SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO

INFORMATION SECURITY: A CASE STUDY

Gabriel Alvarenga Dechechi, Guilherme dos Santos Paixão, Jefferson de Oliveira Penha, José Carlos Cordeiro de Oliveira, Pedro Lucas Martins de Oliveira, Rodrigo Rehme e Fernando Vianna

DECHECHI, Gabriel Alvarenga, et al. ***Segurança da Informação: Um estudo de caso****. Revista Tecnológica da FATEC-PR, v.1, n.11, p. 68-80, jan/dez, 2020.*

RESUMO

Com o crescente avanço das tecnologias, empresas estão cada vez mais, buscando soluções para alavancar os negócios através da Internet, potencializando assim suas vendas, maximizando seus processos e garantindo maior expansão no mercado competitivo. Porém com o aumento da utilização da tecnologia nos processos, surgiram novas ameaças e vulnerabilidades, crescendo a preocupação com os riscos que, antes, pouco existiam com a utilização da internet e sistemas interconectados. Portanto hoje, mais do que nunca, é um fator primordial a ser estudado e colocado em prática nas organizações que prezam por boas práticas. Segurança da Informação é uma das áreas em alta no mercado, sem ela todo o ambiente corporativo está vulnerável e propenso ao fracasso total, já que os crimes virtuais vêm aumentando a cada dia e dando prejuízos gigantescos a grandes corporações. Este trabalho tem o objetivo de analisar uma empresa e propor soluções com Políticas de Segurança da Informação, com o intuito de prevenir que ameaças que venham a trazer danos a infraestrutura e toda a informação que é armazenada, levando a conscientizar oscolaboradores dessa empresa da importância sobre procedimentos, normas e boas práticas para manter a saúde do ambiente corporativo que elas estão inseridas.

Palavras-chave: Segurança da Informação. Internet. Redes.

ABSTRACT

With the increasing advancement of technologies, companies are increasingly looking for solutions to leverage business through the Internet, thus boosting their sales, maximizing their processes and ensuring greater expansion in the competitive market. However, with the increase in the use of technology in the processes, new threats and vulnerabilities have arisen, growing concern about the risks that, before, little existed with the use of the internet and interconnected systems. So today, more than ever, it is a key factor to be studied and put into practice in organizations that value good practices. Information Security is one of the hot areas in the market, without it the entire corporate environment is vulnerable and prone to total failure, since cybercrime is increasing every day and causing huge losses to large corporations. This work aims to analyze a company and propose solutions with Information Security Policies, in order to prevent threats that may damage the infrastructure and all the information that is stored, leading to the awareness of employees of that company on procedures, standards and good practices to maintain the health of the corporate environment in which they are inserted.

Keywords: *Information Security. Internet. Networks.*

1 INTRODUÇÃO

O presente trabalho tem por objetivo focalizar o assunto “segurança em provedores”, por meio de um estudo de caso, evidenciando as reais necessidades da implantação de um sistema de segurança de rede.

Atualmente as corrporações necessitam cada vez mais da segurança da informação no seu dia a dia, pois suas funcionalidades e produtividades estão sendo diretamente afetadas pela falta de segurança. No mundo corporativo existem ameaças constantes a qualidade da segurança, agentes ou condições que causam incidentes que comprometem as informações e seusativos por meio da exploração de vulnerabilidades, levando a impactos negativos aos negócios de uma empresa.

O que é realmente necessário em um ambiente corporativo deve ser analisadode acordo com sua importância, e com os grandes benefícios que ele pode trazer a organização. É impossível que um ambiente corporativo exista sem que as questões relacionadas à segurança sejam discutidas e solucionadas. Portanto entendendo a internet como um ambiente hostil. Empresas que investem em aprimoramento estão menos propicias a sofrerem ataques. Por isso é importante ter uma visão corporativa em segurança adequada à natureza do seu negócio.

2 OBJETIVOS

Desenvolver um estudo sobre a Segurança da Informação com ênfase emProvedores de Internet, expondo as deficiências que possuem nessa determinada área. Seguindo as ações necessárias para alcançar este objetivo, será necessário: a) Conceitualização de Provedores e Segurança da Informação; b) Elaborar um estudo de caso de segurança da informação em provedores; c) Mostrar deficiências encontradas no estudo de caso; d) Buscar informação e soluções sobre as falhas em provedores; e) Desenvolver Políticas de Segurança como forma de prevenção e f) Métodos de abordagem corretiva.

