DANILLO LUSTOSA WANDERLEY

POLÍTICAS DE SEGURANÇA

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras, como parte das exigências do curso de Pós-Graduação *Latu Sensu* em Administração em Redes Linux, para obtenção do título de especialista em Administração em Redes Linux.

Orientador
Prof. Joaquim Quinteiro Uchôa

LAVRAS
MINAS GERAIS – BRASIL
2005

DANILLO LUSTOSA WANDERLEY

POLÍTICAS DE SEGURANÇA

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras, como parte das exigências do curso de Pós-Graduação *Latu Sensu* em Administração em Redes Linux, para obtenção do título de especialista em Administração em Redes Linux.

Aprovada em

Prof.

Prof.

Prof. Joaquim Quinteiro Uchôa
(Orientador)

LAVRAS
MINAS GERAIS – BRASIL

Resumo

Política de Segurança é o conjunto de diretrizes destinadas a regulamentar como uma organização gerencia suas informações e recursos. Aliado a uma política de segurança tem-se a política de uso, que tem por objetivo deixar claro para o usuário o que ele pode ou não fazer com os recursos da instituição. Com isso, o tema deste trabalho é Políticas de Segurança e irá abranger a parte de segurança física, segurança lógica e política de uso.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1. INTRODUÇÃO

1.1 COMENTÁRIOS INICIAIS

Desde o surgimento da informática, em meados da década de 1940, nos Estados Unidos, já existia a preocupação com a segurança dos sistemas. Naquela época os cientistas já pensavam em interligar os computadores e seus sistemas de informação para transmitir dados através de uma rede. Com a interligação dos computadores as informações se propagaram com maior velocidade e com isso, surgiu a necessidade de fazer com que essas informações não se perdessem ou fossem interceptadas por alguém.

Com o passar dos anos e com o surgimento da Internet muitas organizações se lançaram no mundo virtual, sendo que muitas delas só existem neste ambiente. Portanto, proteger suas informações e seu ambiente computacional é vital para a realização dos negócios e a manutenção da mesma no mercado.

Conforme Geus & Nakamura (2003), investir em segurança é indispensável para a sobrevivência e lucratividade da empresa uma vez que a informação é seu bem mais precioso. Mas, o que é de fato segurança? Segurança é a tentativa de se manter imutável uma situação estável, por exemplo, quando se contrata um seguro residencial procura-se minimizar as perdas em caso de sinistro.

Segurança é um processo e não uma tecnologia que se pode comprar a fim de tornar uma empresa mais segura. É um estado muito difícil de ser alcançado ou às vezes impossível, porque ela não é estática. Para manter-se no mesmo nível e conseguir maior segurança é necessário um esforço contínuo a fim de administrar um nível aceitável de risco, porque um processo cem por cento seguro não existe (WADLOW, 2000).

1.2 PRINCIPAIS AMEAÇAS AOS SISTEMAS DE INFORMAÇÃO

Dado a grande importância que a informática tem hoje dentro das organizações pode-se dizer que ela se tornou um instrumento essencial para a realização dos trabalhos de maneira mais rápida, fácil e eficiente. E o principal responsável por isso são as redes que tem por finalidade interligar os computadores com o objetivo de compartilhar recursos.

Mas as informações que os usuários acessam precisam ser confiáveis, íntegras e estarem disponíveis quando forem necessárias. Para isso é preciso protegê-las contra possíveis ameaças como:

- ***Hackers:*** termo utilizado para identificar quem realiza ataques em um sistema computacional. Porém é preciso dizer que existem diversas ramificações, sendo o termo *hacker* melhor empregado àqueles que são especialistas em computação (fanáticos) que gostam de mostrar seu poder de conhecimento invadindo sistemas (UCHÔA; ALVES, 2002). E os *crackers,* que são elementos que invadem sistemas para roubar informações e causar danos às vítimas. Por acreditar que o assunto é muito polêmico e por gerar muita controversa, este texto não abordará este assunto a fundo. É importante salientar que não só *"hackers"* são os causadores de problemas de segurança ao sistema de informação, muitos usuários autorizados ou não, podem causar danos aos serviços de redes devido a seus erros ou sua própria ignorância.
- **Código Malicioso:** *software* criado com finalidade de destruir dados sem a intenção do usuário. Podem ser citados os:
    1) Vírus: é um programa capaz de infectar programas e arquivos em um computador. Diversos problemas podem ocorrer, desde travamentos na máquina à perda total dos dados do usuário. Existem vários tipos de vírus como por exemplo: vírus de *boot*, vírus de arquivo, vírus de macro, vírus de *e-mail*.

2) Vermes (*worm*): é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente dos vírus, os *worms* não necessitam ser executados para se propagarem. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas existentes na configuração de *software* instalados em computadores.
3) Cavalo de Tróia (*Trojan Horse*): é um programa que além de executar funções para as quais foi projetado, também executam outras funções normalmente maliciosas e sem conhecimento do usuário. Algumas de suas funções são: alteração ou destruição de arquivos, furtos de senhas e outras informações como números de cartões de crédito e inclusão de *backdoors* para permitir que o atacante tenha controle sobre o computador.

Para mais informações sobre tipos de códigos maliciosos o autor deste trabalho recomenda a leitura de Uchôa (2003), NBSO (2003) e Cronkhite; Mccullough (2001).

- ***Backdoors:*** é um programa que permite ao invasor retornar a um computador comprometido sem ser notado e sem ter que recorrer às técnicas de invasão. A forma usual de inclusão de um *backdoor* consiste na adição de um novo serviço ou substituição de um determinado serviço por uma versão alterada, normalmente incluindo recursos que permitam acesso remoto (através da Internet).
- **Negação de Serviços (DoS):** nos ataques de negação de serviço o atacante utiliza-se de um computador para tirar de operação um serviço ou computador conectado à Internet. Por exemplo, tirar serviços importantes de um provedor do ar, impossibilitando o acesso dos usuários às suas caixas de correio no servidor de *e-mail* ou ao servidor *web* (SCHETINA; GREEN; CARLSON, 2002).
- **Engenharia Social:** O termo utilizado para descrever um método de ataque,

onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Com isso, a proteção tem por objetivo manter o acesso às informações que são disponibilizadas ao usuário, de forma que toda informação seja confiável. Para isso é necessário que todos os elementos envolvidos na transmissão da informação devem estar disponíveis, e devem também preservar a integridade e sigilo das informações.

Mas, a segurança das informações ou segurança de redes deve estar além da proteção contra *"hackers"* ou outras ameaças, ela deve ser considerada algo que permita que as organizações busquem lucros, ou melhor dizendo, que seja o elemento habilitador dos negócios da organização. Pesquisas comprovam que muitas pessoas já deixaram de realizar uma compra via Internet por não confiarem na segurança de um *site,* e para empresas que vivem do comércio eletrônico isso pode ser o fim de seus negócios (GEUS; NAKAMURA, 2003).

1.3 POLÍTICA DE SEGURANÇA

Com o intuito de exprimir formalmente as regras que devem ser seguidas para se ter acesso aos recursos tecnológicos de uma organização é que se cria uma Política de Segurança. A Política de Segurança esta relacionada com a proteção da informação e abrange aspectos humanos, culturais e tecnológicos.

É com base nessa política que as normas e procedimentos que devem ser seguidas por todos usuários são criadas, obedecendo às questões culturais e legais de determinada região ou país.

Segundo Wadlow (2000), uma Política de Segurança deve ser pró-ativa, onde os agentes envolvidos estejam atentos a possíveis brechas na segurança e que seja possível corrigi-la o mais rápido possível, e não reativa, onde se espera acontecer para depois procurar resolver os possíveis danos causados.

A Política de Segurança deve ser o mais abrangente possível, mas não entrar em detalhes técnicos porque o intuito é fazer com que ela seja entendida por todos e principalmente aceita, desde o nível de usuários até o nível gerencial da organização.

É possível que a adoção de uma Política de Segurança possa trazer alguns transtornos iniciais, pois toda mudança é acompanhada de um atraso nas atividades que eram rotineiramente executadas. Mas, o importante é que ela seja verdadeira e atenda a real necessidade da organização e de seus funcionários.

