ESAB – ESCOLA SUPERIOR ABERTA DO BRASIL

ANÁLISE DE SEGURANÇA E PROTEÇÃO PARA UM SERVIDOR CORPORATIVO

Willian Gonçalves[1]
Janaina Costa Binda[2]

Resumo

Este artigo aborda o tema de segurança em servidores corporativos e para isso buscou-se autores diversos que abordam o assunto em questão. O estudo teve como intuito analisar os requisitos básicos de segurança para um servidor corporativo identificando ameaças e vulnerabilidades, seja ela na parte física ou lógica do servidor, visto que as empresas cada dia mais se preocupam em fornecer aos seus clientes e fornecedores uma imagem de uma organização sólida e confiável, necessitam cada vez mais de segurança em seus processos, por meio de uma pesquisa descritiva e coleta de dados bibliográficos, concluiu-se por meio do estudo realizado que deve ser definida, estruturada e implementada uma política de segurança, para que as ameaças e vulnerabilidades sejam minimizadas e consequentemente proporcionando um nível de segurança satisfatório.

Palavras-chaves: Segurança em redes. Segurança em servidores. Segurança de hardware. Segurança lógica. Segurança física.

1. Introdução

Ao longo das últimas décadas, acumulou-se um significativo acervo científico e tecnológico no campo da Tecnologia da Informação, especificamente na última década, foram muitos os estudiosos que contribuíram para a Ciência da Informação. Devido aos estudos a esta ciência estará sempre em constante mudanças, sua evolução está cada dia mais acelerada. As organizações em busca de otimizar seus processos e ampliar os negócios estão cada vez mais aderindo a tecnologia, hoje para uma empresa que busca se manter no mercado é indispensável a utilização da mesma. Deste modo a segurança em rede e servidor é um fator extremamente importante para o sucesso ou o fracasso da empresa, e isso vem se

[1] Graduado em Tecnologia em Análise e Desenvolvimento de Sistemas pela Univel – Faculdade de Ciências Sociais e Aplicadas de Cascavel, Pós-Graduando em Sistemas para a Internet e Dispositivos Móveis pela UNIPAR – Universidade Paranaense e Pós-Graduando em MBA Profissional em Engenharia de Sistemas na Escola Superior Aberta do Brasil. Professor de Curso Técnico em Informática no Colégio Estadual Amâncio Moro – Corbélia-PR. willian@solucorpti.com.br

[2] Mestra em Administração de Empresas pela FUCAPE; Especialista em Gerência de Projetos (PMI) pelo Centro Universitário de Vila Velha e em Marketing e Tecnologia da Informação pela UFES; Bacharel em Administração com habilitação em Análise de Sistemas pela UNESC. Experiência docente, coordenação de curso superior e orientação de trabalhos de conclusão de cursos de graduação e pós-graduação. Professora orientadora de TCC dos cursos pós-graduação da Escola Superior Aberta do Brasil ESAB, Vila Velha, ES.

tornando um tema cada vez mais relevante no mercado da tecnologia da informação, visto a crescente necessidade de proteção dos usuários e os dados por eles acessados e transmitidos (CARUSO, 1993).

Segundo Soares et al (1995) o termo segurança é usado com o significado de minimizar vulnerabilidades de bens e recursos.

Ainda de acordo com os autores, a necessidade de proteção de uma rede deve ser definida em termos de evitar possíveis ameaças e riscos à segurança das organizações, e estes procedimentos devem estar formalizados nos termos de uma política de segurança.

O presente estudo busca analisar os requisitos básicos de segurança para um servidor corporativo, identificando ameaças e vulnerabilidades, seja ela na parte física ou lógica do servidor.

Neste intuito este trabalho foca-se descrever os requisitos básicos de segurança para um servidor corporativo e identificar possíveis falhas na segurança física (hardware) e lógica (software) do servidor.

