Part 1. Queries". In: Journal of the American Society for Information Science, New York, v.47, n.2, p.146-158, 1996.

LINDQVIST, U.; JONSSON, E. (1997). **How to systematically classify computer security intrusions.** Proceedings of the 1997 IEEE Symposium on Security & Privacy, Oakland, California, USA, May 4-7, IEEE Computer Society Press, 154–163.

Livro Verde para a Sociedade da Informação em Portugal: Disponível em: <http://www.missao-si.mct.pt/livroverde/lvfinal.zip> Acesso em: 09.ago.2006.

LOUGH, L. D. (2001) **A taxonomy of computer attacks with applications to wireless networks.** PhD dissertation, Faculty of the Virginia Polytechnic Institute and State University, Blacksburg, Virginia.

MAGALHÃES, João. **Empresas investem pouco em segurança digital.** O Estadão. São Paulo, 08 jan. 2004. Tecnologia. Disponível em: <http://www.estadao.com.br/tecnologia/internet/2004/jan/08/93.htm>. Acesso em: 10.mai.2004.

MAIA, Marco Aurélio. **Engenharia social.** Disponível em: <http://geocities.yahoo.com.br/jasonbs_1917/seguranca/leiamais_engsocial.html>. Acesso em: 12.abr.2004.

MARTINEZ, Manuela. **Engenharia social é a grande ameaça da internet, diz ex-hacker.** Folha online, São Paulo, 18 set. 2003. Informática. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u13942.shtml>. Acesso em: 17.abr.2004.

MASKUS, Keith. **Intellectual property rights in the global economy.** Washington DC: IIE, 2000.

MICROSOFT. **Glossário de segurança Microsoft .** Cavalo de Tróia. Disponível em: <http://www.microsoft.com/brasil/security/glossary.mspx#c>. Acesso em: 01.ago.2005.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar:** ataques de hackers – controlando o fator humano na segurança da informação. São Paulo: Pearson Education, 2003.

MITNICK, Kevin. **O conhecimento que assusta.** InformationWeek Brasil. São Paulo, 2003. Entrevista. Disponível em: <http://www.informationweek.com.br/iw70/mitnick/>. Acesso em: 27.mar.2005.

MODULO E-SECURITY MAGAZINE, **Tendências** 2002, 2002. Disponível em: <http://www.modulo.com.br>. Acesso em 31.jul.2005.

MÓDULO SECURITY SOLUTIONS S.A. **9ª Pesquisa Nacional de Segurança da Informação.** Rio de Janeiro, 2003. Disponível em: <http://www.modulo.com.br/temp/9aPesquisaNacional_Modulo.zip>. Acesso em: 15.set.2004.

MÓDULO SECURITY SOLUTIONS. **9ª Pesquisa Nacional sobre Segurança da Informação.** 2003. Disponível em:<http://www.modulo.com.br/empresa/noticias/pesquisa/pesquisa03.htm>. Acesso em: 21.out.2005.

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

MULLER, Ives P. **Metodologia de auditoria com foco em riscos.** In: CONGRESSO LATINO AMERICANO DE AUDITORIA INTERNA Y ADMINISTRACIÓN DE RIESGOS, 8., 2004, Cuba. Anais eletrônicos. Bogotá: FBL, 2004. Disponível em: <http://www.latinbanking.com/memorias_congreso_clain_2004/metodologia_auditoria_com.pdf>. Acesso em: 15.set.2004.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos.** São Paulo: Berkeley Brasil, 2002.

NATIONAL COMMUNICATIONS SYSTEM. **Public switched network security assessment guidelines.** Setembro, 2000.

NEUMANN, P. G. (1995). **Computer related risks.** ACM Press.

NEUMANN, P. G.; PARKER, D. B. (1989). **A summary of computer misuse techniques.** 12th National Computer Security Conference, pp. 396-407.

NIC BR SECURITY OFFICE (NBSO). **A cultura em segurança contra fraudes.** 2003. Disponível em: <http://www.nbso.nic.br/docs/reportagens/2003/2003-05-13.html>. Acesso em: 29.mar.2004.

