

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO GRANDE DO
NORTE**

SEGURANÇA DA INFORMAÇÃO: AVALIANDO RISCOS E ESTABELECENDO
DIRETRIZES PARA UMA POLÍTICA DE SEGURANÇA

Felipe Sampaio Dantas da Silva

**SEGURANÇA DA INFORMAÇÃO: AVALIANDO RISCOS E ESTABELECENDO
DIRETRIZES PARA UMA POLÍTICA DE SEGURANÇA**

bacharelado em Engenharia de Informática da
Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte
como requisito para obtenção do título de Bacharel em Engenharia de
Informática.

Orientador:

Alagim Ferreira da Rocha Neto, M.Sc.

NATAL/RN

**NATAL/RN
2007**

FELIPE SAMPAIO DANTAS DA SILVA

SEGURANÇA DA INFORMAÇÃO: AVALIANDO RISCOS E ESTABELECENDO DIRETRIZES PARA UMA POLÍTICA DE SEGURANÇA

SEGURANÇA DA INFORMAÇÃO: AVALIANDO RISCOS E ESTABELECENDO DIRETRIZES PARA UMA POLÍTICA DE SEGURANÇA

Monografia apresentada ao curso de Bacharelado em Sistemas de Informação da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte como requisito obrigatório para a obtenção do título de Bacharel em Sistemas de Informação.

Orientador:

Aluizio Ferreira da Rocha Neto, M.Sc.

NATAL/RN

- 2007

RB. 31.464 M
004.7
558M
2007
0x 01

FARN BIBLIOTECA Nº Reg. <u>M000965</u> <u>17.09.08</u>

Catálogo na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Silva, Felipe Sampaio Dantas da

Segurança da informação: avaliando riscos e estabelecendo diretrizes para uma política de segurança / Felipe Sampaio Dantas da Silva. – Natal: FARN, 2007.
34f.

Orientador: Aluizio Ferreira da Rocha Neto (M. Sc.)
Monografia (Bacharelado em Sistemas de Informação) – Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Segurança da Informação – Monografia. 2. tecnologia da Informação – Riscos – Monografia. 3. Informação – Política de Segurança – Monografia.
I. Título.

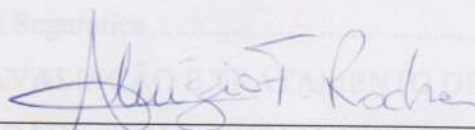
RN/FARN/BC

CDU 004.7

FELIPE SAMPAIO DANTAS DA SILVA

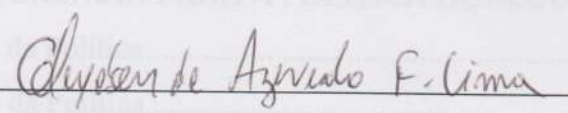
SEGURANÇA DA INFORMAÇÃO: AVALIANDO RISCOS E ESTABELECENDO
DIRETRIZES PARA UMA POLÍTICA DE SEGURANÇA

Monografia apresentada ao curso de Bacharelado em Sistemas de Informação da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte e aprovada em 12 de dezembro de 2007, pela banca examinadora composta pelos seguintes membros:

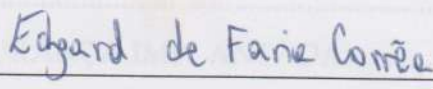


Aluizio Ferreira da Rocha Neto, M.Sc.

Orientador



Gleydson de Azevedo Ferreira Lima, M.Sc.



Edgard de Faria Corrêa, Dr.

SUMÁRIO

1	INTRODUÇÃO	8
1.1	PROBLEMA DE PESQUISA	9
1.2	OBJETIVOS	9
1.2.1	OBJETIVOS GERAIS	9
1.2.2	OBJETIVOS ESPECÍFICOS	9
1.3	JUSTIFICATIVA	10
2	REFERENCIAL TEÓRICO	11
2.1	SOCIEDADE DA INFORMAÇÃO	11
2.2	INFORMAÇÃO: ATIVO ESSENCIAL AOS NEGÓCIOS	12
2.3	SEGURANÇA DA INFORMAÇÃO	13
2.3.1	Aspectos associados à segurança da informação	15
2.3.2	Ameaças	15
2.3.3	Vulnerabilidades	16
2.3.4	Riscos à Segurança	16
2.4	ANÁLISE, AVALIAÇÃO E TRATAMENTO DE RISCOS	17
2.5	CONFORMIDADE COM A NORMA NBR ISO/IEC 17799	19
2.6	POLÍTICA DE SEGURANÇA	21
3	ESTABELECENDO DIRETRIZES PARA A POLÍTICA DE SEGURANÇA	22
3.1	GUIA DE REFERÊNCIA PARA A POLÍTICA DE SEGURANÇA	23
3.1.1	Propósito da Política	24
3.1.2	Conteúdo da Política	24
3.1.3	Implementação da Política	25
3.1.4	Atendendo às especificações	25
4	ESTUDO DE CASO	27
4.1	POLÍTICA DE SEGURANÇA IMPLANTADA	29
4.1.1	Introdução	29
4.1.2	Estações de Trabalho	29
4.1.3	Ambiente Físico	29
4.1.4	Sistema Operacional	30
4.1.5	Credenciais do Usuário	30
4.1.6	Utilização de Softwares	30

4.1.7	Restrições nas Estações de Trabalho	31
4.1.8	Utilização da Internet.....	31
4.1.9	Auditoria.....	32
5	CONCLUSÃO.....	33

Palavras-Chave: Segurança da Informação, Avaliação de Riscos, Política de Segurança.

RESUMO

Ao longo do tempo a informação constitui-se como sólida ferramenta para gestão e apoio à tomada de decisão aos negócios de forma que se tornar dependente dela passou a ser inevitável. Tendo em vista esta representação, alguns mecanismos tiveram que ser estabelecidos e adotados para manter sua integridade, confiabilidade e disponibilidade, assim como avaliar os riscos que porventura possam levar a perda de algum dos princípios básicos que a protegem, seja extinguindo ou os tornando aceitáveis. Desta forma, para que se consiga atingir todos os objetivos propostos e necessários à organização, é necessário que sejam estabelecidas diretrizes a serem adotadas durante o processo de elaboração da Política de Segurança, conjunto de orientações destinadas a regulamentar o gerenciamento das informações e recursos que a manipulam.

Palavras-Chave: Segurança da Informação, Avaliação de Riscos, Política de Segurança.

ABSTRACT

Over time, the information becomes as solid tool for management and support to decision-making for business, so becomes it dependent is inevitable. In view of this fact, some mechanisms had to be established and adopted to maintain its integrity, confidentiality and availability, as analyze the risks that perhaps could lead the loss of some basic principle that protects, eliminating or making acceptable. In order, to successfully achieve all the organization purpose, it's need to be established guidelines to be followed during the process of security policy development, set of rules intended to regulate the management of the information and resources that handle it.

Keywords: Information Security, Risk Assessment, Security Policy.

