UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO SEMIPRESENCIAL EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

LUCIANO MONTEIRO LEITE

POLÍTICAS DE SEGURANÇA FÍSICA E LÓGICA DE TECNOLOGIA DA INFORMAÇÃO EM REDES DE COMPUTADORES E SEUS ATIVOS

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2018

LUCIANO MONTEIRO LEITE

POLÍTICAS DE SEGURANÇA FÍSICA E LÓGICA DE TECNOLOGIA DA INFORMAÇÃO EM REDES DE COMPUTADORES E SEUS ATIVOS

Monografia de Especialização, apresentada ao Curso de Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. M. Sc. Luis José Rohling

CURITIBA

2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização Semipresencial em Configuração e
Gerenciamento de Servidores e Equipamentos de Redes

TERMO DE APROVAÇÃO

POLÍTICAS DE SEGURANÇA FÍSICA E LÓGICA DE TECNOLOGIA DA INFORMAÇÃO EM REDES DE COMPUTADORES E SEUS ATIVOS

por

LUCIANO MONTEIRO LEITE

Esta monografia foi apresentada em 23 de Novembro de 2018 como requisito parcial para a obtenção do título de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. M.Sc. Luis José Rohling
Orientador

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Membro titular

_____
Prof. M.Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

AGRADECIMENTOS

Agradeço a todos que contribuíram, me deram incentivo, atitudes e me apoiaram até o momento. Aos amigos e colegas, que não negaram força e ficaram na torcida, meu muito obrigado.

Agradeço a Deus pela que me deu o dom da vida, sabedoria, luz e me abençoa todos os dias com seu amor infinito. Aos meus pais Vanda e Heleno pela paciência, incentivo, palavras de apoio e que sempre me deram forças nos momentos difíceis, com palavras de carinho e amor que despertam felicidade em meu coração.

Ao meu irmão Cristiano, com sua sabedoria, conselhos, fonte de garra e inspiração, que sempre acreditou no meu potencial e nunca negou uma palavra de incentivo.

A Maira Karoline por estar ao meu lado durante a elaboração deste trabalho, pessoa que admiro muito e tenho imensa gratidão, por me apoiar em minhas decisões, companheirismo, carinho e amor.

Ao professor orientador e M. Sc. Luis José Rohling por dedicar seus ensinamentos e conselhos deste trabalho.

Aos meus colegas de trabalho João Paulo Dolny, Matheus Gelinski, Salustriano Bessa, Fabio Araujo do Carmo, Emerson Della Montagna Misturini, Jean Carlos Paris, Alexandre Alvizi e Adilson Guranda.

“Amo a liberdade, por isso, deixo as coisas que amo livres, se elas voltarem é porque as conquistei, se não voltarem, é porque, nunca as possuí. ” (John Lennon)

RESUMO

LEITE, Luciano Monteiro. **Políticas de segurança física e lógica de tecnologia da informação em redes de computadores e seus ativos**. 2018. 33 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

Este estudo aplicado a segurança da informação para ambientes empresariais, consiste em criar uma política de segurança para ambientes de redes de computadores e seus ativos. O objetivo é descrever as diretrizes de segurança física e lógica para empresas onde se utilizam equipamentos de tecnologia da informação, garantindo a segurança, integridade e imagem de uma organização. Durante a pesquisa é abordado os riscos e vulnerabilidades na falta de normas e regras estabelecidas, o uso da política de segurança em organizações assim como as instruções de implementação. Durante a pesquisa são citadas quais as normas e responsabilidades, quais os critérios utilizados para na análise dos profissionais de tecnologia da informação em identificar riscos e probabilidades de ataques cibernéticos assim como o uso da engenharia social afim de obter informações e acessos privilegiados.

Palavras-chave: Segurança da informação. Políticas de segurança. Riscos. Vulnerabilidades. Tecnologia da informação.

ABSTRACT

LEITE, Luciano Monteiro. **Physical and logical security policies on information technology on computer networks and its assets.** 2018. 33 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

This study applied to information security for business environments is to create a security policy for computer network environments and their assets. The objective is to describe the physical and logical security guidelines for companies that use information technology equipment, ensuring the security, integrity and image of an organization. During the research, the risks and vulnerabilities are addressed in the absence of established norms and rules, the use of the security policy in organizations as well as the implementation instructions. During the research, it is mentioned the norms and responsibilities, the criteria used in the analysis of information technology professionals in identifying risks and probabilities of cyber-attacks as well as the use of social engineering in order to obtain information and privileged access..

Keywords: Information security. Security policies. Scratches. Vulnerabilities. Information Technology.

LISTA DE FIGURAS

LISTA DE SIGLAS

ACL	*Access Control List*
CFTV	Circuito Fechado de TeleVisão
EAP	*Extensible Authentication Protocol*
EIA	*Electronic Industries Alliance*
ISO	*International Organization for Standardization*
NBR	Norma Brasileira
NIST	*National Institute of Standards and Technology*
PSI	Política de Segurança da Informação
RADIUS	*Remote Authentication Dial In User Service*
SOX	*Sarbanes-OXley*
TI	Tecnologia da Informação
TIA	*Telecommunication Industries Association*
VLAN	*Virtual Local Area Network*

SUMÁRIO

1 INTRODUÇÃO

A informação é um bem ativo muito importante para empresas e pessoas, essencial para o funcionamento e, consequentemente, necessita ser protegida. Neste trabalho serão abordados o desenvolvimento e a aplicação de políticas de segurança física e logica de tecnologia da informação com foco em redes de computadores e seus ativos.

Com as mudanças tecnológicas e uso de equipamentos de grande porte, a infraestrutura de TI e a comunicação tornaram se mais sofisticados, atingiram tamanha complexidade que foi necessário criar equipes e métodos mais seguros. Os sistemas tornaram-se ferramentas de trabalho essencial nas empresas. Compartilhar dados passou a ser uma pratica moderna, trazendo maior velocidade de comunicação e agilidade no processo. Segundo Marciano (2006), a camada humana é a que carece de maior atenção por parte das empresas, pois foi a que apresentou o menor índice de controles implantados. Os dados confirmam que as empresas investem principalmente em controles tecnológicos para diminuir o risco de incidentes de segurança da informação, porém esquecem que o fator humano é uns dos grandes responsáveis por falhas na segurança.