NICCOLAI, M.; BEZERRA, M.; VERAS, F. **Tudo pela segurança da informação.** São Paulo. Junho, 2004. Disponível em: <http://www.nextgenerationcenter.com/br/>. Acesso em: 02.jun.2004.

NONAKA, Ikujiro; TAKEUCHI, Hirotaka. **Criação de conhecimento na empresa:** Como as empresas japonesas geram a dinâmica da inovação. 11.ed. Rio de Janeiro: Campus, 1997.

O JOGO da segurança; descubra as ameaças e vulnerabilidades em ambiente corporativo. Módulo Security Magazine. São Paulo, n. 345, 14 jun. 2004. Disponível em: <http://www.modulo.com.br/arquivoboletins/2k4/msnews_no345.htm>. Acesso em: 02.jul. 2004.

OGC. **IT infrastructure library:** service suport. London: OGC, 2000. 472 p.

OGC-Office of Government Comerce. **ITIL:** the key to managing it services – best practice for service support. printed in the United Kingdom for the stationery office, 2001. ISBN0 11 330015 8.

OLIVEIRA, W. **Segurança da informação:** Técnicas e soluções. Florianópolis: Visual Books, 2001. 182p.

PANKO, R. R. (2002). **Corporate computer and network security.** Prentice Hall.

PARKER, D.B. (1998). **Fighting computer crime:** a new framework for protecting information, New York, John Wiley and Sons.

PELISSARI, F. A. B. **Segurança de redes e análise sobre a conscientização das empresas da cidade de Bauru (SP) quanto ao problema.** Bauru, 2002. Curso de Especialização em Informática – UNESP, 2002. 112f. Disponível em: <http://suporte.planetarium.com.br/suporte/documentacao/download/monografia_Fernando_Pelissari.pdf>. Acesso em: 31Jul.2005.

PERRY, T. S.; WALLICH, P. (1984). **Can Computer Crime Be Stopped?** IEEE Spectrum, 21(5), pp. 34-45. Maio, 1984.

POR QUE preocupar-se com a segurança. In: KONSULTEX Informática. 1993. Disponível em: <http://www.konsultex.com.br/ktex/download/info/seguranca.doc>. Acesso em: 01.mar.2004.

PROCEEDINGS of the 37th Hawaii International Conference on System Sciences. 2004.

REDE NACIONAL DE ENSINO E PESQUISAS (RNP). **Alerta do cais ALR - 02042003:** fraudes em internet banking. 2004. Disponível em: <http://www.rnp.br/cais/alertas/2003/cais-alr-02042003.html>. Acesso em: 29.mar.2004.

RFC 2828. **Internet security glossary.** Disponível em: <http://www.elook.org/computing/rfc/rfc2828.html>. Acesso em: 1.ago.2006.

RIGATIERI, V.; DOLENC, L.; DUARTE, M.; ZARZA, C. ; CAMPOY, E. **Segurança**. São Paulo. Maio. 2004. Disponível em: <http://www.nextgenerationcenter.com/br/>. Acesso em: 04.mai.2004.

RÍO, M. G. **Metodologia de la investigación social**. Técnica de recolección de datos. Amalgama, 1997.

ROCHA, L. F. **Crimes virtuais:** ameaça ao admirável mundo novo. 3, julho, 2002. Disponível em: <http://www.modulo.com.br/index.jsp>. Acesso em 25.jul.2004.

RUDD, Colin. **An introductory overview of ITIL.** Publicado por iTSMF Ltd, Webbs Court, United Kingdom, 2004. Version 1.0a. Disponível em: <http://www.itsmf.com/publications/ITIL/Overview.pdf>. Acesso em: 22.mar.2005.

SANTOS, Luiz Carlos. **Como funciona a criptografia?** Artigo de acesso exclusivo por meio eletrônico. Disponível em: <http://www.clubedasredes.eti.br/rede0009.htm>. Acesso em: 01.ago.2005.

SCHULTZ, E. E. (2002). **A framework for understanding and predicting insider attacks.** Computers & Security, Vol. 21, No. 6, pp. 526-531.

SCIP – Society of Competitive Intelligence Professionals. Disponível em: <http://www.scip.org>. Acesso em: 31.jul.2006.

