UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

CRISTIANO MONTEIRO LEITE

POLÍTICAS DE SEGURANÇA FÍSICA E LÓGICA EM AMBIENTES INSTITUCIONAIS QUE UTILIZAM TECNOLOGIA DA INFORMAÇÃO

MONOGRAFIA

CURITIBA
2011

CRISTIANO MONTEIRO LEITE

POLÍTICAS DE SEGURANÇA FÍSICA E LÓGICA EM AMBIENTES INSTITUCIONAIS QUE UTILIZAM TECNOLOGIA DA INFORMAÇÃO

Monografia apresentada como requisito parcial à obtenção do título de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Augusto Foronda

CURITIBA

2011

AGRADECIMENTOS

Agradeço as pessoas que de alguma maneira contribuíram com incentivos, atitudes e me apoiaram até o presente momento.

Agradeço a DEUS não pelo que tenho mais sim por quem ele é na minha vida! "Pela intercessão de São Miguel Arcanjo e do Coro Celeste dos Arcanjos, o Senhor nos conceda o dom da perseverança na fé e boas obras."

Aos meus pais, Heleno e Vanda, e irmão, Luciano, pela demonstração de paciência, amor, carinho e alegria que despertam em meu coração quando lembro da sua existência. Por instruir e educar para que os valores da vida, como respeito e dignidade possam ser realidades no meu dia a dia.

A Samantha Reikdal Oliniski, por ser esta pessoa tão especial a quem tenho imensa admiração pela disposição, competência, inteligência, solidariedade, simplicidade, carinho e incentivo, que me faz sentir motivação para buscar novos objetivos na vida.

Ao Professor e orientador Dr. Augusto Foronda, por dedicar seus ensinamentos e colaborar para realização deste trabalho.

Aos colegas de profissão em especial, Luiz domingos Caleffi, Denise Grossi, Alexandre Batista, Roberson Araújo, Antonio Oliveira, Simone Cassemiro, Andre Avila Kaminski, Rodrigo Gusso, Luiz Fabricius, Frederico T. Martins, Andre de Barros, Flavio Mildenberg, Pablo, Altair Baptista.

“Nunca deixe que lhe digam que não vale à pena acreditar no sonho que se tem ou que seus planos nunca vão dar certo ou que você nunca vai ser alguém” Renato Russo.

RESUMO

LEITE, Cristiano Monteiro. **Políticas de segurança física e lógica em ambientes institucionais que utilizam tecnologia da informação**. 2011. 35 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Rede) – Universidade Tecnológica Federal do Paraná, Curitiba, 2011.

Esta é uma pesquisa explicativa aplicada a respeito de políticas de segurança para ambientes empresariais, na qual será utilizado o método bibliográfico. O objetivo deste trabalho é descrever diretrizes de segurança física e lógica para os ambientes institucionais que utilizam recursos de tecnologia de informação, de modo que possam por meio destas implantar ou implementar uma política de segurança e assim proteger seus equipamentos e informações. Com isso pretende-se minimizar a vulnerabilidade dos equipamentos e ativos de TI de meio físico e lógico, uma vez que o desvio ou perda de informações por falta de segurança pode comprometer o desempenho das atividades realizadas pelas instituições e conseqüentemente seu desenvolvimento econômico e financeiro. Além disso, profissionais de TI e instituições poderão aplicar estas diretrizes em seu ambiente profissional, podendo proteger seu patrimônio de avarias e furtos.

Palavras-chave: Segurança de TI. Segurança física e lógica. Segurança em ambientes institucionais. Tecnologia da Informação.

ABSTRACT

LEITE, Cristiano Monteiro. **Physical and logical security policies in institutional environments that use information technology.** 2001. 35 p. Monograph. (Specialization Curse in Management and Configuration of Servers and Network Equipment) – Universidade Tecnológica Federal do Paraná, Curitiba, 2011.

This is an explanatory and applied research about security policies to business environment, in which the bibliographic method was used. The aim of this paper is to describe guidelines of physical and logical security to institutional environments that use resources of information technology, in such way through these they can apply or implement a security policy and thus protecting their information and equipments. This way is intended to minimize the vulnerability of equipments and information technology assets of physical and logical means, since the deviation or loss of information due to lack of security can compromise the performance of activities undertaken by the institutions and therefore its economic and financial development. In addition, institutions and professionals of information technology will be able to apply these guidelines in their professional environment, and so protecting their assets from damage and theft.

Key words: Security of information technology. Physical and logical security. Security in institutional environments. Information Technology.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Neste capitulo é apresentado o tema da pesquisa: políticas de segurança física e lógica em ambientes institucionais que utilizam tecnologia da informação (TI).

1.1 TEMA

Em virtude da grande disseminação de recursos de Tecnologia da Informação (TI) pode-se enfatizar o aumento significativo das informações armazenadas, valorização dos recursos arquivados e utilizados pelas instituições. Diante de um cenário em grande ascensão e necessidade de utilizar os recursos de TI, não se deve esquecer ou deixar de se preocupar com a segurança que se deve aplicar a configurações lógicas e a infraestrutura física utilizada para acessar estas informações.

Ao refletir qual é o alicerce para produção de um produto, pesquisa, desenvolvimento ou aquisição de matéria prima a fim de suprir o ciclo de fabricação de um produto, normalmente estão relacionados valores como: criticidade, investimento, conhecimento, informação e mão de obra qualificada. Para que se possam colocar em prática as aplicações das atividades avaliando o objetivo principal das organizações com ou sem fins lucrativos é de suma importância o valor da informação, para que desta forma se possa atingir o objetivo principal de cada empresa, assim como, prospecto para crescimento e permanência destas no mercado.

Para Moresi (2000, p. 14) a importância da informação para as organizações se constitui um dos recursos mais importante e diretamente relacionado ao sucesso do empreendimento. De acordo com o autor ela também é considerada e utilizada como um fator estruturante e um instrumento de gestão. Para ele “a gestão efetiva de uma organização requer a percepção objetiva e precisa dos valores da informação e do sistema de informação”.

Este estudo visa descrever como identificar e assegurar que os recursos (TI) disponibilizados dentro de uma instituição, possam ser utilizados com uma política

básica de segurança em tecnologia da informação, para que o impacto destes acessos indevidos, infiltrações e roubos sejam minimizados no ambiente institucional. Uma política de segurança bem estruturada e aprovada pelos gestores e ou responsáveis pode prevenir a entrada e a saída de pessoas, de recursos e de informações inadequadas com grau de criticidade delimitada no ambiente em questão. As definições sobre o trabalho apresentado se limitam a indicações de procedimentos de segurança, devendo ser avaliado o grau de risco físico, lógico e vulnerabilidade dos ativos de (TI) para cada instituição.

1.2 PROBLEMA

A vulnerabilidade em ambientes institucionais que os equipamentos de TI e acessos às informações de instituições sofrem quando não há uma política de segurança definida ou ainda quando esta possui déficits estruturais. Com isso é necessário que as empresas invistam adequadamente em segurança de TI; para que assim não percam, além dos investimentos em recursos materiais e financeiros, informações essenciais para gestão e realização de suas tarefas.