Uma Política de Segurança tem por princípio informar aos funcionários da organização de uma forma geral suas obrigações para proteção da tecnologia e acesso às informações bem como oferecer os requisitos mínimos necessários para aquisição de equipamentos (*hardware*) e programas de usuário (*software* aplicativo e utilitário).

A Política de Segurança 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 à segurança.
- **Perda de informações:** perda de dados (os dados da organização podem ser corrompidos ou excluídos), violação de privacidade (informações podem ser lidas por pessoas não autorizadas) e perda de serviços (usuários não conseguem acessar seus *e-mails*).

1.3.2 Características essenciais à 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, também 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 defina;
- 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. De nada adianta senhas difíceis se elas estão afixadas ao teclado servindo como lembrete. Seria importante que todo usuário fosse 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.

Assim como questões sobre controle de acesso lógico, é importante que a política também abranja questões sobre a segurança física. É preciso proibir o acesso aos equipamentos por parte de pessoas não autorizadas. Um outro fator que pode ocorrer é catástrofes naturais, por isso, é de fundamental importância que o plano de contingência faça parte da Política de Segurança.

As atividades envolvidas no processo de segurança devem ser constantes como o processo de cuidar de um jardim, caso contrário a grama toma conta. A

implantação, manutenção e cumprimento da política dar-se-á através das pessoas envolvidas, caso não haja dedicação por parte de todos nada adiantará o investimento realizado.

1.3.2 Princípios de uma Política de Segurança

Quando se fala em segurança computacional alguns elementos devem ser destacados, elementos estes que são os paradigmas básicos para composição de uma Política de Segurança:

- Integridade: condição na qual a informação é protegida contra modificações não autorizadas, ou seja, garantir que o que está sendo acessado é idêntico ao que foi armazenado;
- Confidencialidade: fazer com que as informações não sejam disponibilizadas sem autorização do proprietário, ou seja, garantir que os dados só sejam acessados por quem é de direito, protegendo assim a privacidade dos usuários e dos dados;
- Disponibilidade: característica relacionada diretamente a possibilidade de acesso às informações por parte daqueles que necessitam para a realização de suas atividades;
- Confiança: garantir que os dados armazenados estarão disponíveis quando necessários e que o mecanismo de *backup* seja utilizado com eficiência para que as informações sejam recuperadas com facilidade.

Além disso, em toda política devem estar inclusos componentes que irão definir os direitos e privilégios de cada usuário, definindo assim uma linha de conduta a ser seguida. Também é importante elaborar um guia de compras para equipamentos, onde estarão os requisitos ou características que cada produto deve ter.

Dada a importância da política de segurança nas instituições, este trabalho tem por objetivo elaborar um conjunto de diretrizes que devem ser

seguidas na elaboração de uma política. Assim, abrangerá temas como:

- Segurança Física: onde serão abordados assuntos como a proteção dos equipamentos da instituição, integridade física dos dados, controle de acesso físico, infra-estrutura, plano de contingência;
- Segurança Lógica: como garantir a integridade lógica dos dados, proteção dos dados da instituição, proteção da privacidade dos usuários;
- Política de Uso: papel do usuário na implantação da política.

2. SEGURANÇA FÍSICA DAS INSTALAÇÕES

2.1 COMENTÁRIOS INICIAIS

Segundo Caruso & Steffen (1999), dentre os componentes de uma Política de Segurança pode-se dizer que a segurança física é um dos mais importantes. É ela que vai ditar as normas de acesso físico, normas para garantir a integridade física dos dados e dos equipamentos, infraestrutura das instalações e um plano de contingência.

Toda vez que se fala em segurança física lembra-se logo de alguns filmes que foram sucesso nos cinemas de todo mundo. Nestes filmes agentes tentam entrar em centros de computadores escalando paredes com apoios à base de sucção, atravessam grades de alarmes a laser e uma série de outras artimanhas. Tudo isso para conseguir informações que são valiosas.

Informações são os bens mais preciosos de uma organização, por isso é como se o local onde estão armazenadas parecesse com um caixa-forte cercado de medidas para impedir acesso de pessoas estranhas ao ambiente. O porque de tais medidas é que estas informações têm o poder de promover o crescimento da organização gerando mais dinheiro e lucratividade.

Entretanto, é fácil perceber que a questão da segurança física muitas vezes é deixada para segundo plano e só se percebe sua falta quando algo acontece e paralisa o funcionamento da área de informática.

Foi o que aconteceu em 2001, quando o CPD do Tribunal de Justiça do Estado do Tocantins pegou fogo, sendo o autor deste trabalho testemunha do ocorrido. Naquela ocasião todos os conceitos de segurança física não foram observados. A começar pelo ar condicionado que não funcionava e por ser um Estado no qual faz muito calor os funcionários traziam ventiladores para o centro de informática.

No dia do incidente alguns *no-breaks* e baterias foram entregues e pelo

avançado da hora os auxiliares de serviços gerais já haviam ido embora. Então todos os equipamentos que foram recebidos ficaram depositados no CPD próximo de um dos ventiladores, aguardando que no dia seguinte fossem transportados para o local apropriado.

Só que uma fatalidade já se anunciava, uma vez que esse ventilador que ficara próximo do material recebido estava apresentando defeito, às vezes sem mais nem menos ele parava de funcionar e permanecia ligado. Após todo material ser acomodado todos foram embora e não perceberam que o ventilador que estava parado permanecia ligado o que acabou por gerar super aquecimento no aparelho.

Devido ao super aquecimento as partes plásticas do ventilador foram derretendo e pingando sobre as baterias no centro da sala. Com isso, todo material estocado se incendiou, causando um estrago muito grande. Como conseqüência, o setor de informática ficou parado por 30 dias, paralisando assim toda a movimentação de processos do órgão.

Depois disso algumas mudanças aconteceram, mas muito tímidas e a preocupação com a segurança sempre relegada a segundo plano, talvez porque a falta de cultura dos diretores e magistrados ou a "falta de verbas" do Poder Judiciário impediam que profundas mudanças acontecessem.

No geral é o que acontece com a maioria das empresas, porque o investimento em segurança física é caro e, por isso, às vezes existe uma tendência para reduzir bastante os custos e eliminar a proteção que é necessária.

Outras ameaças também afetam os centros de informática e podem ocorrer quase todos os dias, como por exemplo:

- Funcionários que manipulam incorretamente equipamentos;
- Cópias de segurança mal feitas e local de armazenamento de tais fitas inapropriado. Isso se evidencia porque nem sempre são feitos testes para restauração dos *backups* e quando realmente precisa, verifica-se que algo saiu errado, ou porque o funcionário responsável não executou a tarefa

corretamente ou por problema na mídia. Foi o que aconteceu no exemplo citado anteriormente;

- Sobrecarga do circuito de energia pelo acréscimo de equipamentos não previstos;
- Faltas constantes de energia, o que pode ser ocasionado pelas condições meteorológicas. Por isso, é importante sempre ter uma fonte de energia alternativa;
- Roubo;
- E por último, as catástrofes naturais.

Observa-se que os centros de informática estão sujeitos a vários tipos de ameaças, o que faz necessário adotar medidas de prevenção. São estas medidas que vão minimizar possíveis danos em caso de algum incidente acontecer. Nas próximas seções serão citadas algumas medidas para garantir um maior nível de segurança.

2.2 LOCALIZAÇÃO DO CPD

O centro de processamento de dados por ser uma área sensível e de fundamental importância para a organização deve ficar em um local livre de quaisquer fatores de risco evitando-se a proximidade com as seguintes áreas (CARUSO;STEFFEN, 1999):

- Depósitos de materiais combustíveis ou explosivos;
- Terrenos abaixo do nível de rios, lagos e quaisquer locais sujeitos a inundação;
- Tubulações destinadas a transportar qualquer tipo de líquidos ou gases;
- Locais sujeitos a alta incidência de descargas atmosféricas;
- Local sujeito a vibrações ou impactos de alta intensidade, como por exemplo, rodovias, vias públicas de trânsito intenso, ferrovias e metrô;
- Local com alto nível de poluição atmosférica, que ofereça riscos de corrosão

de equipamentos e de mídias magnéticas;

- Antenas de transmissão de rádio, TV, microondas, telefonia celular e de comunicações em geral (sujeitas a interferência de radiofreqüência);
- Estações de energia elétrica e linhas de transmissão de alta tensão (sujeitas a interferência eletromagnéticas) .