SELLTIZ, Claire et. all. **Métodos de pesquisa nas relações sociais.** São Paulo: EPU/EDUSP, 1975.

SÊMOLA, M. **Gestão da segurança da informação:** Uma visão executiva. 3.ed. Rio de Janeiro: Elsevier, 2003. 160p.

SHOVER, N. and Wright, J. P. (2001). **Crimes of privilege:** readings in white-collar crime, Oxford University Press.

SILVA, E. L. da e MENEZES, E. M. **Metodologia da Pesquisa e Elaboração de Dissertação**. 2. ed. Revisada. Florianópolis: UFSC/PPGEP/LED, 2001.

SMEDINGHOFF, T. J. (1996). **Online Law**, The SPA's Legal Guide to Doing Business on the Internet, Addison-Wesley Developers Press.

SOPHOS. **Top 10 viruses reported to Sophos in July 2006**. Disponível em: <http://www.sophos.com/security/top-10/>. Acesso em: 20.jul.2006.

SOUZA, Edney. **Atenção:** ataque de engenharia social aos usuários do registro.br. In: METARECICLAGEM. Lista do Projeto Metareciclagem. Disponível em: <http://groups.google.com/groups?q=engenharia+ social&hl=pt&lr=&ie=UTF-8&oe=UTF-8&selm=134oD-2zc- 29%40gated-at.bofh.it&rnum=1>. Acesso em: 31.mar.2004.

STALLINGS, W. (1995). **Network and Internetwork Security Principles and Practice.** Prentice Hall, Englewood Cliffs, NJ.

STANDARDS AUSTRALIA. **Standards Australia AS/NZS 4360 Risk Management.** Standards Australia, Sydney, 1999

STEVENSON, G. (2000). **Computer Fraud:** Detection and Prevention. Computer Fraud & Security, vol. 2000, no. 11, pp. 13-15.

STEWART, T. **A Riqueza do Conhecimento:** o capital intelectual e a nova organização do século XXI. Rio de Janeiro: Campus, 2002. 517p.

STONEBURNER, Gary, Draft –Rev. **A NIST Special Publication 800** - XX, Risk Management Guide, February 16, 2001.

STONEBURNER, Gary. **Developing a commercial security architecture:** tutorial presented at the 11th Computer Security Applications Conference, New Orleans, LA. Dezembro, 1995.

STONEBURNER, Gary. **Underlying technical models for information technology security recommendations of the national institute of standards and technology**. Gaithersburg, Dezembro, 2001. p. 18.

SWANSON, Marianne; BARBARA, Guttman. **NIST:** Special Publication 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP),

TAKAHASHI, T. (org.). **Sociedade da informação no Brasil:** livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000.

TARAPANOFF, K. (org.) **Inteligência organizacional e competitiva.** Brasília: Editora Universidade de Brasília, 2001.

TAVARES, Mauro Calixta. **Gestão estratégica**. São Paulo. Atlas, 2000.

THIOLLENT, M. **Metodologia da pesquisa-ação**. 10. ed. São Paulo : Cortez, 2000.

UNITED NATIONS (1994). **Manual on the prevention and control of computer-related crimes.** International review of criminal policy, Nºs. 43 and 44.

VARGAS, A. **Ameaça além do Firewall.** Por que as empresas devem se preparar contra a engenharia social? 10 abr. 2002. Disponível em:<http://www.modulo.com.br/index.jsp>. Acesso em 19.mai.2002.

VASCONCELOS, Maria C. R. L. **Cooperação universidade/empresa na pós-graduação: contribuição para a aprendizagem, a gestão do conhecimento e a inovação na indústria mineira**. Programa de Pós-Graduação em Ciência da Informação da Escola de Ciência da Informação da UFMG, 2000. 248 p. (Tese de Doutorado).

VASIU, L, WARREN, M & MACKAY, **Defining Fraud** : In 7th Pacific Asia Conference on Information Systems, 10-13 July 2003, Adelaide, South Australia. Disponível em:< www.pacis-net.org/file/2003/papers/is-strategy/>. Acesso em: 20.jul.2006

VIANA, Túlio Lima. **Hackers:** um estudo criminológico da subcultura cyberpunk. In: CERQUEIRA, Tarcísio Queiroz; IRIARTE, Erick; PINTO, Márcio Morena (Coords.). Informática e Internet: aspectos legais internacionais. Rio de Janeiro: Esplanada, 2001. p.173-190.

