Faculdade de Tecnologia de Americana
Curso de Analise de Sistemas e Tecnologia da Informação

Políticas de Segurança em Tecnologias da Informação

Caio César Andrieta

Americana,SP
2010

CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

Faculdade de Tecnologia de Americana
Curso de Analise de Sistemas e Tecnologia da Informação

Políticas de Segurança em Tecnologias da Informação

Caio Cesar Andrieta

caio.andrieta@gmail.com

Monografia apresentada como requisito parcial a obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas, de Faculdade de Tecnologia.

Americana,SP
2010

DEDICATÓRIA

Dedico este trabalho à minha mãe, Denise e ao meu irmão Alessandro que são as pessoas mais importantes da minha vida. À Ágata, que também esteve presente nos momentos de dificuldade.

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela dádiva do presente.
À minha mãe e irmão, Denise e Alessandro, por sua dedicação para comigo. Ao meu orientador, pelo suporte no desenvolvimento deste trabalho. À Ágata, pelo apoio no período de faculdade.

Sumário

Resumo

Este trabalho trata da Segurança da Informação, área importante e em crescimento dentro da Tecnologia da Informação. Conceitua Segurança da Informação, as principais características de uma Política de Segurança, como é desenvolvida e implantada dentro de uma Empresa. A Segurança é tema de pesquisas e alvo de investimentos pelas organizações que prezam pela segurança e integridade de seus dados e tem levado as empresas e seus executivos a adquirirem conhecimentos nessa área. Através do conhecimento da Segurança da Informação torna-se mais fácil o entendimento da importância dessa área.

Abstract

This work deals with information security, an important and growing area within the Information Technology. It conceptualizes Information Security, the main characteristics of a Security Policy, how it is developed and deployed within a company. Safety is subject of researches and target for investments by the organizations, which care for security and integrity of their own data and has led companies and their executives to acquire knowledge in this area. Through the knowledge of information security it's much easier to understand the importance of this area.

Introdução

A segurança deve ser um compromisso, uma vez que a convivência de acesso remoto via redes é essencial. Embora haja perda de segurança quando se compartilha dados, esta pode ser minimizada criando-se Políticas de Segurança, que garantam o sigilo dos dados que se deseja proteger.

Os computadores conectados a qualquer tipo de rede estão sujeitos a riscos por duas razões. A primeira delas é que em uma rede, existem outros pontos a partir dos quais um ataque pode ser feito, e a segunda é que a rede estende o perímetro do sistema físico do computador. Em um computador desconectado, tudo está na CPU, que busca dados de autenticação a partir de memória, sendo que não se pode alterar ou espionar tais dados. Quando há vários computadores conectados, o risco de invasão para alteração dos dados compartilhados aumenta.

A informação está sempre presente e cumpre papel importante na gestão de negócios, pois é a partir dela que se visa melhor produtividade, redução de custos, competitividade, entre outros fatores. (Sêmola, 2003).

Pela presença desses fatores, a segurança da informação tem sido objeto de pesquisas, motivando a realização deste trabalho, que avalia o valor da informação para o negócio, disseca aspectos ligados à segurança bem como as propriedades a serem preservadas para que a informação fique sob controle.

Objetivo

Este trabalho visa o estudo dos principais conceitos de Segurança da Informação e de Políticas de Segurança, mostrar as etapas desenvolvidas num Ciclo de uma Política de Segurança e quais os princípios que devem ser levados em consideração para que tal Política alcance os objetivos propostos. Também tem o objetivo de mostrar as vantagens e desvantagens de uma Política de Segurança bem elaborada, implementada, monitorada e auditada, para que a Segurança da Informação da Organização alcance êxito.

Neste trabalho procura-se identificar as dificuldades de elaboração e implantação de uma Política de Segurança assim como as possíveis soluções.

Organização do Trabalho

O trabalho se divide em duas partes. A primeira aborda a Informação de maneira geral, trazendo as definições e conceitos envolvidos com Segurança da Informação. A segunda parte traz o conceito e as etapas da elaboração da Política de Segurança. Apresenta desenvolvimento e a implantação de uma Política de Segurança. Define o comportamento de uma empresa frente a um documento normativo como esse. Esclarece as etapas e quais são os profissionais envolvidos nesse processo, assim como, a importância da conscientização dos recursos quanto ao propósito da Política de Segurança.

As dificuldades são identificadas nas etapas do Ciclo de Implementação da Política de Segurança sugerindo método para melhoria e diminuição de falhas.

1 Segurança da Informação

A segurança é essencial para que as empresas possam, com liberdade, criar oportunidades de negócio de forma a proporcionar confidencialidade, integridade e disponibilidade, sendo estes os princípios básicos para a garantia da segurança da informação. (NBR17999, 2003; Krause e Tipton, 1999).

A confidencialidade se relaciona ao acesso à informação, uma vez que esta deve estar disponível apenas sob autorização. Para que um dado seja íntegro, o sistema deve apresentar desempenho correto e a informação envolvida não pode ser destruída ou corrompida. O serviço e os recursos do sistema devem estar disponíveis sempre que necessário, para que o sistema atenda ao requisito disponibilidade. (Sêmola, 2003).

As formas de utilização dos sistemas de informação foram modificadas nas redes de computadores e na internet, uma vez que nesta as possibilidades de uso são muito mais amplas comparados aos sistemas fechados. Porém, tal liberdade trouxe riscos à privacidade e integridade da informação, o que deixa claro que mecanismos de segurança de sistemas de informação devam ser projetados de forma a impedir acessos não autorizados aos recursos e dados destes sistemas. (Laureano, 2004).

Ter segurança da informação é proteger os sistemas de informação contra negação de serviços a usuários autorizados, contra intrusão e modificação não autorizada de dados armazenados. Ela abrange segurança dos recursos humanos, do material e da documentação, das áreas e instalações das comunicações, assim como à prevenção, detecção, detenção e documentação de eventuais ameaças ao seu desenvolvimento. (NBR 17999, 2003; Dias, 2000; Wadlow, 2000; Krause e Tipton, 1999).

Existem outras propriedades utilizadas como, as extensões dos requisitos fundamentais que foram incorporadas aos componentes da comunicação segura, bem como a privacidade, autenticidade, não-repúdio, controle de acesso, legalidade, auditoria. (Sêmola, 2003; Dias, 2000).

Stoneburner (Stoneburner, 2001) diz que a segurança apenas pode ser obtida com a relação e implementação correta dos princípios de confidencialidade, integridade, disponibilidade e auditoria.