1.3 OBJETIVOS

Nesta sessão são apresentados os objetivos geral e específicos do trabalho.

1.3.1 Objetivo geral

Descrever diretrizes de ações de segurança física e lógica para os ambientes institucionais que utilizam recursos de tecnologia de informação, de modo que se facilite a implantação ou a implementação de uma política de segurança e assim haja a proteção dos seus equipamentos e informações.

1.3.2 Objetivos específicos

- Identificar as principais vulnerabilidades descritas na literatura científica a que estão submetidos os recursos de TI;

- Selecionar os itens de maior relevância para aplicação de políticas de segurança sob o aspecto físico em ambientes institucionais;
- Selecionar os itens de maior relevância para aplicação de políticas de segurança sob o aspecto lógico em ambientes institucionais;
- Descrever as diretrizes básicas de segurança da estrutura física que se aplicam aos ambientes institucionais que utilizam recursos de TI;
- Descrever as diretrizes básicas de segurança da estrutura lógica que se aplicam aos ambientes institucionais que utilizam recursos de TI.

1.4 JUSTIFICATIVA

Em virtude da crescente utilização e aplicação de recursos de TI no cotidiano há necessidade de assegurar que as informações contidas ou enviadas, bem como os equipamentos utilizados não sofram ataques ou violações por terceiros. Com a ascensão deste uso as empresas confiam aos recursos de TI à facilitação de seus processos produtivos, da comunicação e do armazenamento de informações. Tais aplicações apresentam relevância em função de seu teor e funcionalidade utilizados nas instituições, ou seja, possuem grande valor para a empresa, pois é por meio deles que as informações são mantidas e guardadas.

O valor da informação está relacionado ao tipo de dado gerado ou armazenado pelos recursos de TI e ao sigilo empresarial ou segredo industrial que envolve a marca ou processo. Por exemplo, quanto vale a fórmula de um refrigerante, cosmético ou sistema de informação? Ou então qual o lucro que uma indústria automobilística teve no último ano? Ou ainda quanto vale uma planilha com balanço financeiro e outras informações contábeis de um banco? Certamente, para seus donos e acionistas estas informações têm muito valor. Afinal, o acesso de uma destas informações por um concorrente ou a perda de dados utilizados em processos internos pode representar prejuízos e danos imensuráveis, seja sob o aspecto financeiro ou comercial.

Portanto, quando se tem diretrizes de segurança física e lógica as instituições podem aplicá-las na prática, de modo eficaz e efetivo, e com isso proteger seu patrimônio financeiro e de informações. Além disso, com a aplicação de

uma política de segurança é possível aumentar a produtividade das empresas, pois com o controle e monitoramento das informações se restringe o acesso à conteúdos impróprios e de fins empresariais.

1.5 PROCEDIMENTOS METODOLÓGICOS

Esta é uma pesquisa explicativa aplicada a respeito de políticas de segurança para ambientes empresariais. Quanto ao método é predominantemente bibliográfico. Foram utilizados como fontes de pesquisa livros, artigos científicos, revistas, normas técnicas, internet, catálogos de fabricantes e outros. Além disso, foram investigadas políticas de segurança em algumas instituições, as quais serviram de campo de pesquisa.

Foram utilizadas as frases: segurança em TI, segurança em ativos de rede, políticas de segurança em TI, vulnerabilidade de equipamentos de TI; como descritores ou palavras-chave para a pesquisa em meios eletrônicos e bases de dados científicos. Foram selecionados como fontes de pesquisa os materiais publicados entre 2000 e 2011.

2 EMBASAMENTO TEÓRICO

A política de segurança deve ser estabelecida visando à prevenção de incidentes, inviabilizando acessos indevidos, risco aos equipamentos e a estrutura lógica dos ativos de TI.

Considerando os fatos atuais em que existem diversas formas de criminalidades, não se pode deixar de citar os crimes cibernéticos (fraudes que utilizam recursos de eletrônica ou TI), que de um modo geral estão cada vez mais presentes no cotidiano. Dentre as de operações mais comuns a serem fraudadas se destacam o acesso às contas bancárias, desvios de informação e invasão de computadores.

Devido à facilidade em acessar equipamentos de informática e à grande evolução de conhecimento técnico, estas fraudes estão se disseminando, pois normalmente tornam-se lucrativa delimitando assim um grande investimento. Os especialistas em crimes cibernéticos possuem uma visão estratégica e planejamento para aplicar golpes e lesionar ose concorrentes do mercado comercial, afinal uma simples falha de segurança pode representar uma infiltração e conseqüentemente o roubo de informação ou falha no procedimento habitual das instituições.

A Gestão de Segurança da Informação é “a ação que protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio” (ABNT ISO/IEC 17799).

No entanto, a política de segurança “não define procedimentos específicos de manipulação e proteção da informação, mas atribuem direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação” (MENEGUITE, 2010, p. 14). Por meio destas definições as pessoas podem saber as expectativas e atribuições que lhe cabem em relação aos riscos a que as informações estão submetidas. Mediante a documentação e aprovação de uma política de segurança é possível estabelecer também penalidades aos usuários dos recursos de TI.

Um dos aspectos fundamentais para o planejamento e implementação de uma política de segurança é a avaliação de risco, valores e vulnerabilidades. A vulnerabilidade é definida como um “ponto potencial de falha, ou seja, um elemento relacionado à informação que é passível de ser explorado por alguma ameaça”. Esta

ameaça pode estar relacionada a um servidor, sistema computacional, instalação física, usuário ou gestor de informações (MARCIANO, 2006, p. 49).

Para compreensão do tema são apresentadas a seguir algumas sessões que tratam especificamente dos principais enfoques relacionados à segurança de redes de informação.

2.1 INFRAESTRUTURA FÍSICA EM TI

Para utilizar os recursos de informatização de maneira eficaz e correta é necessário manter os dispositivos de *hardware* e ativos de redes de forma segura e restrita. Muitas vezes a facilidade no acesso aos ativos de rede deixa uma grande vulnerabilidade ao sistema de informação. Desta forma, as informações podem ser capturadas de maneira indevida ou até mesmo sofrer uma sabotagem aos recursos de TI.

Dentre os maiores riscos e preocupações relacionados à rede de informação pode-se citar:

- Roubos e furtos;
- Sabotagem e vandalismo;
- Sequestro e chantagem;
- Terrorismo ideológico ou criminoso;
- Problemas em sistemas de suporte como ar-condicionado e ventilação;
- Fogo e fumaça;
- Vazamentos de água e enchentes;
- Fenômenos climáticos como vento, chuva, granizo, neve ou furacões;
- Desmoronamento de prédios.

Diante da necessidade em manter uma segurança e conforto para os administradores e gestores da organização, deve-se indicar que os equipamentos sejam mantidos protegidos contra qualquer acesso indevido e não autorizado. No entanto, também é importante manter com segurança o fluxo de passagens de cabos lógico e elétrico, obedecendo às normas específicas e de forma inacessível aos usuários e visitantes da empresa.