VIEIRA, S. **Segurança da informação com selo de qualidade.** São Paulo: Junho, 2004. Disponível em: <http://www.nextgenerationcenter.com/br/>. Acesso em: 02.jun.2004.

WALLER, L.; WILLIAMS, C. R. (2001). **Criminal law:** Text and cases, 9th Ed., Butterworths. Fonte: “Management Update: Progress Toward Trustable Computing Means Securer IT Systems” de C. Hirst, C. Heidarson. 6 de Outubro, 2004.

YIN, Robert K. **Case study research:** design and methods. Beverly Hills: SAGE, 1984.

ANEXO A – Objetivos e Controles da Norma ABNT NBR ISO/ IEC 17799:2005

A seleção de controles de segurança da informação depende das decisões da organização, baseadas nos critérios ara aceitação de risco, nas opções para tratamento do risco e no enforque geral da gestão de riscos aplicada à organização. Neste anexo, são detalhados os objetivos e os controles das onze seções de controle da norma ABNT NBR ISO/ IEC 17799:2005 (Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação). Cujo início se dá na seção 5 conforme se vê abaixo:

5) Política de Segurança da Informação;

Objetivo: Prover uma orientação e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Controles:

5.1) Política de segurança da informação;

5.1.1) Documentação da política de segurança da informação;

5.1.2) Análise crítica da política de segurança da informação.

6) Organizando a Segurança da Informação;

Objetivo: Gerenciar a segurança da informação dentro da organização.

Controles:

6.1) Infra-estrutura da segurança da informação;

6.1.1) Comprometimento da direção com a segurança da informação;

6.1.2) Coordenação da segurança da informação;

6.1.3) Atribuição de responsabilidades para a segurança da informação.

6.1.4) Processo de autorização para os recursos de processamento da informação;

6.1.5) Acordos de confidencialidade;

6.1.6) Contato com autoridades;

6.1.7) Contato com grupos especiais;

6.1.8) Análise crítica independente de segurança da informação;

6.2) Partes externas;

6.2.1) Identificação dos riscos relacionados com partes externas;

6.2.2) Identificando a segurança da informação, quando se trata com clientes;

6.2.3) Identificando segurança da informação nos acordos com terceiros;

7) Gestão de Ativos;

Objetivo: Alcançar e manter a proteção adequada dos ativos da organização.

Controles:

7.1) Responsabilidade pelos ativos;

7.1.1) Inventário dos ativos;

7.1.2) Proprietário dos ativos;

7.1.3) Uso aceitável dos ativos;

7.2) Classificação da informação;

7.2.1) Recomendações para classificação;

7.2.2) Rótulos e tratamento da informação.

8) Segurança em Recursos Humanos;

Objetivo: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos.

Controles:

8.1) Antes da Contratação;

8.1.1) Papéis e responsabilidades;

8.1.2) Seleção;

8.1.3) Termos e condições de contratação;

8.2) Durante a contratação;

8.2.1) Responsabilidades da direção;

8.2.2) Conscientização, educação e treinamento em segurança da informação;

8.2.3) Processo disciplinar;

8.3) Encerramento ou mudança da contratação;

8.3.1) Encerramento de atividades;

8.3.2) Evolução de ativos;

8.3.3) Retirada de direitos de acesso;

9) Segurança Física e do Ambiente;

Objetivo: Prevenir o acesso físico não-autorizado, danos e interferências com as instalações e informações da organização.

Controles:

9.1) Áreas seguras

9.1.1) Perímetro de segurança;

9.1.2) Controles de entrada física;

9.1.3) Segurança em escritórios, salas e instalações;

9.1.4) Proteção contra ameaças externas e do meio ambiente;

9.1.5) Trabalhando em áreas seguras;

9.1.6) Acesso do público, áreas de entrega e de carregamento;

9.2) Segurança de equipamentos;

9.2.1) Instalação e proteção do equipamento;

9.2.2) Utilidades;

9.2.3) Segurança do cabeamento;

9.2.4) Manutenção dos equipamentos;

9.2.5) Segurança de equipamentos fora das dependências da organização;

9.2.6) Reutilização e alienação segura de equipamentos;

9.2.7) Remoção de propriedade;

10) Gestão das Operações e Comunicações;

Objetivo: Garantir a operação segura e correta dos recursos de processamento da informação.