A integridade depende da confidencialidade, pois, se alguma informação confidencial se perde os mecanismos de integridade poderão ser desativados, o contrário também é verdadeiro, pois se um sistema possuir sua integridade afetada, os mecanismos de controle da confidencialidade são perdidos. Para a auditoria e a disponibilidade há a dependência da integridade e da confidencialidade, pois ambos garantem a auditoria do sistema e sua disponibilidade (AAOSANTOS).

1.1 Ciclo de Vida da Informação

Conhecendo o valor da Informação e os fatores que a influenciam, é preciso entender o Ciclo de Vida da Informação, que é composto e identificado pelos instantes que a colocam em situação de risco, esse instante é quando ativos físicos, tecnológicos e humanos fazem uso da informação. Sêmola (Sêmola, 2003) aponta quatro fases distintas para o ciclo de vida da informação, o manuseio, armazenamento, transporte e descarte.

1.2 Principais Mecanismos para Assegurar a Informação

É igualmente importante entender sobre os principais mecanismos relacionados à Segurança. Mas, para entender o que é uma Política e os principais conceitos relacionados a ela, é preciso definir itens básicos dessa realidade.

1.2.1Cookies

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT-BR), o termo *Cookie,* em inglês, se refere a grupos de dados trocados entre o navegador de Internet e o servidor de páginas e armazenados em um arquivo de texto criado no computador do usuário.
Esse cookies tem como função manter a persistência de sessões HTTP. Como exemplo, podemos citar os *Web sites*, no armazenamento de informações como identificação e senha quando se muda de página, ou ainda manter listas de compras ou listas de produtos preferidos em *Web sites* de comércio.

1.2.2 Engenharia Social

Segundo o CERT-BR esse termo é utilizado para descrever um método de ataque, em que alguém faz uso da persuasão para obter informações que possam ser utilizadas para acessar, de maneira não autorizada, computadores ou informações. As situações em que são usadas essas técnicas induzem o usuário à realização de determinada ação sendo que o êxito do ataque depende unicamente do fornecimento de informações solicitadas pelo atacante. Por exemplo, quando alguém pelo telefone, diz ser do suporte técnico do seu provedor de *internet,* informa que sua conexão está apresentando problemas e pede sua senha para corrigi-lo, induzindo o usuário a revelar dados confidenciais.

1.2.3 Vulnerabilidade

Para o CERT-BR, vulnerabilidade é uma falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.
Existem casos onde um *software* ou sistema operacional instalado em um computador contem uma vulnerabilidade que permite sua exploração remota, ou

seja, através da rede. Um atacante que esteja conectado à *internet*, ao explorar tal vulnerabilidade, pode obter acesso não autorizado ao computador vulnerável.

1.2.4Códigos Maliciosos

Código Malicioso ou *Malware* (*Malicious Software*) é definido pelo CERT-BR como um termo genérico que abrange todos os tipos de programas, especificamente desenvolvidos para executar ações maliciosas em um computador, como exemplo, um vírus, *worms* e *bots*, *backdoors*, cavalos de tróia, *keyloggers* e outros programas *spyware*, *rootkits*, etc.

1.2.5Negação de Serviço

Nesses ataques (*DoS – Denial of Service*) se utiliza um computador para tirar de operação outros computadores e serviços conectados à *Internet*.
Caracteriza-se pelo desconhecimento da sua origem e têm o objetivo de interromper atividades legítimas, aproveitando-se de falhas ou vulnerabilidades existentes na máquina da vítima. Este objetivo se alcança quase sempre pelo envio de pacotes pelo atacante a uma taxa maior do que pode ser tratado pela vítima, tornando requisições legitimas inacessíveis. Há ainda uma versão distribuída dos Ataques de Negação de Serviço, os *Distributed DoS* (*DDoS*), em que os pacotes enviados são de diversas origens e o tráfego gerado inutiliza totalmente os serviços da vítima (Mirkovic e Reiher, 2004).
O CERT enfatiza que quando um computador ou rede sofre um ataque deste tipo o objetivo é indisponibilizar o uso dos mesmos, pois tendem a ocupar toda a banda disponível para um acesso, por exemplo, gerar uma sobrecarga no processamento de um computador, de tal forma que o usuário não consiga utilizá-lo;

1.2.6Criptografia

A criptografia converte textos originais em uma informação codificada e, para o CERT-BR é a ciência de escrever mensagens cifradas ou em código, sendo que apenas o destinatário a compreenda. Tem a finalidade de autenticar a identidade de usuários, proteger o sigilo de comunicações pessoais e de transações comerciais e a integridade de transferências eletrônicas de fundos.

As primeiras técnicas criptográficas utilizavam somente um algoritmo de codificação, então, bastava que o receptor da informação conhecesse tal algoritmo para extraí-la.

As técnicas mais eficazes envolvem as chamadas “chaves criptográficas”, em que chave é um conjunto de *bits*, seqüência de caracteres, dígitos e símbolos, baseado em um algoritmo com capacidade para decodificar informações. Então se o receptor utilizar uma chave incompatível com a chave do emissor, não conseguirá extrair a informação criptografada.

1.2.6.1 Criptografia de Chave Única

A também chamada Criptografia de Chave Simétrica utiliza uma única chave tanto para codificar quanto decodificar mensagens. Embora apresente eficiência quanto ao tempo de processamento esse método é limitado, pois o emissor e o receptor têm antes de conhecer a chave, sendo necessário utilizar uma maneira segura para que ela seja compartilhada entre ambos.

1.2.6.2 Criptografia de Chave Pública e Privada

Diferentemente da anterior aqui se utiliza chaves distintas para codificar e decodificar mensagens. O emissor e o receptor têm duas chaves cada um, sendo uma chave pública, que poderá ser livremente divulgada e outra privada, que deverá ser mantida em segredo. Através da chave pública as mensagens são

codificadas e só poderão ser decodificadas pela chave privada correspondente. Também conhecido como Criptografia de Chave Assimétrica.

1.2.7 Assinatura Digital

O CERT-BR e a Justiça Federal definem esta como sendo uma tecnologia que garante a integridade e autenticidade de arquivos eletrônicos, utilizando-se uma chave privada (que confere segurança ao método) de tal maneira que o receptor consiga verificar se o remetente é real, se possui a chave privada para a assinatura e saiba se a mensagem recebida sofreu modificações.
Mas assinar digitalmente uma mensagem não significa gerar uma mensagem sigilosa.