De uma maneira geral os CPD's têm passado por uma evolução, estão deixando de ser aquele lugar que era aberto à visitação de pessoas, ou seja, toda vez que a empresa ia ser apresentada a alguém o primeiro setor visitado era o centro de informática, talvez para mostrar o grau de informatização.

Em muitas empresas os CPD's ficavam tão expostos que pareciam mais vitrines do que o centro de informática. Neste caso eles ficavam de frente à rua separados apenas por janelas de vidro. Em outra situação, para proteger o CPD as empresas quase que literalmente o enterravam. Eram construídos no subsolo dos prédios na tentativa de isolá-lo, mas na verdade estavam era deixando sujeito, por exemplo, a inundações.

Muitas empresas já se atentaram para a necessidade de um local mais seguro e menos exposto para implantar seus centros de processamento de dados. Apesar disso, a maioria das instalações são adaptadas em prédios já existentes, onde nos quais não houve preocupação com a segurança das instalações.

Mas, independente do local a ser construído o CPD algumas normas de segurança jamais deverão ser esquecidas, como por exemplo:

- Materiais resistentes ao fogo;
- Tubulações de água e esgoto não devem passar pela sala de equipamentos de informática;
- As condições do ambiente devem ser adequadas, como por exemplo: climatização, condicionamento de ar, proteção dos dutos de ventilação, umidificação, aterramento adequado, piso falso para que os cabos de força e lógica não fiquem espalhados pela sala evitando assim, em casos de incêndio, a propagação do fogo e de gases.

2.3 SEGURANÇA CONTRA FOGO

Todas as instalações de uma empresa, principalmente seu centro de informática, devem utilizar mobiliário e equipamentos fabricados com materiais incombustíveis para minimizar os riscos de um eventual incêndio. Na hipótese de ocorrência de um incêndio, as instalações devem ser pensadas de forma que as chamas não se propaguem facilmente.

Em relação a localização das áreas de processamento de informação, é importante que elas estejam isoladas das outras áreas, até mesmo podendo ficar em edifícios separados. É importante também que os materiais utilizados na construção do edifício deva apresentar um baixo índice de combustibilidade e que suas divisórias apresentem, no mínimo, uma resistência de 30 minutos ao fogo.

Outro ponto que precisa ser levado em consideração é que qualquer material combustível utilizado na limpeza de equipamentos não pode em hipótese alguma ser armazenado no CPD. Estes materiais devem no máximo permanecer no CPD em quanto determinada tarefa esteja sendo executada, depois devem ser levados para local apropriado.

2.3.1 – Equipamentos de combate ao fogo

Os equipamentos mais utilizados no combate a incêndios em áreas sensíveis de uma empresa são os extintores, hidrantes e *sprinklers* (chuveiros automáticos). Só que nas instalações dos centros de informática é conveniente que métodos de extinção que utilizem água (por conduzir eletricidade) não sejam utilizados.

Algumas características dos equipamentos mais utilizados no combate a incêndios nas empresas:

- Extintores: são destinados ao combate de pequenos focos, quando o incêndio

está na fase inicial. Devem ficar em local que permita fácil visualização (devem estar bem sinalizados) e livres de obstáculos para não dificultar o acesso aos mesmos.

- *Sprinklers:* sistema automático de combate ao fogo por meio de água. Eles são instalados em vários pontos do forro e são conectados a tubulações provenientes do reservatório de água . Assim que a temperatura do ambiente aumenta uma espécie de gatilho é disparado liberando a água.

Cada um desses equipamentos apresentam vantagens e desvantagens quanto a sua aplicação. Então, os sistemas de combate a incêndio devem ser instalados observando as características de cada ambiente e dos equipamentos ali instalados, sendo os *sprinklers,* por serem baseados em água, não recomendados para CPD's .

Existem quatro classes de incêndio, de acordo com o combustível envolvido e para cada uma delas existe um agente extintor que melhor se aplica, como mostra a Tabela 2.1, extraída de Caruso; Steffen (1999). Dada essa tabela, é recomendável que nos centros de informática se utilizem sistemas à base de gás, como o CO_2 .

2.4 CLIMATIZAÇÃO

Em ambientes destinados para processamento de dados é preciso que haja uma preocupação com o sistema de condicionamento de ar, pois ele é vital para o pleno funcionamento dos equipamentos de informática.

O dimensionamento do sistema de climatização deve ser feito de acordo com o ambiente, ou seja, de acordo com o número de equipamentos, pessoas e lâmpadas utilizadas no recinto. É preferível que se use lâmpadas fluorescentes ao invés das incandescentes, pois estas geram mais calor conseqüentemente gerará um maior consumo de energia para resfriar o local.

Tabela 2.1: Classes de incêndio e seus agentes extintores (Caruso; Steffen, 1999)

Classes / **Agentes Extintores**	**Classe A** Papel, madeira, fibras, etc.	**Classe B** Líquidos inflamáveis, graxas, óleos, tintas, etc.	**Classe C** Equipamento elétrico com eletricidade presente.	**Classe D** Metais combustíveis(magnésio, potássio, sódio)
CO_2	Sim(pouco eficiente). Atua somente sobre as chamas.	Sim(bom). Apaga por resfriamento e abafamento.	Sim(ótimo). Apaga por resfriamento e abafamento. Não é condutor.	NÃO.
ESPUMA	Sim(razoável) Para fogos superficiais e de pequena extensão.	Sim(bom). A espuma flutua sobre líquidos inflamáveis, abafando as chamas.	NÃO. A espuma é condutora elétrica.	NÃO.
PÓ QUÍMICO	Sim(pouco eficiente). Somente atua sobre as chamas.	Sim(ótimo). Apaga por abafamento.	Sim(bom). Apaga por abafamento. Não é condutor elétrico. Pode estragar o equipamento.	Sim(bom). Somente pó especial à base de limalha de ferro, areia ou grafite. Apaga por abafamento.
ÁGUA	Sim(ótimo). Apaga por resfriamento e satura o material combustível.	Sim(razoável) A água como neblina resfria e abafa o fogo. Espalha chamas.	NÃO. A água é condutora elétrica.	NÃO.

A manutenção da temperatura, umidade, taxa de poeira e gases dentro de um certo limite vai possibilitar a estabilidade no funcionamento dos equipamentos de informática, eliminação da eletricidade estática e mais conforto para todos que ali trabalham.

2.5 INSTALAÇÕES ELÉTRICAS

Um dos fatores que mais podem prejudicar o crescimento de qualquer negócio ou empresa é a falta de energia elétrica. Literalmente falando, a energia elétrica é o combustível indispensável para que qualquer organização entre em operação, pois desde uma simples lâmpada a um computador todos necessitam da eletricidade.

Assim, é importante que seja assegurado um fornecimento contínuo de energia e que seja à prova de falhas, mesmo que para isso sejam necessárias fontes alternativas para assegurar que o fornecimento seja constante.

Pode-se dizer, que os *no-breaks* são a fonte de energia alternativa mais utilizada. Eles garantem o fornecimento de energia quando ocorrem falhas na rede elétrica, tendo sua autonomia variando de uns poucos minutos, suficientes para que os usuários salvem seus trabalhos e desliguem o computador, a até algumas horas.

Os *no-breaks,* além de garantir a continuidade do fornecimento de energia, podem também funcionar como estabilizadores de tensão corrigindo as variações de voltagem e mantendo-a em níveis apropriados para o uso dos equipamentos de informática. Além disso, alguns deles têm uma interface para comunicação com o computador, o que automatiza o processo de salvamento dos arquivos e promove o desligamento da máquina com segurança, sem o risco de danificar, por exemplo, o disco rígido.

Interface para comunicação é muito indicado para os servidores de rede, pois passa a não depender da ação do operador e permite que determinados procedimentos sejam programados até o restabelecimento da energia elétrica e caso não aconteça, iniciar o processo de desligamento antes que as baterias se esgotem.