No mundo globalizado do século XXI, é de vital importância para empresas que pretendem se manter em um mercado cada vez mais competitivo, uma análise minuciosa de sua estrutura de servidores para adequar a organização e a segurança oferecida aos clientes/usuários, ao ambiente em que estão inseridos.

O delineamento do presente estudo foi realizado com base na técnica de pesquisa bibliográfica, pois segundo Gil (2002, p.45), “a principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente.”

Assim, a pesquisa se classifica como pesquisa descritiva com coleta de dados bibliográficos, sendo que o presente estudo iniciou-se desta forma e foi construído estruturado em materiais já elaborados, em sua maioria livros e artigos científicos.

2. A Necessidade de Segurança

A tecnologia da informação é um mercado que está em constante crescimento e evolução, a cada dia se faz mais presente nas organizações corporativas. Caruso (1993) afirma que a partir dos anos 1990 houve um crescimento explosivo do uso de computadores pessoais, e o objetivo é substituir o máximo possível do processamento coorporativo. Ainda enfatiza o autor que devido a popularização de computadores pessoais houve um aumento significativo

no risco de exposição de dados. Sendo assim tratar a vulnerabilidade e segurança está ficando cada vez mais difícil e preocupante.

De acordo com Moraes (2010) pode-se definir Segurança da Informação como um processo de proteger informações do mau uso sendo ele intencional ou não, sendo por pessoas internas ou externas à organização. Ress (2011) segue a mesma linha afirmando que a segurança tem como objetivo garantir a confidencialidade, integridade e disponibilidade dos elementos no qual os dados utilizam.

Segundo Comer (2006, p. 359):

> A segurança implica em proteção incluindo a garantia da integridade dos dados, impedimento de acesso não-autorizado de recursos computacionais, impedimento de escutas ou grampos e impedimento de interrupção do serviço. Naturalmente, assim como nenhuma propriedade física é absolutamente segura contra crime, nenhuma rede é completamente segura. As organizações se esforçam para proteger as redes pelo mesmo motivo pelo qual se esforçam para proteger prédios e escritórios: medidas de segurança podem desencorajar o crime, tornando-o significativamente mais fácil.

A segurança é um fator determinante para o sucesso ou fracasso de uma organização, este tema é cada vez mais discutido no mercado da tecnologia, tendo a crescente necessidade de proteção dos dados armazenados e transmitidos. Isso se afirma pelos constantes estudos.

Para Comer (2006, p.359), “Fornecer segurança para a informação exige proteger os recursos físicos e abstratos”. Para Soares, et al (1995, p.448) “o termo segurança é usado com o significado de minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos”.

Ainda segundo os autores, uma política de segurança deve ser formalizada para evitar possíveis ameaças e riscos à segurança da organização.

De acordo com Moraes (2010), um modelo de referência de segurança é constituído por alguns componentes que são: Equipamentos, sistemas de autenticação, sistemas de segurança e sistemas de auditoria.

2.1 Política de Segurança

Segundo Tanenbaum (2003), a maioria dos problemas de segurança são causados por pessoas maliciosas tentando obter algum benefício ou prejudicar alguém. Ainda de acordo com o autor, as pessoas e empresas utilizam sistemas e redes para fazer compras, realizar transações bancárias e arquivar devolução de impostos. Devido ao gigantesco leque de opções e visando proteger as informações transmitidas e recebidas a segurança deve ser observada

como um fator preferencial conforme afirmam Nakamura e Geus (2010, p.188) “A política de segurança é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações”.

Nakamura e Geus (2010) explicam que uma política de segurança é o primeiro passo para a estratégia de segurança de uma organização. Moraes (2010) define política de segurança como diretrizes quanto ao uso das informações no ambiente corporativo o autor ainda diz que o propósito é definir como uma organização irá se proteger de incidentes de segurança.