1.2.8 Certificado Digital

É um arquivo eletrônico que traz informações sobre a entidade, pessoa ou instituição para o qual o certificado foi emitido e que são utilizados para comprovar sua identidade. Este arquivo pode ser armazenado em um computador ou em outro tipo de mídia, como um *token* ou *smart card*. Cada um desses certificados contém informações que identificam a instituição ou pessoa e a autoridade que a garante. Qualquer certificado digital possui uma assinatura que indica a garantia da procedência das informações contidas nesse certificado.
Para ser válido o certificado digital deve conter informações como, dados que identifiquem a entidade para a qual o certificado foi emitido; nome e assinatura digital da Autoridade Certificadora (AC) que afirma que a chave pública contida no certificado é condizente com as informações contidas no mesmo; e número de série e período de validade.

1.2.9 Autoridade Certificadora (AC)

Responsável pela emissão de certificados digitais para diferentes entidades, como pessoa, computador, departamento de uma instituição, etc. Ela funciona como um “Cartório Eletrônico”, pois confere caráter fidedigno a um certificado digital, pela assinatura digital da AC emissora.

1.3 Fraudes na Internet

São crimes eletrônicos que solicitam e conduzem transações fraudulentas, através da manipulação.
Este tipo de fraude ocorre quando um *hacker* ou *cracker*, ilegalmente, consegue e faz uso de dados pessoais, para envolver qualquer manipulação ilegal.
Utilizando-se de *e-mails* com textos que envolvem engenharia social, os fraudadores induzem a vítima a fornecer dados sigilosos.
Os fraudadores obtêm dados bancários e senhas dos usuários efetuando os roubos, em grande parte, pelo envio de algum tipo de código malicioso, que é executado pela vítima.

1.3.1Scam e Phishing

O *scam* (que é um spam) tem como finalidade obter vantagens financeiras através de *Web sites* fraudulentos com ofertas atrativas que induzem o usuário a acessá-lo, como os *Web sites* de leilões.
A utilização de iscas para pescar senhas e dados financeiros dos usuários de *internet*, tem um termo criado pelos próprios fraudadores que faz uma analogia ao *fish* (pescar): é o *phishing*. É um tipo de fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida.

1.3.2Incidentes de Segurança Digital

É qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas ou a redes de computadores.
Define-se como uma invasão a um computador, ataque de negação de serviço, furto de informações, atividade em rede não autorizada ou ilegal, como por exemplo, tentativas de acesso não permitido a sistemas; alterações em um sistema, sem conhecimento, instrução ou consentimento prévio do administrador; etc.

1.3.3Notificações de Incidentes

Um ataque pode ser originário de um programa malicioso que faz o ataque de maneira automática (*bot* ou *worm*) ou de uma pessoa que pode ou não utilizar se de ferramentas que automatizam ataques.
Um Incidente de Segurança deve ser notificado, segundo o CERT, para que se o ataque partir de uma máquina vítima de um bot ou worm, o responsável possa a partir da origem do ataque identificar e corrigir o problema. Mas se o ataque não se originar de um programa, a Política de Segurança pode ter sido violada e sendo assim o responsável pela máquina deve ser notificado quanto ao comportamento errado de um usuário, ou ainda, sobre uma invasão que não tenha sido identificada anteriormente.
O CERT coordena a resposta aos incidentes, gera estatísticas e desenvolve documentos de apoio a usuários e administradores de redes de *internet*, ou seja, é o ponto central para notificações de incidentes

1.3.4 Dados essenciais de uma notificação

Para que os números de incidentes de segurança que ocorrem no Brasil sejam consolidados pelo CERT é importante que as vítimas os reportem para que este possa ser identificado: *logs* completos gerados pelo sistema; horário, data e

timezone dos *logs* ou da ação a ser notificada; dados completos sobre o incidente ou outras informações que tenham sido utilizadas para identificar a ação.

1.3.5 Registros de Eventos

1.3.5.1 Logs

É a descrição do registro de ocorrência de eventos em um sistema computacional. Esse registro poderá ser utilizado para conhecer o comportamento de um sistema no passado ou, para restabelecer um sistema em seu estado original. Um arquivo de *log* também pode ser usado para auditorias e diagnóstico de problemas num sistema. Na definição do CERT, é um registro de atividades gerado por programas computacionais. Os *logs* referentes a incidentes de segurança, normalmente são gerados por *firewalls* ou por sistemas de detecção de intrusão.

1.3.5.2 Sistema de Detecção de Intrusão

IDS, do inglês Intrusion Detection System é um dispositivo que detecta principalmente ações maliciosas, tentativas de ataques ou obtenção de informações confidenciais, analisando o sistema e a rede quanto suas atividades e identificando entradas não autorizadas. Seu objetivo é capturar fraudadores em ação antes que se danifiquem os recursos do sistema, segundo o CERT.
Esses sistemas podem gerar, tanto *logs* de invasão com sucesso como para sua tentativa. É possível determinar se um ataque alcançou seu objetivo, analisando detalhadamente os *logs* gerados por um *IDS.*

1.3.5.3 Falso Positivo

Termo que classifica uma situação em que um dispositivo de *firewall*, *IDS* ou “antivírus” aponta uma ação comum como sendo de ataque. Um *firewall* em uma rede de computadores, que não esteja configurado adequadamente este indica solicitações e respostas feitas pelo usuário da rede como possível ataque, é um exemplo de “falso positivo”.

2 Políticas de Segurança

A Segurança da Informação compreende um conjunto de medidas com objetivo de proteger e preservar informações e sistemas, assegurando integridade, disponibilidade e confidencialidade. (Amoroso, 1994).

Informações incorretas ou vazamento de assuntos confidenciais de uma Organização podem acarretar num desastre com proporções irreversíveis, então as decisões coletivas que determinam a postura de uma Organização quanto à segurança, formam, segundo Fontes (Fontes, 2000) a Política de Segurança.

Mais precisamente, esta Política determina os limites de comportamento aceitáveis e as medidas a serem tomadas caso ela seja violada.

Sendo um conjunto de normas e procedimentos que garantem o controle e a segurança da informação, a Política de Segurança formaliza a necessidade da Organização de proteger sua informação corrente, portanto se ela respeita as diretrizes estabelecidas no documento dessa Política, seu sistema é considerado seguro. A Organização personaliza essa Política de acordo com suas necessidades e deve estabelecer padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido.

Para o CERT-BR a Política de Segurança de uma Organização atribui direitos e deveres aos que lidam com a informação, estipulando penalidades àqueles que descumprem as regras estabelecidas em tal Política.

O sucesso de uma Política de Segurança depende de recursos financeiros para implementação, deve ser válida para todos os colaboradores, deve ser simples, com o apoio da alta direção, implementar medidas de proteção, analisar ameaças, estabelecer responsabilidades e ainda corrigir objetivamente as violações da informação.