A política de segurança da informação é necessária para definir quais são as melhores práticas, normas e transmitir o foco e visão da empresa na utilização dos recursos de tecnologia.

Para manter um ambiente com seus dados protegidos são necessárias regras e normas, evitando vazamento de informações sigilosas e confidenciais por exemplo arquivos de áudio, imagem, vídeo e voz.

1.1 PROBLEMA

O principal problema, foco deste trabalho, é a falta de segurança da informação em equipamentos de TI quando não há uma política de segurança definida ou quando não é executada de maneira eficiente. Assim é necessário que as empresas e instituições invistam e sigam as normas adequadas em segurança de TI, prevenindo o acesso indevido a informação e evitando o roubo de dados com informações sigilosas, servindo como apoio para as tarefas do cotidiano. Para Sêmola

(2003), a gestão da segurança da informação pode ser classificada em três aspectos: tecnológicos, físicos e humanos. As organizações preocupam-se principalmente com os aspectos tecnológicos: redes, computadores, vírus, hackers, interne; e se esquecem dos outros, físicos e humanos, tão importantes e relevantes para a segurança do negócio quanto os aspectos tecnológicos. Também nesta pesquisa, é abordado como a política de segurança serve como base para evitar as brechas e vulnerabilidades em empresas que utilizam recursos de TI.

1.2 OBJETIVOS

Todos os dias o uso de recursos e derivados de tecnologia da informação cresce. Cada vez mais a sociedade e os sistemas estão integrados, o volume de dados e exposição como consequência sofrem, muitas vezes por falta de informação até para quem atua na profissão. Os riscos aumentaram com o uso dos microcomputadores, a utilização de redes locais e remotas, a abertura comercial da Internet e a disseminação da informática para diversos setores da sociedade (SILVA NETTO; SILVEIRA, 2007, p. 376).

A análise de risco e mão de obra qualificada são necessários para um estudo e desenvolvimento de normas e regras. Esta pesquisa tem como objetivo a proteção de dados de tecnologia da informação, prevenindo que a informação não seja disseminada sem consentimento e garantindo os pilares de segurança: confiabilidade, integridade e disponibilidade.

1.3 JUSTIFICATIVA

O valor da Informação e aumento da conectividade faz necessária uma atenção especial com a segurança em tecnologia, mas nada adianta se não houver regras a serem seguidas, tanto pelos usuários quanto pelos administradores de TI, estes irão criar estas regras e exercer sua atividade profissional na área. Manter a política de acordo com as atualizações sistêmicas, manter os dados em sigilo e ao mesmo tempo definir quais pessoas irão utilizá-los sem prejudicar uma companhia,

são as principais atividades dos profissionais envolvidos com a segurança da informação.

Hoje o vazamento de informação são os piores inimigos das empresas, desde uma formula de cosmético ou produto alimentício, até contratos, interesses e estratégias da empresa podem causar prejuízos imensuráveis. A política de segurança pode ser aplicada e aumentar a produtividade através do controle de acesso e normas. A defesa é mais complexa do que o ataque, pois para o hacker basta que ele consiga explorar apenas um ponto de falha da organização para causar prejuízo. Caso uma determinada técnica não funcione, ele pode tentar explorar outras, até que seus objetivos sejam atingidos (NAKAMURA; GEUS, 2007, p. 8).

1.4 PROCEDIMENTOS METODOLÓGICOS

Está é uma pesquisa para políticas de segurança em ambientes corporativos. Foram utilizadas fontes bibliográficas como artigos, livros, revistas, normas e metodologias aplicadas a segurança da informação para infraestrutura e redes de computadores.

As frases utilizadas foram: segurança da informação, políticas de segurança, vulnerabilidades e acesso a informação.

1.5 EMBASAMENTO TEÓRICO

A política de segurança sempre deve manter como principal fonte a prevenção de roubo de arquivos confidenciais, uma das principais maneiras é gerenciando e atualizando políticas e camadas de segurança em equipamentos de redes de computadores, tanto física como logica. O fato é que nos dias atuais existem tantos métodos para roubar dados como ataques a sistemas, engenharia social e outros, que os próprios profissionais de TI necessitam de uma política de segurança a ser seguida. Deste modo pessoas, sistemas, equipamentos e os próprios fluxos seguidos pelos conteúdos informacionais devem ser devidamente considerados por ocasião da planificação da segurança da informação (MARCIANO, 2006, p. 47).

2 NECESSIDADE DE SEGURANÇA

A informação é um recurso que tem seu valor determinado exclusivamente pelo usuário, só se perde quando se torna obsoleta ou quando não há o devido cuidado. É um recurso que deve ser gerenciado de forma adequada e consciente. O propósito da informação é garantir que a empresa atinja seus objetivos pelo uso eficiente dos recursos, desde pessoas, tecnologia, financeiro, história e a própria informação. Muitas vezes esses dados devem ser preservados e mantidos em sigilo. Qual seria o impacto se todas as informações contendo clientes, fornecedores, registros fosse perdido? As consequências podem ser irreversíveis, com prejuízos enormes e muitas vezes pode levar a empresa a falência. “A segurança da informação abrange mais que o ambiente da tecnologia da informação, porem este ambiente de tecnologia, cada vez mais, processa e armazena as informações da organização.” (FONTES, 2012, p. 13).

Para aqueles que pensam que são só empresas que estão sujeitas ao roubo de dados, a pratica também ocorre com pessoas físicas, nesta estão inclusas redes sociais, sites de relacionamento, compras online, troca de conversas sigilosas e outros.

A segurança da informação é a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como intrusão e a modificação não-autorizada de dados, estejam eles armazenados, em processamento ou em trânsito. Ela deverá abranger a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações computacionais, assim como as medidas destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (ABNT, 2005).

Para falar de segurança devemos citar os pilares principais que compõem seus fundamentos e regras.

- Confidencialidade: “Garantia de que o acesso à informação é restrito aos seus usuários legítimos.” (BEAL, 2005, p. 1). Ou seja, seu acesso é permitido apenas a determinados usuários.