Controles:

10.1) Procedimentos e responsabilidades operacionais;

10.1.1) Documentação dos procedimentos de operação;

10.1.2) Gestão de mudanças;

10.1.3) Segregação de funções;

10.1.4) Separação dos recursos de desenvolvimento, teste e de produção;

10.2) Gerenciamento de serviços terceirizados;

10.2.1) Entrega de serviços;

10.2.2) Monitoramento e análise crítica de serviços terceirizados;

10.2.3) Gerenciamento de mudanças para serviços terceirizados;

10.3) Planejamento e aceitação dos sistemas;

10.3.1) Gestão de capacidade;

10.3.2) Aceitação de sistemas;

10.4) Proteção contra códigos maliciosos e códigos móveis;

10.4.1) Controles contra códigos maliciosos;

10.4.2) Controles contra códigos móveis;

10.5) Cópias de segurança;

10.5.1) Cópias de segurança da informação;

10.6) Gerenciamento da segurança em redes;

10.6.1) Controles de redes;

10.6.2) Segurança dos serviços de redes;

10.7) Manuseio de mídias;

10.7.1) Gerenciamento de mídias removíveis;

10.7.2) Descarte de mídias;

10.7.3) Procedimentos para tratamento de informação;

10.7.4) Segurança da documentação dos sistemas;

10.8) Troca de informações;

10.8.1) Políticas e procedimentos para a troca de informações;

10.8.2) Acordos para a troca de informações;

10.8.3) Mídias em trânsito;

10.8.4) Mensagens eletrônicas;

10.8.5) Sistemas de informação do negócio;

10.9) Serviços de comércio eletrônico;

10.9.1) Comércio eletrônico;

10.9.2) Transações on-line;

10.9.3) Informações publicamente disponíveis;

10.10) Monitoramento;

10.10.1) Registros de auditoria;

10.10.2) Monitoramento do uso de sistema;

10.10.3) Proteção das informações dos registros (log);

10.10.4) Registros (log) de administrador e operador;

10.10.5) Registros (log) de falhas;

10.10.6) Sincronização dos relógios;

11) Controle de Acesso;

Objetivo: Controlar o acesso à informação.

Controles:

11.1) Requisitos de negócio para controle de acesso;

11.1.1) Política de controle de acesso;

11.2) Gerenciamento de acesso do usuário;

11.2.1) Gerenciamento de privilégios;

11.2.2) Gerenciamento de senha do usuário;

11.2.3) Análise crítica dos direitos de acesso de usuário;

11.3) Responsabilidade dos usuários;

11.3.1) Uso de senhas;

11.3.2) Equipamento de usuário sem monitoração;

11.3.3) Política de mesa limpa e tela limpa;

11.4) Controle de acesso à rede;

11.4.1) Política de uso dos serviços de rede;

11.4.2) Autenticação para conexão externa do usuário;

11.4.3) Identificação de equipamento em redes;

11.4.4) Proteção e configuração de portas de diagnóstico remotas;

11.4.5) Segregação de redes;

11.4.6) Controle de conexão de rede;

11.4.7) Controle de roteamento de redes;

11.5) Controle de acesso ao sistema operacional;

11.5.1) Procedimentos seguros de entrada no sistema (log-on);

11.5.2) Identificação e autenticação de usuário;

11.5.3) Sistema de gerenciamento de senha;

11.5.4) Uso de utilitários de sistema;

11.5.5) Desconexão de terminal por inatividade;

11.5.6) Limitação de horário de conexão;

11.6) Controle de acesso à aplicação e à informação;

11.6.1) Restrição de acesso à informação;

11.6.2) Isolamento de sistemas sensíveis;

11.7) Computação móvel e trabalho remoto;

11.7.1) Computação e comunicação móvel;

11.7.2) Trabalho remoto;

12) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;

Objetivo: Garantir que a segurança é parte integrante de sistemas de informação.