As auditorias internas periódicas são importantes ao definir punições para o não cumprimento das diretrizes estabelecidas, assim o objetivo da Política é alcançado.

2.1 Objetivos de uma Política de Segurança

O maior objetivo dessa Política é a conscientização da proteção da informação e da tecnologia do Sistema, pelos seus usuários, gerentes e colaboradores, através de regras sobre manuseio, controle, proteção e descarte das informações.
Ela deve especificar os mecanismos utilizados para alcançar tal proteção.
Outro objetivo é o de oferecer um ponto de referência, do qual se possa adquirir e auditar sistemas computacionais adequados aos requisitos propostos pela Política de Segurança estabelecida.
É utopia acreditar que essa Política mantenha um Sistema totalmente seguro, pois com o passar do tempo ele se torna obsoleto e com o uso de tecnologias específicas, pode ser invadido. Portanto pode-se dizer que a finalidade dessa Política é alocar recursos que gerenciem adequadamente a segurança da informação, e para que tal gerência seja efetuada de uma forma ótima são necessárias práticas como, estudo e otimização de investimentos com materiais, equipamentos e treinamentos.
Alguns determinantes estabelecem segundo Aurélio, os objetivos específicos de uma Política de Segurança, como:

- Serviços oferecidos *x* segurança fornecida: serviços oferecidos aos usuários carregam consigo riscos de segurança, e se esse risco é superior ao benefício, antes de tentar torná-lo mais seguro a Política deverá optar pela eliminação desse serviço;
- Facilidade de uso *x* segurança: a solicitação de senhas torna o sistema menos conveniente para seu uso, mas confere maior segurança;
- Custo da segurança *x* risco de perda: muitos custos envolvem a segurança de um sistema como o monetário, de desempenho e facilidade de uso. Há também vários níveis de risco: perda de privacidade, de dados, de serviços, etc.

Essa determinante mostra que cada custo deve ser comparado ao tipo de perda. A partir disso são estabelecidos os objetivos de uma Política de Segurança.

Um objetivo importante é analisar as necessidades da Organização, embasada nas pessoas e processos envolvidos, para que os objetivos específicos sejam traçados e o plano criado.

2.2 Características Principais de uma Política de Segurança

As informações da maioria das empresas brasileiras com acesso à *internet* segundo a TIC estão completamente vulneráveis e expostas a ameaças. Isso mostra a importância da Política de Segurança e de sua boa elaboração nas empresas, portanto não bastam investimentos em segurança, licenças de conceituados antivírus, locação de renomados servidores de *e-mail* e fornecedores de *internet*, etc.

Atendendo alguns propósitos, segundo Wadlow, essa Política pode ser elaborada seguindo o seguinte roteiro:

- descrever o que está sendo protegido e por qual motivo;
- definir prioridades sobre o que deve ser protegido e qual o custo envolvido;
- permitir e estabelecer um acordo com várias partes da empresa com relação ao valor da segurança;
- fornecer ao departamento de segurança um motivo válido para se negar algo quando necessário, de modo que o processo seja continuamente revisado e melhorado;
- impedir que o departamento de segurança tenha um desempenho fútil, definindo claramente quais atividades e privilégios esses administradores precisarão desempenhar para a mantenedora da política;
- definir responsabilidades, como o responsável pela informação e pela sua correta utilização;
- definir penalidades: a política deve mencionar alguma forma de punição caso a mesma seja desrespeitada, o que impede que os usuários a ignorem;

- ser simples: para permitir que os usuários entendam o que a Política propõe; deve envolver aspectos técnicos, humanos e organizacionais com foco na proteção da informação, também exprimir o pensamento da empresa e ser coerente com suas ações;
- ser objetiva: explanando os objetos que trata e, estabelecendo normas pontuais sem ser um documento extenso;
- ser consistente: da mesma maneira que as organizações cumprem leis e regulamentos do governo, a Política de Segurança deve estar em conformidade com essas normas. O mais alto executivo ao assinar esse documento normativo, explicita seu apoio à implementação da Política.

Todos os usuários ao consultar o documento da Política de Segurança devem compreender a filosofia da empresa sobre tal recurso, considerando as características operacionais e culturais da empresa. Essa Política e seu documento principal devem tratar a informação como um bem da empresa definindo as regras estruturais e os controles básicos para acesso e uso da informação.

2.3 Visão da Empresa a uma Política de Segurança

É importante analisar as expectativas e conceitos esperados pela corporação, antes de se iniciar qualquer estudo para a elaboração e implementação de uma Política de Segurança, a partir do pressuposto de que essa Política muda com o tipo de corporação em que será implantada. A maior influência na elaboração de uma Política é o tipo de negócio realizado, de informação utilizada e o fluxo dela na empresa.

A partir de um levantamento das necessidades da corporação, a administração junto aos membros responsáveis pela elaboração, implementação e manutenção da Política de Segurança estabelecem as principais funções da Política em questão.

Depois se define a missão principal do Departamento de Segurança e traçam-se os objetivos a serem alcançados.

Para Moreira (Moreira, 2001), quando o sistema de segurança duma empresa é falho, o mesmo torna-se vulnerável a um ataque de pessoas mal intencionadas ou até mesmo de um vírus de computador e, assim, as informações estratégicas e confidenciais da empresa podem ser destruídas ou compartilhadas de forma errada.

Uma falha na segurança pode levar a um incidente que afeta diretamente o negócio da empresa, gerando impacto negativo à sua imagem no mercado, aos seus produtos e clientes.

É dever dos profissionais relacionados à Política de Segurança monitorar e verificar se as diretrizes implementadas estão de acordo com os princípios do documento da Política de Segurança.

Feita a análise da abrangência, responsabilidades e critérios de segurança, os objetivos a serem trabalhados também devem ser estudados.

O conjunto de decisões da Política de Segurança determina a postura da organização quanto à segurança de seus dados, limita o comportamento e define as medidas tomadas em caso de violação.

Para que a informação de uma empresa seja confiável ela depende da segurança que garante seus aspectos principais, a integridade, confidencialidade e disponibilidade.

2.4 Ciclo de Implementação de uma Política de Segurança

A Política de Segurança deverá garantir à organização o máximo dela, através de um processo de implementação criterioso e planejado, com organização, disciplina e determinação dos envolvidos e o comprometimento da alta gerência (Case Solectron, 2000).