Deve-se levar em consideração se o centro de informática vai ser instalado em um prédio já existente, possuindo uma rede de alimentação já

instalada ou se vai para um prédio a ser construído. No primeiro caso, será necessário fazer alterações para garantir o adequado fornecimento de energia, para que não ocorram ruídos elétricos, variações de tensão devido ao mau dimensionamento da rede interna e constantes interrupções no fornecimento de energia. Já no segundo caso, o projeto de alimentação elétrica fará parte do projeto do edifício, o que permitirá uma melhor adequação às condições exigidas pelos equipamentos de informática.

Outro fator não menos importante e que deve ser levado em consideração é o aterramento elétrico, pois garantirá que eventuais descargas elétricas não danifiquem os equipamentos da organização.

2.6 CONTROLE DE ACESSO FÍSICO

O controle de acesso físico aos centros de informática está relacionado à permissão ou não para adentrar as instalações. O acesso físico pode ser menos sujeito a riscos do que o acesso lógico às informações, mas pode ser considerado ao menos mais complicado, uma vez que depende muito da intervenção humana.

Tem como requisito básico a identificação de cada pessoa para que ela possa permanecer no ambiente. Tal identificação exige das pessoas um tipo de documento que pode ser uma identificação funcional e uma senha que após digitada é conferida por um computador que estando correta permitirá acesso. Utilizando-se de mais sofisticação, algumas organizações fazem o reconhecimento através de impressão digital, timbre de voz e padrão retínico.

Para realização desta tarefa, a de identificar cada pessoa, alguns métodos de bloqueio podem ser implementados. Desde o mais simples onde uma pessoa em uma portaria confere documentos e permite ou não o acesso, até métodos automatizados onde não há a intervenção humana e cada um usa sua identidade digital conforme técnicas citadas no final do parágrafo anterior.

Além do acesso de pessoal deve-se levar em conta também o acesso de

equipamentos aos centros de processamento de dados. Se o CPD ficar num pavimento superior como equipamentos mais pesados irão chegar até lá? Escada, rampa inclinada, elevador? Tudo isso deve ser pensado na fase de projeto da edificação e se o centro de informática estiver sendo montado num prédio já existente a questão da localização do mesmo será um fator preponderante no momento de sua instalação.

Com isso, para concluir este capítulo, observa-se que todas as instituições sejam elas públicas ou privadas, são altamente dependentes de segurança física. Caso ocorra a destruição do seu centro de informática é capaz de ter sua sobrevivência comprometida, pois os prejuízos acarretados seriam muito grandes.

E, para que incidentes como o citado no início deste capítulo não ocorra é necessário que as normas de segurança sejam seguidas à risca e que um bom plano de contingência seja elaborado.

3. SEGURANÇA DOS MEIOS DE ARMAZENAMENTO

3.1 COMENTÁRIOS INICIAIS

Como comentado no item 1.3.2, um sistema computacional para ser considerado seguro deve atender a quatro requisitos básicos: integridade, confidencialidade, disponibilidade e confiança. Quando fala-se em confiança pretende-se dizer que os dados armazenados estarão disponíveis quando necessários.

Este item terá como finalidade mostrar algumas medidas necessárias na hora de armazenar as informações, levando-se em consideração os agentes de riscos que envolvem os meios de armazenamento. Também será abordada a questão da segurança dos equipamentos.

3.2 CONDIÇÕES DO AMBIENTE DE ARQUIVO

Segundo Caruso & Steffen (1999), as mídias, de uma forma geral, estão sujeitas às condições do ambiente, principalmente calor e poluição. Independentemente das mídias magnéticas serem mais sensíveis que os discos ópticos, os dois estão sujeitos a agentes de risco que podem afetar o seu conteúdo.

Entre os principais agentes de risco, podem ser citados: a temperatura, umidade, poeira, campos eletromagnéticos e choques mecânicos. Grandes variações de temperatura e umidade e a existência de poeira no ambiente de arquivamento podem levar à decomposição química das mídias, principalmente as magnéticas.

Outro fator de risco que poderia levar à perda dos dados contidos nos meios de armazenamento seria a proximidade com objetos imantados ou campos magnéticos (como os gerados por aparelhos telefônicos).

Então, como recomendado em NBSO (2003), os meios de armazenamento devem ser guardados em locais climatizados e livres de poeira. Recomenda-se também, que o local seja de acesso restrito, sendo que apenas pessoas autorizadas poderão adentrar ao recinto.

Vale ressaltar que em ambientes de arquivamento de dados e nas salas do CPD deve ser proibido fumar e fazer qualquer tipo de refeição. O piso deste ambiente não pode ser revestido de carpete, pois acumulam poeira e geram cargas eletrostáticas.

Para preservação dos arquivos de dados muitas empresas utilizam cofres de segurança (cofres-data) que localizam-se fora de suas instalações. Estes cofres são resistente ao fogo, umidade, calor, gases corrosivos e arrombamentos, tornando-se uma alternativa eficaz na proteção das mídias de armazenamento.

Conforme NBSO (2003) um meio muito utilizado para proteção dos dados de um computador é a realização de *backups*. Este assunto será tratado no próximo item com o intuito de mostrar a importância dos *backups* como forma de garantir a integridade dos dados.

3.3 SEGURANÇA OPERACIONAL

Os *backups* são cópias de segurança dos dados armazenados em um computador. Segundo NBSO (2003), essas cópias não são importantes somente para garantir a recuperação dos dados em caso de perda, mas também para minimizar as conseqüências de uma infecção por vírus e de uma invasão.

As cópias de segurança devem ser realizadas periodicamente e dependendo da importância das informações é aconselhável fazer mais de uma cópia. Além disso, uma rotina administrativa deve ser seguida para identificar cada mídia com informações do tipo: data, hora, conteúdo e pessoa responsável pelo *backup.*

A periodicidade dos *backups* vai depender do ritmo no qual os usuários

criam e modificam arquivos. Como isto é uma constante, cabe à política de segurança ditar as normas de realização destas cópias.

Mas, de fato quais informações devem fazer parte das cópias de segurança? Segundo NBSO (2003), somente informações de total confiança do usuário devem fazer parte dos *backups.* Apenas programas e arquivos criados pelo próprio usuário e nada de arquivos de sistemas operacionais e de instalação de *software*, pois os mesmos podem ter sido trocados por versões maliciosas.

Ainda segundo NBSO (2003), o tipo de mídia adotada para a realização de cópias de segurança é de fundamental importância, pois isto influenciará na vida útil que a cópia deve ter. Para poucos dados um simples disquete pode ser suficiente, mas para grandes volumes de dados que necessitam durar mais tempo, mídias como CD's e Fitas DAT são mais recomendáveis.

O local de armazenamento das mídias deve seguir as recomendações citadas no item 3.2. É recomendável ainda armazenar uma outra cópia em local diferente, mas que mantenha condições adequadas para o arquivamento.

Os *backups* podem conter informações vitais para a empresa o que torna necessário armazenar os dados em um formato criptografado. Assim, obtêm-se um nível maior de segurança, impedindo que estas informações sejam facilmente decifradas por alguém de fora da empresa.

Uma coisa importante em relação aos *backups,* é que eles devem ser testados periodicamente para que surpresas desagradáveis não apareçam.

Para concluir, vale ressaltar que segundo Caruso & Steffen (1999), dependendo da utilização, é recomendável manter um equipamento de reserva, em caso de problemas com o principal. Com isso, a segurança dos microcomputadores será tratada no próximo item.

3.4 SEGURANÇA DOS MICROCOMPUTADORES

Os computadores de uma empresa são utilizados para inúmeras tarefas,

como por exemplo: armazenamento de dados, comunicação através de *email*, transações bancárias, compra de produtos e serviços, etc.

Segundo NBSO (2003), é importante que os computadores utilizados na empresa estejam protegidos para evitar que dados pessoais (como senhas, números de cartão de crédito) e comerciais (informações financeiras, entre outras) sejam interceptadas por alguém.

