Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

CARLOS ALBERTO DUARTE MAROCCO

PROPOSTA DE TOPOLOGIA DE REDE DE DADOS COM SEGURANÇA E FOCO NA PRODUTIVIDADE, UTILIZANDO FERRAMENTAS DE *SOFTWARE* LIVRE

BRASÍLIA
2015
CARLOS ALBERTO DUARTE MAROCCO

PROPOSTA DE TOPOLOGIA DE REDE DE DADOS COM SEGURANÇA E FOCO NA PRODUTIVIDADE, UTILIZANDO FERRAMENTAS DE *SOFTWARE* LIVRE

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/IPCD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Rede de Computadores com Ênfase em Segurança.

Orientador: Prof. Me. Marco Antônio de Oliveira Araújo

BRASÍLIA
2015

CARLOS ALBERTO DUARTE MAROCCO

PROPOSTA DE TOPOLOGIA DE REDE DE DADOS COM SEGURANÇA E FOCO NA PRODUTIVIDADE, UTILIZANDO FERRAMENTAS DE *SOFTWARE* LIVRE

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/IPCD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Rede de Computadores com Ênfase em Segurança.

Orientador: Prof. Me. Marco Antônio de Oliveira Araújo

Brasília – DF, 14 de setembro de 2015

Banca Examinadora:

_____
Prof. Dr. Gilson Ciarallo

_____
Prof. Esp. Sylas Rodrigues Mendes

AGRADECIMENTOS

Dedico esta vitória e agradeço a todos aqueles que, de forma direta ou indireta, colaboraram para a realização de mais um sonho. À minha família, individualmente ao meu pai Sr Irenio e minha mãe Dona Diva, pelo exemplo, carinho, dedicação e presença em todos os momentos da minha vida. À minha amiga, companheira, confidente, parceira, a mais amada de todas as mulheres a minha querida esposa Débora, o meu grande amor, quem me mostrou que é possível realizar os sonhos, lutando, vencendo desafios, superando os mais diversos obstáculos que a vida nos apresenta, a essa incrível mulher o meu mais sincero obrigado. Aos meus amados filhos, amigos, colegas, parceiros João Pedro e Luiz Henrique, que me enchem de orgulho, felicidade e transformam a minha vida diariamente. Ao meu grande amigo, meu irmão Luiz Eduardo, meu símbolo de superação, pela postura diante de todas as agruras impostas ao longo da sua trajetória, mostrou o quanto é forte o desejo de realizar os seus sonhos, ele venceu. À minha eterna menininha, minha irmã Rosana, pelas orientações, pelo carinho e pelas discussões temáticas, as quais contribuíram e contribuem para o meu aperfeiçoamento como ser humano. Agradeço também à minha sogra Véra, que de maneira abnegada dedicou anos da sua vida ao equilíbrio e fortalecimento da minha família, sempre com muito carinho demonstrou e demonstra diariamente que é a grande mãe de todos. Aos professores e demais integrantes do UNICEUB, pela correção, sabedoria, orientação e organização demonstrados ao longo do curso. A cada amigo que esteve ao meu lado e me proporcionou meios para que eu chegasse até aqui. Em especial e, sobretudo ao nosso grande Deus, corresponsável por meu crescimento espiritual, moral, financeiro e intelectual.

RESUMO

Este trabalho é uma pesquisa bibliográfica que busca apresentar uma opção de rede de dados com foco na segurança da informação, utilizando soluções de baixo custo que concorrem em desempenho e produtividade com as proprietárias, passando por um breve histórico sobre rede de computadores, as topologias e tecnologias mais utilizadas, os dispositivos básicos que compõem um ambiente de informática e algumas ferramentas que podem ser empregadas nas medidas de segurança contra as diversas ameaças às quais o ambiente está exposto, chegando à discussão sobre a relação segurança da informação versus a produtividade e alguns procedimentos simples adequados para o fechamento do ciclo PDCA, concluindo com uma proposta de ambiente de rede viável para organizações de qualquer porte.

Palavras chave: Rede. Dados. Segurança. Custo. Produtividade.

ABSTRACT

This work is a literature that seeks to present a data network option with a focus on information security, using low cost solutions that compete in performance and productivity with the owners, through a brief history of computer network topologies and most used technology, the basic devices that make up a computer room and some tools that can be employed in the security measures against the various threats to which the environment is exposed, coming to the discussion of security regarding information versus productivity and some simple procedures suitable for the closure of the PDCA cycle, concluding with a proposal for a viable network environment for organizations of any size.