Recomenda-se observar os seguintes aspectos quanto às ameaças ambientais e acesso não autorizado:

a) Instalação dos equipamentos de modo que o acesso à área de trabalho seja reduzido;
b) Posicionamento dos equipamentos que processam e armazenam informações sensíveis de maneira a reduzir os riscos de espionagem durante o uso;
c) Isolamento dos itens que precisam de proteção especial de forma a reduzir o nível de proteção exigida;
d) Adoção de controles para minimizar ameaças potenciais como roubo, fogo, explosivos, fumaça, água, poeira, vibração, efeitos químicos, fornecimento elétrico e radiação eletromagnética;
e) Adoção de políticas organizacionais relacionadas à alimentação, bebida e fumo nas proximidades das instalações de processamento da informação;
f) Monitoramento de aspectos ambientais para evitar situações que afetem de modo adverso o funcionamento dos equipamentos de TI;
g) Uso de proteção especial, como capas para teclados, para os equipamentos instalados em ambiente industrial; e
h) Adoção de estratégias que reduzam o impacto de desastres (incêndios, vazamento de água, explosões) nas proximidades das instalações de TI (SALGADO, BANDEIRA E SANCHES DA SILVA, 2004).

Outra ação que deve ser adotada é a instalação de um sistema de monitoramento, com gravação e se possível um dispositivo de alarme 24h. Estas imagens devem ser armazenas e arquivadas somente por uma pessoa ou equipe autorizada, e as informações devem ser registradas e repassadas aos responsáveis.

Os equipamentos devem estar alojados dentro de uma estrutura adequada para armazenamento com fechadura e ou acesso controlado, como por exemplo, *rack* e *brackets*. Deve-se também respeitar a temperatura de funcionamento e condicionamento indicada pelo fabricante do equipamento.

Esta prática de condicionamento se faz necessária para manter um bom funcionamento e performance do equipamento, e desta forma garantir a durabilidade e garantia ofertada de acordo com as exigências do fabricante. Para avaliar o tempo médio em que o aparelho pode apresentar falhas deve se observar o MTBF (*Mean Time Between Failure*), ou seja, tempo médio entre falhas, que é um número que indica a confiabilidade de um equipamento. Assim, quanto maior for este número, melhor é o desempenho do equipamento. De acordo com o guia de *switches* da Cisco (2006) é demonstrado na tabela abaixo a especificação do equipamento que contém informações referentes aos modelos de *switches* e a característica requerida do MTBF.

Especificações

Característica	WS-C2950-12	WS-C2950-24	WS-C2950C-24	WS-C2950SX-48-SI
Switching Fabric	8.8 Gbps	8.8 Gbps	8.8 Gbps	13.6 Gbps
Forwarding Bandwidth	2.4 Gbps	4.8 Gbps	5.2 Gbps	13.6 Gbps
Forwarding Rate	1.8Mpps	3.6Mpps	3.9 Mpps	10.1 Mpps
DRAM Memory	16MB	16MB	16MB	32MB
Macs	8.000 macs	8.000 macs	8.000 macs	8.000 macs
MTBF	482,776 horas	398,240 horas	477,080 horas	274,916 horas
Portas	12 10/100	24 10/100 + 2 100 BaseFX	24 10/100 + 2 10/100/1000BaseFX	48 10/100 + 2 1000Base-SX

Figura 1 – Especificação do MTBF para *switches* Cisco.
Fonte: Cisco, 2006.

Desta forma, enfatiza-se a importância de manter os equipamentos como *Hub, Switches, Router* e *Access Point* entre outros ativos de redes de maneira adequada, condicionada, restrita e monitorada.

Considerando o grande número de ataques e tentativas de acessos indevidos, infiltrações e vírus na internet, é fundamental a utilização de mecanismos para bloquear e proteger a rede interna contra aplicativos prejudiciais aos sistemas de informação como: vírus, *trojan, spywares, keylogger,s* entre outros *malwares*, que podem paralisar, capturar informações ou causar falhas nos sistemas. Para isso é necessário manter uma solução de antivírus atualizada e com mecanismos

eficientes para combater as diversas formas de ataques e ameaças encontradas nos sítios e arquivos disponíveis na internet.

Atualmente existem algumas maneiras de criar barreiras, “filtros” de acesso da rede externa para rede interna. Os meios mais comuns e utilizados na segurança de TI são regras de bloqueio no acesso à pacotes, portas e protocolos como, por exemplo: HTTP, TCP, UDP, entre outros. Os equipamentos chamados de *firewall* são utilizados para gerenciar e criar estas barreiras entre a rede externa para rede interna tem como finalidade bloquear através de regras aplicadas no seu sistema de gerenciamento o acesso indevido da rede externa (internet) para a rede interna.

É possível encontrar algumas formas de utilizar o dispositivo de *firewall*, pode ser um computador normal utilizando um sistema operacional, como *ipchains* ou *iptables*, com as funções e regras para bloqueio e liberação de portas e protocolos de acesso à internet; duas placas de rede para ter acesso externo e interno para acessar a rede; ou um equipamento fisicamente projetado para realizar tal função, chamado de *appliance*. Existem diversos fornecedores e fabricantes de *firewall*, os mais conhecidos são: Pix Firewall (Cisco), Sonic Wall,Checkpoint.

Pequenas e médias empresas observaram que as principais ferramentas e técnicas para a gestão de segurança são: antivírus, sistema de *backup* e *firewall* (SILVA NETTO E SILVEIRA, 2007).

Para proteção do patrimônio investido pelas empresas devem ser adotados alguns padrões e políticas com relação aos investimentos de TI. Todo equipamento *desktop* deve ser instalado e remanejado somente pela equipe de TI ou caso necessário a remoção por outra pessoa, esta deve solicitar e receber autorização formal para executar tal procedimento, sob pena de advertência verbal, escrita ou demissão de acordo com a política de segurança estabelecida pela empresa. Os equipamentos devem ser identificados, instalados e adequados ao ambiente de maneira que permaneçam fixos e com lacre nos gabinetes, evitando desta maneira o acesso aos dispositivos de *hardware* como: memória, disco rígido, processador e leitores de mídias.

Os equipamentos portáteis devem ter atenção redobrada com relação à segurança física e lógica, uma vez que normalmente não permanecem somente nas dependências internas da empresa. Assim como nos *desktops,* os *notebooks* devem possuir lacres adequados, senhas para acesso ao disco de armazenamento (HD) e criptografia dos dados. Os funcionários devem ter permissão formal dos

responsáveis para entrar e sair com os equipamentos da empresa, o documento deve conter informações como: data de saída, entrada, localização na empresa e o responsável.

Caso o funcionário necessite deslocar o equipamento diariamente da empresa, deve ser estabelecido na política de segurança da empresa um documento mensal ou trimestral. Outro item importante que deve ser estabelecido pela equipe de TI é a política de *backup,* pois devido ao deslocamento dos funcionários é maior a probabilidade e risco de furto, cabendo a TI intensificar a cópia das informações destes equipamentos a fim de prevenir e minimizar o impacto com grandes perdas de informações.