Uma forma de proteger os microcomputadores contra vírus e possíveis invasões é ter, no mínimo, um programa anti-vírus instalado em cada máquina. Entretanto, de nada adianta ter este tipo de *software* instalado se ele não é usado corretamente. Recomenda-se mantê-lo sempre atualizado e periodicamente fazer uma verificação das mídias utilizadas para detectar e eliminar arquivos nocivos ao sistema.

O sistema operacional deve estar sempre atualizado, tão logo seja descoberta alguma vulnerabilidade o pacote de correção deve ser baixado. Segundo Uchôa (2003) a maior parte das invasões ocorrem em máquinas que não são atualizadas com freqüência e, para que isso não ocorra é essencial manter-se vigilante.

Além da segurança lógica é importante que haja uma preocupação com a integridade física dos equipamentos. "De nada adianta senhas de BIOS ou ultra-elaboradas, se qualquer funcionário recém demitido pode roubar o HD do servidor para vender ao concorrente" (Uchôa, 2003).

Cuidados com o ambiente no qual os equipamentos serão instalados deverão ser tomados conforme citado no item 2. Como lembram Caruso & Steffen (1999), alguns procedimentos em relação ao manuseio devem ser seguidos:

- Os equipamentos devem ser protegidos contra a incidência de raios solares;
- Os equipamentos deverão ser desligados corretamente. Comandos específicos para este fim devem ser utilizados para que o disco rígido não seja danificado;

- Proximidade com comida, bebida e fumaça de cigarro deve ser evitada;
- Não remanejar ou movimentar o equipamento enquanto ele estiver ligado;
- Evitar vibrações na mesa na qual o computador se encontra. É importante que equipamentos como impressora estejam em outro móvel;
- Executar uma manutenção preventiva no equipamento;
- Utilizar sempre um estabilizador de tensão ou *no-break;*
- E, por fim, todas as tomadas devem ter aterramento.

Mas, mesmo que depois de todas as precauções terem sido tomadas ainda ocorrer algum problema que paralise os serviços de informática da empresa, é preciso existir meios para contornar essa situação. Isto é definido no plano de contingência, o qual será tratado no item 5.2.

4. CONTROLE DE ACESSO ÀS INFORMAÇÕES

4.1 SEGURANÇA DA INFORMAÇÃO

Segundo Uchôa (2003), com o avanço das redes de computadores o número de invasões aos sistemas de informação tem aumentado consideravelmente. Isso leva a necessidade do administrador da rede estar sempre se atualizando de modo que ele possa combater esta prática.

Cabe ao administrador a configuração segura dos sistemas que estarão na rede e todas estas configurações devem estar documentadas. Um sistema só poderá estar disponível na internet após alguns passos terem sido seguidos, conforme ilustra NBSO (2002):

- **Instalação:** a instalação do sistema deve ser feita a partir de dispositivos de armazenamento local[1], fora da rede. Além disso, deve ser observada a configuração do *hardware* da máquina, qual o propósito do sistema que está sendo instalado e quais serviços estarão disponíveis. Evitar a concentração de vários serviços de rede em uma única máquina, isso pode diminuir o impacto causado caso o computador possa vir a apresentar problemas;
- **Particionamento:** é recomendável dividir o disco em várias partições ao invés de uma só. Isso facilita a realização dos *backups,* caso uma partição apresente problemas possivelmente não afetará as demais. Usuários ou programas podem encher uma partição e se os programas estiverem em outra eles não serão afetados e o sistema não ficará parado. As partições a serem criadas dependem de sistema para sistema e não existe uma regra, sendo que é recomendável criar partições separadas para dados de usuário, *logs,* arquivos temporários, programas do sistema

1CD, fitas e discos.

operacional, *emails,* filas de impressão, entre outros;

- **Documentação:** é importante que toda instalação e configuração realizada no sistema seja documentada em forma de um *logbook* (diário de bordo). A existência de um *logbook* facilita sobremaneira o trabalho do administrador da rede, pois nele constará os passos que foram seguidos para instalação/configuração de determinado serviço, a versão dos pacotes instalados, quais usuários foram criados, o sistema operacional instalado, particionamento do(s) disco(s), as portas que ficaram ativas após a instalação. A existência deste tipo de documento facilita a recuperação do sistema no caso de uma falha. Toda modificação que for realizada, ao ser registrada, deve conter a data, o responsável, o motivo e a descrição do que foi modificado;
- **Instalação mínima:** instalar o mínimo possível de pacotes e componentes. Este mínimo depende do propósito que terá o sistema, por exemplo, uma estação de trabalho não precisa ter um servidor *web* instalado. Serviços não utilizados normalmente não são monitorados e caso haja alguma vulnerabilidade ela pode ser explorada por algum atacante, por isso é importante que estejam desativados;
- **Instalação de correções:** após a instalação e configuração do sistema é necessário verificar se não existem correções para vulnerabilidades encontradas nos programas instalados. Toda atualização do sistema tem que ser registrada no *logbook* e deverá ser realizada toda vez que uma nova vulnerabilidade for descoberta. Recomenda-se que o administrador da rede verifique a configuração do sistema após a instalação de correções para certificar-se que nada foi alterado;
- **Prevenção de Abuso de Recursos:** serviços mal configurados, como por exemplo, *email* e *proxies* de *web* podem permitir que usuários externos utilizem a rede de forma mal intencionada, abusando dos recursos disponíveis. Isso faz com que usuários legítimos fiquem impossibilitados

de utilizar os serviços. Alguns servidores SMTP vêm com *relay* aberto, permitindo que sejam usados para enviar mensagens de e para qualquer rede ou domínio, independente dos endereços envolvidos serem da rede ou não o que facilita a prática do *spam.* A configuração do servidor SMTP deve permitir apenas envio de mensagens com endereço de origem local e endereço de destino local ou externo; recepção de mensagens com endereço de origem local ou externo e endereço de destino local. O *software* que faz *proxie* de *web* também pode ser utilizado por usuários externos para acessar recursos de forma anônima. Um *proxie* bem configurado é aquele que libera acesso somente aos endereços IP de usuários que fazem parte da rede.

4.2 ADMINISTRAÇÃO DE USUÁRIOS

4.2.1 Educação dos usuários

Segundo NBSO (2002), a maioria dos problemas que afetam a segurança da rede interna da organização são causados pelos próprios funcionários que desconhecem conceitos básicos de segurança. Para minimizar estes problemas, educar os usuários é uma atividade muito importante e deve fazer parte do cotidiano do administrador de rede.

É importante que na organização exista um canal de comunicação com os usuários informando-os sobre questões relevantes à segurança, como:

- O surgimento de um novo vírus e sua forma de infecção;
- A maneira correta de configurar o cliente de *email*[2]*;*
- A maneira mais correta e eficiente de se escolher uma senha;
- Prevenir o usuário contra técnicas de Engenharia Social, etc.

2 Uma maneira mais segura de configurar um cliente de *email* é fazer com que arquivos anexos não sejam automaticamente abertos ou executados, evitando-se a disseminação de vírus e a instalação de *backdoors.*

4.2.2 Política para as senhas

Conforme Geus & Nakamura (2003), as senhas são utilizadas para autenticação de usuários e são consideradas necessárias como um meio de proteção. Todavia, são também perigosas, pois dependem dos usuários que por sua vez podem escolher senhas óbvias e fáceis de serem descobertas.

Ainda conforme Geus & Nakamura (2003), uma política de senhas pode auxiliar o usuário na escolha de seu *password,* o que aumenta o nível de segurança de toda organização. Uma boa senha para o usuário é aquela que ele possa memorizar sem precisar de papelzinho em baixo do teclado ou colado no monitor.

Na hora de elaborar uma senha não deve-se usar sobrenomes, datas de uma forma geral, número da placa do carro, números de telefone, pois estes dados são fáceis de serem descobertos. Segundo NBSO (2002), algumas regras devem ser seguidas para elaborar uma senha, como:

- Jamais utilizar palavras que fazem parte de dicionários, pois existe *software* que tenta descobrir senhas combinando e testando palavras em diversos idiomas;
- Uma boa senha é aquela que tem pelo menos oito caracteres e que não sejam somente letras ou números. Deve-se combinar letras maiúsculas e minúsculas, números e caracteres especiais. Uma boa senha seria pegar a letra inicial de cada palavra em uma frase, por exemplo “O macaco bombeiro, a girafa Agripina e os dois peixinhos dourados”. A senha ficaria Omb,gA2pd .
- Nunca usar a mesma senha para acessar a caixa de email, a conta bancária, o cartão de crédito, ou seja, deve-se escolher uma senha distinta para cada local onde for empregá-la;
- As senhas devem ser trocadas regularmente, evitando períodos muito longos.