Key words: Network. Data. Security. Cost. Productivity

LISTA DE FIGURAS

LISTA DE QUADROS

GLOSSÁRIO

- ACL - (*Access Control List*) – regras de navegação via PROXY inseridas em arquivos, que são lidas pelo servidor para controlar o acesso dos usuários à *internet*.

- Atenuação - diminuição da intensidade de energia de um sinal ao propagar-se através de um meio de transmissão, ou seja, a potência do sinal diminui conforme a distância que ele percorre através do meio físico.

- *Backbone* - é o termo utilizado para identificar a via principal pela qual os dados de todos os clientes da rede passam. É a espinha dorsal da rede.

- *Browser* - aplicativo de interação com o usuário que facilita a navegação na *internet* (*Internet Explorer, Mozilla Firefox, Google Chrome, Iceweasel* etc).

- BYOD (*Bryn Your Own Device*) - uso de dispositivos pessoais no ambiente de trabalho e, consequentemente, a extensão desse ambiente para qualquer lugar do mundo.

- Cabeçalho - parte de um pacote de dados onde são inseridas informações que o identificam com relação ao protocolo utilizado, sua origem e destino, portas de origem e destino, número de sequência de transmissão etc.

- Cascateamento - é a simples interconexão de dois ou mais HUBs ou *switchs* em série. Para estas conexões entre os *switchs*, são empregadas portas ou interfaces convencionais; as mesmas portas/interfaces que são utilizadas para conectar qualquer dispositivo cliente (ex: computadores, *laptops*, roteadores, *firewalls*, pontos de acesso etc).

- Colisão de pacotes - ocorre quando dois ou mais nós do mesmo domínio de colisão transmitem dados simultaneamente, provocando mistura das transmissões e aumento da amplitude do sinal nos meios físicos.

- Domínio de Colisão - é uma área lógica onde os pacotes podem colidir uns contra os outros, em particular no protocolo Ethernet.

- DSLAN (*Digital Subscriber Line Access*) - é um dispositivo de rede, normalmente de uma companhia telefônica, que recebe sinais de múltiplas conexões de clientes *Digital Subscriber Line* (DSL) e os coloca em uma linha de *backbone* de alta velocidade usando técnicas de multiplexação.

- Engenharia Social - termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

- *Frame* - é um “envelope” ou uma camada de endereçamento que envolve os dados para transmissão via rede.

- *Gateway* - é um dispositivo que fica numa posição intermediária geralmente destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos.

- *Hub* - dispositivo concentrador, passivo de rede de camada física (Camada 1) do modelo OSI, que permite a distribuição do sinal da rede para outros nós sem qualquer tratamento do sinal.

- Nó - qualquer dispositivo conectado à rede, pode ser um computador, impressora, *switch*, roteador etc.

- Pacote - é uma fração dos dados transmitidos pela rede que contém informações sobre o protocolo utilizado, a origem e o destino, número de sequência etc.

- *Patch Panel* - painel empregado normalmente em *racks* para a conexão dos cabos de rede.

- PDCA (*Plan, Do, Check, Act*) - processo realizado durante os projetos que objetiva destacar o planejamento, a execução, o monitoramento e a ação.

- Protocolo - padrão que especifica o formato dos dados e as regras a serem seguidas, para que a comunicação entre os nós aconteça.

- PSTN (*Public Switched Telephone Network*) - sigla em inglês para o termo RTPC (Rede de Telefonia Pública Comutada), que é a rede de telefonia tradicional.

- Roteador - dispositivo capaz de regenerar sinais, concentrar conexões múltiplas, converter formatos dos dados transmitidos e gerenciar as transferências de dados, além de comutar os pacotes com base no endereço da camada de rede (Camada 3) do modelo OSI e é dele a função de escolher o melhor caminho para a entrega dos pacotes.

- *SHELL* - é um termo UNIX para a interface interativa do usuário com o sistema operacional. O *Shell* é uma camada de programação que entende e executa os comandos que um usuário insere. Em alguns sistemas, o *Shell* é chamado de interpretador de comandos.

- *Switch* - dispositivo ativo de rede que pode operar na camada de enlace (Camada 2) ou na camada de rede (Camada 3) do modelo OSI, filtrando, inserindo o endereço de destino de cada quadro e os enviando.

- URL (*Universal Resource Locator*) - é o endereço de um recurso disponível em uma rede, seja na *internet*, ou em uma rede corporativa, uma *intranet*. Exemplo de uma URL: www.uniceub.com.br.