3 JUSTIFICATIVA

Este tema de segurança da informação já vem de tempos, pode-se observar que desde a criação de novas tecnologias de comunicação encontradas no mercado, as pessoas têm cada vez mais facilidade para compartilhar dados, quando querem e de onde estiver, tornando o contato mais rápido. Em contra partida estudos mostram que aonda de ataques a esses dados, e o roubo de informação, vêm crescendo exponencialmente nos últimos anos, obrigando empresas a se preocuparem com osigilo e a proteção de sua organização.

Pesquisas são realizadas constantemente sobre o assunto em questão, pois assim como

as tecnologias não param de se atualizar e segurança também não pode parar. É possível encontrar estudos sobre diversas aplicações da segurança da informação, e esta pesquisa irá demonstrar as falhas que um provedor de internet e as consequências de um sistema de políticas de segurança com brechas. (CARTILHA CERT, 2019)

4 METODOLOGIA

Como método de pesquisa foram feitas algumas buscas bibliográficas com definições sobre segurança da informação e para obter informações foi realizada uma entrevista a uma empresa provedora de internet, foram também analisadas outras empresas que já haviam implantado Políticas de Segurança da Informação, como objeto de estudo para enriquecer o conteúdo no tocante a normas, procedimentos e boas práticas. O trabalho foi desenvolvido como uma pesquisa bibliográfica e aplicada à um estudo e caso, ou seja, a aplicação de uma teoria na prática (GIL, 2002)

5 FUNDAMENTAÇÃO TEORICA

5.1 PROVEDORES DE INTERNET

Um ISP (internet *service provider*) é responsável por estabelecer conexões locais, regionais, nacionais ou até mesmo mundiais para disponibilizar a transmissão dedados entre usuários, outros ISPs e serviços de Internet, suas principais funções na pratica se definem em disponibilizar acesso a rede mundial de computadores e a ofertarao usuário o acesso a estes serviços junto as demais funcionalidades, o ISP é aquele que intermediará a conexão do usuário com o provedor *backbone*, que é formado pelas operadoras gigantes de internet.

Os provedores de aplicação ofertam funcionalidades que podem ser acessadas pelos usuários conectados à internet como provedores de correio eletrônico, provedores de hospedagem e provedores de conteúdo. Com essa necessidade de expansão da necessidade de acesso à internet os ISPs vêm se formando em locais onde a internet, seja por Radio, Fibra, satélite, cabos metálicos (CARVALHO, 2005).

5.2 SEGURANÇA DA INFORMAÇÃO

A Segurança da informação é definida segundo SEMOLA (2003) sendo a área de conhecimento dedicada a proteção de ativos e informações. Tendo como pilares 5 pontos (C.I.D.A.L) cruciais quealicerçam a segurança em rede:

- Confidencialidade: Garante que somente pessoas autorizadas tenham acesso à informação através de *login* conferindo a autenticação do usuário (informações cadastradas no sistema).

- Integridade: quando recebido uma informação, é importante que esses dados não estejam corrompidos, modificados.
- Disponibilidade: Garantia de que a informação estará disponível em temporeal ao solicitante, evitando ataques, Exemplo: DOS e DDOS...
- Autenticidade: garantir a veracidade do emissor e receptor da informação.
- Legalidade: garante a legalidade (jurídica) com base na legislação vigente.

6 ESTUDO DE CASO

6.1 ENTREVISTA ISP

O ISP entrevistado se chama ARAUFIBRA e está localizado em Araucária-PR região metropolitana de Curitiba em um dos bairros da cidade chamado Capela Velha,a empresa iniciou seus serviços de distribuição de internet no local a 4 meses e hoje já conta com aproximadamente 400 clientes, atendendo um raio de 7 quilômetros de fibra já passadas, realizamos uma visita técnica até o local aonde desenvolvemos um vídeo apresentando a empresa e mostrando sua infraestrutura.