Existem alguns ataques que tem como objetivo descobrir senhas de usuários. Por exemplo o uso de *sniffers*[3], ataque de dicionário, adivinhação de senhas fracas que incluem dados relacionados ao próprio usuário e ataque de força bruta, onde serão realizadas as combinações possíveis de todos os caracteres até que a senha seja encontrada. (Geus;Nakamura, 2003)

Segundo Geus & Nakamura (2003), uma série de medidas podem ser tomadas para configurar, de modo seguro e eficiente, um sistema baseado em senhas. São elas:

- O usuário deve redefinir sua senha pelo menos a cada dois meses;
- Para que o usuário tenha certeza de que sua conta não foi acessada por estranhos é necessário que informações sobre o último acesso, como o tempo de duração, data/hora e origem estejam disponíveis;
- O bloqueio da senha deve ocorrer quando um número limitado de tentativas sem sucesso ocorrer;
- A transmissão da senha deve ocorrer de modo cifrado;
- Cabe ao usuário manter o sigilo de sua senha evitando o uso indevido. Um treinamento a respeito de algumas atitudes básicas para manter um nível aceitável de segurança deve ser ministrado para os usuários.

4.2.3 Administração segura de usuários

A autenticação de usuários em modernos sistemas Linux (e outras variantes do Unix) é realizada utilizando PAM (*Pluggable Authentication Modules).* "O PAM é um conjunto de bibliotecas que controlam as tarefas de autenticação do sistema e suas aplicações" (SICA; UCHÔA, 2003).

Conforme Sica & Uchôa (2003), o PAM pode ser utilizado para controlar a quantidade de recursos disponíveis a cada usuário e permitir que o

3 Programa que permite a escuta de pacotes na rede, permitindo que as senhas utilizadas sem o uso de criptografia sejam capturadas.

usuário faça *login* somente a partir de determinado horário e estação. Possibilita também, manter registros de todas as autenticações efetuadas, uso de senha escondida (*shadow*), *shell* restrito, etc.

Em relação aos limites de recursos disponibilizados a cada usuário, Uchôa (2003) recomenda a estratégia do menor privilégio, liberando ao usuário só aquilo que ele necessita para realizar suas tarefas. Esses limites podem ser impostos via PAM ou usando quotas de usuário, o que permite que os usuários tenham um espaço em disco limitado.

Como citado em Uchôa (2003), a segurança dos usuários também pode ser garantida via configuração segura do sistema de arquivos. Algumas observações devem ser citadas, como:

- A respeito da montagem de dispositivos em sistemas Unix e derivados, é importante que as opções *nosuid*[4]*, nodev*[5] *e noexec*[6] sejam observadas. Por exemplo, somente a partição que contem o diretório */dev* pode ter permissão para criar e usar arquivos de dispositivos. As outras partições devem ser montadas com a opção *nodev*. Os diretórios */tmp* e */home* devem ser montados com *nosuid,* uma vez que não serão permitidos arquivos *suid*;
- Permissões de acesso aos arquivos: o administrador deve verificar quais aplicações são executadas com permissões de administrador (com uso de SUID[7]);
- Arquivos com permissão de escrita global: em arquivos comuns de usuários esse tipo de permissão não deve ser permitido;
- Arquivos sem proprietário: podem ser resultado de restos de usuários excluídos do sistema, *software* mal instalado ou arquivos criados por um

4 Bits SUID e SGID não terão efeito. Se o usuário comum executar um programa SUID ou SGID que force a troca para outro usuário, receberá o erro de permissão negada.
5 Dispositivos especiais de bloco ou caractere do sistema de arquivos não serão interpretados se *nodev* estiver especificado.
6 Não permite a execução de binários.
7 Utilizado para que o aplicativo seja executado utilizando o UID de seu proprietário mesmo que o usuário que solicitou não o seja.

invasor. Como recomendado em Uchôa (2003), é importante que periodicamente execute-se o comando:

```
#find / \ ( –nouser –o –nogroup \)
```

Para concluir, pode-se dizer que este tópico teve por objetivo apresentar algumas medidas que necessitam ser tomadas para administrar usuários de forma segura.

É preciso lembrar que eles são o elo mais fraco da corrente quando se trata da segurança dos sistemas de informação, com isso, orientar e manter informados a respeito de questões mínimas relativas à segurança é importante.

4.3 CONFIGURAÇÃO DE SERVIÇOS DE REDE

Como citado no item 4.1, deve-se evitar a concentração de vários serviços de rede em uma única máquina. Caso algum problema aconteça, seja ele relacionado ao *hardware* ou a uma possível invasão do sistema, todos os serviços serão afetados causando a interrupção total da rede. É recomendável, sobre a ótica da segurança, que exista uma máquina para cada serviço que será implementando. Por exemplo, um computador para realizar a autenticação de usuários, um para funcionar como servidor de arquivos, um para ser servidor de *web,* um para *email*, um para implementar o serviço de *firewall* e um outro para aplicações de banco de dados, etc.

Outro ponto que deve ser observado é em relação a quais serviços estarão configurados. Serviços que não forem utilizados não devem ser instalados. Em se tratando de segurança computacional itens como *firewall, proxy* e criptografia devem ser observados, pois eles podem evitar dores de cabeça para os administradores de rede.

Segundo Uchôa (2003), um *firewall* é uma ferramenta de *software* ou *hardware* situado entre uma rede interna e uma externa que tem por função

filtrar pacotes e impedir o acesso externo a determinados serviços da rede, como ilustra a figura 4.1.

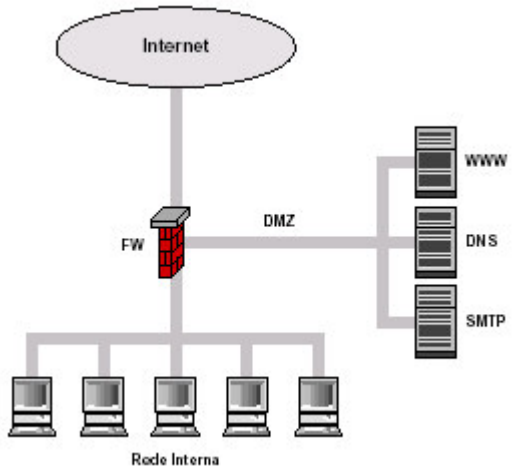

Figura 4.1: Uso de *Firewall*

Apesar de um *firewall* implementar segurança por controle de acesso e ser uma poderosa ferramenta para prevenir ataques externos, ele não deve ser a única forma de defesa porque não é infalível. Conforme NBSO (2002), ele deve ser mais um entre os diversos mecanismos e procedimentos que aumentam a segurança de uma rede.

Segundo NBSO (2002), é recomendável que os servidores acessíveis externamente (*WEB*, FTP, *EMAIL*, etc) estejam em uma sub-rede separada das demais e de acesso restrito, conhecido como DMZ (zona desmilitarizada). Outra recomendação é o uso de *firewalls* internos uma vez que um *firewall* protege contra acessos externos, nada podendo fazer contra ataques que partem da rede interna.

Um outro serviço útil é o *proxy*, que conforme Uchôa (2003) "é um *software* que atua como ponto entre duas redes, controlando o tráfego de acordo com seu conteúdo. Em geral, um *proxy* é utilizado para servir como *cache* WWW ou FTP, mas pode ser utilizado para filtrar a rede, de forma que pode ser

usado como *firewall*."

Um *proxy* pode ser programado para que apenas alguns usuários ou estações tenham acesso aos recursos da *web* ou para que se determinem políticas de acesso aos usuários. Isso faz com páginas com conteúdos indesejáveis, como sexo, páginas de esporte, páginas para *download* de arquivos de música não sejam acessadas.