Recomenda-se observar os seguintes aspectos com equipamentos que são utilizados fora da instituição:

a) Não deixar os equipamentos e mídias desprotegidos em áreas públicas. Carregar os computadores portáteis como bagagem de mão e disfarçados quando utilizados em viagens;
b) Seguir as instruções dos fabricantes para proteção dos equipamentos, como por exemplo, proteção contra exposição a campos magnéticos intensos;
c) Determinar medidas para trabalho em casa por meio da avaliação de risco e controles apropriados de acordo com a necessidade, como gabinetes de arquivo fechados, política de mesa limpa e controle de acesso aos computadores;
d) Ter uma cobertura de seguro para proteger estes equipamentos (SALGADO, BANDEIRA E SANCHES DA SILVA, 2004).

2.2 INFRAESTRUTURA LÓGICA EM TI

Partindo da política de segurança estabelecida pela empresa, acredita-se que o administrador de rede deve ser o único a ter acesso completo a todas as informações, com exceção das solicitações formalizadas através dos diretores e proprietários, ou seja, todo acesso à rede e aos dispositivos de TI devem ser realizado através de autenticação para acessar os diretórios compartilhados. O

objetivo da segurança lógica é proteger as informações, sistemas, programas e aplicativos de acessos indevidos e não autorizados.

É fundamental “avaliar (quando, quem, como), relatar (eventos, ocorrências e situações) e agir (reforçar, implementar e rever medidas)” para segurança em informática sistemática e lógica empresarial. Não se deve deixar intrusos acessar os dados armazenados, caso estes sejam acessados não se deve deixar utilizá-los e que a monitoração das ocorrências é fundamental (CRUDO et al, 2005, p. 4)

O administrador deve atribuir uma rotina de alteração da senha nos equipamentos utilizados na rede. Devido ao grande número de softwares e aplicativos para identificação e intrusão às redes de comunicações, deve-se adotar a prevenção e alteração de senhas periodicamente dos equipamentos que compõe os ativos de rede como: servidores, *hub, switches, router, access point,* entre outros.

As senhas devem ser alteradas em um período médio de 15 dias, podendo o administrador criar um procedimento e registro das alterações de acordo com o seu conteúdo. O cadastro e alteração ideal da senha de acesso devem ser estabelecidos de acordo com sistema utilizado pelo fabricante.

Para realizar o cadastro das senhas é aconselhável não utilizar senhas com fácil vinculo de descoberta como: número do RG, CPF, data de aniversário, casamento, repetir o mesmo número varias vezes, usar como senha o mesmo nome do login ou cadastrar a senha como o login de forma inversa.

Para dificultar a descoberta das senhas e tornar esse código mais difícil de ser quebrado, deve se optar por um cadastro com mais de 6 caracteres utilizando números, letras maiúsculas e minúsculas e expressões alfa numéricas como por exemplo: %, $, #, &.

A utilização dos compartilhamentos e acesso ao servidor de arquivos quando contemplado, deve ser realizado através de permissão autenticada do usuário ou do equipamento utilizado para tal atividade, como *notebook* e *desktops*. A rede que possui usuários com autenticação também é recomendada que o usuário realize a troca da senha no mínimo uma vez por ano, para que desta forma o cliente também não se torne uma maneira exploratória de acessar a rede e dados da empresa.

O controle de acesso físico deve “ter como regra básica a capacidade de diferenciar o usuário autorizado e o não autorizado mediante sua identificação” e atentar para as premissas: “o que a pessoa é: sua identificação ou características

biométricas; o que a pessoa possui: uso de cartões ou chaves; o que a pessoa sabe: uso de senha ou códigos" (SALGADO, BANDEIRA E SANCHES DA SILVA, 2004, p. 87).

Realizar uma cópia de segurança *(backup*), das informações pode ser um dos itens mais importantes da preservação dos dados da empresa. Com a utilização cada vez mais ascendente dos computadores e menos utilização de arquivos em papéis e livros, pode-se dizer que o volume de dados armazenados é cada vez crescente, desta forma o armazenamento das informações passa ser um item de relevância.

Um servidor que apresente falhas no disco, incêndio, alagamento e outros desastres podem levar a empresa à falência por falta de informação. Muitas vezes o valor da informação é muito mais relevante que a localização e espaço físico utilizado. Empresas que utilizam como fonte de renda a pesquisa e desenvolvimento de novos produtos, como por exemplo: indústrias farmacêuticas, laboratórios, institutos de pesquisa e desenvolvimento de novas tecnologias, podem ter um fator crítico com relação à segurança e roubo de informação.

Mecanicamente pode-se dizer que equipamentos possuem segundo seus fabricantes (MTBU) uma durabilidade média e desgaste físico e lógico de acordo com a condição de armazenamento e tempo de vida. Desta forma, "as cópias efetuadas devem ser testadas ao longo do tempo, respeitando-se a vida útil das mídias e o tempo máximo de regravações estabelecidas pelo fabricante, pois existem vários registros de perda de informação por falta de cuidado com esses itens" (SOUZA, 2004, p. 22).

Entende-se que o equipamento terá começo, meio e fim, cabendo ao administrador de rede e demais responsáveis avaliar, realizar manutenções preventivas e corretivas para que desta forma torne possível realizar um planejamento e realizar a manutenção, substituição, aquisição de equipamentos e dispositivos utilizados.

De acordo com um planejamento do corpo técnico da empresa, deve ser realizado um dimensionamento e levado em consideração o *software* utilizado para restauração, gerenciamento e que a realização do *backup* acontece se possível de forma centralizada, ou seja, a cópia deve ser realizada em áreas especificas. Também deve ser levado em consideração como parte fundamental do

planejamento: a criticidade, velocidade, qualidade, crescimento do espaço utilizado para realização do *backup*.

A seguir são apresentados alguns dispositivos e meios utilizados para realização de copias de segurança.

Dispositivos e mecanismo para *backups*:

- Mídias de CDs, DVDs;
- *Pen drive*;
- Fitas magnéticas (DAT);
- Bibliotecas de fitas (LTO);
- Discos externos (HDD);
- Disquetes.

2.3 SEGURANÇA EM *DATA CENTER*

Devido à criticidade e a necessidade de alta disponibilidade nos serviços e equipamentos lotados no interior de um *Data Center* ou também conhecido como Centro de Processamento de Dados (CPD), faz-se necessária atenção redobrada nas questões: acesso, monitoramento, distribuição de infraestrutura elétrica e lógica. Tendo em vista que neste ambiente é comum centralizar os equipamentos que realizam gerenciamento e distribuição de aplicações e serviços de Tecnologia de Informação e Comunicação (TIC).

A norma ANSI/EIA/TIA 942 trata sobre *Data Center* desde sua construção até sua ativação. Dentre os requisitos mencionados estabelece a classificação de segurança, mensurados em nível TIER de 1 a 4.

A escolha do local para implantação do *Data Center* “deve ser feita levando-se em consideração a região, compatível com o Código de Zoneamento do Município, tamanho do terreno, acesso fácil para a entrega de equipamentos, áreas altas sem inundações e existência de infra estrutura básica de esgoto, água, telefonia e energia elétrica” (MORAES, s. d., p. 4). Portanto, a estrutura física do *Data Center* deve contemplar “os detalhes construtivos e arquitetônicos da instalação para se obter o nível adequado de segurança”. Os principais aspectos a

este respeito a serem considerados são: piso, teto e paredes; iluminação e programação visual; e acabamento e mobiliário (SOUZA, 2004, p. 10).