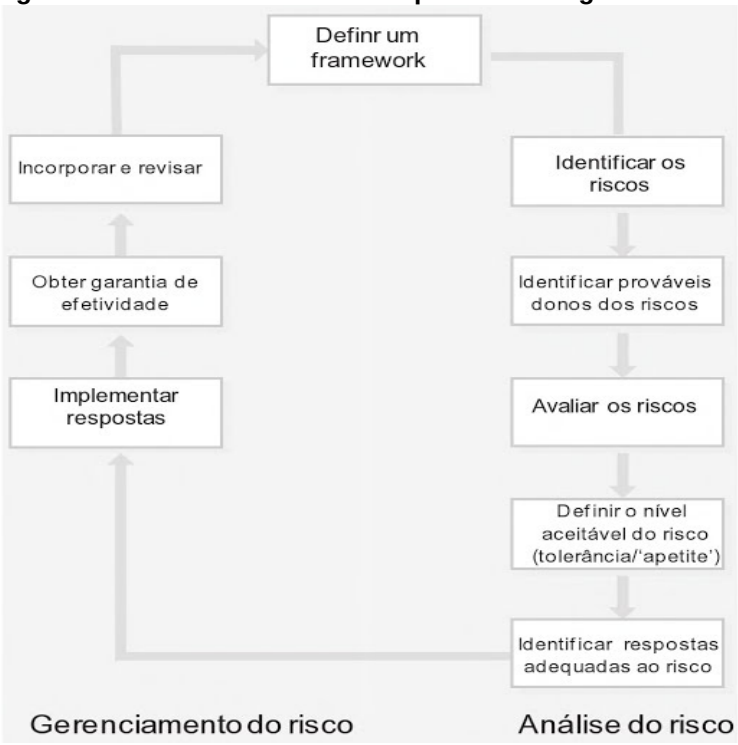
- Integridade: “Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.” (SÊMOLA, 2003, p. 45). Ou seja, informação não adulterada.
- Disponibilidade: “Garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna.” (BEAL, 2005, p. 1). Ou seja, independente da finalidade, a informação deve estar disponível.

2.1 ANÁLISE DE RISCOS EM AMBIENTES CORPORATIVOS

Antes de estabelecer políticas de segurança e colocá-las em pratica devemos entender o que deve ser protegido. Para isto, a análise de risco deve ser estudada e aí então teremos quais são as principais vulnerabilidades e o que deve ser corrigido. “A segurança é necessária, porém sua estratégia de implementação deve ser bem definida, medindo-se custos e benefícios e assumindo-se riscos, pois a segurança total não é possível.” (NAKAMURA; GEUS, 2007, p. 65).

Durante a análise de risco (Figura 1) existem aspectos a respeito de um documento já elaborado, podendo ser em padrões ou normas já criadas com referências de segurança. A partir deste ponto podemos compor uma matriz adequada a necessidade da empresa, pois através dela se dão os controles dos impactos avaliados. Por exemplo, se os riscos forem exclusivamente segurança da informação a ISO/IEC 27002 é suficiente para a análise de risco. Já outros órgãos como SOX, ITIL, DRI e NIST são mais recomendados para continuidade do negócio e será necessário avaliar os controles, mapear o ambiente e encontrar de que forma os acessos são aplicados.

Figura 1 - Fluxo de atividades do processo de gerenciamento de riscos



Fonte: Bridge (2015, p. 7).

Para definir os possíveis riscos de uma empresa, deve se levar em conta quais são os valores dos ativos e entender as possíveis ameaças a que eles estão expostos, as suas consequências podem ser administradas e até prevenidas, como padrão a elaboração de uma matriz de risco tem os seguintes temas:

- Impacto: Avaliar o ambiente com os critérios de segurança da informação, quais são os ofensores e os impactos de cada item.
- Vulnerabilidade: Avaliar quais são os pontos de vulnerabilidade do ambiente de TI, sem as devidas atenção, a vulnerabilidade é a principal porta de entrada a invasões, hackers ou pessoas más intencionadas.
- Probabilidade: Dependendo de qual a demanda da empresa, é possível prever probabilidades de uma ameaça explorar uma vulnerabilidade, as probabilidades indicam o quão perto uma ameaça está.
- Risco: Os riscos está presente em vários papeis na empresa e cabe a segurança da informação identificá-los de acordo com os impactos X vulnerabilidades.

3 SEGURANÇA LÓGICA

Tem como objetivo a forma de como um sistema é protegido seja por regras ou softwares para controle de acesso. Normalmente é utilizada para proteção de ataques e vulnerabilidades, também serve para proteger sistemas de erros não intencionais e a remoção acidental de dados. Para isso são implementados processos tecnológicos como firewalls, antivírus, políticas de segurança entre outros necessários para proteção do usuário. Nesta categoria, existem dispositivos destinados ao monitoramento, filtragem e registro de acessos lógicos, bem como dispositivos voltados para a segmentação de perímetros, identificação e tratamento de tentativas de ataque (SÊMOLA, 2003, p. 21).

3.1 FIREWALL

Equipamento de alta importância para garantir a segurança em redes de computadores, onde é feita a filtragem de pacotes de redes da maneira que o administrador irá configurar de acordo com a necessidade de controle. “Pode-se ver uma rápida evolução nessa área, principalmente com relação ao firewall, que é um dos principais, mais conhecidos e antigos componentes de um sistema de segurança. Sua fama, de certa forma, acaba contribuindo para a criação de uma falsa expectativa quanto à segurança total da organização, além de causar uma mudança ou mesmo uma banalização quanto à sua definição.” (NAKAMURA; GEUS, 2007, p. 220). Os tipos de tecnologias para firewalls são:

- Filtro de pacotes: As regras aplicadas podem ser formadas inserindo os endereços de rede origem e destino com as portas TCP de conexão, tem como desvantagem a falta de controle do estado da conexão, o que abre brechas para softwares e agentes maliciosos introduzindo pacotes falsos com a técnica de IP spoofing.
- Proxy Firewall: Os firewalls implementam gateway de aplicação e, devido a sua forma de funcionar, também são denominados de proxies de aplicação ou proxies em nível de aplicação. Nesse caso por exemplo, uma máquina da intranet, ao acessar a rede externa, tem seu fluxo de informações redirecionado para o gateway de aplicação, ou o contata diretamente, estabelecendo uma

conexão. Em seguida, o gateway de aplicação recebe as requisições do cliente, as analisa e se elas cumprem a política estabelecida, as encaminham para o servidor destino. As respostas provenientes do servidor são tratadas da mesma forma (CARISSIMI; ROCHOL; GRANVILLE, 2009, p. 374).