Para que se inicie o ciclo de implementação, o primeiro passo é avaliar os riscos, o que garantirá o sucesso da política. Ao se iniciar a solução é necessário identificar e segmentar o problema para permitir maior profundidade na análise de suas características.

Existem muitos fatores associados à segurança da informação, portanto é necessário compreender que ela é o foco, e que não se encontra mais confinada a ambientes físicos específicos, ou a processos isolados.

Pela constante circulação da informação dentro da empresa, ela está sujeita a várias ameaças, está vulnerável e suscetível a sofrer impactos (Sêmola, 2003).

O processo de implementação poderia ser dividido em quatro momentos: avaliação; desenho da solução; elaboração da arquitetura de segurança; implementação da solução; monitoração da segurança; recuperação de incidentes e elaboração de um plano de contingência.

Os riscos surgem em decorrência da presença de fraquezas e vulnerabilidades. Por outro lado, as ameaças exploram as vulnerabilidades existentes, devido a falhas de configuração ou inexistência de medidas de proteção adequada. Deste modo, os danos causados trazem impactos negativos ao negocio, aumentando os riscos. Entretanto, medidas de proteção adequadas protegem o negócio, de forma a diminuir os riscos em níveis consideráveis. Por isso, faz-se necessário uma análise detalhada dos riscos, vulnerabilidades e ameaças, para que a solução proposta seja adequada à necessidade da Organização. (Ferreira, 2008).

2.4.1 Etapa de Avaliação

As necessidades de segurança são avaliadas a partir da realização de um estudo sobre a empresa. São levantadas as vulnerabilidades, que são as vias de acesso ou um ponto suscetível a um ataque à informação; ameaças e riscos envolvidos (Bernstein, 1997).

Levam-se em conta os itens: análise de vulnerabilidades; análise de ameaças; análise de riscos; avaliação dos riscos; elaboração de recomendações e planos de ação. Posteriormente à análise dos riscos e suas potencialidades, é gerado um relatório final que deve contemplar a identificação das vulnerabilidades, classificação dos riscos identificados, dimensionamento dos recursos necessários, apresentação das observações e efeitos, sugestões para minimização dos riscos identificados, comentários da administração e conclusão.

Os bens e ativos de uma organização estão sujeitos a vulnerabilidades, cada qual em sua intensidade. Estas proporcionam riscos para a organização que muitas vezes são causados por falhas de controle. Assim, pode-se afirmar que os riscos são oriundos da presença de vulnerabilidades e fraquezas do sistema, em contrapartida, as ameaças aproveitam se das vulnerabilidades existentes, causando danos e impactos negativos à organização, aumentando os riscos. Por essa razão, é importante que medidas de segurança adequadas sejam tomadas, para proteger a informação corrente e diminuir os riscos (Moreira, 2001).

2.4.1.1 Dificuldades Encontradas e Propostas para Redução de Falhas

A etapa anteriormente exposta desempenha papel importante no Ciclo de Implementação de uma Política de Segurança. Portanto é essencial que essa avaliação seja detalhada para que os profissionais consigam conhecer o ambiente e o que deve ser implementado como medida de segurança.

Durante essa etapa alguns problemas são comumente identificados: a análise foca detalhes técnicos do ambiente a ser protegido, os mecanismos de armazenamento de dados, como e com qual freqüência se efetuam *back-up* dos dados, configurações de regras de *firewall* existentes, configurações de usuários, etc.; não se efetua a análise seguindo um roteiro, o que causa desorganização e itens verificados repetidamente; muitos profissionais não possuem experiência então não conseguem identificar um possível risco, ameaça ou vulnerabilidade; quando não se consideram características do histórico da empresa pode-se gerar uma proposta de solução que não se aplica ao cenário da organização; a equipe responsável pela etapa não consegue analisar as particularidades da empresa, como as técnicas, processuais e de recursos humanos, por não dividir tarefas.

Sêmola (Sêmola, 2003) sugere que as empresas podem utilizar o *framework* como base de trabalho, proposto na norma BS7799 (versão brasileira: NBR/ISO17799), que estabelece um SGSI (Sistema de Gestão de Segurança da Informação). A BS7799 tem como objetivo definir um Código de Prática para

Gestão da Segurança da Informação que auxiliará eficazmente na análise de riscos. Esse *framework* orienta a empresa a administrar os riscos de segurança da informação, mas ela é quem deve decidir como executar as propostas nele contidas, pois ele só apresenta o que fazer e não como (Sêmola, 2003).

2.4.2 Etapa de Desenho da Solução – Elaboração da Arquitetura de Segurança

Uma avaliação do grau de envolvimento dos usuários com a confidencialidade, integridade e disponibilidade, requisitos mínimos de segurança e de auditoria são alguns dos benefícios conseqüentemente alcançados após a conclusão da etapa anterior. Então a equipe responsável pela proposta de solução tem condições de elaborar um plano de ação para redução de riscos.

Através da observação dos conceitos anteriormente expostos, como risco, vulnerabilidades e ameaças é possível um estudo aprofundado dentro da organização.

A seguir vem o processo de desenho da solução, ou seja, todas as definições dos tópicos que serão contemplados nos procedimentos e os documentos e formulários a serem criados. As regras deverão estar descritas nos procedimentos, formação do grupo de trabalho para gestão do processo e definição dos profissionais representantes das áreas da empresa (Luz, 1999).

A formulação das diretrizes e estruturas relacionadas à segurança é a base para elaboração da arquitetura de segurança. Aqui devem ser considerados dois aspectos segundo Luz (Luz, 1999): a definição das diretrizes da alta administração e estruturação da função de administração de segurança, a informática para manter o sistema, os usuários na garantia de integridade dos dados e a alta administração para estabelecer as diretrizes e padrões a serem adotados na política de segurança. (Luz, 1999).

A visão de como se conduzirá o trabalho, os tópicos a serem abordados e aplicados na Política a ser implementada se tornam possíveis nesse ponto do desenvolvimento da Política de Segurança.

2.4.2.1 Dificuldades encontradas e Propostas para redução de falhas

O documento normativo escrito durante a Etapa de Desenho da Solução e baseado no relatório final desenvolvido ao término da Etapa de Avaliação deve ser proposto à alta direção da organização.

Nesta etapa são desenvolvidos planos de continuidade do negócio e de ação para a melhoria contínua da segurança na empresa, além do conjunto de normas a serem seguidas.

É imprescindível que a alta administração da empresa se envolva na realização das atividades desta etapa para que seus executivos se conscientizem do quanto este documento agrega à empresa, e também para que seus objetivos sejam levados em conta.