A Araufibra tem planos de internet de 10 megas a 50 megas a partir de 79,90 e fornece internet de alta velocidade toda via fibra ótica onde entrega a velocidade contratada em download e upload e sem franquia e sem fidelidade. A empresa conta com técnicos qualificados na área todos com uma vasta experiência em grandes operadoras e vários anos na área de telecom e todos com as normas em dia NR 10 e NR35 atualizadas, a empresa desenvolve os projetos, executa e faz a instalação e presta serviços para outros provedores de pequeno porte.

6.2 TOPOLOGIA DO PROVEDOR

O Provedor faz uso do padrão PON, rede óptica passiva ethernet (EPON) onde a arquitetura é: Link da operadora> switch> mikrotik> servidor> OLT> fibra óptica> DIO> ONU> usuários finais.

Link de internet dedicada é de 1 Gigabit, onde a fibra chega no switch, tem a função de rotear os pacotes de dados proporcionando conectividade entre a operadora e o mikrotik_1. Mikrotik, é o “cérebro do provedor” serve para armazenar os dados de autenticação do cliente no servidor. Também estabelece um firewall para a rede, que possibilita a filtragem de fluxo de dados, permissões e limitações de acesso externo. Responsável pelo gerenciamento da rede e administrar a OLT.

O Servidor oferece várias ferramentas, como a cobrança do usuário, bloqueio de cliente

inadimplente, autenticação de internet ao cliente, grava todos os acessos na rede pelo usuário, gerador de ordem de serviço, tanto de manutenção, quanto teinstalação nova.

O terminal de linha óptica (OLT) Gera o sinal óptico na rede, nos postes da concessionária Copel, até a casa do cliente. Sua função principal é fornecer acesso aos usuários, concentrando o tráfego até que possa transmiti-los. Possui 8 portas óticas, atendendo 64 clientes para cada porta, chegando no total de 512 assinantes por OLT.O provedor possui duas OLT'S, atingindo 1024 cliente, que é o máximo permitido nessepadrão EPON.

A Fibra óptica é do tipo multiponto, permite atender vários usuários utilizandouma mesma fibra. DIO (Distribuidor Interno Óptico) é feita a fusão da fibra que sai da OLT e vai para o usuário final. Ele é responsável por concentrar e distribuir conexões da fibra óptica dentro de uma rede. ONU (Optical Network Unit) é um dispositivo terminal de banda larga projetado para atender os usuários (de redes de fibra), para fornecer acesso à internet. Todos os equipamentos da estação estão ligados ao nobreak, conforme mostra Figura 1.

Devido a saturação de cliente na OLT do padrão EPON (Ethernet Passive Optical Network), o servidor iria mudar a tecnologia para GPON (Gigabit Passive Optical Network) Possui 8 portas óticas, atendendo 128 clientes por porta, chegando ao total 1024 assinantes por OLT.

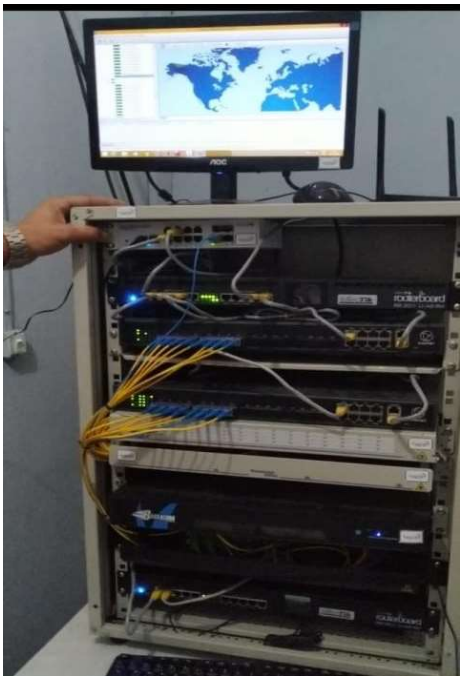

Figura 1 – Infraestrutura Araufibra
Fonte: Autores.

6.3 POLITICAS DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação, também conhecida como PSI, é odocumento

que orienta e estabelece as diretrizes corporativas, ou seja, regras de boas práticas para proteção dos ativos de uma empresa. Tendo por base a ABNT NBR ISO/IEC 27002 (2005) reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes emnosso país.

As políticas implementadas, visam esclarecer aos colaboradores, bem comodeixá-los cientes que, toda a infraestrutura, incluindo os ambientes, estações de trabalho, rede corporativa (intranet) e internet poderão ser auditados, monitorados e gravados, conforme as leis do Brasil.