1 INTRODUÇÃO

A muito, as empresas têm sido influenciadas por mudanças e novidades que, a todo momento, surgem no mercado e provocam alterações de contexto. A todo instante surgem novas descobertas, experimentos e inovações que impulsionadas por seus mentores, sejam eles estudiosos, pesquisadores ou executivos, sempre em busca de novos conceitos, revelam novas tendências promissoras.

Buscando em diversas fases da história como a Revolução Elétrica e Industrial, abertura de mercado e o aumento da competitividade proporcionado por empresas multinacionais, passando pelos momentos relacionados à reengenharia, à terceirização e, mais recentemente, os efeitos da Tecnologia da Informação aplicada aos negócios, é possível identificar que a informação sempre esteve presente, cumprindo importante papel para a gestão dos negócios, objetivando melhor produtividade, redução de custos, aumento de agilidade, competitividade e apoio à tomada de decisão.

Com o passar dos anos, a forma como as empresas usavam a informação e geriam os negócios sofreram bruscas mudanças: Décadas atrás, quando a tecnologia da informação superava pouco mais que esboços, a informação era tratada de forma centralizada e pouco automatizada, o que podia ser justificado pelas limitações de armazenamento e preços restritos dos primeiros computadores *mainframes*.

À medida que a indústria da alta tecnologia se desenvolvia, os computadores se tornavam mais acessíveis, possibilitando às empresas a substituição dos velhos arquivos de ferro por Centrais de Processamento de Dados, que permitiam consultas remotas, símbolo de moderna gestão, além da agilidade nas operações.

Após a popularização das redes de computadores, que digitalizaram as informações e automatizaram os processos, as empresas passaram a ter altos níveis de conectividade e compartilhamento até que os antigos *mainframes* começaram a ser substituídos por computadores pessoais, que tomaram conta dos ambientes corporativos, quebrando o paradigma de acesso local às informações, chegando a qualquer lugar do mundo através de equipamentos portáteis e pela rede mundial de computadores: a Internet.

Logo surgem expressões e aplicações comerciais que se utilizam da moderna infraestrutura de rede e computacional como os sistemas integrados de gestão ERP – *Enterprise Resource Planning*, onde elementos da cadeia produtiva como fornecedores, parceiros e

clientes passam a interagir também eletronicamente, integrando e compartilhando as bases de conhecimento.

É nesse momento que se percebe o alto grau de dependência que as empresas têm da informação, muito mais digitalizada, compartilhada e distribuída, além, conseqüentemente, de todos os elementos da infra-estrutura que a mantém.

Se antes existia um maior controle e segurança a informação por estar mais centralizada, o cenário atual ilustra condições onde o risco foi elevado a níveis nunca vividos, exigindo das empresas mecanismos de controle que permitam reduzi-lo e torná-lo administrável e viável.

Este projeto aborda as melhores práticas para o gerenciamento da segurança da informação em redes de computadores, evidenciando desde seus princípios básicos à aplicação de uma política de segurança, a partir da avaliação de riscos.

1.1 PROBLEMA DE PESQUISA

Com o vertiginoso crescimento da troca de informações através das redes de computadores, e o aumento expressivo da dependência da informação, este ativo tornou-se fator crítico para o sucesso de uma organização e, devido à ausência do conhecimento de práticas para identificação e avaliação de riscos, a segurança da informação passa a ser tratada apenas como mecanismos tecnológicos de proteção.

1.2 OBJETIVOS

1.2.1 OBJETIVOS GERAIS

O foco principal estará voltado às melhores práticas para o gerenciamento da Segurança da Informação em redes de computadores, desmistificando, principalmente, a segurança resumida apenas a aparatos tecnológicos como Firewalls, Sistemas de Detecção de Intrusos ou Antivírus.

1.2.2 OBJETIVOS ESPECÍFICOS

- Assimilar a importância da informação aos negócios;
- Compreender os princípios básicos da segurança da informação;
- Entender os aspectos associados à segurança da informação;

- Compreender a importância da análise de riscos para o gerenciamento da segurança da informação;
- Estabelecer diretrizes básicas para o desenvolvimento de uma política de segurança da informação com base em dados obtidos após um levantamento de análise de riscos;

1.3 JUSTIFICATIVA

A necessidade do desenvolvimento deste projeto surgiu da importância da informação para os negócios, de forma que a comunicação entre clientes e fornecedores sempre seja disponibilizada de forma íntegra e confiável. Para isto, além do entendimento dos princípios e aspectos associados à segurança da informação, é preciso o conhecimento dos meios utilizados para o gerenciamento das operações envolvidas.

2 REFERENCIAL TEÓRICO

2.1 SOCIEDADE DA INFORMAÇÃO

Sociedade da Informação, Sociedade do Conhecimento ou até mesmo Nova Economia é um termo que surgiu no fim do Século XX, originado da expressão Globalização. Este termo é designado a sociedades que se encontram em processo de formação e expansão.

No Brasil e no mundo, a Sociedade da Informação é uma nova Era, onde as transmissões de dados são de baixo custo e as tecnologias de armazenamento são amplamente utilizadas, onde a informação flui a velocidades e em quantidades, antes inimagináveis, assumindo valores políticos, religiosos, sociais, antropológicos, econômicos, fundamentais, etc.

Durante todas as etapas do desenvolvimento corporativo, é fato que as transações de toda a cadeia de produção sempre tiveram na informação uma base fundamental de relacionamento e coexistência, seja para manipulação de segredos estratégicos ou simplesmente pesquisas. Incorporada à crescente complexidade do mercado, à forte concorrência e a velocidade imposta pela modernização das relações corporativas, a informação elevou seu posto na pirâmide estratégica do executivo, tornando-se fator vital para seu sucesso ou fracasso.

Aliada a tecnologia, por meio de instrumentos e soluções sofisticadas (descentralização de informações para compartilhamento em redes, acesso rápido, atualização constante de base de dados, etc.), preparadas para atender a qualquer demanda do mercado, se transformou na principal mola propulsora desta nova fase da informação dentro das corporações, sob o nome já clássico de Tecnologia da Informação (TI).

Neste âmbito, a informação se transformou na principal moeda corrente do mundo corporativo, das transações de automação bancária ao mercado financeiro, do controle de estoque ao comércio eletrônico.

No entanto, da mesma forma que esta mudança de paradigma apresenta constantes oportunidades, com espaço para se criar e ousar sobre os caminhos, acaba também por se tornar um ambiente muitas vezes hostilizado, altamente visado por ações ilícitas e invariavelmente desprovido de instrumentos para combater e lidar com estas ocorrências.

2.2 INFORMAÇÃO: ATIVO ESSENCIAL AOS NEGÓCIOS

Segundo o dicionário Aurélio (1999), informação é o conjunto de dados acerca de alguém ou de algo. Estendendo esse conceito, é possível dizer que a informação é a interpretação desses dados. De nada vale um conjunto de dados sem que se faça a interpretação dos mesmos para se extrair um conhecimento útil.