Moraes (2010) define a Segurança da Informação como um processo para proteger as informações de ameaças, tanto do mau uso, quanto acidental ou intencional seja ela por pessoas internas ou externas à organização. As informações que possuem algum valor econômico para a organização devem receber proteção.

Segundo caso apresentado por Nakamura e Geus (2010), Timothy A. Lloyd foi colaborador da Omega Enginneering Corp por 11 anos, Lloyd era responsável pela segurança de rede da empresa. A falta de uma política de segurança permitiu que ele implantasse uma bomba lógica explodindo dias após a sua demissão o que causou prejuízos calculados em dez milhões de dólares, assim o autor da ênfase que uma política é importante para evitar problemas como os da Omega.

Comer (2006) afirma que a organização depois de avaliar os riscos deve definir uma política de segurança clara com relação ao acesso e proteção das informações. Caruso (1993, p. 39) diz que “no caso de redes locais, este aspecto deve merecer maior atenção devido à grande importância dos dados corporativos nelas contido”.

De acordo com Moraes (2010), uma política de segurança deve ser genérica e variar pouco com o passar dos anos, o autor ainda enfatiza que não deve ser uma lista de ameaças, equipamentos ou pessoas específicas.

Segundo Comer (2006), uma política de segurança deve-se começar com pessoas, pois um trabalhador malicioso pode comprometer a segurança da organização. Nakamura e Geus (2010) seguem a mesma linha afirmando que uma política de segurança trata dos aspectos humanos, culturais e tecnológicos, nela são definido os aspectos envolvidos na proteção dos recursos existentes, desta forma a elaboração e planejamento ocupam grande parte do trabalho dedicado. De modo a uma melhor visualização Nakamura e Geus (2010) ilustra o planejamento da política de segurança através da figura 1.

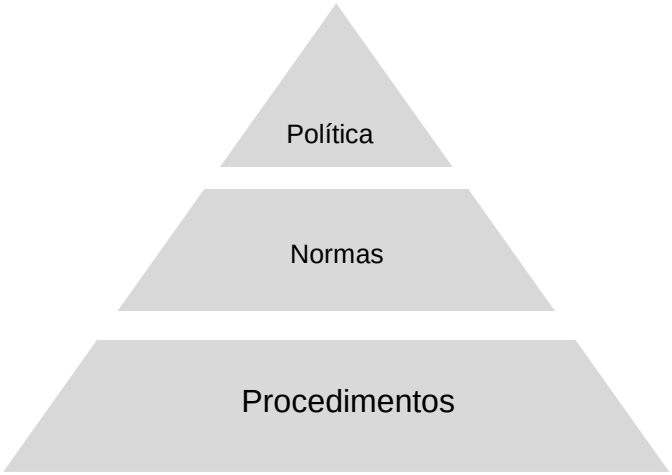

Figura 1 – O planejamento da política de segurança
Fonte: Nakamura e Geus (2010, p.190)

A política que fica no topo da pirâmide é o elemento que orienta as ações e as implementações de uma maneira global, já as normas abordam detalhes, conceitos e práticas de implementação, e por fim para cumprir o que foi definido na política os usuários devem seguir os procedimentos. (NAKAMURA; GEUS, 2010)

2.2 Segurança em Ambiente Físico

Segundo Anonymus (2000), os livros atuais focam mais em segurança de rede, que também, não deixa de ser uma importante questão. Entretanto a segurança física deve ser o primeiro objetivo. Moraes (2010) diz que a segurança física deve ter por objetivo prevenir acessos não autorizados, perda, dano, roubo de informações além de interrupção das atividades da organização. Segue a mesma linha Comer (2006, p.359) que afirma que: "A segurança implica em proteção incluindo a garantia e integridade dos dados, impedimento de acesso não-autorizado de recursos computacionais, impedimento de escutas ou grampos e impedimento de interrupção do sistema". Ainda complementa que se medidas de segurança básicas forem adotadas o crime se torna mais difícil podendo assim ser desencorajado.