Diante deste, o colaborador deverá se manter atualizado em relação a essas Políticas de Segurança da Informação, normas e procedimentos, reportando ao seu gestor direto sempre que houver dúvida ou insegurança quanto aos processos que envolvem a informação.

Essa PSI tem como sua principal aplicação a orientação, esclarecimentos e conscientização dos colaboradores da empresa a fim de reduzir os riscos da vulnerabilidade causada pelo fator humano, que é a ameaça mais crítica segundo (Mitnick e Simon, 2003, p. 4).

MITNICK e SIMON (2003, p. 4), enfatizam: À medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano.

6.4 AUTENTICAÇÃO E SENHA

De acordo com Fontes (2012 p. 184) “A senha de autenticação deve ser de conhecimento apenas do usuário responsável pela identificação.”

- É expressamente proibido solicitar a senha de outro usuário, nem mesmo achefia.
- Quando necessário armazenar a senha de autenticação, obrigatoriamente eladeverá estar criptografada.
- Utilizar sempre tamanho mínimo de seis caracteres para a senha.
- A senha deverá ser trocada no máximo em noventa dias, exigida automaticamente pelo ambiente computacional.
- O usuário poderá trocar a sua senha a qualquer momento.
- Não será permitido reutilizar as últimas dez senhas.
- O usuário deve escolher a sequência de caracteres, de maneira não obvia e com difícil adivinhação por outro usuário ou pessoa.
- Depois de cinco tentativas sem sucesso na autenticação com senha, o usuário será bloqueado.
- Quando o usuário se autenticar corretamente por senha, receberá então, seu último acesso, com data e hora.

- Na eventual perda da senha, será atribuída uma senha provisória ao usuário, que será registrado em arquivo de ocorrências, sem que as mesmas permaneçam gravadas.

6.5 USO DE CORREIO ELETRONICO

Ao utilizar a ferramenta de correio eletrônico (e-mail) com terceiros, o nível de confidencialidade das informações a serem enviadas / recebidas deve ser considerado;

Caso o colaborador utilize o correio eletrônico para envio e recebimento de informações através de conexão de internet pública (vulnerável), será responsabilizado pelas possíveis ameaças e riscos; o colaborador deve usar somente o serviço de e-mail corporativo para troca de informações da empresa;

Anexos de e-mail com as extensões, ex: .**bat**, .**exe**, .**src**, .**lnk.com,** devem ser considerados perigosos e de grande risco, não devem ser abertos e nem salvos na estação de trabalho. Caso receber um e-mail com conteúdo igual ou similar, entrar em contato urgente com o setor de Segurança da Informação para análise.

6.6 POLITICAS DE ACESSO A INTERNET

O uso da internet é usado exclusivamente para fins de trabalho ou pesquisas de mercado e soluções, não se deve utilizar a mesma para fins próprios. Toda a rede é monitorada e todo conteúdo é de responsabilidade do usuário.

Não é permitido acesso a e-mails pessoais, sites de relacionamentos, jogos, entretenimento, conteúdo pornográfico, redes sociais ou mensageiros.

Não são permitidos downloads de conteúdo duvidoso, tudo que for necessário fazer download caso não seja de confiança entrar em contato com o pessoal da TI primeiro. Não é permitido upload dos arquivos e dados da empresa ou de seus clientes.

6.7 EQUIPAMENTOS PARTICULARES

Todo equipamento de propriedade particular dos funcionários ou não, que tem a capacidade de processamento de dados, armazenamento, registro de imagem por foto, vídeo ou streaming, notebooks, smartphones ou qualquer outro dispositivo desnecessário a operação dos equipamentos tecnológicos, são proibidos de serem utilizados nas áreas consideradas de armazenamento de ativos críticos. O funcionário que desejar por motivo que deve ser explícito, utilizar os equipamentos acima citados, deverão ser submetidos previamente a adequação e autorização da área de TI e posteriormente liberados com autorização formal expedida pela superintendência, cientificando o utilizador sobre as sanções administrativas e penais caso faça o uso indevido, causando prejuízos direta ou indiretamente a empresa.