É denominado ativo todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada. (SÊMOLA, 2003)

O termo ativo possui esta denominação, oriunda da área financeira, por ser considerado um elemento de valor para um indivíduo ou organização, e que, por esse motivo, necessita de proteção adequada. (SÊMOLA, 2003)

As organizações necessitam da informação para tomar decisões objetivando seus fins (o sucesso). Isto mostra o quão poderosa é a informação. Sem ela não há estratégias, não há mudanças ou até mesmo não existiria a empresa. Uma consequência natural da importância da informação é a extrema vulnerabilidade a que a empresa se expõe caso haja perda de dados vitais, como plantas de projetos, planilhas de custos, documentos contábeis, financeiros, etc. Quanto maior for a organização maior será sua dependência da informação.

A informação pode estar armazenada de várias formas: impressa em papel, em meios digitais (discos, fitas, CDs, DVDs, disquetes), na mente das pessoas, em imagens armazenadas em fotografias e filmes.
(ACADEMIA LATINO-AMERICANA DE SEGURANÇA DA INFORMAÇÃO, 2006, p. 09).

Considerando a informação como um ativo, cada vez mais valorizado e importante aos negócios, é necessário levar em consideração todos os aspectos ligados à segurança, as propriedades que devem ser preservadas e protegidas para que a informação esteja efetivamente sob controle, e, principalmente, os momentos que fazem parte do seu ciclo de vida.

Toda informação é influenciada por três propriedades principais: Confidencialidade, Integridade e Disponibilidade, além dos aspectos Autenticidade e Legalidade que complementam esta influência.

O ciclo de vida, por sua vez, é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Os momentos são vivenciados justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, por sua vez, mantém a operação da empresa.
(SÊMOLA, 2003, p. 09)

Independentemente da forma como a informação é representada – seja por átomos ou por bits, todos os momentos se aplicam (SÊMOLA, 2003):

- **Manuseio:** momento em que a informação é criada e manipulada, seja ao folhear um maço de papéis, ao digitar informações recém-geradas em uma aplicação Internet, ou, ainda, ao utilizar sua senha de acesso para autenticação, por exemplo;
- **Armazenamento:** momento em que a informação é armazenada, seja em um banco de dados compartilhado, em uma anotação de papel posteriormente postada em um arquivo de ferro, ou, ainda, em uma mídia de disquete depositada na gaveta de uma mesa de trabalho, por exemplo;
- **Transporte:** momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico (e-mail), ao postar um documento via aparelho de fax, ou ainda, ao falar ao telefone uma informação confidencial, por exemplo;
- **Descarte:** momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em seu computador de mesa, ou ainda, ao descartar um CD-ROM usado que apresentou falha na leitura;

É importante que durante o ciclo de vida da informação sejam mantidos os princípios básicos de segurança da informação, de forma a garantir sua Confidencialidade, Integridade e Disponibilidade.

2.3 SEGURANÇA DA INFORMAÇÃO

Segurança da informação é a área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. (SÊMOLA, 2003).

A segurança da informação é obtida através da implantação de controles adequados, políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

(ACADEMIA LATINO-AMERICANA DE SEGURANÇA DA INFORMAÇÃO, 2006).

A segurança da informação tem como objetivo a preservação de três princípios básicos pelos quais se norteiam a implementação desta prática.

Confidencialidade – 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.

Integridade – Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.

Disponibilidade – Toda 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)

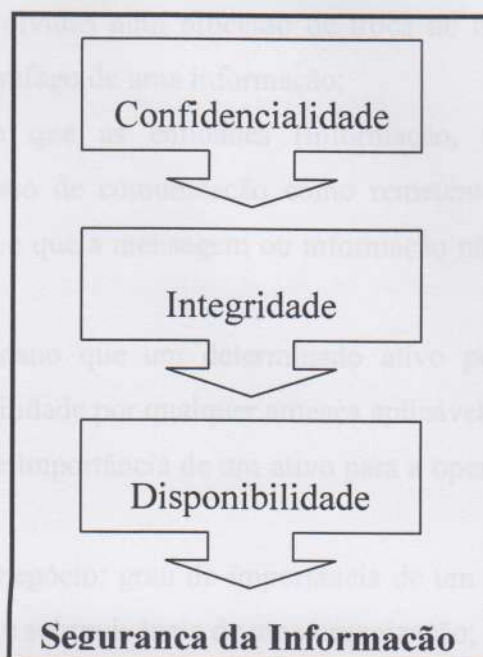


Figura 1: Princípios Básicos da Segurança da Informação

Fonte: Dados da Pesquisa (2007)

Além dos princípios básicos, alguns elementos são considerados essenciais na prática da segurança da informação, dependendo do objetivo que se pretende alcançar.

Autenticação – Processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica que permite o acesso à informação e seus ativos por meio de controles de identificação desses elementos.

Legalidade – Característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.

(SÊMOLA, 2003, p. 46)

2.3.1 Aspectos associados à segurança da informação

- **Autorização:** concessão de uma permissão para o acesso às informações e funcionalidades das aplicações aos participantes de um processo de troca de informações (usuário ou máquinas), após a correta identificação e autenticação dos mesmos;
- **Auditoria:** processo de coleta de evidências de uso dos recursos existentes, a fim de identificar as entidades envolvidas num processo de troca de informações, ou seja, origem, destino e meios de tráfego de uma informação;
- **Autenticidade:** garantia de que as entidades (informação, máquinas, usuários) identificadas em um processo de comunicação como remetentes ou autores sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação;
- **Severidade:** gravidade do dano que um determinado ativo pode sofrer devido à exploração de uma vulnerabilidade por qualquer ameaça aplicável;
- **Relevância do ativo:** grau de importância de um ativo para a operacionalização de um processo de negócio;
- **Relevância do processo de negócio:** grau de importância de um processo de negócio para o alcance dos objetivos e sobrevivência de uma organização;
- **Criticidade:** gravidade referente ao impacto ao negócio causado pela ausência de um ativo, pela perda ou redução de suas funcionalidades em um processo de negócio, ou pelo seu uso indevido e não autorizado;
- **Irretratabilidade:** característica de informações que possuem uma identificação do seu emissor que o autentica como o autor de informações por ele enviadas e recebidas. Sinônimo de não-repúdio; (SÊMOLA, 2003).

2.3.2 Ameaças

As ameaças à segurança da informação são relacionadas diretamente a perda de uma de suas três características principais.

Ameaças são as condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade e, consequentemente, causando impactos aos negócios de uma organização. (SÊMOLA, 2003, p. 47)

Levando em consideração sua intencionalidade, as ameaças podem ser divididas em:

- Naturais: ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, etc.;
- Involuntárias: ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia, etc.
- Voluntárias: ameaças propositais causadas por agentes humanos como *hackers*, invasores, espiões, etc.; (SÊMOLA, 2003).

2.3.3 Vulnerabilidades

Fragilidade ou limitação de um ativo que pode ser explorada por uma ou mais ameaças.

(ACADEMIA LATINO-AMERICANA DE SEGURANÇA DA INFORMAÇÃO, 2006).

2.3.4 Riscos à Segurança

Segundo Sêmola (2003) risco é a probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios.