Embora sejam importantes os usuários e a alta direção para o sucesso da Política de Segurança na organização, o envolvimento deles nem sempre ocorre da melhor maneira possível. Isso pode resultar em problemas na implementação da Política, pois os itens definidos e redigidos deverão ser implantados na empresa para a segurança dos dados. É de responsabilidade do profissional relacionado à proposta da Política certificar-se dos objetivos e expectativas dos membros da direção e dos usuários do sistema quanto à Política de Segurança, pois a maioria deles tem uma visão segregada da mesma: não associam á informação, a proteção que ela requer para que a organização obtenha o sucesso desejado.

A equipe de elaboração e proposta de solução deve esclarecer os objetivos e benefícios que a Política agregará à empresa, e os responsáveis pela segurança da informação devem apresentar a proposta aos executivos que irão validar tal documento.

Quando o tempo dedicado à etapa é insuficiente, a interação entre os profissionais envolvidos pode não ocorrer, e isso torna a proposta de solução vaga e a percepção executiva falha. Conseqüentemente se perde a noção das responsabilidades perante a Política de Segurança, a próxima etapa é prejudicada e itens importantes não são verificados e validados.

Uma adequação de intervalos para realização de cada fase do ciclo minimiza falhas na comunicação e revisão de proposta de solução.

2.4.3 Etapa de Implementação da Solução

No desenvolvimento de uma Política de Segurança se faz necessário uma pesquisa do conteúdo que ela terá, criar o texto que a descreverá, obter o apoio dos níveis hierárquicos mais altos da empresa e disseminá-la em todos os setores (Calheiros, 2004). A dificuldade da Política está na sua sustentação e não no seu início, por isso deve-se verificar sempre, se as normas estão sendo cumpridas e se há necessidade de atualização.

Para Sêmola (Sêmola, 2003), os primeiros a serem conscientizados da importância da segurança para a organização são os funcionários da direção, preocupando-se com a comunicação e compartilhamento da Política de Segurança com os outros funcionários.

A etapa de implementação da solução é baseada na elaboração, identificação e estruturação dos elementos da Política de Segurança. Nela, as atividades planejadas serão implementadas considerando as prioridades e a abrangência de acordo com a administração da empresa, e os resultados deverão ser visíveis no todo da organização.

As maiores dificuldades aparecem para os profissionais responsáveis pela elaboração da proposta de política, pois nesta etapa os usuários do sistema são doutrinados a seguir as normas e padrões estabelecidos no documento normativo, mas os usuários antigos tornam-se irredutíveis às mudanças propostas.

Esta é a fase mais crítica do projeto, que poderá ser dificultada por qualquer tipo de conflito entre áreas ou por interesses alheios ao sucesso das diretrizes, então se torna fundamental a presença de pessoas influentes que apóiem o projeto para que ele siga normalmente suas fases de implementação.

O grupo de profissionais responsáveis pela implementação das diretrizes de segurança forma um comitê de segurança para que tal implementação evolua. É

de responsabilidade do comitê, aprovar e rever periodicamente a Política, de estabelecer as funções e objetivos da segurança da informação, classificar o fluxo de informação dentro da empresa, atentar-se às tendências externas quanto à solução de incidentes de segurança bem como verificar as maiores ameaças a que os recursos de informação estão expostos.

Durante esta etapa os procedimentos de administração da segurança são elaborados a fim de garantir que as atividades críticas sejam rapidamente restabelecidas após um incidente que interfira na integridade da informação, daí a necessidade de identificação de recursos tecnológicos que viabilizem o projeto.

É criado ainda, um documento oficial da organização, que deve conter as regras, metodologias, instruções técnicas, planos e procedimentos a serem seguidos por todos os membros dela, envolvidos ou não com a manipulação de recursos relacionados às informações.

Nesse momento de implementação ocorrem treinamentos que divulgam a Política a todos os funcionários e colaboradores, recebendo uma cópia do documento com o resumo das principais diretrizes da Política.

A definição de um programa de conscientização dos usuários, que explique a importância da implementação, padroniza a forma de manusear a informação, que é um elemento fundamental para integridade e sucesso do negócio. Se esta conscientização e o treinamento forem bem executados, o projeto tem grandes chances de sucesso.

2.4.3.1 Dificuldades encontradas e Propostas para redução de falhas

Além da conscientização dos usuários sobre o valor das informações, os executivos também precisam conhecer as fragilidades de seu ambiente e a Política de Segurança. É responsabilidade da direção essa conscientização de possíveis mudanças para que a informação que circula pelo sistema esteja segura.

Para redução das vulnerabilidades as medidas de segurança apontadas no documento normativo deverão possuir uma metodologia para implantação.

As fragilidades do ambiente de recursos humanos e a Política de Segurança são os responsáveis por uma ou mais fases do processo de segurança da informação, o que faz desses recursos o elo mais frágil da corrente (Sêmola, 2003). Então é fundamental que seja criada uma cultura de segurança, que pode ser cultivada a partir de iniciativas internas da empresa, como seminários, campanhas de divulgação, cursos de capacitação, notas enviadas pela direção aos usuários do sistema e, até mesmo que os usuários assinem termos de ciência quanto às normas estabelecidas.

Sêmola (Sêmola, 2003) diz que implementar é adquirir, configurar e aplicar os mecanismos de controle de segurança com o propósito de alcançar o nível de risco adequado. Entretanto, o universo de controles é muito extenso, pois tais mecanismos não são apenas físicos ou tecnológicos, são também humanos, por isso, é fundamental que a conscientização seja o foco dessa etapa.

É importante sugerir a criação de um processo claro para os usuários que não trabalharam com o sistema anterior à implementação da Política para que tenham acesso às documentações, respondam questionários a respeito do conteúdo abordado ou que assinem termos de responsabilidade e consciência de seus deveres quanto à segurança das informações.

2.4.4 Etapa de Monitoração e Auditoria da Segurança

Segundo Sêmola, o nível de segurança de uma organização tende a oscilar sempre que ocorrer uma mudança endógena ou exógena; por conta disso, é condição de sucesso montar um modelo de administração e monitoração de controles de segurança, formado por índices e indicadores importantes para o negócio, a fim de retro alinhar o processo de gestão coordenado pelo Security Officer. Esses insumos é que irão provocar mudanças de direcionamento, priorização e otimização do retorno sobre o investimento (Sêmola, 2003).

A Etapa de Monitoração é a fase que analisa o cumprimento das diretrizes da política de segurança pelos usuários envolvidos e a definição de critérios que deverão ser acordados. Cria mecanismos para o gerenciamento e dispositivos capazes de medir a efetividade da Política.