6.8 MESA LIMPA

Convém que seja adotada uma política de mesa limpa de papéis e mídias de armazenamento removível e política de tela limpa para os recursos de processamento da informação (ABNT, 2005, p. 70).

O programa Mesa Limpa é utilizado como uma medida preventiva, objetivando o sigilo das informações, evitando que sejam espalhadas, observadas e vazem. A conscientização dos usuários sobre a importância da confidencialidade, que é garantir que somente o usuário correto tenha acesso a informação correta, evitando que informações sigilosas sejam conhecidas por pessoas não autorizadas, o que causaria a perda de segredo. Mantendo sua mesa sempre limpa, torna o ambiente, visualmente mais agradável, possibilitando realizar atividades com eficiência. Ativos importantes devem ser guardados com segurança, como diários, agenda de compromissos, extratosbancários, fichários, pasta de documentos, crachás de acesso, chaves, telefone, smartphones. Evite a impressão de e-mails e qualquer documento impresso, caso for necessária a impressão, guarde-os em local seguro, e no momento de descartá-los, procure fragmentá-los, especialmente quando contém informações de caráter confidencial, evitando a sua visualização por pessoa não autorizada.

6.9 CONVERSAS DE CUNHO PROFISSIONAL EM AMBIENTE PUBLICO

Exposição de ativos por meio conversas informais ou formais dentro do ambiente. É de total responsabilidade dos funcionários, estagiários, prestadores de serviços terceirizados que tem acesso ao ambiente da empresa, o sigilo das informações de propriedade da empresa. Não disseminar, comentar ou expor as informações confidenciais, em conversas informais ou mesmo formais em locais públicos. Quando extremamente necessário utilizar o telefone, smartphone ou qualquer outro meio de comunicação que possa expor os ativos da empresa, deve ser feita de maneira cautelosa, observando sempre a presença de outras pessoas ao seu redor. Quem “divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais”, comete crime de concorrência desleal, Lei Federal 9279, de 14/05/1996.

6.10 CLASSIFICAÇÃO DAS INFORMAÇÕES

Toda e qualquer outra forma de exposição da informação da ORGANIZAÇÃO deve ser classificada e ter explícito o seu nível de confidencialidade.

Interna: Informação que não se deve expor a todos fora da empresa é uma informação que somente os funcionários da mesma tem acesso, onde essa informação vazada pode causar danos à imagem da empresa ou favorecimentos por parte do concorrente.

Confidencial: Uma informação de sigilo onde está aberta a um pequeno grupo depessoas, onde o vazamento da mesma pode gerar causas penais, impactos operacionais, ou ordem

financeira.

Restrita: É a informação onde pode ser acessada somente pela área autorizada “Ex: Recursos Humanos” únicas pessoas que devem ter acesso a essas informações são o Próprio RH ou categorias acimas a divulgação da mesma pode correr váriosriscos até mesmo dentro da empresa para outros setores inferiores.

Pública: É a informação liberada diretamente a todos exclusivamente aos seus clientes em forma de comercial ou promocional geralmente usada como publicidade da empresa.

6.11 SEGURANÇA DO AMBIENTE

Os ativos tecnológicos de armazenamento, processamento e tráfego devem estar protegidos em salas especificas com critérios de segurança para acesso de pessoal autorizado para garantir o sigilo e proteção das informações. O acesso a áreas privadas e sigilosas devem ser baseados em fatores críticos de segurança, sendo obrigatório o uso de identificação oficial (crachá) e uniforme fornecido pela empresa.

O controle de entrada e saída de pessoal vinculado, sendo colaboradores empregados, terceirizados ou visitantes, em áreas privadas ou internas deve ser registrado e controlado. Qualquer colaborador, empregado, terceirizado que por motivo não esteja portando seu crachá oficial, deve ter seu acesso controlado e registrado.

A infraestrutura elétrica e de dados deve ser adequada as especificações dos fabricantes dos equipamentos, seguindo padrões de normas técnicas reconhecidas para manter a estabilidade e continuidade do negócio.

Toda infraestrutura de ativos e cabeamento deve ser devidamente identificada e documentada para, em caso de incidentes, facilitar e agilizar o suporte ou reconexão.