Estas acomodações devem ser permanentemente gerenciadas e monitoradas, pois neste ambiente estão os equipamentos e aplicações que as corporações julgam de maior valor, complexidade e importância como: disponibilidade de serviços de rede, *link* para acesso à internet, *e-mail*, sitio, banco de dados, servidores, áreas de armazenamento (*storages*), *switches, routers,* entre outras. Muitas vezes o gerenciamento e infraestrutura das centrais de telefone também ficam alojadas neste local.

Com o crescimento, ascensão e velocidade em que as informações devem ser repassadas, ferramentas como editores de texto, planilhas eletrônicas, Sistemas Integrados de Gestão Empresarial (SIGE), *e-mail*, acesso à internet e utilização de telefone são serviços imprescindíveis para comunicação interna e externa entre funcionários, colaboradores e clientes.

De acordo com a importância das aplicações e equipamentos alocados em um *Data Center* é necessário estabelecer algumas políticas de acesso e meios de segurança, entre eles: Controle de acesso, monitoramento, combate e extinção de incêndio, climatização e energia. A seguir cada um destes itens é detalhado:

- **Controle de acesso** - deve ser implantado um controle de acesso aos profissionais, terceiros e visitantes. Este controle pode ser realizado através de leitores de proximidade, códigos “senhas”, biometria e novas tecnologias como o reconhecimento de face. No entanto, o ideal para uma melhor segurança, o acesso deve ser realizado através de sistemas biométricos ou que dificultem a passagem de senhas e cartões, reduzindo assim a vulnerabilidade. Por exemplo, sistemas de proximidade e códigos deixam uma fragilidade no acesso e segurança, uma vez que a senha possa ser descoberta e o acesso a um cartão pode ser obtido por meio de furto ou empréstimo. O sistema de controle de acesso ao *Data Center* deve fornecer informações de intrusão, violação e registrar os acessos liberados. Estas informações devem ser arquivadas e avaliadas pela equipe de segurança de TI.
- **Monitoramento** – o ambiente do *Data Center* deve ser monitorado vinte e quatro horas por dia e disparar alertas para os responsáveis. Os

principais meios de monitoramento utilizados são: câmeras, sensores de abertura de porta, sistema de inundação, falta de energia, umidade e temperatura do ar. Todo este acesso e monitoramento devem ser registrados, armazenados e arquivados para auditorias, apreciações e possíveis incidentes.

- **Combate e extinção de incêndio** – devido à grande carga elétrica disponibilizada para atender os equipamentos eletrônicos no interior de um CPD o risco de aquecimento, curto circuito e incêndio deve ser valorizado. O *Data Center* deve conter um sistema de detecção de incêndio, porta corta fogo e soluções que de forma automatizada realizem o procedimento de desligamento de energia (quando necessário) e extinção de incêndio como a utilização dos gases HFC227e a FM200 para extinção e contenção de fogo. Diante de qualquer alerta através do monitoramento, os responsáveis devem ser comunicados imediatamente.
- **Climatização** – Com a grande dissipação de calor gerado pelos equipamentos no interior do *Data Center* e devido à necessidade de atender as especificações técnicas de funcionamento dos equipamentos a temperatura nestes ambientes deve ser climatizada e possuir recursos para controle da umidade do ar. Deve ser realizado um cálculo por um profissional qualificado de acordo com o tamanho do ambiente, potência e dissipação de calor gerada pelos equipamentos. Com relação à infraestrutura os equipamentos devem ser especificados como máquinas de precisão (industriais) ligadas a um circuito de energia separado e a um gerador atuando como *backup,* uma vez que o ambiente é considerado critico.
- **Energia** – para atender a necessidade de alimentação elétrica dos equipamentos e do ambiente é necessário realizar um cálculo por um profissional qualificado para o dimensionando da utilização de dispositivos como: lâmpadas, cabo de energia, conectores, dijuntores e o quadro elétrico. Este cálculo deve levar em consideração também a expansão de alguns equipamentos. A energia deve ser adequada, estabilizada e monitorada, para que em caso de queda ou falha no fornecimento o sistema de redundância seja automaticamente acionado.

> Normalmente, utiliza-se um *no-break* para estabilizar e alimentar o *Data Center,* até que o gerador de energia assuma seu papel – restabelecimento da energia.

2.4 ENGENHARIA SOCIAL

É um método utilizado para realizar ataques a empresas através da utilização do fator humano. Esta técnica “explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. Ela tem como objetivo enganar, ludibriar pessoas assumindo-se uma falsa identidade, a fim de que elas revelem senhas ou outras informações que possam comprometer a segurança da organização” (NAKAMURA e GEUS, 2003, p. 70).

Existem duas formas de realizar este tipo de ataque: o meio físico, que se dá através do processo de vasculhar lixos e mesas, entre outros móveis da empresa; e o outro processo que se dá por meio de contato telefônico ou via e-mail, para que desta forma o usuário seja induzido a preencher falsas pesquisas e questionários com objetivo de capturar informações relevantes, como por exemplo, senhas e informações de acesso à rede.

As pessoas que praticam este tipo de ação são chamadas de engenheiros sociais. Têm como característica serem educados, simpáticos, criativos, astutos, bem articulados, dinâmicos e muito envolventes. São especialistas na arte de persuadir, manipular e distrair aqueles que são seus alvos (PEIXOTO, 2006).

Portanto, mesmo com uma segurança assídua em meios físicos e lógicos não existe ambiente 100% seguro. Deve-se manter o melhor padrão de segurança possível, para que desta forma se minimize a vulnerabilidade e a indisponibilidade de equipamentos, serviços e dados relacionados à paralisação ou captura de forma indevida.

A empresa deve elaborar junto à política de segurança termos de compromisso e confidencialidade; e os funcionários devem receber treinamento e explanação da necessidade e importância de não passar informações pertinentes aos termos estabelecidos. Diante deste cenário a elaboração de uma política de segurança de TI deve também atentar para intervenção humana.

3 POLÍTICAS DE SEGURANÇA EM TI

Pode-se considerar que a política de segurança em TI é o meio formal de aplicar regras para a organização, recomendando e explanando as necessidades para diminuir o risco de acesso indevido às informações. Uma política de segurança deve conter de forma detalhada e clara as decisões de inventário dos equipamentos, liberação e bloqueio no acesso ao sistema de informação da empresa.

Para tanto é fundamental criar um grupo para gestão de segurança de TI e estabelecer os principais objetos da política a serem considerados: confidencialidade, integridade e disponibilidade. Esta medida deverá ser definida e apresentada ao conselho diretor da organização, para que além de aprovada a política de segurança em TI, seja disseminada e valorizada em virtude de sua importância para a instituição. Os executivos, diretores, gestores da empresa e profissionais da área de TI devem ser informados e instruídos sobre a necessidade de cumprir e manter periodicamente a política de segurança em TI atualizada.