Caruso (1993) divide em quatro grupos os ricos físicos em microinformática, que são: Infraestrutura de instalação, condições ambientais, controle de acesso físico e condições operacionais.

Em nível empresarial alguns cuidados devem ser tomados em relação à infraestrutura de instalação (CARUSO 1993).

Anonymus (2000), expõe que a localização do servidor e o acesso físico são dois pontos importantes em relação à segurança física de computadores. O autor ainda completa

que os controles de segurança são inúteis quando usuários maliciosos possuem acesso físico ao servidor.

De acordo com Caruso (1993), dentro da infraestrutura de instalação um dos pontos que é de extrema importância é a instalação elétrica, sempre observando a qualidade e a instalação do material. Velloso (2003) afirma que visando a segurança dos sistemas, em instalações de microcomputadores equipamentos de proteção elétrica devem ser utilizados, o autor complementa que sempre deve se possuir equipamentos como: *No-Break*, estabilizador de tensão e filtro de linhas, visando a proteção dos circuitos, pois anomalias podem ser apresentadas nas as redes de abastecimento.

Corroborando com Velloso (2003), Caruso (1993) afirma que a utilização de aterramento e filtros de linhas é muito importante e sempre recomendado. Velloso (2003) explana que as instalações elétricas que chegam as máquinas devem sempre possuir um terceiro pino em suas tomadas ligados a um aterramento. Para Vasconcelos (2009), o terceiro fio denominado fio terra, não existe corrente elétrica, o objetivo deste fio é manter a um potencial a ZERO o mesmo do solo a carcaça externa dos equipamentos, o autor explica que um aterramento ideal, consiste introduzir no solo uma haste de cobre de com 3 metros de profundidade.

Caruso (1993), dentro do contexto de condições ambientais, fala sobre precauções que devem ser tomadas para um bom funcionamento e longevidade dos equipamentos, entre elas encontram-se: Arranjo físico; iluminação; combate ao fogo; temperatura e umidade.

Anonymus (2000) diz que as organizações devem proteger o seu servidor abrigando-o em uma área restrita denominada centro de operações de redes, que consiste em uma sala segura, onde poucas pessoas tenham acesso preferivelmente separada e não no térreo. Caruso (1993), afirmando sobre arranjo físico diz que, para se determinar o local onde será instalado é preciso ter conhecimento das dimensões dos equipamentos e do espaço livre. Ainda afirma que a sala deve ser bem iluminada evitando a luz solar, extintores devem ser instalados para combate ao fogo, evitar ambientes muito quentes ou úmidos, isso evita o mau funcionamento.

De acordo com Caruso (1993), o controle de acesso físico se torna complexo, pois deve-se ter controle de acesso a sala do servidor, evitando assim que pessoas não autorizadas e ou mal-intencionadas consigam se munir de informações de valor corporativo. Anonymus (2000) corrobora com essa visão afirmando que poucas pessoas devem possuir acesso a sala do servidor e as que possuem deve ter uma chave e manter um log de acesso. Ainda cita que um bom método para esse controle são chaves-cartão que podem restringir acesso até mesmo de pessoas autorizadas em certas horas.

No quesito controle operacional Caruso (1993) cita *backup* com um de seus itens, afirmando que cópias de segurança devem ser feitas periodicamente, assim se a empresa for vítima de um roubo ou de uma invasão esta prática facilita a recuperação dos dados. Ainda complementa que se possível mais de uma cópia deve ser gerada.

2.3 Segurança em Ambiente Lógico

As organizações utilizam *firewalls* e equipamentos para proteger suas redes, mas isto não é o suficiente, pois os *hackers* a cada dia possuem novas técnicas de invasão. (MORAES 2010). Esta ideia também é complementada por Nakamura e Geus (2010), que afirmam que somente o *firewall* não garante a segurança de uma organização.