Perda de Confidencialidade: ocorre quando existe uma quebra de sigilo de uma informação específica, ou seja, informação deixa de ser confidencial a um determinado grupo, e passa a ser acessível a outro(s) usuário(s).

Perda de Integridade: ocorre quando uma informação perde sua forma original. Pessoa não autorizada e de posse de determinada informação, efetua alterações sem aprovação e sem o controle do proprietário (corporativo ou privado) da informação.

Perda de Disponibilidade: ocorre quando informação não está mais disponível a entidade que necessita dela. Na maioria das vezes acontece a perda de comunicação com um sistema importante para a empresa, como a queda de um servidor de uma aplicação crítica de negócio. (SILVA, 2007)



Figura 2: Exemplo de Risco à Segurança - Vulnerabilidade x Ameaças
 Fonte: Academia Latino-Americana de Segurança da Informação (2006)

2.4 ANÁLISE, AVALIAÇÃO E TRATAMENTO DE RISCOS

Gerenciar segurança da informação inclui a análise, avaliação de riscos e como reduzi-los a um nível aceitável. É necessário levar em conta os objetivos da organização, bem como as necessidades específicas de cada sistema e seus riscos. Portanto, avaliar riscos, passa pela avaliação de ameaças e vulnerabilidades (ACADEMIA LATINO-AMERICANA DE SEGURANÇA DA INFORMAÇÃO, 2006).

A avaliação de riscos e ameaças não resulta em uma seleção de mecanismos de prevenção, detecção e resposta para redução de riscos. Ao contrário ela simplesmente indica as áreas onde esses mecanismos devem ser aplicados, e a prioridade que deve ser designada para o desenvolvimento de tais mecanismos. No contexto de gerenciamento de riscos, a avaliação de riscos e ameaças irá recomendar como minimizar, prevenir e aceitar os riscos.

Como os riscos e ameaças podem mudar com o passar dos tempos, é importante que a organização periodicamente reavalie os mesmos e reconsidere as políticas e controles selecionados.
 (ACADEMIA LATINO AMERICANA DE SEGURANÇA DA INFORMAÇÃO, 2006, p. 52)

Há uma quebra de paradigma ao compreender que os riscos de uma empresa não estão apenas associados ao volume de falhas tecnológicas, à qualificação de ameaças que poderiam explorá-las ou, ainda, aos impactos potenciais. A análise de riscos tem de ser encarada como um instrumento fundamental para diagnosticar a situação atual de segurança da empresa, através da sinergia entre o entendimento dos desafios do negócio, o mapeamento das funcionalidades dos processos de negócio e o relacionamento deles com a diversidade de ativos físicos, tecnológicos e humanos que hospedam falhas de segurança. (SÊMOLA, 2003)

Segundo Sêmola (2003), a vulnerabilidade por si só não causa qualquer dano ao ativo, sendo apenas uma situação de fragilidade. O dano só se efetivará mediante a exploração da vulnerabilidade por parte de uma ameaça.

São considerados aspectos em uma análise de riscos:

- Relação de relevância que um processo de negócio tem para o negócio;
- Relação de dependência que um ou mais processos de negócio tem do ativo;
- Projeção do impacto resultante da concretização da ação de uma ameaça;
- Probabilidade da ameaça explorar uma vulnerabilidade;
- Severidade potencial da exploração no ativo;
- Qualificação das vulnerabilidades presentes nos ativos;
- Qualificação das ameaças potenciais;

Por se tratar de uma análise que contempla ativos físicos, tecnológicos e humanos, a fase de identificação de ameaças e vulnerabilidades deve ser orientada por entrevistas com gestores e usuários, observação comportamental dos recursos humanos, inspeção física presencial nos ambientes, estudo de documentos e análises técnicas dos ativos tecnológicos, a fim de coletar evidências da presença de falhas. A justificativa para ações presenciais, entrevistas, análises físicas e, até mesmo, parte das análises técnicas se dá pela impossibilidade natural de coletar todas as evidências através de dispositivos automatizados ou informatizados.

Calculada a probabilidade e severidade de uma ameaça explorar cada uma das vulnerabilidades encontradas em cada ativo, obtém-se o nível de risco final de cada ativo. De posse desses resultados parciais, é possível projetar o nível de risco de cada processo de negócio, considerando os riscos de cada ativo que o sustenta. A partir disso, se pode estimar o risco do negócio como um todo, calculando de forma ponderada os riscos de cada um dos processos de negócio que o suporta.

O resultado obtido permite organizar as prioridades e dimensionar um plano de ação de curto, médio e longo prazo, baseando-se na distribuição dos processos de negócio e/ou ativos. Desta forma, tem-se a orientação necessária para apoiar as decisões e modelar contramedidas específicas para cada perímetro da empresa, como eliminar, reduzir, transferir ou aceitar o risco. Em qualquer uma dessas situações, limitações orçamentárias, dificuldades técnicas ou fatores externos tendem a impedir a implementação total das contramedidas especificadas, levando qualquer empresa a buscar o nível de risco controlado e de acordo com a natureza de seu negócio, através de um posicionamento consciente.

Segurança é administrar riscos. Toda empresa possui características próprias, objetivos e planos específicos; por isso, precisa encontrar o nível de risco mais adequado para operar. Dentro desse panorama a análise de riscos é o instrumento perfeito para dimensionar a situação de segurança atual, tornando-a consciente dos riscos e orientando-a a buscar soluções que a conduzam para o patamar de risco aceitável. Contudo, pelo dinamismo das mudanças sofridas pelo ambiente corporativo, devido a fatores ambientais, mercadológicos, estratégicos, econômicos, tecnológicos, estruturais etc., a análise de riscos deve fazer parte de um processo contínuo de gestão, capaz de diagnosticar novas vulnerabilidades e ameaças, garantindo, assim, a manutenção no nível de risco controlado. (SÊMOLA, 2003, p. 113)

Tem-se delineado como tendência, a realização de análises de riscos baseadas na medição de presença e ausência de controles de segurança, e não somente nas vulnerabilidades presentes nos ativos como eixo principal. Este movimento já é um reflexo da credibilidade adquirida pela norma de gestão de segurança da informação ISO17799. Sua proposta se baseia no interesse e necessidade principal dos gestores de segurança em proteger o ativo, sem, no entanto, ter que se preocupar em eliminar ou administrar cada uma das vulnerabilidades individualmente. Assim, em vez de ter que mapear e buscar soluções individuais para cada uma das centenas de vulnerabilidades de um sistema operacional, por exemplo, a preocupação se concentra na verificação da presença ou ausência de aplicação do *patch*, ou programa de correção, disponibilizado pelo fabricante. Desta forma, tem-se ganho de desempenho, eficiência na obtenção dos resultados e, principalmente, aproxima a empresa dos controles recomendados pela ISO. (SÊMOLA, 2003).

2.5 CONFORMIDADE COM A NORMA NBR ISO/IEC 17799

Com o crescimento exponencial dos sistemas de informações e atividades colaborativas através das redes de computadores, é cada vez mais crucial manter essas informações mais seguras e suas fontes confiáveis. Entretanto, para que essas fontes tenham seu armazenamento e transmissão realizada de forma segura, é preciso que sejam estabelecidos controles que garantam a qualidade e integridade da informação.