É crescente a preocupação com a implantação e gestão de uma atividade envolvendo segurança em TI, pois as empresas estão a cada dia mais percebendo e valorizando a estabilidade, controle, sigilo e cautela de suas informações. Dentre os principais focos de preocupação estão: a paralisação dos sistemas (SIGE), acesso à internet, dados pessoais, informações financeiras, lista de funcionários, folha de pagamento, entrada e saída de profissionais, projetos, fornecedores, informações de clientes e novos produtos.

Se estas informações forem capturadas de modo indevido, por exemplo, por um concorrente, podem representar para ele um grande passo estratégico e até ser utilizada para tomada de decisões, inclusive para antecipar o desenvolvimento de novos projetos e/ou até mesmo prejudicar a imagem e reputação da empresa fonte.

Assim, tendo em vista a necessidade de manter a disponibilidade, confidencialidade e integridade das informações institucionais, mediante a utilização de normas, pode-se fundamentar a estruturação de uma política de segurança em TI. Esta política deve conter um inventario dos equipamentos, o levantamento do ambiente e a classificação do nível de criticidade da informação, bem como considerar os fatores: processos, pessoas e ferramentas, os quais estão inclusos como objetos de vulnerabilidade.

Ao realizar a avaliação do nível de segurança físico, lógico e humano deve também ser considerado a área e o perímetro de segurança entre os ambientes que acomodam equipamentos de TI; definir a passagem de pessoas e veículos; e considerar fatores e riscos ambientais como a queda de árvores e inundações de lagos e rios.

A seguir são apresentados alguns exemplos, sugestões de informações e regras que devem estar contempladas na elaboração da estrutura de um documento utilizado como política de segurança de TI.

Introdução

Nesta parte são apresentadas as diretrizes para a política de segurança da tecnologia de informação para empresa em questão de forma regulatória.

Objetivos

De modo geral, os principais objetivos de uma política de segurança são:

a) Implantar e monitorar as diretrizes da segurança de TI;

b) Diminuir a vulnerabilidade no acesso aos dispositivos e sistemas de TI preservando o sigilo, integridade e disponibilidade dos serviços e informações;

c) Informar e explicar os riscos, importância e necessidade de aplicar as políticas estabelecidas neste documento.

Abrangência

Neste item devem ser descritos os conteúdos que abrangerão a política de segurança. Neste trabalho serão tratados os aspectos envolvendo:

a) Segurança Física de TI;

b) Segurança Lógica de TI.

Patrimônio de TI

Fazem parte deste aspecto:

a) Todo equipamento ou ativo de TI que esta ou será utilizado para manipulação e acesso ao sistema informatizado da empresa;

b) Hardware e Software adquiridos ou desenvolvidos por profissionais contratados ou terceirizado de acordo com recursos e necessidades estabelecidas pela empresa;

c) Controle de Acesso – permissão e restrição para acessar dispositivos, ambientes e sistemas que estejam sob a responsabilidade do setor de TI. Estas regras são válidas somente para funcionários e colaboradores de forma individual, não cabendo, em nenhuma hipótese, o repasse de informação ou utilização do recurso por outra pessoa;

d) Empréstimo – permissão para utilizar determinado equipamento, local ou software. O empréstimo fica caracterizado como temporário com data de inicio e fim e sob a responsabilidade do solicitante;

e) Incidente de Segurança – qualquer evento que altere o procedimento e disponibilidade no funcionamento dos recursos estabelecidos nesta política de segurança;

f) Criticidade de equipamentos e softwares – equivale a sensibilidade, relevância e prioridade que definem determinado patrimônio.

Conselho de Gestão da Segurança de TI

A formação do conselho para gestão da política de TI deve ser realizada por executivos responsáveis pela administração da empresa e profissionais de TI com qualificação e experiência nas atividades correlatas a sua área.

Ao conselho de gestão cabem algumas responsabilidades como:

- Gerenciar e aprimorar as políticas estabelecidas no documento;
- Participar de reuniões, avaliar e tomar decisão com relação às informações discutidas;
- Avaliar e atualizar normas e diretrizes legais sobre a política de segurança da informação;
- Executar e aplicar as normas, regras e definições descritas nesta política de acordo com as diretrizes e políticas da empresa;
- Administrar e zelar pelo patrimônio da empresa;
- Participar e elaborar um planejamento estratégico para obter a aprovação dos participantes e executivos responsáveis quando

necessário a alocação e disponibilização de recursos humanos, financeiros e tecnológicos pertinentes a segurança de TI.

Em sua formação, o Conselho da Gestão de Segurança de TI terá como membros:

- Diretor/Gestor - Executivo de Operações e TI;
- Diretor/Gestor de TI – Sistemas e desenvolvimento;
- Diretor/Gestor de TI – Infraestrutura;
- Diretor/Gestor de Recursos Humanos;
- Diretoria executiva, administrativa, técnica, produção ou representantes autorizados formalmente pelo diretor imediato.

As reuniões do Conselho de Segurança de TI ficam sob a responsabilidade do Diretor Executivo de Operações de TI, ao qual cabe convocar os demais representantes para reuniões, em um período máximo de 90 dias. Este prazo pode ser antecipado caso ocorra algum incidente de segurança, sugestão de melhoria, detecção de vulnerabilidade ou motivos relevantes e importantes para a organização.

Toda reunião deve ser registrada e arquivada em local seguro. Não será permitida a permanência de outras pessoas salvo quando convidado formalmente pelos membros do conselho. As decisões só podem ser aprovadas com a autorização formal e quando decidida pela maior parte dos integrantes do conselho.

Regras da política de segurança de TI

A política se aplica aos recursos humanos, físicos e lógicos da empresa. Neste sentido as principais regras são:

1. Informar sobre a política de segurança de TI quando do ingresso de um colaborador que necessite utilizar recursos de TI e realizar um treinamento na contratação de um ou mais funcionários. Em caso de contratação de serviços e profissionais terceirizados que utilizando os recursos por um período maior que 20 dias também deve ser realizado um treinamento;

2. Realizar treinamento e conscientização sobre segurança da informação de acordo com a política estabelecida neste documento e conforme o monitoramento dos recursos realizado na empresa;
3. Elaborar ata de reunião e treinamento a cada informação repassada aos colaboradores convocados para treinamento ou conscientização;
4. Formalizar e arquivar através de arquivo eletrônico ou outro mecanismo todo remanejamento de colaborador ou mudança de atividade, com a finalidade de registrar o fluxo e alteração de permissões utilizadas;
5. O documento de ingresso e responsabilidade deve conter informações de permissão de acesso, compartilhamento, privilégio no acesso à rede, *login*, conta de *e-mail* e aplicativos e ferramentas utilizadas para o trabalho;
6. Bloquear imediatamente quando ocorrer um incidente de segurança o acesso a todos os recursos de responsabilidade da TI físico, lógico, assim que informado formalmente pelo setor de recursos humanos ou por usuário participante do conselho de gestão da política de segurança de TI;
7. Toda aquisição de bens, aplicativos, e serviço de TI deve ser homologada e aprovada pela equipe ou responsável da TI;
8. Proibir toda atividade que manipule recursos físicos e lógicos por qualquer pessoa sem o consentimento do gestor da TI ou responsável pelo setor de TI;
9. Estabelecer como um dever o cumprimento da política de segurança em TI, sob pena de incorrer sanções e legais cabíveis;
10. Estabelecer como um dever o cumprimento das regras específicas de proteção ao patrimônio de TI;
11. Manter o sigilo da senha de controle de acesso e recursos de TI;
12. Proibir a utilização dos recursos e informações internas ou de propriedade intelectual da empresa, bem como a cópia, armazenamento de programas de computador ou qualquer outro material, que não autorizado pelo gestor ou responsável imediato;
13. Proibir o roubo, desvio ou deslocamento de equipamentos, licenças de *software* ou qualquer recurso de TI sem autorização formal do gestor ou responsável pelo setor de TI;
14. O Gestor deve avaliar e monitorar o cumprimento da Política de Segurança de TI dos seus subordinados e prestadores de serviços;