Conforme NBSO (2002), deve-se evitar na medida do possível protocolos sem criptografia (POP3, FTP, IMAP, TELNET). Protocolos onde não haja autenticação através de senhas ou onde as senhas trafegam em claro devem ser substituídos por outros que corrijam o problema.

Uma solução seria usar o SSH, uma vez que ele faz com que o tráfego entre cliente e servidor seja criptografado. Em relação ao POP3 seria usar o POP seguro, ou seja, uma variante (APOP, KPOP, RPOP) deste protocolo que elimina o tráfego de senhas em claro, tornando a autenticação de usuários mais segura. O problema é que nem todos os clientes de *email* suportam estas variantes. Para finalizar, também poderia ser usado *WebMail* combinado com HTTPS (HTTP+SSL) e ao invés de FTP anônimo, SFTP (Uchôa, 2003).

5. CONSTRUÇÃO DA POLÍTICA DE SEGURANÇA

5.1 COMENTÁRIOS INICIAIS

A política de segurança é um conjunto de diretrizes que expressam as regras que devem ser seguidas para se ter acesso aos recursos tecnológicos da empresa. Segundo Uchôa (2003), é a política que define o que deve ter acesso restrito e o que pode ser liberado e, também, quais as pessoas que terão acesso a certos recursos.

Atualmente, as empresas apresentam como bem muito valioso suas informações. A política tem por objetivo proteger essas informações mostrando aos usuários que as utilizam qual a filosofia da empresa sobre este patrimônio.

Um conjunto de normas precisa ser observado na elaboração da política, como comentado nos itens anteriores. Conforme Uchôa (2003), é imprescindível que na política conste itens como segurança física, lógica, privacidade dos usuários e legalidade dos programas utilizados.

Como citado em Caruso & Steffen (1999), a política de segurança é composta por documentos importantes como plano de contingência e a política de uso. Estes documentos serão comentados nos itens 5.2 e 5.3, respectivamente. Como sugestão de leitura o autor deste trabalho recomenda Caruso; Steffen (1999), Uchôa (2003), Cronkhite; McCullough (2001) e Schetina; Green; Carlson (2002).

5.2 PLANO DE CONTINGÊNCIA

Contingência é a incerteza que alguma coisa possa acontecer ou não. Segundo Caruso & Steffen (1999), um fato gerador da contingência é um evento que faz com que os sistemas de informação fiquem indisponíveis por um período, ocasionando prejuízos para a empresa.

Um plano de contingência consiste em procedimentos de recuperação definidos previamente, tendo por finalidade minimizar os impactos gerados sobre a empresa em caso de algum dano ou desastre acontecer.

O plano de contingência serve como guia para tomar decisões em relação às ações que deverão ser executadas para dar continuidade aos serviços essenciais da organização.

O restabelecimento da capacidade de operação do CPD está diretamente ligado à avaliação periódica que sofre. Assim, obviamente, não se esperam contingências acontecerem mas testam-se suas condições de ocorrência sob determinadas hipóteses. As falhas encontradas servem para atualizar o Plano.

5.2.1 Metodologia de um Plano de Contingência

Segundo Caruso & Steffen (1999) a elaboração de um plano de contingência se resume nos seguintes passos:

- Equipe de planejamento da contingência: deve incluir representantes de todas as áreas que possam ser afetadas. Deve envolver pessoal do suporte técnico, desenvolvimento de sistemas, usuários, comunicação, etc;
- Avaliação das atividades e dos sistemas prioritários: a equipe deve selecionar os principais sistemas e atividades, ou seja, aqueles que a empresa não pode ficar sem em hipótese alguma;
- Lista de pessoal necessário para o processamento e suporte aos sistemas que são prioritários;
- Equipamentos necessários;
- Dados, *software* e documentação necessária;
- Manuais de contingência: documentação relativa aos procedimentos que devem ser seguidos. É de fundamental importância que este documento seja sempre atualizado;
- Realização contínua dos *backups;*

- Testes de contingência periódicos: nesses testes é que se descobrem os principais problemas que poderiam causar impactos em uma situação real.

Como já foi dito anteriormente, a segurança não é um produto que pode proteger 100% a empresa e sim um processo que deve ser aprimorado dia após dia. Então, é necessário que cada membro de uma empresa siga as regras estabelecidas na política de segurança e dê sua parcela de contribuição para manter os serviços de informática, pois a falta destes serviços pode acarretar problemas sérios e até prejuízos irreparáveis para organização.

5.3 POLÍTICA DE USO: AS RESPONSABILIDADES DO USUÁRIO

Uma política de uso tem por princípio informar aos usuários do sistema computacional suas obrigações para proteção da tecnologia e o acesso às informações. Tal política é um documento que será assinado pelo usuário, assim ele estará manifestando sua concordância com as regras impostas.

Segundo Uchôa (2003), a política de uso é um documento definido pela política de segurança a qual deve definir claramente as áreas de responsabilidade para usuários e administradores do sistema, bem como as sanções que serão impostas caso as regras de uso sejam violadas.

5.3.1 Regulamento de Uso dos Recursos Computacionais

O regulamento tem por finalidade estabelecer a política de uso dos recursos computacionais da empresa. Para tanto, primeiro é necessário estar definido em tal documento quem será o responsável pela gestão dos sistemas de informação bem como dos recursos computacionais.

Os recursos computacionais são os equipamentos, as instalações e bancos de dados, mantidos ou operados pela empresa , tais como:

- computadores e terminais de qualquer espécie;

- impressoras;
- dispositivos de redes;
- bancos de dados ou documentos residentes em disco, CD ou outros meios;
- salas de computadores, mobiliário, material de consumo e periféricos.

Conforme citado em ETF (2005), o usuário é qualquer pessoa, desde que empregado, autorizada a utilizar os recursos da empresa. Em relação ao uso dos equipamentos, cabem aos usuários tais responsabilidades:

- Autorização Apropriada - Para utilizar os recursos da rede interna de computadores da empresa, o usuário deve antes assinar o Termo de Responsabilidade, no qual declara conhecer as diretrizes em vigor e se compromete a cumpri-las;
- Responsabilidade pela Conta - Toda conta é de responsabilidade e de uso exclusivo de seu titular, não podendo esse permitir ou colaborar com o acesso aos recursos computacionais da empresa por parte de pessoas não autorizadas;
- Alteração de dados ou de equipamentos - Os usuários, a menos que tenham uma autorização específica para esse fim, não podem tentar, permitir ou causar qualquer alteração ou destruição de ambientes operacionais, dados ou equipamentos de processamento ou comunicações instalados na empresa, de sua propriedade ou de qualquer outra pessoa ou organização;
- Uso ético - Não é permitido aos usuários, utilizar os recursos de modo dissociado das atividades administrativas a que se destinam (por exemplo: jogos, atividades comerciais ou que visem lucros próprios, "*chat*", entre outros), bem como, exibir na tela do monitor qualquer matéria que, mesmo não caracterizando ilícito penal, provoque constrangimento aos demais usuários ou sejam incompatíveis com o ambiente de trabalho;
- Prejuízos a terceiros - Os recursos computacionais da empresa não podem ser utilizados para constranger, assediar ou ameaçar qualquer pessoa. Esses recursos não podem ser usados para alterar ou destruir recursos

computacionais de outras empresas;

- Os recursos computacionais da empresa não podem ser utilizados para acessar ou promover a divulgação de material (texto, som ou imagem) de caráter ofensivo de qualquer natureza, de caráter sexualmente implícito e/ou explícito ou que divulgue atividades ilegais. É proibido praticar qualquer tipo de discriminação relativa à raça, sexo ou credo religioso. Como, também manter links para páginas com este tipo de conteúdo;
- Correntes de cartas e outras comunicações eletrônicas indesejadas - É proibida a distribuição voluntária ou desapercebida de mensagens não desejadas, como circulares, correntes de cartas ou outros esquemas que possam prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar os sistemas computacionais;
- Remoção de documentos - Sem uma autorização específica, os usuários não podem remover dos recursos computacionais nenhum documento de propriedade da empresa ou por ela administrado;
- Direitos Autorais - Os usuários devem respeitar os direitos de propriedade intelectual, em particular a lei de direitos autorais de *software*;
- Contratos - Todo e qualquer uso dos recursos computacionais deve estar de acordo com todas as obrigações contratuais da empresa, inclusive com as limitações definidas nos contratos de *software* e outras licenças.