De forma que cada instituição trabalha de uma maneira diferente, assim como, assume valores e prioridades distintos entre os níveis de segurança para sua informação, isso aliada à carência de metodologia e controles que atendam as necessidades, foram criadas normas que proporcionassem as organizações os controles devidos para a segurança de sua informação.

Com isso a International Organization for Standardization (ISO), que tem como objetivo a criação de normas e padrões universalmente aceitos, criou a Norma ISO 17799

(atualmente renomeada para ISO 27002), sendo no Brasil controlada pela Associação Brasileira de Norma Técnicas (ABNT), como NBR ISO/IEC 17799, que tem como nome Tecnologia da Informação – Código de prática para a gestão da segurança da informação, proporcionando para as organizações os controles necessários para a segurança da informação.

A norma ABNT NBR ISO/IEC 17799 estabelece diretrizes e princípios para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. (ACADEMIA LATINO AMERICANA DE SEGURANÇA DA INFORMAÇÃO, 2006)

A NBR ISO/IEC 17799 tem como objetivo estabelecer um referencial para que as organizações desenvolvam, implementem e avaliem a gestão da segurança da informação.

Em sua documentação a ABNT NBR ISO/IEC 17799 aborda 11 tópicos principais (ASCIUTTI, 2007):

- Política de Segurança: descreve a importância e relaciona os principais assuntos que devem ser abordados numa política de segurança;
- Segurança Organizacional: aborda a estrutura de uma gerência para a segurança de informação, assim como aborda o estabelecimento de responsabilidades incluindo terceiros e fornecedores de serviços;
- Classificação e controle de ativos de informação: trabalha a classificação, o registro e o controle dos ativos da organização;
- Segurança em pessoas: tem como foco o risco decorrente de atos intencionais ou acidentais feito por pessoas. Também é abordada a inclusão de responsabilidades relativas à segurança na descrição dos cargos, a forma de contratação e o treinamento em assuntos relacionados à segurança;
- Segurança ambiental e física: aborda a necessidade de se definir áreas de circulação restrita e a necessidade de proteger equipamentos e infra-estrutura de tecnologia de informação;
- Gerenciamento das operações de comunicações: aborda as principais áreas que devem ser de especial atenção da segurança. Dentre estas áreas destacam-se as questões relativas a procedimentos operacionais e respectivas responsabilidades, homologação e implantação de sistemas, gerência de redes, controle e prevenção de vírus, controle de mudanças, execução e guarda de backup, controle de documentação, segurança de correio eletrônico, entre outras;
- Controle de acesso: aborda o controle de acesso a sistemas, a definição de

competências, o sistema de monitoração de acesso e uso, a utilização de senhas, dentre outros assuntos;

- Desenvolvimento e manutenção de sistemas: são abordados os requisitos de segurança dos sistemas, controles de criptografia, controle de arquivos e segurança do desenvolvimento e suporte de sistemas;
- Gestão de incidentes de segurança: incluída na versão 2005, apresenta dois itens: Notificação de fragilidades e eventos de segurança da informação e gestão de incidentes de segurança da informação e melhorias;
- Gestão da continuidade do negócio: reforça a necessidade de se ter um plano de continuidade e contingência desenvolvido, implementado, testado e atualizado;
- Conformidade: aborda a necessidade de observar os requisitos legais, tais como a propriedade intelectual e a proteção das informações de clientes;

2.6 POLÍTICA DE SEGURANÇA

Os dois itens mais importantes na hora de manter as informações da empresa em segurança são: a elaboração de políticas de segurança e o gerenciamento de suporte adequados, seguido do nível de conscientização dos funcionários. Este é o resultado de um estudo conduzido pela ONG educacional especializada em certificar profissionais de segurança. (MÓDULO SECURITY NEWS, 2006).

Com o propósito de fornecer orientação e apoio às ações de gestão de segurança, a política tem um papel fundamental e, guardadas as devidas proporções, tem importância similar à constituição federal para um país (SÊMOLA, 2003).

A Política de Segurança é o mecanismo que vai dar subsídios ao administrador para que ele possa avaliar os possíveis riscos envolvidos no processo, dentre eles:

- Serviços oferecidos aos usuários: cada serviço apresenta seu próprio risco, por isso, o administrador deve avaliar sua necessidade. Serviços que não forem utilizados não devem ser instalados;
- Facilidade de uso: sistemas mais fáceis de usar dão ao usuário acesso total e irrestrito às informações. No mínimo, seria necessário exigir de cada usuário uma senha. Em geral, comodidade costuma ser inversamente proporcional a segurança;
- Perda de informações: perda de dados, violação de privacidade e perda de serviços;

3 ESTABELECENDO DIRETRIZES PARA A POLÍTICA DE SEGURANÇA

Considerando que a política de segurança é a expressão formal das regras pelas quais é fornecido o acesso aos recursos tecnológicos da empresa e que seu principal propósito é informar aos usuários, equipe e gerentes, as suas obrigações para a proteção da tecnologia e do acesso à informação, a política deve especificar os mecanismos através dos quais estes requisitos podem ser alcançados.

Por ser responsável pelo estabelecimento de padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a empresa, a política deve ser personalizada (SÊMOLA, 2003).

Conforme SÊMOLA (2003), as diretrizes, que por si só, têm papel estratégico, precisam expressar a importância que a empresa dá para a informação, além de comunicar aos funcionários seus valores e seu comprometimento em incrementar a segurança à sua cultura organizacional. Também é notória a necessidade do envolvimento da alta direção, refletida pelo caráter oficial com que a política é comunicada e compartilhada junto aos funcionários. Este instrumento deve expressar as preocupações dos executivos e definir as linhas de ação que orientarão as atividades táticas e operacionais.

Convém-se que uma boa política de segurança da informação obedeça aos seguintes princípios:

- Seja implementável através de procedimentos de administração, publicação de regras de uso aceitáveis, ou outros métodos apropriados;
- Seja exigida como ferramenta de segurança, onde apropriado, e com sanções onde a prevenção efetiva não seja tecnicamente possível;
- Defina claramente as áreas de responsabilidades para os usuários, administradores e gerentes;

Outro propósito é oferecer um ponto de referência a partir do qual se possa adquirir, configurar e auditar sistemas computacionais e redes, para que sejam adequados aos requisitos propostos. Portanto, uma tentativa de utilizar um conjunto de ferramentas de segurança na ausência de pelo menos uma política de segurança implícita não faz sentido.

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 que ela tenha o impacto desejado.

Os componentes de uma boa política de segurança devem incluir normas que detalhem situações, ambientes, processos específicos e forneçam orientação para o uso adequado das informações. Procedimentos e instruções também deverão estar presentes na política, onde é necessário descrever meticulosamente cada ação e atividade associada a cada situação distinta de uso das informações. A natureza detalhista destes componentes pressupõe ainda mais a necessidade de manutenção freqüente (SÊMOLA, 2003).