15. É dever do gestor após o treinamento identificar os desvios praticados e adotar as medidas apropriadas;
16. Preservar o patrimônio físico e lógico de TI no interior e exterior da empresa;
17. O gestor deve informar formalmente o setor de recursos humanos ou responsável o desligamento ou afastamento de um colaborador que utilize os recursos de TI na organização.

Atualização da Política de Segurança em TI

Neste item devem ser tratados os seguintes temas:

- Inventário – anualmente deve ser realizado um inventário dos dispositivos e recursos de TI. Todo patrimônio descontinuado, danificado ou sem utilidade para empresa deve ser baixado e registrado após análise do conselho de gestão da segurança;
- Atualização e monitoramento – deve ser realizada reunião para apresentação dos registros, sugestões e avaliação do monitoramento coletado em no prazo máximo de noventa dias;
- Aquisição de patrimônio – cada vez que detectada a necessidade de aquisição de novas soluções ou investimento em TI a compra deverá ser justificada com embasamento técnico para o conselho de gestão de segurança. Caso a necessidade torne aplicável o conselho deve apresentar para os executivos e diretores para aprovação e atualização da política de segurança;
- Período de revisão de regras - anualmente revisar as regras de proteção estabelecidas;
- Arquivos de *Logs* – os registros de acessos e monitoramento de portas, bem como documentos, devem ser avaliados pelo gestor e armazenados de acordo com a criticidade da empresa. Recomenda-se o arquivamento por no mínimo dois anos;
- Normas e leis – manter a política de segurança atualizada de acordo com a legislação, sem ferir os conceitos éticos e moral dos colaboradores e prestadores de serviço de acordo com a legislação vigente.

Treinamento e capacitação na utilização de recursos de TI

Deve abordar os seguintes itens:

- Objetivo – conscientizar e explanar sobre a importância da segurança em TI a todos os envolvidos, enfocando o valor da informação e compromisso individual e coletivo para atingir os melhores recursos do sigilo, disponibilidade e integridade da informação disponível;
- Erros humanos – instruir e conscientizar os funcionários sobre a vulnerabilidade dos objetos descuidados sobre mesas, computadores, *login* com sessão aberta quando não utilizado, furto, apropriação indébita, fraude ou uso não apropriado do patrimônio;
- Funcionários e terceiros - capacitar todo o pessoal envolvido na realização de trabalhos diretamente relacionados à empresa que utilizam recursos de TI, permanentemente ou de modo temporário.

Recursos Humanos: Ingresso, afastamento e desligamento

Neste item devem ser contemplados os aspectos abaixo:

- Funcionários – todo funcionário deve ser treinado e capacitado no momento em que for integrado à empresa sobre a política de segurança de TI. O profissional recém-contratado deve receber um documento com as permissões e uma cópia da política de acesso da empresa;
- Estagiários – não deve ser realizada liberação de acesso para o estagiário que não possuir autorização da gerência imediata para qualquer atividade que utilize recursos sobre a responsabilidade da TI;
- Termo de Responsabilidade – todo funcionário, estagiário ou terceiro deve assinar um termo de compromisso assumindo o cumprimento da política de segurança de TI da empresa, de acordo com os termos estabelecidos como o sigilo e integridade elencados pela empresa.
- Avaliação antes e depois do treinamento – deve ser elaborada uma avaliação básica sobre segurança e sua importância antes e após o treinamento. O resultado deve ser repassado ao setor de recursos humanos ou responsáveis;

- Falha na utilização dos recursos após o treinamento – deve ser analisada junto ao setor responsável a necessidade de um novo treinamento, ou tomada decisão do que fazer com colaborador que mal utiliza os recursos de TI;
- Identificação - o funcionário deve sempre usar nas dependências internas ou quando estiver representando a empresa externamente um crachá para identificação. De acordo como sistema de controle de acesso às portas e ambientes serão realizadas regras de permissão e bloqueio do usuário;
- Utilização imprópria dos recursos – o resultado de utilização incompatível com a política de segurança estabelecida deve ser analisado e comunicado à chefia imediata;
- Gestores e supervisores – os responsáveis pelos setores e consequentemente os colaboradores vinculados à sua responsabilidade devem assinar um termo de compromisso, confirmando que estão aptos e conscientes sobre a política de segurança estabelecida pela empresa;
- Férias e afastamento - todo colaborador terá o acesso restrito quando afastado de suas atividades laborais, salvo quando solicitado formalmente por seu gerente o acesso a determinados aplicativos ou recursos como *e-mail*. O acesso interno ao ambiente de trabalho deve ser restrito ou bloqueado;
- Desligamento do profissional – o colaborador deve ser orientado e informado sobre a restrição com relação ao acesso às informações da empresa. Após o desligamento deverá ser registrado e arquivado, por tempo determinado pelo setor de recursos humanos ou responsável, um documento formalizando o término do contrato e exclusão do usuário da rede e política de segurança em TI.

Computadores e estações Servidores

O acesso físico e lógico a computadores e estações servidores deve ser monitorado de acordo com a criticidade estabelecida pelo conselho de segurança em TI. Devem ser monitorados e arquivados os registros de acesso, bem como as alterações nas permissões de acessos dos usuários. Ao usuário deve ser

expressamente proibido acessar ou violar física ou logicamente qualquer recurso de TI sem autorização formal.

O *backup* deve ser avaliado de acordo com a estrutura e recursos da empresa. O indicado é centralizar as informações em uma máquina dedicada ao armazenamento, com a devida exploração de viabilidade de regras para acesso. Entretanto, o cliente deve estar orientado com relação ao período e frequência em que é realizada a cópia de segurança, seja esta diária, semanal ou mensal. Os dados devem ser mantidos de forma que permaneçam em segurança contra furtos e condições climáticas. É comum empresas guardarem seus *backups* em outras unidades, filiais ou na matriz para prevenção de acidentes ou desastres causados por incêndio ou fenômenos naturais como, chuva, vento ou raios.

O acesso à rede deve ser estabelecido de acordo com o sistema operacional utilizado e de acordo com a criticidade e disponibilidade do serviço a ser executado. O ambiente de rede *wireless* (rede sem fio) deve ser restrito às aplicações e usuários com permissão formal da gerência imediata. A disponibilidade de acesso aos pontos de rede deve ser avaliada de acordo com a decisão de controle de acesso estabelecida pelo conselho de gestão da segurança em TI.