Controles:

12.1) Requisitos de segurança de sistemas de informação;

12.1.1) Análise e especificação dos requisitos de segurança;

12.2) Processamento correto nas aplicações;

12.2.1) Validação dos dados de entrada;

12.2.2) Controle do processamento interno;

12.2.3) Integridade de mensagens;

12.2.4) Validação de dados de saída;

12.3) Controles criptográficos;

12.3.1) Política para o uso de controles criptográficos;

12.3.2) Gerenciamento das chaves;

12.4) Segurança dos arquivos do sistema;

12.4.1) Controle de software operacional;

12.4.2) Proteção dos dados para teste de sistema;

12.4.3) Controle de acesso ao código-fonte do programa;

12.5) Segurança em processos de desenvolvimento e de suporte;

12.5.1) Procedimentos para controle de mudanças;

12.5.2) Análise crítica técnica das aplicações após mudanças no sistema operacional;

12.5.3) Restrições sobre mudanças em pacotes de software;

12.5.4) Vazamento de informações;

12.5.5) Desenvolvimento de terceirizado de software;

12.6) Gestão de vulnerabilidades técnicas;

12.6.1) Controle de vulnerabilidades técnicas;

13) Gestão de Incidentes e Segurança da Informação;

Objetivo: Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

Controles:

13.1) Notificação de fragilidades e eventos de segurança da informação;

13.1.1) Notificação de eventos de segurança da informação;

13.1.2) Notificando fragilidades de segurança da informação;

13.2) Gestão de incidentes de segurança da informação e melhorias;

13.2.1) Responsabilidades e procedimentos;

13.2.2) Aprendendo com os incidentes de segurança da informação;

13.2.3) Coleta de evidências;

14) Gestão da Continuidade do Negócio;

Objetivo: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.

Controles:

14.1) Aspectos da gestão da continuidade do negócio, relativos à segurança da informação;

14.1.1) Incluindo segurança da informação no processo de gestão da continuidade de negócio;

14.1.2) Continuidade de negócios e análise/ avaliação de riscos;

14.1.3) Desenvolvimento e implantação de planos de continuidade relativos à segurança da informação;

14.1.4) Estrutura do plano de continuidade do negócio;

14.1.5) Testes, manutenção e reavaliação dos planos de continuidade do negócio;

15) Conformidade;

Objetivo: Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

Controles:

15.1) Conformidade com requisitos legais;

15.1.1) Identificação da legislação vigente;

15.1.2) Direitos de propriedade intelectual;

15.1.3) Proteção de registros organizacionais;

15.1.4) Proteção de dados e privacidade de informações pessoais;

15.1.5) Prevenção de mau uso de recursos de processamento da informação;

15.1.6) Regulamentação de controles de criptografia;

15.2) Conformidade com normas e políticas de segurança da informação e conformidade técnica;

15.2.1) Conformidade com as políticas e normas de segurança da informação;

15.2.2) Verificação da conformidade técnica;

15.3) Considerações quanto à auditoria de sistemas de informação;

15.3.1) Controles de auditoria de sistemas de informação;

15.3.2) Proteção de ferramentas de auditoria de sistemas de informação;

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Administração
Baixar livros de Agronomia
Baixar livros de Arquitetura
Baixar livros de Artes
Baixar livros de Astronomia
Baixar livros de Biologia Geral
Baixar livros de Ciência da Computação
Baixar livros de Ciência da Informação
Baixar livros de Ciência Política
Baixar livros de Ciências da Saúde
Baixar livros de Comunicação
Baixar livros do Conselho Nacional de Educação - CNE
Baixar livros de Defesa civil
Baixar livros de Direito
Baixar livros de Direitos humanos
Baixar livros de Economia
Baixar livros de Economia Doméstica
Baixar livros de Educação
Baixar livros de Educação - Trânsito
Baixar livros de Educação Física
Baixar livros de Engenharia Aeroespacial
Baixar livros de Farmácia
Baixar livros de Filosofia
Baixar livros de Física
Baixar livros de Geociências
Baixar livros de Geografia
Baixar livros de História
Baixar livros de Línguas