Os *Firewalls* são sistemas que ajudam a proteger as informações para que uma empresa não esteja vulnerável se tornando indispensáveis dentro de uma organização. Segundo Moraes (2010, p.159) "o *firewall* pode autorizar, negar, além de registrar tudo que está passando por ele". Corroboram com a afirmação Nakamura e Geus (2010) afirmando que o *firewall* recebe as informações e avalia, as não autorizadas são descartadas.

Strebe (2002) afirma que existem diversos tipos de *firewall* sendo destinados a garantir a segurança de uma rede. O autor explica que os *firewalls* ficam conectados à internet analisando os pacotes, ou seja aprovando ou não os pacotes que pela rede trafegam. Segundo Moraes (2010, p. 160), "embora existam muitos programas vendidos com a denominação de *firewall*, um *firewall* não é um programa e sim um conjunto de recursos de *hardware* e *software* destinados a garantir a segurança de uma rede".

Em segurança de ambiente lógico, outro aspecto se destaca quando falamos de servidor corporativo. De acordo com Nakamura e Geus (2010), o *firewall* é apenas um componente que participa da estratégia de segurança, em um ambiente corporativo é essencial a implementação de sistema de detecção de intrusão que tem por objetivo auxiliar na proteção do ambiente contra ataques e invasão do sistema. Anonymus (2000) complementa a ideia afirmando que quando utilizado ferramentas automatizadas e inteligentes pode-se detectar invasões em tempo real.

Segundo Nakamura e Geus (2010), quando um *firewall* é implementado algumas portas são permitidas e um sistema de detecção de intrusão é capaz de detectar invasões que de algum modo foram permitidos pelo *firewall*. Ainda complementa que este sistema é capaz de detectar, analisar e responder as atividades consideradas suspeitas.

Para ajudar a conter a vulnerabilidade e proteger os dados das organizações podemos contar com a ajuda da criptografia.

Segundo Moraes (2010, p. 770, grifo do autor) "Criptografia é a ciência que utiliza algoritmos matemáticos para criptografar/encriptar (cripto = esconder) dados (textos claro) numa forma aparentemente não legível (texto cifrado) e recupera-los (descriptografa-los)".

Segundo Tanenbaum (2003), a criptografia é uma palavra grega que quer dizer escrita secreta.

De acordo com Nakamura e Geus (2010), a criptografia é a ciência de manter mensagens segura, e a cada vez é mais fundamental dentro de uma organização. Ainda afirma que a criptografia possibilita a integridade; autenticidade; não-repudio e sigilo. Corrobora com a ideia Moraes (2010), afirmando que a criptografia pode ser utilizada para: garantir que pessoas não autorizadas tenham acesso as informações transmitidas, manter a integridade dos dados; não-repudio além de garantir que não seja alterado os dados transmitidos. Ainda completa que a criptografia é uma ciência que existe muito antes dos computadores, era utilizada no império romano para esconder mensagens enviadas, e somente tinha significado para quem sabia como decifrar a mensagem.

Para Nakamura e Geus (2010), o ambiente cooperativo é formado por matriz, filiais, fornecedores, usuários e clientes, e por meio desta cooperação os negócios são realizados e formalizados. Os Autores afirmam que dentro do ambiente cooperativo um importante componente é a rede privada virtual que consiste em garantir uma conexão segura em uma rede pública.

De acordo com Moraes (2010), uma VPN[3] ou rede virtual privada é baseada em criptografia tornando-se assim uma conexão segura. Ainda afirma que seu objetivo é transportar informações por meio de uma rede insegura. Corroboram com a ideia Nakamura e Geus (2010), afirmando que as redes virtuais possibilita criar conexões privadas por meio de uma única ligação com a rede pública.

Segundo Strebe (2002, p. 167), "as VPNs são uma forma economicamente viável de estender uma rede local pela internet até redes remotas e computadores clientes remotos". Complementa essa afirmação Nakamura e Geus (2010), explicam que as redes privadas virtuais possui um custo relativamente mais baixo quando comparado com uma conexão dedicada.