Os recursos de acesso a pontos de rede normalmente são restritos e somente com solicitação formal deve ser realizada a liberação para acessar a rede. De acordo com a decisão do conselho de gestão de segurança pode ser acordado que a melhor maneira de interagir é bloquear todas as portas dos *switches* e liberar somente conforme a solicitação e autorização dos responsáveis.

Recomenda-se a realização de um inventario e mapeamento dos dispositivos e recursos de infraestruturura de TI no prazo máximo de vinte 20 meses. Neste indispensável conter: cabeamento lógico, *switches, routers*, iluminação e estabilizadores de energia elétrica. A elaboração deste inventário é necessária para realização de um planejamento estratégico e consequente identificação da necessidade de ampliação dos recursos e visualização do aproveitamento dos recursos existentes.

Riscos

Este item deve contemplar os principais riscos existentes na infraestrutura de TI. Destacam-se os riscos:

1. Físicos – falha em equipamentos, disponibilidade, dispositivos e periféricos;

2. Lógicos – falha na integridade, informações, vírus, ataques aos sistemas, acesso indevido, aplicativos e documentos;
3. Humanos – furtos, vandalismo, engenharia social, integridade, exclusão de informação, sabotagem, imprudência, negligência, erro;
4. Naturais - Tempestades, terremotos, alagamento e incêndio.

Decisões sobre os riscos

Após o levantamento dos riscos existentes devem ser planejadas ações a respeito. Recomenda-se:

- Riscos Naturais - avaliar a probabilidade e frequência em que ocorrem, e tomar decisão sobre a viabilidade do projeto;
- Riscos Humanos – adotar medidas e métodos de acordo com a sistemática definidos pelos Recursos Humanos da empresa, por exemplo, sanções quando da má utilização dos recursos de TI, acesso à informações indevidas, instalação de dispositivos ou *softwares* sem autorização, entre outras;
- Riscos Físicos – avaliar novos investimentos, recursos, tecnologias e decisão com base na política de segurança em TI;
- Riscos Lógicos – avaliar impacto da vulnerabilidade, falha na segurança e apresentar um novo planejamento para o conselho de gestão de segurança em TI.

Ao se elaborar uma política de segurança TI é essencial se considerar os fatores: pessoas, processos e ferramentas. Além disso, ela deve ser adaptada pelo comitê gestor de segurança TI de acordo com a realidade e necessidade da empresa. É importante que seja aprovada e apoiada pelo alto escalão executivo, bem como esteja integrada com a política de qualidade da empresa.

4 CONCLUSÃO

Conforme as informações descritas neste trabalho é possível identificar a existência de vários dispositivos e mecanismos que são utilizados para manter o acesso a recursos da tecnologia de informação com integridade, disponibilidade e sigilo. Desta forma, pode se dizer que com a implantação ou melhoria de uma política de segurança em TI, a empresa pode organizar, padronizar, administrar e criar mecanismos para diminuir a vulnerabilidade que seus bens e valores ficariam expostos.

A política de segurança de TI deve ser elaborada, avaliada, atualizada e gerenciada constantemente. Para tanto, é fundamental a criação de um conselho composto por executivos e gestores que devem cumprir efetivamente as regras e diretrizes estabelecidas no documento e assim alcançar suas metas e objetivos, assegurar e minimizar o impacto relativo a falhas e vulnerabilidades físicas, lógicas e humanas para proteção do patrimônio e informações relevantes da empresa.

Considerando que o investimento em segurança física e lógica é permanente, pois os equipamentos possuem um tempo de vida útil e também há necessidade de ampliação dos recursos de TI conforme a expansão, substituição e atualização do equipamento ou sistema. Diante deste cenário, avalia-se de forma positiva o investimento com infraestrutura, controle de acesso e segurança dos recursos físicos e lógicos na empresa, uma vez que aplicando este investimento os posteriores ocorrerão de forma gradativa.

Após realizar pesquisas correlatas ao tema segurança em TI e desenvolver este trabalho, despertou a preocupação com a fragilidade de riscos e situações relativas à segurança envolvendo recursos humanos (pessoas). Enfatiza-se, então como de suma importância monitorar, controlar, realizar cópias de segurança, treinar e conscientizar os colaboradores sobre a relevância e consequências com relação à implantação da Política de Segurança em TI na empresa.

Para os próximos estudos se recomenda avaliar mecanismos para detecção das vulnerabilidades nos sistemas, ferramentas de controle de acesso, gerenciamento, monitoramento, bem como pesquisas com fundamentos teóricos e técnicos para conscientizar, informar e auxiliar na tomada de decisão relacionada aos riscos de segurança, investimento financeiro, profissional e tempo despendido para implantar uma Política de Segurança em TI.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, ABNT. **NBR ISO/IEC 17799: Tecnologia da informação** - Código de prática para a gestão da segurança da informação, 2001.

CRUDO, Adriana P. et al. Auditoria de segurança lógica e da confidencialidade em computação. **Anais do VII SemeAD**. São Paulo: FEA-USP, realizado nos dias 11 e 12 ago. 2005.

GUIA de Switches – Cisco Systems. **Switches.** Mude: São Paulo, jul. 2006.

MARCIANO, João Luiz P. **Segurança da informação**: uma abordagem social. 2006. 212 f. Tese (Doutorado em Ciência da Informação) – Programa de Pós-Graduação em Ciência da Informação do Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2006.

MENEGUITE, Ronaldo Louro. **Segurança da informação.** 2010, 37f. Trabalho de conclusão de curso (Curso Técnico de Informação Industrial), Unidade de Ensino Descentralizada de Leopoldina, Centro Federal de Educação Tecnológica de Minas Gerais. Leopoldina, 2010.

MORAES, Pollette B. de. **Infra-estrutura de internet data Center (IDC).** Disponível em: www.projetoderedes.com.br. Acesso em: 10 de novembro de 2011.

MORESI, Eduardo Amadeu D. Delineando o valor do sistema de informação de uma organização. **Ci. Inf.**, Brasília, v. 29, n. 1, p. 14-24, jan./abr. 2000.

NAKAMURA, Emilio T.; GEUS, Paulo L. **Segurança de redes em ambientes cooperativos.** Minas Gerais: Futura, 2003.

PEIXOTO, Mário César P. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro: Brasport, 2006.

SALGADO, Ivan J. C.; BANDEIRA, Ronaldo; SANCHES DA SILVA, Rivanildo. **Análise de segurança física em conformidade com a Norma ABNT NBR ISO/IEC 17799.** 2004, 325 f. Trabalho de conclusão de curso (Graduação em Tecnologia em Segurança da Informação), Instituto Científico de Ensino Superior e Pesquisa, Faculdades Integradas ICESP. Guará, 2004.

SILVA NETTO, Abner da; SILVEIRA, Marco Antonio P. da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **Rev. Gest. Tecn. Sist. Inf.,** São Paulo, v. 4, n. 3, p. 375-397, 2007.

SOUZA, Leonardo Henrique L. **Segurança física de redes de computadores**. 2004, 39 f. Monografia (Especialização em Informática), Coordenação de Pós-Graduação, Universidade Estácio de Sá. Rio de Janeiro, 2004.