- Stateless e Stateful Firewall: Para os modelos mais atuais os firewalls stateless oferece um recurso de avaliação de pacotes de uma maneira independente, eles não estão “cientes” do padrão de tráfego e fluxo de dados e monitoram o trafego com base nos endereços de origem e destino. Ou seja, cada pacote que é filtrado pelo firewall é avaliado pelas regras do administrador, sendo uma conexão nova ou já existente. Já o Firewall Stateful tem como foco corrigir os problemas da primeira geração como por exemplo o IP spoofing. As diferenças são que os mecanismos de filtragem são orientados a conhecer as conexões, desta maneira ele valida um pacote ou não. Esse recurso ficou conhecido por tabela de conexões ou tabela de estados, onde há economia de recursos devido não haver necessidade de validar toda regra e as conexões estabelecidas pois já estão cientes dos caminhos de comunicação de cada pacote.

É importante entender os tipos de firewall, mesmo que de maneira simplificada, pois para os administradores de redes será útil em prevenir as principais vulnerabilidades do ambiente. Lembrando que os firewalls, com o modelo apresentado na Figura 2, são medidas preventivas de garantir a segurança da informação controlando acessos e monitorando a rede, cada um tem argumentos e particularidades para atender as necessidades da empresa.

Figura 2 - Modelo básico de utilização de firewall

Fonte: Autoria própria.

3.2 ROTEADORES

Os roteadores são essenciais para o roteamento e interligação de uma rede para outra, o que na grande maioria está em ligação externa com a internet, são diversos modelos no mercado e possuem sistemas operacionais, sendo que uma das funções é que funcione também como um hardware de segurança. No caso dos roteadores Cisco, o sistema operacional nos permite criar regras conhecidas como listas de acesso, com elas podemos configurar quem tem os acessos ao roteador e qual a origem do acesso.

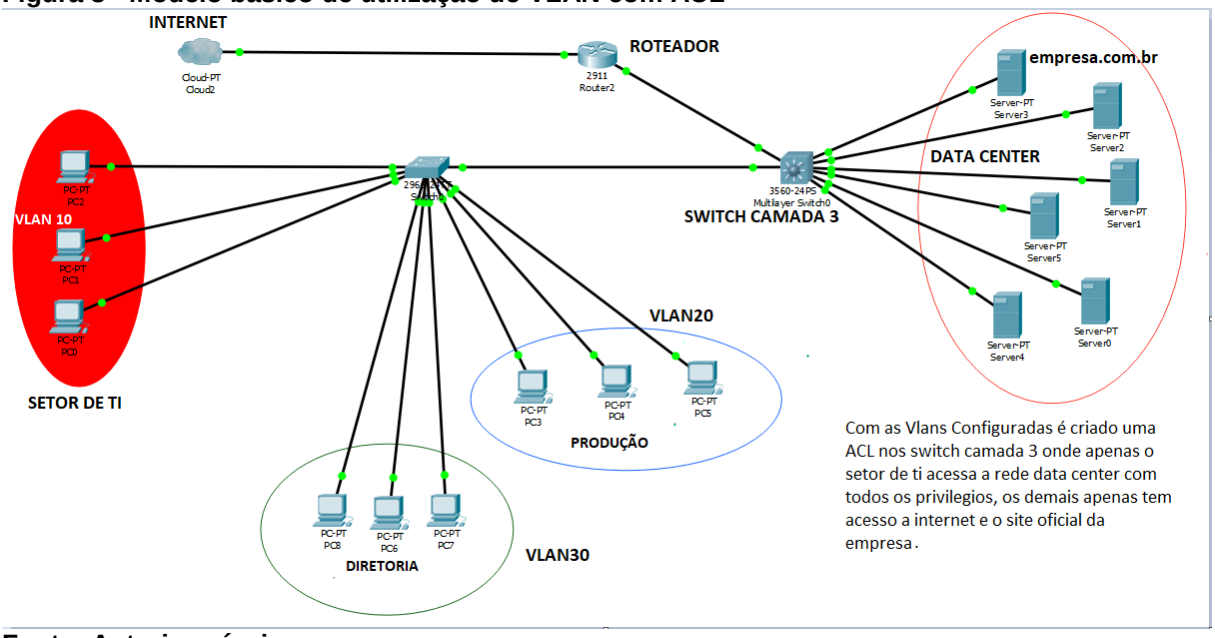
Além de acesso é possível filtrar os pacotes, bloquear serviços e seus protocolos através das listas de acesso, é recomendável utilizar esta função com a visão de garantir que somente o setor de Tecnologia da informação tenha acesso ao recurso.

3.3 SWITCHES

Os Switches têm como função distribuir as conexões de uma rede, são responsáveis por uma malha entre vários dispositivos e possuem várias categorias onde o recomendável são os gerenciáveis, devido a esta conter um sistema operacional com funcionalidades de segurança. Os Switches gerenciáveis podem ser configurados para controlar acessos em todas as portas e alguns atuam na camada de protocolo IP (camada 3).

Possuindo um switch gerenciável é possível criar *Virtual Local Area Network* (VLAN), com o modelo apresentado Figura 3, que são redes virtuais e dividir os setores da empresa, com intuito de restringir acessos a cada grupo especifico. Sabendo disso, o essencial é criar uma VLAN apenas de gerenciamento de dispositivos de rede onde apenas equipamentos autorizados terão acesso.

Figura 3 - Modelo básico de utilização de VLAN com ACL



Fonte: Autoria própria.

3.4 IEEE 802.1X

O protocolo 802.1x (também conhecido como dot1x) utilizado em redes cabeadas e wireless, define um padrão para autenticação de três entidades: suplicantes (cliente), autenticadores e um servidor de autenticação, utiliza o protocolo EAP para comunicação entre as entidades e pode ser usado como controle de acesso. Torna-se robusto quando utilizado com *Virtual Local Area Network* (VLAN) e *Access Control List* (ACL) dinâmicas.