As instalações devem estar adequadas contra riscos de ordem natural ou acidental, tais como: incêndios, alagamentos, inundações, etc. Mantendo em sua infraestrutura dispositivos de detecção e contenção para proteção dos ativos que armazenam informações, manter equipamentos de contingência para eventual incidente.

Convém que os equipamentos sejam colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizados (ABNT, 2005, p. 35).

É proibido fumar, beber ou comer em áreas que se encontram ativos críticos (Data Center), os colaboradores que frequentam essas áreas devem ser comunicados e conscientizados.

7 CONCLUSÃO

A atual infraestrutura de comunicação de dados está crescendo junto a globalização e

interligando todo o mundo em redes de internet. Esta infraestrutura demanda segurança da informação como softwares, firewalls, políticas de segurança, separação de redes publica das privadas, visando proteger os dados de clientes, usuários e empresas.

Conforme a pesquisa foi evoluindo ficou claro a importância da segurança da informação não somente para o usuário final, mas para toda organização que lida com informação.

O Trabalho aqui apresentado teve o intuito de mostrar alguns conceitos sobre segurança da informação e como parte pratica entrevistamos um ISP, um provedor de pequeno porte que trabalha com distribuição de internet via fibra ótica e está nomercado a pouco tempo, o objetivo é trazer soluções para prevenir que ameaças venham a causar danos tanto na infraestrutura, como também prejuízos financeiros a empresa. Para isso foi designado um estudo de implantação de Políticas de Informaçãocom foco em Segurança da Informação.

Este estudo coloca em pauta arquitetura de fornecimento, formas de ataques e defesas, assim como boas praticas “na” relação (usuário/rede), concluindo que com exceção de grandes corporações a sociedade em geral não se preocupa o quanto deveria com segurança, gerando excesso de vulnerabilidades perdendo assim qualidade de serviço.

REFERENCIAS BIBLIOGRÁFICAS

ANDRADE, Marcon, **O que é Ethical Hacking e como ser um Hacker Profissional?** Disponível em: https://www.marcoandrade.com.br/o-que-e-ethical-hacking-e-como-ser-um-hacker-profissional/. Acesso em: 13 nov 2019

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002** – Tecnologia da informação — Técnicas de segurança — Código de prática paracontroles de segurança da informação. São Paulo, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002** – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestãoda segurança da informação. Rio de Janeiro, 2005.

BRASIL. **Lei 12.965 Marco Civil da Internet**. Brasília, 2014.

CARVALHO, Luciano Gonçalves. **Segurança de Redes**. Rio de Janeiro: Ciência Moderna Ltda., 2005.

CARTILHA CERT, **Ataques na Internet**. Disponível: https://cartilha.cert.br/ataques/ Acesso em: 11 nov 2019

FONTES, Edison. **Políticas e Normas para a Segurança da Informação:** Como desenvolver, implantar e manter regulamentos para a proteção da informação nasorganizações. Rio de Janeiro: Brasport, 2012.

HACK Notes: **Segurança de Redes**. Rio de Janeiro: Elsevier, 2003.

LARA, Rodrigo. **O que é provedor de internet?** Disponivel em: https://www.uol.com.br/tilt/noticias/redacao/2019/06/11/o-que-e-provedor-de- internet.htm Acesso em: 09 set 2019

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George (2000) **Hackers expostos:** Segredos e soluções para a segurança de redes. São Paulo: Makron Books, 2000.

MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar**. São Paulo: Pearson, 2003.

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

SEMOLA. M. **Gestão de segurança da informação uma visão executiva 2003.** Disponível: em https://www.portalgsti.com.br/ethical-hacking/sobre/ Acesso em: 15 nov 2019.

SERRA, J. Paulo. **Manual de Teoria da Comunicação.** Covilhã: Livros Labcom.p. 93-101.

SANTOS, Andre H O. **Principais Dispositivos de uma Rede de Computadores [Parte 1]:** Dispositivos Ativos. 2016. Disponível em: https://www.uniaogeek.com.br/principais-dispositivos-de-uma-rede-de-computadores-p1/. Acesso em: 19 nov. 2019.

SANTOS, Andre H O. **Principais Dispositivos de uma Rede de Computadores[Parte 2]:** Dispositivos Ativos. 2016. disponível em: <https://www.uniaogeek.com.br/principais-dispositivos-de-uma-rede-de-computadores-p2/>.