Diante disso, já se é possível perceber o quão complexo é desenvolver e, principalmente, manter atualizada a política de segurança da informação com todos os seus componentes. Esta percepção torna-se ainda mais latente ao ser considerado o dinamismo do parque tecnológico de uma empresa e, ainda, as mudanças previsíveis e imprevisíveis que o negócio pode sofrer.

Segundo SÊMOLA (2003), a conformidade com requisitos legais, envolvendo obrigações contratuais, direitos de propriedade intelectual, direitos autorais de software e todas as possíveis regulamentações que incidam no negócio da empresa devem ser respeitados e, portanto, deve ser a linha de conduta da construção da política de segurança.

3.1 GUIA DE REFERÊNCIA PARA A POLÍTICA DE SEGURANÇA

Conforme Geus & Nakamura (2003), algumas orientações devem ser seguidas para a elaboração de uma boa Política de Segurança, são elas:

- A política deve representar o pensamento da organização e ter o apoio de todos;
- Nesse documento não devem conter definições técnicas, assim como não deve ser um manual de implementações, pelo contrário, deve ser simples o bastante para que todos possam entender e utilizar;
- A responsabilidade de cada membro envolvido, inclusive a do gestor da política, deve ser definida;
- Adoção de medidas disciplinares caso ocorra o descumprimento da política;
- Avaliação dos custos para implementação de tal política;
- Avaliação de serviços que são estritamente necessários. Aquilo que não for expressamente permitido será proibido;

Outro ponto a se levar em consideração é sobre os aspectos humanos. Todo investimento em segurança pode se perder se o usuário não estiver preparado para seguir as normas da política. É importante que todo usuário seja conscientizado da importância da

segurança através de um treinamento, o que minimizaria as chances de falhas no processo e também possíveis ataques que usam a engenharia social.

Como forma de regulamentar os deveres e obrigações dos usuários, a Política de Uso pode ser utilizada.

Tal política é um documento definido pela política de segurança, a qual deve definir as áreas de responsabilidade para usuários e administradores do sistema, bem como as sanções que serão impostas caso as regras de uso sejam violadas. A política de uso será assinada pelo usuário, assim ele estará manifestando sua concordância com as regras impostas.

Durante um processo de adoção de uma política de segurança devem ser levados em consideração:

3.1.1 Propósito da Política

- Deve apoiar sempre os objetivos da organização e nunca se apoiar em ferramentas e plataformas;
- Deve descrever o programa geral de segurança da rede;
- Deve demonstrar os resultados de sua determinação de risco, com as ameaças que está combatendo e as proteções propostas;
- Deve definir responsabilidades para implementação e manutenção de cada proteção;
- Deve definir normas e padrões comportamentais para usuários, para que o documento seja utilizado como prova, caso haja alguma violação;

3.1.2 Conteúdo da Política

- Deve relacionar os recursos que se quer proteger e que software são permitidos em quais locais;
- Deve relatar o que acontece quando programas e dados não homologados são detectados no ambiente operacional;
- Deve relacionar quem desenvolveu as orientações, que as aprovou, quem detém privilégios e quem determina autorizações e quem é afetado pelas orientações;
- Deve descrever procedimentos para fornecimento e revogação de privilégios;
- Deve determinar gerência e responsabilidades dos envolvidos no controle e manuseio do ambiente operacional;
- Deve trazer explicações da importância da adoção dos procedimentos de segurança, justificando-os junto aos usuários para que o entendimento dos mesmos leve ao comprometimento com todas as ações de segurança;

3.1.3 Implementação da Política

Nenhuma política deve ser implementada até que os usuários sejam treinados nas habilidades necessárias para segui-la. As boas políticas de segurança dependem do conhecimento e cooperação dos usuários. Isto é particularmente relevante para segurança contra vírus e *malwares* e políticas sobre gerência de senhas.

Segurança requer mais conhecimento. Todo usuário deve saber como agir quando estiver diante de uma violação ou possível violação, assim como, saber quem chamar se tiver perguntas ou suspeitas, e deve saber o que fazer e o que não fazer para minimizar riscos de segurança.

Estes usuários devem ser incentivados a sentir que as medidas de segurança são criadas para seu próprio benefício.

3.1.4 Atendendo às especificações

Nesta seção serão apresentadas as especificações básicas que guiam a implantação de uma política de segurança em uma empresa qualquer:

- Guias para a compra de tecnologia computacional que especifiquem os requisitos ou características que os produtos devem possuir;
- Um mecanismo de privacidade que defina expectativas razoáveis de privacidade relacionadas a aspectos como a monitoração de correio eletrônico, logs de atividades, e acesso aos arquivos dos usuários;
- Um mecanismo de acesso que define os direitos e os privilégios para proteger a organização de danos, através da especificação de linhas de conduta dos usuários, pessoal e gerentes. Ela deve oferecer linhas de condutas para conexões externas, comunicação de dados, conexão de dispositivos a uma rede, adição de novos softwares, etc. Também deve especificar quaisquer mensagens de notificação requeridas;
- Um mecanismo que defina as responsabilidades dos usuários. Deve especificar a capacidade de auditoria e oferecer a conduta no caso de incidentes;
- Uma forma de autenticação que estabeleça confiança através de uma política de senhas efetiva, e através da linha de conduta para autenticação de acessos remotos e o uso de dispositivos de autenticação;
- Um documento de disponibilidade que define as expectativas dos usuários para a disponibilidade de recursos. Ele deve endereçar aspectos como redundância e

recuperação, bem como especificar horários de operação e de manutenção. Também deve incluir informações de contato para relatar falha de sistema e de rede;

- Um sistema de tecnologia de informação e política de manutenção de rede que descreva como, tanto o pessoal de manutenção interno como externo devem manipular e acessar a tecnologia. Deve ser tratado como a manutenção remota é permitida e como tal acesso é controlado. Outra área para considerar é a terceirização e como ele é gerenciada;
- Uma política de relatório de violações que indique quais os tipos de violações devem ser relatadas e a quem estes relatos devem ser feitos;
- Suporte que ofereça aos usuários informações de contato para cada tipo de violação;
- Linha de conduta sobre como gerenciar consultas externas sobre um incidente de segurança, ou informação que seja considerada confidencial ou proprietária;

Após a avaliação os seguintes resultados foram encontrados:

- Inventário Tecnológico – 48 Computadores (36 com Windows XP Professional Service Pack 2 e 12 com Windows 98), 6 notebooks (ambos com Windows XP Professional Service Pack 2); 05 impressoras, 02 servidores (um com Windows 2003 Server com finalidade de prover autenticação de domínio interno e o outro com Linux, com a finalidade de prover a conectividade com a Internet).
- Proteção Antivírus – Inexistente em 19 computadores e desatualizado em 23. Normalmente, a maioria dos utilizadores tem consciência da ameaça representada pelos vírus, mas não estava tão consciente em relação às medidas possíveis para evitá-los.
- Firewall – O sistema de conectividade com a Internet não possui nenhum tipo de proteção contra acesso não autorizado oriundo de rede externa.
- Senhas – Alguns usuários colocam sua senha em um papel colado no monitor, como lembrete.
- Segurança Física – Os servidores não possuem nenhum tipo de acomodação especial (ficam alojados no chão, dentro do ambiente da empresa). Nenhum computador tem o número de série gravado na respectiva caixa e os números de série não estavam registrados. Alguns usuários utilizam notebooks pessoais conectados à rede da empresa. Foram identificadas várias ocorrências de presença de alimentos sob os equipamentos. Também foi constatado que todos os membros do pessoal, incluindo uma secretária e um diretor, estão a utilizar a mesma

4 ESTUDO DE CASO

Este estudo de caso foi desenvolvido com base em um levantamento de análise de riscos para a implementação de uma política de segurança em uma empresa fictícia com o nome de S&R Advogados que, devido a crescente demanda ao qual estava sendo submetida e exposta, resolveu adotar os procedimentos adequados para a segurança de suas informações.