O padrão de funcionamento das mensagens pelo 802.1x (Figura 4) no protocolo EAP são encaminhadas de um cliente (host da rede) para o autenticador (switch ou access point), o autenticador encaminha as mensagens ao servidor de autenticação (Radius).

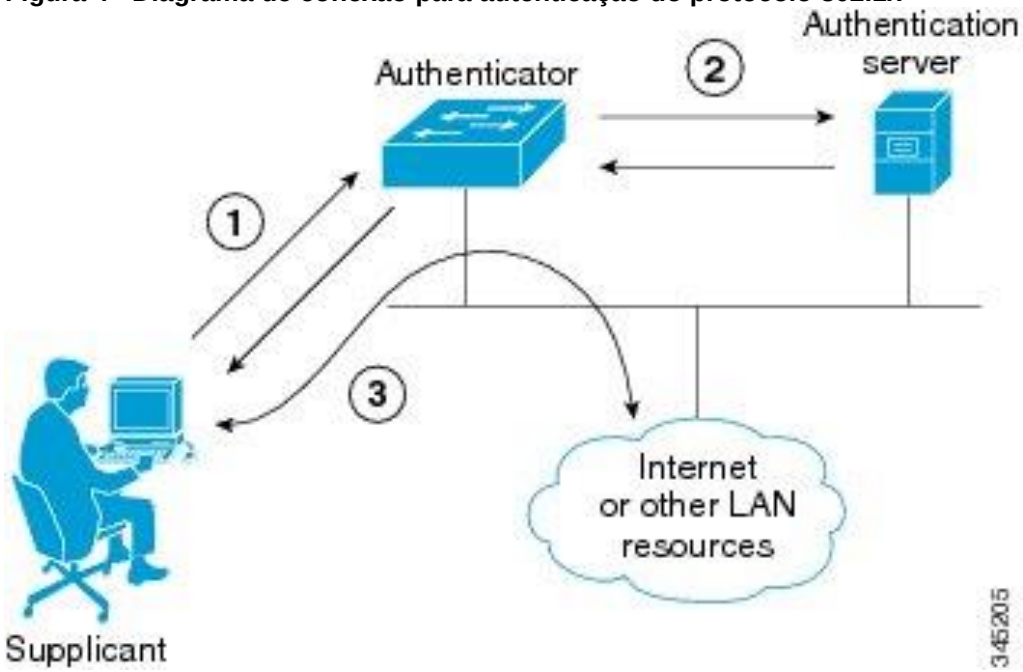
Os elementos do diagrama de conexão 802.1x, apresentado na Figura 4, são (CISCO, 2015):

1. Suplicante (*Supplicant*): também conhecido como cliente ou um host com suporte a 802.1x, pode ser um telefone IP, desktop ou equipamentos de rede.
2. Autenticador (*Authenticator*): Geralmente Switchs e controladoras wireless, funciona basicamente como uma ponte entre o suplicante e o servidor de autenticação, recebe a informação da identidade do cliente pelo protocolo EAP, que então é verificado e encapsulado pelo protocolo RADIUS para chegar até

o servidor de autenticação. Nos Switches geralmente é criado uma VLAN para direcionar para os clientes que não atendem os requisitos estabelecidos, tendo acesso apenas como visitante.

3. Servidor de Autenticação (*Authentication server*): O servidor RADIUS tem como função, autorizar ou negar as mensagens após validação do usuário, fica transparente para os suplicantes pois se comunica apenas com o autenticador. Por exemplo, caso o cliente não atender os pré-requisitos configurados no RADIUS como um certificado digital ou usuário e senha cadastrado no servidor de autenticação ele não se conectara a rede.

Figura 4 - Diagrama de conexão para autenticação do protocolo 802.1x



Fonte: Cisco (2015).

4 SEGURANÇA FÍSICA DE EQUIPAMENTOS DE REDES

Contribui para proteção dos equipamentos e ativos de infraestrutura, estes geralmente representam algo de valor para a organização e devem ser protegidos e monitorados, faz-se necessário muita atenção em questões de acesso, infraestrutura predial, elétrica e monitoramento. A maioria dos casos são centralizados em datacenters, com lugares estratégicos contendo no interior os equipamentos de redes que garantem a total comunicação com a empresa e sistemas.

Para esta categoria temos várias regras que podem ser usadas. Para Data Center podemos utilizar a EIA/TIA 942 internacional que serve como base para projetos. Além disso temos também as normas brasileiras, que são NBR 5410, NBR 15247, NBR 27002, NBR 11515, entre outras.

- Acesso Físico: A entrada e saída das pessoas do datacenter deverão ser registradas e somente por pessoas autorizadas, assim como materiais e equipamentos, deve ter datas, horários e os responsáveis. Supervisionar a atuação de equipes terceirizadas (limpeza, manutenção predial, vigilância, fornecedores). E como recomendação é essencial utilizar fechaduras eletrônicas, controles de acesso sendo por crachá, biometria ou leitura facial para abertura de portas, assim como portas corta fogo.
- Essencial: Falar sobre segurança física depende muito de cada empresa, tipo de informação, tamanho da demanda e valor dos ativos os principais itens para segurança física de um data center são:
  - Alarmes: Os alertas gerados por alarmes instalados no data center são ótimos aliados para prevenção de incêndios, manutenção de *hardware* e detecção de intrusos.
  - Detecção de intrusos: A detecção de acessos físicos não autorizados podem ser por câmeras de segurança utilizando por exemplo os sistemas de CFTV e controles de acesso.
  - Recepção: A entrada do datacenter deve conter uma recepção onde primeiramente será solicitado que a pessoa que se identifique.
  - Central de gerenciamento e controle dos equipamentos: Também conhecido como *Command Center* é monitorado os alarmes de

segurança logica e física, por exemplo o aumento de temperatura no data center, falhas de hardware, falhas elétricas.