[3] VPN – *Virtual Private Network* (redes privadas virtuais)

São características das VPNs de acordo com Moraes (2010, p.108, grifo do autor), “Autenticação: identificar com quem se está comunicando; Tunelamento: encapsular os dados roteados através da rede pública; Criptografia: garantir segurança.” Corrobora com Moraes (2010), Nakamura e Geus (2010), afirmando que os fundamentos das redes privadas virtuais são criptografia e tunelamento.

Segundo Comer (2006), para entender as VPNs é preciso pensar em cada túnel separadamente como um circuito alugado em uma rede privada.

Para Nakamura e Geus (2010), a criptografia tem por objetivo dentro das redes privadas virtuais garantir a autenticidade, sigilo e integridade das conexões, para que as informações sejam transmitidas com segurança pela rede pública, as duas partes da conexão formam um túnel.

De acordo com Moraes (2010), as VPNs são utilizadas para ampliar ou substituir redes privadas e quanto mais espalhada geograficamente está à organização maiores serão os benefícios obtidos das redes privadas virtuais.

3. **Considerações Finais**

Devido a necessidade eminente de implementação tecnológica das diversas formas da tecnologia da informação, as organizações deram um salto muito importante nos últimos anos, pois estão aptas a desenvolverem serviços e parcerias antes consideradas impossíveis em razão das distâncias geográficas.

Muitos dos profissionais da área de tecnologia da informação dedicam-se a estudar sobre o termo segurança corporativa, pois segundo Moraes (2010), uma rede nunca está 100% segura. Baseando-se nisso, no decorrer do trabalho foi possível analisar, que apesar de não existir uma rede ou 100% segura, alguns requisitos básicos devem ser analisados e implementados para tornar a organização menos vulnerável. As empresas vêm se tornando alvos de muitos ataques, pois é em seu servidor que os dados dos usuários e clientes são mantidos. Esses ataques visam sempre capturar ou alterar os informações das organizações.

O objetivo desta pesquisa foi analisar como um servidor corporativo deve ser instalado e configurado de forma a se obter o máximo de segurança possível, sempre lembrado que não são somente ataques de *hackers* que ameaçam a segurança dos dados da organização. A segurança física é um fator extremamente importante para garantir a segurança do servidor e das informações armazenadas por ele.

Por meio deste trabalho foi possível identificar que, para a empresa garantir a segurança necessária, uma política de segurança deve ser implementada pela organização. Esta política deve se preocupar tanto com a parte física quanto a lógica de seu servidor e equipamentos.

Os autores estudados e pesquisados neste trabalho têm uma grande preocupação com a instalação e acesso do servidor sempre buscando minimizar a vulnerabilidade do mesmo. No momento de se escolher o local para a instalação do servidor, alguns itens devem ser observados, levados em consideração como: possuir um local separado dentro da empresa, sempre bem arejado e seco, pois ao contrário disto pode danificar o hardware, é recomendado que o servidor seja instalado evitando o andar térreo quando possível e com uma cobertura adequada e resistente, pois ninguém está livre de desastres naturais como enchentes e granizo. Outro ponto crucial para a parte física é a instalação elétrica, que deve sempre possuir aterramento, isto previne a queima dos equipamentos por descarga elétrica ou raios. E por fim visando o combate ao fogo extintores carregados com carga adequadas devem ser instalados, não somente na sala do servidor mas em toda a organização em pontos de fácil acesso sempre com instruções de como utilizar.