Essa etapa pode ser dividida em duas: elaboração e implementação do Plano de Monitoração e medição de indicadores e apuração de índices. Na primeira o plano poderá ser executado através de uma auditoria de segurança que deve ser executada periodicamente incidindo mais freqüentemente nas áreas mais críticas, podendo ser executada por auditores externos ou internos para controlar a observância das medidas de segurança aprovadas.

A segunda cria medidores que gerenciarão e fornecerão dados para avaliação dos efeitos com a implementação da Política, e com eles a alta direção da organização poderá tomar decisões visando a sua melhoria continua.

Auditoria significa examinar com o intuito de verificar (Pereira, 2004), portanto a equipe responsável por ela deve verificar se o dia-a-dia das operações das tarefas de segurança da organização está em alinhamento com sua política de segurança, que deve ser a base para a auditoria. A ausência de uma política de segurança compreensiva não permite saber se a organização está mantendo um ambiente seguro.

2.4.4.1 Dificuldades encontradas e Propostas para redução de falhas

Para os envolvidos no projeto esta etapa delimita o início do ciclo de segurança, pois é nela que a Política é auditada internamente pelos seus desenvolvedores.

Os mecanismos desenvolvidos nas etapas anteriores são monitorados pelo acompanhamento de indicadores de mudança a fim de analisar se os requisitos propostos estão sendo atendidos pela Política implementada.

2.4.5 Etapa de Recuperação de Incidentes (ou Plano de Continuidade do Negócio) e Elaboração de um Plano de Contingência

Esse é o momento de reavaliar os riscos e os propósitos aos quais a Política está atendendo, se está sendo eficiente e se é possível melhorá-la.

Segundo Sucesu (Sucesu, 2004) essa etapa tem a finalidade de minimizar o impacto da ocorrência de um dano que os procedimentos iniciais da Política de Segurança não puderam evitar.

Foi após os ataques ao *World Trade Center* em setembro de 2001, que algumas empresas começaram a compreender a importância do Plano de Continuidade do Negócio (Fontes, 2008). Neste ataque, algumas organizações deixaram de existir ou pela tragédia, por não possuírem um Plano de Continuidade, ou por possuírem um plano que utilizava recursos depositados na torre ao lado.

O Plano de Contingencia é um documento que contem rotinas a serem executadas quando houver desastre na área de Informática, um dano físico ou lógico às informações armazenadas. A situação de emergência deverá sempre ser analisada em concordância com os trechos descritos no plano, atentando-se às decisões a serem tomadas em situações emergenciais.

Este plano segundo Lemos (Lemos, 2001) visa a continuidade das atividades necessárias à organização permitindo superar com êxito qualquer situação adversa. Estando toda e qualquer instalação sujeita a hipótese de desastres de diversas naturezas, sendo estas ameaças de origem natural ou acidental, a ocorrência de um desastre pode proporcionar a paralisação total ou parcial dos ambientes tecnológicos, ocasionando perda de informação e vulnerabilidade, assim como perda financeira para a empresa sinistrada.

Para outros autores como Gil (Gil, 1998), o plano de contingência é um conjunto de procedimentos que visa restabelecer a continuidade dos serviços no ambiente informacional após um desastre. Portanto, seu objetivo é direcionar as ações a serem tomadas para garantir continuidade dos serviços essenciais às áreas de negócios.

Lemos defende que este Plano deve ser desenvolvido e testado com freqüência mínima de duas vezes ao ano, simulando condições emergenciais, definindo-se a equipe responsável por inspecionar os itens da política, bem como examinar o cumprimento das rotinas especificadas relatando à administração o resultado dos testes. Se o plano de recuperação apresentar falhas no decorrer das inspeções, estas deverão ser corrigidas rapidamente atendendo as necessidades da política de segurança da organização.

Tanto o Plano de Contingência como o documento normativo devem ser elaborados com atenção aos mínimos detalhes, pois é com esse documento que a equipe de administração da segurança da informação se norteará em casos de incidentes, ou seja, o Plano deverá ser eficaz recebendo todo apoio da alta direção da organização, definindo responsabilidades, formando grupos voltados ao desenvolvimento, treinamento, manutenção e execução da segurança. Havendo um bom plano, o risco pode ser identificado, evitando problemas de *software* ou de *hardware*, falhas nas comunicações, no fornecimento de energia e de pessoal. (Calheiros, 2002).

2.4.5.1 Dificuldades encontradas e Propostas para redução de falhas

O que irá detalhar as ações corretivas a serem tomadas, como e onde elas serão realizadas, é o Plano de Contingência, para que as informações perdidas ou indisponibilizadas possam ser recuperadas após um incidente.

Para Fontes (Fontes, 2008), o Plano de Continuidade de Negócios deverá atingir uma determinada área ou solução, considerando o cenário e as ameaças.

Ao propor a solução pela primeira vez, a organização comete um erro elaborando um único plano que referencie todas as situações de incidentes de segurança.

O ideal é iniciar com as situações que oferecem maior risco à segurança desenvolvendo um plano distinto para cada situação, pois o objetivo do Plano de Recuperação de Incidentes é restaurar as interrupções não programadas num curto período de tempo.

O Plano de Contingência deve ser testado e revisado periodicamente com a revalidação periódica da Política, pois se uma organização não possui esse Plano os profissionais não saberão como e por onde iniciar um processo de recuperação de informação após um incidente de segurança.

Destacam-se alguns itens que podem ser seguidos durante a elaboração do Plano de Continuidade de Negócios:

- definir situações de risco;
- analisar as situações de maneira individual, elaborando hipóteses e possíveis situações para a crise;
- definir metas, objetivos e prioridades para que o problema apontado seja solucionado rapidamente;
- organizar a equipe, de forma a suportar o plano elaborado;
- definir procedimentos-chave para execução do plano quando necessário.

3 Conclusão

O trabalho apresentou definições sobre a informação e sua segurança, explicou também sobre a Política de Segurança e as etapas principais para o seu desenvolvimento e implantação.

A revisão literária possibilitou mostrar neste trabalho as dificuldades enfrentadas num projeto de implementação de uma Política de Segurança e apontar ações para que se atinja com eficácia os objetivos das fases do Ciclo de Implementação de uma Política de Segurança.

4 Referências Bibliográficas

1-SÊMOLA, Marcos. **Gestão da Segurança da Informação. Visão executiva da segurança da informação**. 4ª Edição. Rio de Janeiro: Elsevier, 2003.

2-NBR ISO/IEC 17799 – **Tecnologia da Informação, Código de Prática para Gestão da Segurança da Informação**. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2003.