- Analise de condições ambientais: A análise do ambiente é importante, alagamentos, tempestades e fatores climáticos que podem interferir na segurança dos equipamentos.
- Refrigeração: Controlar a temperatura do datacenter é fundamental contra riscos de incêndio e também preservar a vida útil dos equipamentos, portanto a temperatura da sala deve ser monitorada.
- Equipamentos contra incêndio: São itens de segurança para prevenção de incêndios no data center, devem ser obrigatórios, extintores, portas corta fogo e dependendo do risco gás FM-200 para supressão de calor.

5 ACESSO

Os tipos de permissão para cada dispositivo sendo físico ou logico é um dos principais ofensores da segurança da informação, o acesso dos dados ou do suporte ao ambiente muitas vezes pode ser a principal ameaça a companhia. Cada um tem como papel preservar o sigilo de seus acessos, afim de garantir que a informação privilegiada não seja transmitida de forma indevida. O controle de acesso tem como meta a proteção dos softwares, aplicativos, modificação e divulgação não autorizada da informação.

- Controle de acesso logico: Os acessos lógicos devem ter como controle os procedimentos e regras com o objetivo de proteção aos dados. Neste devem ser utilizados programas e softwares na tentativa de combater o uso de ferramentas não autorizadas, pode ser diferenciado de duas maneiras: a partir do recurso onde se quer proteger ou a partir do usuário a quem é concedido os privilégios. É importante manter a identificação do usuário sendo por lD e senha durante um logon no sistema, também é necessário um sistema robusto onde basicamente tenham os logs de entrada e saída do usuário, nesta terá informações da data complementando com as informações de origem de conexão. Abaixo tem-se os principais tópicos envolvidos:
  - Aplicativos: O acesso não autorizado pode modificar códigos fontes de aplicativos, por exemplo financeiros ou bancários, onde é possível alterar dados pessoais e transferir fundos para outra conta corrente.
  - Arquivo de dados: Arquivos de transações e banco de dados devem ter proteção para garantir a integridade que não sejam alterados, por exemplo arquivos estratégicos e sistemas de recursos humanos.
  - Sistema operacional: Principal alvo para os ataques, se encontra várias informações de sistemas e aplicativos que muitas vezes estão diretamente relacionados aos arquivos de dados e configurações de sistema. Esta como chave de esquema da segurança da informação devido a ter todo o conjunto de aplicativos e utilitários. Sofrem constantes atualizações para corrigir bugs e vulnerabilidades afim de manter o sistema operacional e seus hospedeiros protegidos.

- Logs: Arquivos de logs podem conter informações sigilosas como endereços e logins, são utilizados para registrar ações do usuário onde na maioria dos casos contem aplicativos acessados, arquivos de dados e utilitários. Um invasor mal-intencionado pode apagar os logs onde modificou o sistema operacional para que o administrador de redes ou do sistema não identifique o que foi alterado.
- Senhas: As senhas muitas vezes são salvas em arquivos e anotações rápidas sendo virtual ou papel, o que acaba criando brechas na segurança e comprometendo todo o sistema, uma pessoa má intencionada e não autorizada ao se ter o ID e uma senha com altos privilégios de acesso, pode roubar informações ou causar danos a todo o sistema. Este usuário dificilmente será identificado pelos controles de segurança, pois irá se passar por um usuário autorizado.

5.1 AUTENTICAÇÃO

O ato de estabelecer ou confirmar algo é chamado de autenticação, para segurança da informação este processo pode ter várias camadas. Sabendo disso existem vários mecanismos de autenticação que compõem o processo estes são os principais: senhas, impressão digital, padrão de voz, assinatura, token, biometria, padrão ocular.

Com todos os recursos para autenticação disponíveis foram criados sistemas onde se utiliza destes recursos, os softwares atuais possuem integração para que o usuário na hora de se identificar garanta sua autenticidade, frequentemente é utilizado a autenticação em dois fatores, onde é necessário se autenticar duas vezes de maneira diferente.

5.2 SENHAS

O conceito básico de senha é que primeiramente ela é privada, ou seja, algo que apenas seu ID de login registrado deve saber. Se outra pessoa sabe sua senha ela já não é mais privada e seus dados registrados já não estão mais seguros. Um

invasor mal-intencionado pode utilizar suas credenciais, se passar por você no universo online e trocar seus dados pelos deles, assim expandindo as possibilidades de impacto e prejuízo. Portanto para garantir que ninguém tenha suas senhas o ideal é não reutilizar credenciais antigas, uma senha simples para você, também é simples para os outros.

As boas práticas para utilização de senhas é sempre ter a maior complexidade possível, não utilizar nomes próprios, datas comemorativas, nomes de parentes. Basicamente palavras simples de dicionários são senhas fracas, os softwares atuais possuem dicionários internos onde as senhas fracas são facilmente descobertas. As senhas ideais são aquelas que possuem acima de 6 caracteres, com letras maiúsculas e minúsculas, números e caracteres especiais por exemplo: “S#nh2SEgur2”.

5.3 ENGENHARIA SOCIAL

Invasões a sistemas ou ataques cibernéticos, muitas vezes é planejado e orquestrado para que se tenha o sucesso. É utilizado a engenharia social para obter informações e dados das empresas que serão vítimas. “O Engenheiro Social sabe explorar facetas como vaidade, humildade, egocentrismo, utilizando técnicas de galanteio social, a fim de obter informação a respeito de alguém ou de uma instituição. ” (MARCELO; PEREIRA, 2005, p. 4).

A cautela com a engenharia social é muito importante para garantir a segurança nas empresas. O principal meio de explorar o alvo é garantir sua confiança, isto muitas vezes pode demorar certo tempo e paciência, o alvo é investigado e suas principais fraquezas são utilizadas para conseguir informações privilegiadas, dentre delas e-mails, endereços, contatos privilegiados e muitas vezes se obtém a própria senha do usuário. Abaixo estão, as principais maneiras de conseguir informações por engenharia social:

a) Telefone: desta maneira o hacker utiliza telefones públicos para dificultar o rastreio, neste tenta coletar o máximo de informações e procura sempre adquirir dados sobre cargos ou para confirmar se a informação obtiva anterior é verdadeiro, muito utilizado em golpes.

b) E-mail: Devido ao crescimento da internet a comunicação por e-mail passou a ser ferramenta de trabalho essencial, neste são trafegados dados importantíssimos, o hacker envia e-mails com keyloggers de arquivos tentadores, promoções imperdíveis, pornografia, relatórios importantes, boletos e cobranças bancarias.
c) Presencial: Está maneira é mais arriscada para o hacker, o mesmo é aparece pessoalmente no alvo, se passando por alguém em busca de informações ou até representando falsamente ser vendedores, faxineiro e até funcionário da empresa, afim de adquirir informações.