A S&R Advogados é uma empresa de assessoria jurídica com cerca de 45 funcionários e a ausência de um especialista ou departamento de TI, dificulta bastante a presença de normas para melhoria da segurança. Outro fator crítico é que o todo o suporte em TI é terceirizado, sendo este realizado via telefone.

A primeira etapa do processo consistiu em entrevistas com os gestores e usuários e análise técnicas dos ativos tecnológicos, a fim de **coletar evidências da presença de falhas**.

Ao final da avaliação os seguintes resultados foram encontrados:

- Inventário Tecnológico – 48 Computadores (36 com Windows XP Professional *Service Pack 2* e 12 com Windows 98), 6 *notebooks* (ambos com Windows XP Professional *Service Pack 2*); 05 impressoras, 02 servidores (um com Windows 2003 Server com finalidade de prover autenticação de domínio interno e o outro com *Linux*, com a finalidade de prover a conectividade com a *Internet*).
- Proteção Antivírus – Inexistente em 19 computadores e desatualizado em 23. Normalmente, a maioria dos utilizadores tinha consciência da ameaça representada pelos vírus, mas não estava tão consciente em relação às medidas possíveis para evitá-los.
- Firewall – O sistema de conectividade com a internet não possuía nenhum tipo de proteção contra acesso não autorizado oriundo da rede externa.
- Senhas – Alguns usuários colocam sua senha em um papel colado no monitor, como lembrete.
- Segurança Física – Os servidores não possuem nenhum tipo de acomodação especial (ficam alojados no chão, dentro do almoxarifado da empresa); Nenhum computador tem o número de série gravado na respectiva caixa e os números de série não estavam registrados; Alguns usuários utilizam *notebooks* pessoais conectados à rede da empresa; Foram identificadas várias ocorrências da presença de alimentos sob os equipamentos; Também foi constatado que todos os membros do pessoal, incluindo uma secretária e um diretor, estão a utilizar a mesma

impressora, o que significa que existe o risco de os documentos confidenciais serem acidentalmente confundidos.

- Utilização da Internet – Através de uma auditoria de filtro de conteúdo foi constatado que 40% da navegação na *Internet* não estavam relacionadas com o trabalho; Utilização do *e-mail* corporativo para envio de correntes e fins pessoais;
- Utilização do Computador e Sistema – Identificada a presença de diversos *softwares* que não condizem com o trabalho dos usuários; Em alguns casos a imagem de fundo da área de trabalho continha imagens com conteúdo explícito; Constatado vários compartilhamentos nas máquinas, alguns para troca de arquivos de música e filmes;
- Backup – Efetuada semanalmente uma cópia de segurança dos dados do servidor para uma unidade *DAT (Digital Audio Tape)*, mas o restauro não foi testado. Caso os utilizadores não se lembrem de copiar os arquivos locais para o servidor, esses arquivos não terão cópia de segurança.
- Suporte em Informática – Devido ao suporte ser terceirizado e realizado mais comumente via telefone, não existe nenhuma política de manutenção preventiva dos equipamentos, nem fiscalização da utilização dos ativos.

Com base nos resultados da avaliação, considerou-se que as **prioridades de segurança** são as seguintes:

- Instalação de um *firewall* no servidor de *Internet*;
- Instalação e atualização dos *softwares* antivírus;
- Atualização dos computadores com Windows 98 para Windows XP Professional;
- Treinamento para conscientização dos usuários;
- Deslocamento dos servidores para uma sala segura que possa ter controle de acesso;
- Contratação de profissionais de TI para estabelecer o Depto. de Informática da empresa;
- Criar um plano de *backup* melhorado e com local seguro para armazenamento das fitas;
- Limitar a utilização de impressoras por departamento;
- Testar periodicamente as operações de restauro de *backup*;
- Conscientização dos usuários com a questão das senhas;
- Controle do conteúdo de acesso à *Internet*;

Após o levantamento de prioridades a serem adotadas, a empresa fundou o DINFO (Departamento de Informática da S&R Advogados) composta por profissionais especializados em TI, que prontamente atenderam as prioridades identificadas no processo de avaliação de riscos.

4.1 POLÍTICA DE SEGURANÇA IMPLANTADA

Tendo reconhecido todo o conjunto de melhorias provido após o funcionamento do DINFO, a Direção da S&R Advogados optou pela implantação de uma Política de Segurança para formalizar e prover os requisitos de segurança, baseados nas necessidades da instituição e, principalmente, focada em seus usuários. Tal documento foi denominado PSISRA – *Política de Segurança da Informação da S&R Advogados* e foi organizada da forma explanada nas próximas seções.

4.1.1 Introdução

A PSISRA (Política de Segurança da Informação da S&R Advogados) é um documento que descreve os procedimentos e regras que devem ser seguidas pelos usuários e gestores para garantir os princípios de segurança nesta instituição.

A elaboração deste documento foi um resultado do levantamento feito pela Diretoria da empresa em conjunto com o DINFO (Departamento de Informática da S&R Advogados), sendo este o responsável por fiscalizar seu funcionamento e mantê-la atualizada, salvo autoridade que a Diretoria desta empresa lhe concedeu para administrá-la.

4.1.2 Estações de Trabalho

Todas as estações de trabalho utilizadas pelos usuários da S&R Advogados possuem um conjunto de configurações bem definidas. Essas configurações foram aprovadas pela direção da empresa e não devem, em hipótese alguma, serem alteradas pelos usuários.

4.1.3 Ambiente Físico

O Usuário terá ao seu dispor infra-estrutura necessária e apropriada para o desempenho das atividades institucionais. Cada usuário deve utilizar racionalmente a infra-estrutura disponibilizada.

Para o uso adequado, o usuário deverá evitar qualquer tipo de colisão ou dano físico aos equipamentos de informática, tão pouco derramar líquidos ou substâncias nas proximidades de qualquer ativo de informática, salvo produtos de limpeza devidamente autorizados e manuseados por pessoal adequado.

Não é permitido o uso de equipamentos de uso pessoal, como *notebooks*, para as atividades institucionais dos usuários, exceto aqueles autorizados pelo DINFO.

4.1.4 Sistema Operacional

Todas as estações de trabalho estarão configuradas com sistema operacional Microsoft Windows XP *Service Pack 2*.