3-KRAUSE, Micki e TIPTON, Harold F. **Handbook of Information security Management**. Auerbach Publications, 1999.

4-LAUREANO, Marcos Aurélio Pchek. **Uma Abordagem para a Proteção de Detectores de Intrusão Baseadas em Máquinas Virtuais**. Paraná: Pontifícia Universidade Católica do Paraná. Dissertação de Mestrado apresentado ao Programa de Pós-Graduação em Informática Aplicada, 2004.

5-DIAS, Claudia. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books, 2000.

6-WADLOW, Thomas A. **Segurança de Redes**, Rio de Janeiro: Campus, 2000.

7-STONEBURNER, G. **Computer Security, Underlying Technical Models for Information Technology Security**, NIST Special Publication, 2001.

8-AAOSANTOS. **Segurança de Dados e Informações**. Disponível em http://www.aaosantos.pro.br/segdados/aula2.pdf. Último acesso em 20/06/2010.

9-CERT Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – **Cartilha de Segurança para Internet**. Disponível em http://www.cartilha.cert.br. Brasil. Último acesso em 15/06/2010.

10-MIRKOVIC, J. e REIHER, P. **A Taxonomy of DDoS Attack and DDoS Defense Mechanisms**. ACM SIGCOMM Computer Communications Review, 2004.

11-INFOWESTER **Criptografia**. Disponível em http://www.infowester.com. Último acesso em 11/06/2010.

12-PORTAL DA JUSTIÇA FEDERAL. Disponível em http://www.jf.jus.br/cfj. Último acesso em 14/06/2010.

13-IMASTERS **Chaves Assimétricas**. Disponível em http://imasters.uol.com.br/artigo/3624/seguranca/chaves_assimetricas_e_a_assinatura_digital/. Último acesso em 17/06/2010.

14-WOT Web of Trust. Disponível em http://mywot.com. Último acesso em 13/06/2010.

15-BRASIL, Tribunal de Contas da União. **Boas práticas em segurança da informação / Tribunal de Contas da União**. 2ª Edição. Brasília: TCU, Secretária de Fiscalização de Tecnologia da Informação, 2007.

16-FONTES, Edson. **Os Dez Mandamentos**. Revista Network Computing Brasil, São Paulo: It.midia, ano 2, n. 18, p. 18, Agosto 2000.

17-AMOROSO, E. **Fundamentals of Computer Security Technology**. Prentice Hall, 1994.

18-LUZ, Giovani A., REIS, Gutierres B. **Proposta de Política de Segurança e de Arquiteturas de Firewall para a Universidade de Taubaté**. São Paulo: Departamento de Informática da Universidade de Taubaté – UNITAU. Monografia de Conclusão de Curso, 1999.

19-AURELIO, Marco. **Por que ter uma Política de Segurança da Informação**. Disponível em http://www.malima.com.br/article_read.asp?id=18. Último acesso em 19/06/2010.

20-TIC Empresas 2008. Disponível em http://www.cetic.br/empresas/2008/index.htm/. Último acesso em 01/06/2010.

21-MOREIRA, Nilton S. **Segurança Mínima Uma Visão Corporativa da Segurança de Informações**, Rio de Janeiro: Axcel Books, 2001.

22-SOLECTRON, Case. **Segurança da Informação – Apostila da Apresentação do Projeto de Segurança da Informação**. Sâo José dos Campos: Solectron, 2000.

23-FERREIRA, F. N. F. e ARAUJO, Marcio T. **Política de Segurança da Informação**. 2ª Edição. Rio de Janeiro: Ciência Moderna, 2008.

24-BERNSTEIN, Terry, BHIMANI, Anish B. SCHULTZ, Eugene, SIEGEL, Carol A. **Segurança na Internet**. Rio de Janeiro: Campos, 1997.

25-CALHEIROS, Rosemberg F. **Segurança de Informações: uma questão estratégica**. Rio de Janeiro. Universidade Candido Mendes. Projeto a vez do Mestre. Monografia de Conclusão de Curso, 2004.

26-PEREIRA, Claudio. **Plano de Continuidade de Negócios – Garantindo a Sobrevivência**. Disponível em http://www.modulo.com.br. Último acesso em 31/05/2010.

27-SUCESU – ES. **Segurança de Informações e Governança em Pequenas Empresas**. Disponível em http://www.sucesu.org.br. Brasil. Últmo acesso em 02/06/2010.

28-FONTES, Edson. **Praticando a Segurança da Informação**. Rio de Janeiro: Brasport, 2008.

29-LEMOS, Aline Morais de. **Política de Segurança da Informação**. Rio de Janeiro. Universidade Estácio de Sá. Monografia de Conclusão de Curso, 2001.

30-GIL, Antonio de L. **Segurança em Informática**. 2ª Edição. São Paulo: Atlas, 1998.

31-CALHEIROS, Rosemberg F. **Segurança de Informações nas Empresas. Uma Prioridade Corporativa**. Rio de Janeiro. Escola de Biblioteconomia da Universidade do Rio de Janeiro, Monografia de Conclusão de Curso, UNIRIO, 2002.

32-NBR ISO/IEC 27000 – **Tecnologia da Informação, Código de Prática para Gestão da Segurança da Informação**. Associação Brasileira de Normas

Técnicas. Rio de Janeiro, 2005.

33-REANI, Valéria. **Certificação de Sistemas de Segurança da Informação (SGSI) segundo a norma ISO27001**. Disponível em: http://www.valeriareani.com.br/?p=982. Último acesso em 21/06/2010.

34-FONTES, Edson. **Vivendo a Segurança da Informação – Orientações Práticas para Pessoas e Organizações**. São Paulo: Sicurezza, 2000.

35-GIL, Antionio de L. **Segurança Empresarial e Patrimonial: Segurança dos Negócios, Planos de Contingências, Segurança em informática**. São Paulo: Atlas, 1995.

36-LAUREANO, Marcos Aurélio Pchek. **Gestão da Segurança da Informação**. São Paulo, 2005. Disponível em http://laureano.eti.br/ensino/puc/gst/. Último acesso em 24/05/2010.

37-MARTINS, José C. C. **Gestão de Projetos de Segurança da Informação**. Rio de Janeiro: Brasport, 2003.

38-MODULO. **Security Solutions**. Disponível em http://www.modulo.com.br. Brasil. Último acesso em 15/05/2010.

39-TERRA INFORMÁTICA. **Scam**. Disponível em http://informatica.terra.com.br/virusecia/spam/interna/0,,OI12403,00.html. Último acesso em 17/06/2010.