6 POLÍTICA DE SEGURANÇA EM REDES DE COMPUTADORES

Após a análise de risco e já conhecendo a necessidade de segurança da empresa, podemos criar a política de segurança para os equipamentos de redes tanto física como logica, também a política irá abordar de que maneira a política se torna rotina no dia-a-dia. Ou seja “diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações” (TCU, 2012).

Durante a formação da política devem ter como participantes integrantes de recursos humanos, gestores e profissionais em segurança da informação. Estes irão elaborar o documento oficial, revisar e aprovar a política, assim como atribuir os papeis de quem irá garantir que as regras sejam aplicadas. Uma política de segurança da informação protege a empresa e o usuário caso ocorra alguma violação de ambos, para que tenham recursos e meios legais na justiça.

Toda PSI não deve ficar restrita apenas ao setor de TI, deve estar ligada diretamente a visão, missão e metas de negócio institucionais. Seu conteúdo, pode variar de instituição para instituição, por motivos de cada empresa ter informações e prioridades diferentes, além do grau e maturidade dos usuários. Empresas de tecnologias geralmente possuem maturidade suficiente para discernir erros, problemas ou situações suspeitas, algo que em uma empresa do setor de contabilidade por exemplo, está mais sucessível a erros de segurança da informação. Os itens que devem ser abordados e serão discutidos na criação da PSI são:

- A importância da segurança da informação e como ferramenta de compartilhamento de dados.
- Comprometimento com a gerencia da PSI, apoiando a visão da empresa e princípios.
- Objetivos da segurança na empresa.
- Responsabilidades e riscos.
- Padrão mínimo de qualidade dos sistemas.
- Gestão da continuidade do negócio.
- Conformidade dos sistemas.
- Sistemas de detecção de vírus e procedimentos de prevenção.
- Treinamento.

- Elaboração da proposta.
- Revisão.

6.1 APLICAÇÃO

A política de segurança deve valer para todos que irão utilizar equipamentos de microinformática ou irão prestar suporte a estes, “A PSI é o primeiro de muitos documentos com informações cada vez mais detalhadas sobre procedimentos, práticas e padrões a serem aplicados em determinadas circunstâncias, sistemas ou recursos. ” (TCU, 2012). As normas criadas podem incrementar com a documentação de admissão de um funcionário por exemplo, assim antes de utilizar os equipamentos o empregado já terá conhecimento das melhores práticas de segurança da informação.

Digamos que a demanda da empresa o setor de segurança e redes de TI, seja de alto sigilo, e que as informações trocadas durante o trabalho entre os funcionários sejam de alto valor aos concorrentes, pode-se sugerir as regras da seguinte maneira:

1. A política deve estar inclusa no processo de admissão de funcionários que irão trabalhar no setor de TI.
2. O documento deve conter quais serão os acessos e permissões que serão concedidos, privilégios, logins, entradas, saídas e quais ferramentas de trabalho.
3. Todo equipamento de rede deve estar registrado como patrimônio.
4. Realizar treinamentos sobre segurança da informação, de acordo com a importância dos dados e imagem da empresa.
5. Nenhuma mudança ou movimentação de recursos físicos e lógicos devem ser executados sem o de acordo da alta gestão.
6. Não anotar senhas em arquivos internos, papeis ou bilhetes.
7. Respeitas as regras de acesso à internet.
8. Zelar o patrimônio físico dos equipamentos e respeitar as condutas da segurança de trabalho.
9. Utilizar as ferramentas exclusivamente da empresa.

10. É mandatório que a organização esteja submetida a leis ou órgãos regulamentadores, que tem poder sobre todas as organizações da área de negócio.
11. Colaboradores de Férias e afastamento devem ter seus acessos bloqueados.
12. Colaboradores que mudarem de setor, devem perder os acessos anteriores caso seja de equipes onde não irá se exercer a mesma função.
13. Os Equipamentos de redes só devem ser acessados dos computadores de TI.
14. Equipamentos de redes, desktops e servidores devem estar com os últimos patches de atualização do fornecedor.
15. Crie rotinas para prevenir falhas.
16. Utilizar tecnologias que são adequadas para as necessidades da rede.
17. Manter os backups e redundâncias em pleno funcionamento.
18. Reportar a segurança da informação o recebimento de e-mails e ligações suspeitas de fatores externos.
19. Todo e qualquer incidente deve ser registrado.
20. Todos os participantes do documento são responsáveis em garantir a segurança dos sistemas e redes de informações.
21. Gestores tem como função identificar em seu setor se há desvios das regras impostas.
22. Nenhum equipamento entra em produção sem monitoramento.
23. Terceiros ou fornecedores, só terão acessos as dependências da empresa com o de acordo da gerencia e acompanhado de um funcionário da área de TI.
24. Sempre priorizar os ativos relacionados a informação e que são considerados críticos.
25. Reportar mal funcionamento de softwares ou hardware dos equipamentos.
26. O gestor deve informar o setor de recursos humanos, violações das regras impostas da política.

6.2 AVALIAÇÃO E RENOVAÇÃO DA POLÍTICA

Após alguns anos, novos processos e a evolução da tecnologia a política de segurança pode se tornar obsoleta, ou já não estar adequada aos negócios da

empresa, isto define como acontecerá a manutenção e atualização de regulamentos. Também com mais detalhes de quem é o responsável pelas atualizações da política.