É vedada a instalação de qualquer outro sistema operacional pelos usuários, bem como a utilização de discos de *boot* ou *live cd* que executem algum sistema operacional.

Necessidades especiais devem ser encaminhadas a Diretoria da S&R Advogados.

4.1.5 Credenciais do Usuário

Para utilização das Estações de Trabalho, cada usuário deverá possuir obrigatoriamente uma credencial de acesso, composta por *login* e senha. Sem essa credencial, o usuário não poderá utilizar a Estação de Trabalho nem os serviços e recursos disponibilizados pela empresa.

A S&R define as regras envolvidas na utilização de senhas, visando garantir os princípios de segurança da informação, conforme apresentado a seguir.

- As senhas devem ter, no mínimo, 08 dígitos;
- São permitidos letras, números e caracteres especiais, para as senhas;
- As senhas expiram a cada 90 dias. Após este prazo, o usuário deverá obrigatoriamente modificar sua senha;
- Um histórico de senha é mantido para evitar repetição de senhas, por no mínimo 05 (cinco) senhas;
- Após três tentativas sem sucesso do procedimento de *logon*, a credencial do usuário será bloqueada;

4.1.6 Utilização de Softwares

Para a utilização das Estações de Trabalho, o DINFO especificará os *softwares* que poderão ser utilizados, bem como aqueles que preliminarmente estão desautorizados ao uso.

Somente os *softwares* autorizados e instalados pelo DINFO poderão ser utilizados pelos usuários.

4.1.7 Restrições nas Estações de Trabalho

As Estações de Trabalho são devidamente configuradas para bloquear tentativas de acesso a opções de configuração e operação do Sistema Operacional Windows. Exemplos desses bloqueios é possibilidade de acesso ao Painel de Controle e a Lançador de Aplicação do Windows. Os recursos habilitados nas Estações de Trabalho são apenas aqueles necessários à execução das tarefas relacionadas à S&R Advogados.

- a) Compartilhamentos – Não será concedido ao usuário o direito de compartilhar recursos locais nas estações, cabendo somente ao DINFO realizar tais procedimentos e configurar novos compartilhamentos, através de mecanismo apropriado.
- b) Área de Trabalho – Toda vez que um usuário faz *logon*, ícones padrões da área de trabalho são carregados, a remoção ou inserção de ícones pelo usuário na área de trabalho não estarão presentes no próximo *logon*. O usuário não poderá alterar as configurações de papel de parede nem de resolução de tela, salvo sobre autorização do DINFO.

4.1.8 Utilização da Internet

O DINFO bloqueia o acesso a sites de conteúdo impróprio, sexual, ilícito ou contraproducente. Um site é considerado bloqueado quando, na tentativa do acesso, for informada uma mensagem de erro de autoria do DINFO.

Os sites de conteúdo apresentados acima que não forem bloqueados não devem ser acessados.

Caso seja necessário, o uso de credenciais poderá ser requisitado no acesso a sites, a fim de facilitar procedimentos de autorização sobre o uso dos recursos de rede.

- a) Downloads – O *download* de arquivos é um meio comum de entrada de vírus, *trojans*, *worms* e outras ameaças. Dessa forma, o DINFO bloqueia o *download* de diversos tipos de arquivos considerados danosos para a infra-estrutura de informática da empresa. Exemplos de arquivos que não devem ser copiados são filmes, músicas, jogos e programas diversos. O usuário deve ter cuidado na hora de efetuar qualquer tipo de *download*.

- b) E-mail – O uso de serviços de *e-mail* é permitido para comunicação ligada as atribuições institucionais dos usuários. Não é permitida a utilização das contas de e-mail para envio de mensagens promocionais, correntes, anúncios diversos ou qualquer tipo de mensagem que não diga respeito as atividades desempenhadas no trabalho. Caso *e-mails* de conteúdo duvidoso ou não autorizado seja recebido, o DINFO deve ser imediatamente informado. Os *e-mails* dos usuários são verificados quanto a existência de vírus e a ocorrência de comportamentos de *spam*. Além disso, anexos considerados danosos a segurança da S&R Advogados são bloqueados.

4.1.9 Auditoria

Todas as atividades são automaticamente registradas e passíveis de auditoria sem prévio aviso. O não atendimento às normas de segurança apresentadas serão devidamente analisadas e documentadas, sendo estas encaminhadas a Direção, caso necessário.

5 CONCLUSÃO

A segurança da informação deve ser tratada como a área que se dedica à proteção dos ativos que manipulam a informação, a contar dela própria, e não apenas aos mecanismos de proteção utilizados por meio da tecnologia.

A avaliação de riscos é um importante aliado do processo de gerenciamento da segurança da informação, pois através de seus indicadores é possível identificar as áreas onde os mecanismos de proteção devem ser aplicados, sempre levando em consideração que as reavaliações devem ser periódicas.

Com o intuito de proteger a informação, a Política de Segurança deve constituir o mecanismo formal das práticas de gerenciamento e conduta, sendo esta desenvolvida a partir do levantamento de diretrizes pré-estabelecidas que expressem a importância e relevância de determinado ativo ao negócio da instituição.

Com isso, o autor espera que este trabalho possa servir como guia de pesquisa na elaboração de projetos que envolvam a segurança de recursos computacionais em qualquer instituição.

REFERÊNCIAS

ACADEMIA LATINO-AMERICANA DE SEGURANÇA DA INFORMAÇÃO. **Entendendo e Implementando a Norma ABNT NBR ISO/IEC 17799:2005.**

ASCIUTTI, César Augusto. **Alinhando ABNT-NBR-ISO/IEC 17799 e 27001 para a Administração Pública – USP.** Disponível em <http://www.security.usp.br/artigos/2-ESECOM_USP-09-11-2006-Artigo-By-Asciutti-Cesar-A-V1-04.pdf> Acessado em 09 Out 2007.

GEUS, Paulo Lício de; NAKAMURA, Emílio Tissato. **Segurança de Redes em Ambientes Cooperativos.** São Paulo: Futura, 2003.

INFORMAÇÃO. In: NOVO Dicionário Aurélio: O Dicionário da Língua Portuguesa. Rio de Janeiro: Nova Fronteira, 1999

INTERFOCUS CONSULTORIA, **Segurança das Informações em Redes.** Disponível em <<http://galileu.interfocus.com.br/interfocus-2/>> Acessado em 15 Nov. 2007

MÓDULO SECURITY NEWS, **Tecnologia por si só não garante segurança da informação.** Disponível em <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=7&objid=4885&pagenumber=0&idiom=0> Acessado em 09 Out 2007.

SÊMOLA, M. **Gestão da Segurança da Informação – Uma visão executiva.** 3. ed. Rio de Janeiro: Elsevier, 2003.

SILVA, Giliard Francisco da. **A informação: O maior patrimônio de uma organização.** Disponível em <<http://artigos.com/artigos/tecnologia/a-informacao:-o-maior-patrimonio-de-uma-organizacao-1867/artigo/>> Acessado em 01 Out 2007.