Nas instalações da empresa usuários dos recursos computacionais devem permitir identificar-se sempre que solicitado, apresentando documento ou autorização especial do pessoal responsável, sob pena de imediata suspensão da conexão.

Em relação ao acesso aos dados, deve ser garantido o maior grau possível de confidencialidade no tratamento dos dados dos usuários, de acordo com as tecnologias disponíveis. Entretanto, os administradores de redes poderão acessar arquivos de dados pessoais ou corporativos nos sistemas da empresa sempre que isso for necessário para *backups* ou diagnóstico de problemas nos

sistemas, inclusive nos casos de suspeita de violação de regras.

Sob o ponto de vista da segurança de uso dos recursos computacionais, cabem aos usuários as seguintes responsabilidades (ETF, 2005):

- Os usuários não podem se fazer passar por outra pessoa ou camuflar sua identidade quando utilizam os recursos computacionais da empresa com exceção dos casos em que o acesso anônimo é explicitamente permitido;
- Os usuários não devem, deliberadamente, efetuar ou tentar qualquer tipo de acesso não autorizado a dados dos recursos computacionais, ou tentar sua alteração, como, por exemplo, ler mensagens pessoais de terceiros ou acessar arquivos confidenciais da empresa;
- Os usuários não podem violar ou tentar violar os sistemas de segurança dos recursos computacionais da empresa, como quebrar ou tentar adivinhar identificação ou senhas de terceiros;
- Os usuários não podem interceptar ou tentar interceptar transmissões de dados não destinados ao seu próprio acesso, monitorando barramentos de dados ou seja através da rede;
- Os usuários são responsáveis pela segurança de suas contas e de suas senhas. A conta e a respectiva senha são atribuídas a um único usuário e não devem ser compartilhadas com mais pessoas;
- Comunicação de Violação - Os usuários devem comunicar ao Administrador da rede local qualquer evidência de violação das normas em vigor, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros;
- O usuário suspeito de violação dessas normas será notificado da acusação e terá oportunidade de se pronunciar antes da decisão da pena pelo setor e/ou pessoa responsável;
- As penalidades a serem aplicadas por infração às normas vão desde uma simples advertência à demissão do emprego.

5.4 TERMO DE RESPONSABILIDADE

Conforme Uchôa (2003), a forma de garantir uma validade jurídica ao documento que regula o uso dos recursos computacionais é através da assinatura do usuário em um termo de responsabilidade, onde ele declara ter pleno conhecimento das normas vigentes ao uso dos recursos da empresa.

Neste termo ele assumirá todas as responsabilidades decorrentes do uso de sua conta e declarará ter ciência de todas as sanções que poderá sofrer caso viole as normas de uso.

O usuário deverá também, assumir o compromisso de acompanhar as eventuais mudanças que por ventura venham a ocorrer no regulamento de uso dos recursos computacionais. Um exemplo de termo de responsabilidade pode ser verificado na figura 5.1.

Termo de Responsabilidade

Eu, _____ - _____(cargo que ocupa), assumo todas as responsabilidades decorrentes do uso da conta_____ de acesso à Rede interna e *Webmail* da _____(empresa) e declaro ter pleno conhecimento dos termos e condições explicitados ou referidos pelo regulamento de uso dos recursos computacionais amplamente divulgados e de conhecimento público, o qual deverá reger as relações entre a Administração da Rede da EmpresaX e os seus usuários.

Assumo também o compromisso de acompanhar as eventuais mudanças a serem feitas no documento que regulamenta o uso dos recursos computacionais o qual poderá ser alterado pelo_____(setor/pessoa responsável) a qualquer tempo, com ampla divulgação nos meios eletrônicos.

Local e Data

_____

Assinatura

Figura 5.1 – Termo de Responsabilidade

6. CONSIDERAÇÕES FINAIS

Com o intuito de proteger suas informações e seus recursos computacionais as empresas criam regras (Política de Segurança) que devem ser seguidas por todos os seus integrantes. Tal política deve estar voltada para itens como segurança física dos recursos tecnológicos, segurança lógica dos dados e privacidade em relação aos dados do usuário.

A segurança das informações é vital para a sobrevivência de qualquer organização. Ainda mais nos dias de hoje, quando as empresas se lançaram no mundo virtual fazendo com que suas informações se tornassem o bem mais precioso.

Proteger-se de *hackers,* vírus e outras ameaças é importante e um ponto que deve ser lembrado é que a segurança deve ser encarada como um processo contínuo de aperfeiçoamento. Com isso, os agentes envolvidos devem estar atentos a possíveis brechas na segurança para que dessa forma seja possível corrigi-las o mais rápido possível.

Sendo assim, este trabalho teve como principal meta discutir a respeito de diretrizes gerais que devem ser observadas na hora de proteger os ativos de uma organização. Com isso, o autor espera que este trabalho possa servir como guia de pesquisa na elaboração de projetos que envolvam a segurança dos recursos computacionais de qualquer instituição.

Desta forma, pretende-se que ao ser elaborada uma política de segurança seguindo as normas aqui apresentadas, isso traga como benefício para a instituição uma redução na probabilidade de ocorrências. Mas, caso incidentes venham a ocorrer, que haja uma redução dos danos causados por eles.

7. REFERÊNCIAS BIBLIOGRÁFICAS

CARUSO, Carlos A. A., STEFFEN, Flavio Deny. *Segurança em Informática e de Informações*. São Paulo: Senac/SP, 1999. 366p.

GEUS, Paulo Lício de; NAKAMURA, Emílio Tissato. *Segurança de Redes em Ambientes Cooperativos*. São Paulo: Futura, 2003. 472p.

WADLOW, Thomas A; tradução Fabio de Freitas da Silva. *Segurança de Redes: projeto e gerenciamento de redes seguras*. Rio de Janeiro: Campus, 2000. 269p.

UCHÔA, Joaquim Quinteiro. *Segurança em Redes e Criptografia*. Lavras: UFLA/FAEPE, 2003. (Curso de Pós-Graduação "Latu Sensu" (Especialização) a Distância: Administração em Redes Linux). 59p.

UCHOA, Kátia Cilene Amaral, ALVES, Rêmulo Maia. *Introdução à Cibercultura*. Lavras: UFLA/FAEPE, 2002. (Curso de Pós-Graduação "Latu Sensu" (Especialização) a Distância: Administração em Redes Linux). 106p.

SICA, Fernando Cortez; UCHOA, Joaquim Quinteiro. *Administração de Sistemas Linux*. Lavras: UFLA/FAEPE, 2003. (Curso de Pós-Graduação "Latu Sensu" (Especialização) a Distância: Administração em Redes Linux). 150p.

NIC BR Security Office (NBSO). *Práticas de Segurança para Administradores de Rede Internet.(2002)* [on-line]. Disponível na Internet via www. url: `http://nbso.nic.br/`. Arquivo capturado em 01 de março de 2005.

NIC BR Security Office (NBSO). *Cartilha de Segurança para Internet.(2003)* [on-line]. Disponível na Internet via www. url: `http://nbso.nic.br/docs/cartilha`. Arquivo capturado em 01 de março de 2005.

Escola Técnica Federal de Palmas. *Regulamento de Uso dos Recursos Computacionais.* [on-line]. Disponível na Internet via www. url: `http://www.etfto.gov.br/documentos`. Arquivo capturado em 24 de maio de 2005.

SCHETINA, Erik; GREEN, Ken; CARLSON, Jacob; tradução de Altair Dias Caldas de Moraes. *Sites Seguros: aprenda a desenvolver e construir.* Rio de Janeiro: Campus, 2002. 436p.

CRONKHITE, Cathy; McCULLOUGH, Jack; tradução Daniel Vieira. *Hackers, acesso negado.* Rio de Janeiro: Campus, 2001. 253p.