6.3 OBJETIVOS DO NEGÓCIO E ORGANIZAÇÃO

Visando sempre os interesses da empresa como visão de negócio, a política de segurança deve refletir os objetivos da empresa. “O gestor de segurança da informação é o especialista que irá levantar as questões, recomendar controles e indicar os riscos referentes a proteção da informação para a organização especifica.” (FONTES, 2012, p. 88). No entanto quem irá tomar as decisões e grau dos controles de ser o gestor da área de negócio, por exemplo a TI irá fornecer a infraestrutura e meios técnicos para garantir o armazenamento dos dados, mas a área de negócio irá definir por quanto tempo aqueles dados devem ser mantidos, porque o gestor conhece os regulamentos e legislações que devem ser cumpridos, inclusive essas decisões são ofensoras de qual mídia de armazenamento será utilizado, ou como o setor de TI irá definir o melhor meio de cumprir com o solicitado. Aqui vão ser tratados os seguintes temas:

- Monitoramento: Apresentar se os dados de coletas são verdadeiros, sugestões de melhoras, bugs com os prazos estabelecidos pela área de negócio.
- Patrimônio: Com a necessidade novos ativos irão fazer parte da empresa e devem ser registrados, também a compra pode variar de acordo com a necessidade e expansão, o que muitas vezes dependendo da tecnologia gere uma nova política de segurança.
- Revisão: avaliar se a política ainda está de acordo com a visão e imagem da empresa, também se a política torna as atividades confusas ou tópicos que muitas vezes podem não fazer mais sentido com o passar dos anos.
- Arquivamento: Monitoramento, logs e registros dos acessos bem como documentos com as assinaturas por exemplo de funcionários, algo importante a se zelar visto que qualquer prova é útil para o funcionário e empregador para defesas legais em caso de incidentes ou vazamento de informações.
- Leis: Manter a política de segurança atualizada de acordo com as leis e legislação.

- Plano de Continuidade: A revisão da política para os usuários com questionários e perguntas pela intranet, é um meio de inserir as normas e regras no cotidiano dos usuários, ou seja, a política acaba fazendo parte da rotina de trabalho dos funcionários.

7 CONCLUSÃO

De acordo com o que foi apresentado nesta pesquisa para manter informações seguras, com disponibilidade, integridade e total sigilo para equipamentos e ativos de TI, demostramos que a criação e revisão da política de segurança da informação pode padronizar, organizar, gerenciar e prevenir vulnerabilidades, e também que informações e dados sejam expostos.

A análise de risco como um dos principais pilares para criação da política nos dá visão da imagem e valores da empresa, assim como quais os pontos fracos de cada organização, dando contexto da importância de obter segurança física e logica dos equipamentos de redes, em manter os ativos atualizados e do quanto esforço e necessário para garantir a integridade dos serviços.

O emprego de uma política de segurança deve ser revisado e avaliado. Por ser um documento oficial da empresa foram abordados o que os gestores e executivos tem como participação, pois estes que vão garantir a eficácia das normas, assim como cláusulas contratuais. Desta maneira todos devem cumprir as regras com o intuito de alcançar as metas estabelecidas sem prejuízos a corporação, de acordo com a legislação vigente.

Depois de várias pesquisas ao tema de segurança da informação, é comprovado que mesmo tendo políticas e equipamentos avançados de segurança, o maior risco são os recursos humanos, despertando uma certa preocupação e o quanto o tema é frágil e crítico. Para meios legais de defesas tanto para o empregado e empregador as normas estabelecidas nas políticas de segurança assinada e oficial é um meio de proteção legislativo.

Para futuros estudos é recomendado inserir controles de acesso e explorar melhor as vulnerabilidades da segurança logica, analisando mais a fundo o trafego da rede com sistemas mais sofisticados e tomadas de decisões por violações da política de segurança. Também o tempo necessário para implantação da política e como o investimento gasto.

REFERÊNCIAS

ABNT. **ABNT NBR ISO/IEC 17799. Tecnologia da informação - Técnicas de Segurança:** Código de prática para a gestão da segurança da Informação. Associação Brasileira de Normas Técnias (ABNT). Copyright© ABNT, 2005.

BEAL, Adriana. **Segurança da informação**: Princípios e melhores práticas para a proteção dos ativos de informação nas organizações. 1. ed. São Paulo: Atlas, 2005.

BRIDGE**. Os riscos de TI e seus impactos no negócio: Como gerenciar os riscos de TI usando o ITIL**. Copyright© Bridge Consulting, publicado em: out. 2015. Disponível em: <http://www.bridgeconsulting.com.br/wp-content/uploads/2015/10/artigo_riscos_de_ti.pdf>. Acesso em: 17 out. 2018.

CARISSIMI, Alexandre da Silva; ROCHOL, Juergen; GRANVILLE, Lisandro Zambenedetti. **Redes de computadores**. 1. ed. Porto Alegre: Bookman, 2017.

CISCO. **Cisco TelePresente system administration guide**. Copyright© Cisco Systems, Inc., publicado em: out. 2015. Disponível em: <https://www.cisco.com/c/en/us/td/docs/telepresence/ix_sw/8_x/admin/guide/ix_8_admin_guide.pdf>. Acesso em: 22 out. 2018.

FONTES, Edison. **Políticas e normas para a segurança da informação**: Como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012.

MARCELO, Antônio; PEREIRA, Marcos. **A arte de hackear pessoas**. Rio de Janeiro: Brasport, 2005.

MARCIANO, João Luiz Pereira. **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. Disponível em: <http://www.enancib.ppgci.ufba.br/premio/UnB_Marciano.pdf>. Acesso em: 20 out. 2018.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lúcio de. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec Editora, 2007.

SÊMOLA, Marcos. **Gestão da segurança da informação**: Uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2003.

SILVA NETTO, Abner da; SILVEIRA, Marco Antonio Pinheiro da**. Gestão da segurança da informação: Fatores que influenciam sua adoção em pequenas e médias empresas**. Revista de Gestão da Tecnologia e Sistemas de Informação, Journal of Information Systems and Technology Management**,** v. 4, n. 3, p. 375-397, São Paulo, 2007. Disponível em: <http://www.scielo.br/scielo.php?pid=S1807-17752007000300007&script=sci_abstract&tlng=pt>. Acesso em: 22 out. 2018.

TCU. **Boas práticas em segurança da informação**. Tribunal de Contas da União (TCU), Secretaria de Fiscalização de Tecnologia da Informação. 4. ed. Brasília: TCU, 2012.