Conforme apresentado, Moraes (2010) diz que a cada dia os hackers exercitam sua capacidade com novas técnicas de invasão e visando minimizar/reduzir estas invasões algumas ferramentas devem ser adotadas pela organização como: a implementação de VPNs, pois assim as parcerias com fornecedores e acessos externos acabam sendo feitos por meio de túneis encapsulados tornando assim a conexão segura como uma rede local. A organização deve implementar um *firewall* de acordo com suas necessidades definidas na política de segurança, assim, bloqueando portas não utilizadas e consequentemente dificultando a invasão ao servidor. Ferramentas de criptografia devem ser utilizadas para que pessoas não autorizadas não se aposse de informações na qual não a diz respeito.

Contudo não é só os acessos que dever receber uma atenção, os dados e informações dos clientes precisam ser mantidos seguros, o mínimo neste caso seria copias de segurança, ou seja, *backups* frequentemente, para tornar ainda mais seguro, seria adequado realizar várias cópias onde uma fica em outro servidor (local) e outra em um servidor que esteja em outro espaço físico.

Por fim devemos relembrar que com uma estrutura adequada pode-se garantir um bom nível de segurança, e com isso garantir um serviço de qualidade para os clientes e até mesmo uma empresa mais sustentável e com credibilidade nos serviços prestados.

Abstract

This article discusses the security issues in enterprise servers and for that we sought to several authors that address the issue at hand . The study was meant to examine the basic safety requirements for an enterprise server identifying threats and vulnerabilities , be it the physical part or logical server , as companies every day more care in providing its customers and suppliers an image of a solid organization and reliable, increasingly need security in their processes , for this, it was through the study that should be defined , structured and implemented a security policy , that the threats and vulnerabilities are minimized and thus providing a satisfactory level of security.

Keywords: Network Security. Server Security. Hardware Security. Logical Security. Physical Security

REFERÊNCIAS

ANONYMUS. **Segurança Máxima Para Linux:** o guia de um hacker para proteger seu servidor e sua estação de trabalho Linux. Trad. Edson Furmankiewicz e Joana Figueiredo. Rio de Janeiro: Campus, 2000.

CAMPBELL, Patrick T. **Instalando Redes em Pequenas e Médias Empresas:** resolvendo os problemas de redes em pequenos e médios ambientes. São Paulo: Makron Books, 1997.

CARUSO, Carlos A.A. **Segurança em microinformática e em redes locais**. Rio de Janeiro: Livros Técnicos e Científicos, 1993.

COMER, Douglas E. **Interligação de redes com TCP/IP**: princípios, protocolos e arquitetura. Vol.1.5.ed. Rio de Janeiro: Elsevier, 2006.

GIL, Antonio Carlos. **Como Elaborar Projetos de Pesquisa**. 4 ed. São Paulo: Atlas, 2002.

MARCONI, Marina de Andrade e LAKATOS, Eva Maria. **Fundamentos da Metodologia Científica.** 5 ed. São Paulo: Atlas, 2003.

MORAES, Alexandre Fernandes. **Segurança em Redes:** fundamentos. 1ed. São Paulo: Érica, 2010.

NAKAMURA, Emilio Tissato, GEUS, Paulo Lício de. **Segurança de Redes em Ambientes Cooperativos.** São Paulo: Novatec, 2007.

RESS, Weber. Começando a segurança. 2011. Disponível em: https://msdn.microsoft.com/pt-br/library/ff716605.aspx Acesso em maio 2015.

SOARES, Luiz Fernando Gomes, ET AL. **Redes de Computadores:** das *LANs*, *MANs* e *WANs* as Redes ATM. 2ed. Rio de Janeiro: Campus, 1995.

STREBE, Matthew. **Firewall:** São Paulo: MAKRON Books, 2002.

TANENBAUM, Andrews S. **Redes de Computadores.** Rio de Janeiro: Campus, 2003.

VASCONCELOS, Laércio. **Hardware na prática**. 3ed. Rio de Janeiro: Laércio Vasconcelos Computação, 2009

VELLOSO, Fernando de Castro. **Informática:** conceitos básicos. 7ed. Rio de Janeiro: Elsevier 2004.