- *Worm* - é um *malware* capaz de se propagar automaticamente nas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm*

não embute cópias de si mesmo em outros *softwares* ou arquivos e não necessita ser explicitamente executado para se propagar.

SUMÁRIO

INTRODUÇÃO

A tecnologia da informação evoluiu substancialmente nas últimas décadas principalmente a partir da invenção do computador pessoal, o que barateou e popularizou a utilização dos recursos de informática.

Mas esses dispositivos empregados isoladamente deixaram de ser suficientes por si só, sendo necessário aumentar a sua empregabilidade compartilhando recursos entre os integrantes de uma rede de dados, que passou a ser uma ferramenta poderosa para colaborar com o aumento do desempenho produtivo das organizações.

O surgimento e o consequente movimento irreversível de expansão das redes evidenciaram outros problemas inerentes ao ambiente de informática. Dessa forma, este trabalho tem por objetivo principal apresentar uma proposta de rede de dados que contemple a segurança da informação e a sua relação com a produtividade, utilizando ferramentas de baixo custo.

Para atingir os objetivos propostos e concluir com informações concretas, foram feitas pesquisas bibliográficas em diversas fontes, como livros, normas, trabalhos acadêmicos e sites especializados na área de tecnologia da informação e testes de estabilidade e funcionamento realizados em ambientes virtuais.

Este trabalho inicia discorrendo sobre as redes de dados, um breve histórico abordando das suas origens mais remotas até os dias atuais, as topologias nas quais são elaboradas e configuradas, as tecnologias mais comuns, a classificação das redes conforme a abrangência geográfica e hierarquia, terminando com os seus principais componentes ativos e passivos.

A segurança da informação é abordada em vários aspectos, destacando as normas e padrões a serem respeitados, a segurança da informação nas organizações, o conceito de vulnerabilidades, alguns dispositivos de segurança física e lógica que podem ser empregados, chegando à definição de ameaças que podem ser internas ou externas.

Em seguida é apresentada a relação entre a segurança da informação e a produtividade nos ambientes de informática, assim como a produtividade empresarial e o impacto que a segurança tem na produtividade das organizações.

Assim chega-se à proposta de ambiente produtivo com segurança, abordando uma topologia sugerida, os componentes para a segurança, desempenho, monitoramento, tudo com baixo custo, além da adequação do ambiente físico a ser utilizado para instalação dos equipamentos.

Por fim foram listados alguns testes que devem ser realizados para a verificação das vulnerabilidades, estabilidade da rede, funcionamento do *firewall* e as formas de soluções para esses problemas, caso existam, além de enfatizar a importância de uma auditoria, que pode ser interna ou externa.

Concluindo com a exposição de quais dos dispositivos, topologias, tecnologias e demais ferramentas e equipamentos citados ao longo do trabalho podem compor um ambiente de rede de dados com segurança sem perder o foco na produção e no custo reduzido para instalação.

1 REDES DE DADOS

Para Silva (2010, p. 23) uma rede de dados pode ser definida como sendo um conjunto de computadores interconectados capazes de compartilhar informações. Reiter (2006, p. 21) aprofunda um pouco mais a definição dizendo que uma rede de computadores é um conjunto de dispositivos computacionais, conectados por uma estrutura de comunicação de dados com a finalidade de compartilhar recursos, sendo que a informação é considerada um recurso.

1.1 Breve Histórico

Segundo Freund (2009, p. 16) no século XIX surgiram as primeiras ideias de transmissão de dados por meio de pulsos elétricos, essa era a funcionalidade dos telégrafos que, utilizam fios metálicos como meio para transmitir mensagens codificadas em símbolos binários (código Morse). Esse foi o ponto inicial para o surgimento dos grandes sistemas de comunicação como o telefone, o rádio e a televisão.

Em 1946, John W. Mauchly e J. Presper Eckert projetaram para fins militares, na Universidade da Pensilvânia, o ENIAC – *Eletronic Numerical Interpreter and Calculator*, o primeiro computador digital eletrônico de grande escala, atendendo uma demanda do Departamento de Material de Guerra do Exército dos Estados Unidos (FREUND, 2009, p. 17).

Na década de 1950, os computadores eram máquinas muito grandes e complexas, exigiam pessoal muito especializado para a sua operação e não possuía nenhuma forma de interação direta com o usuário (FREUND, 2009, p. 18).

Na década de 1960 surgiram os primeiros terminais iterativos que juntamente com os sistemas operacionais da época, que permitiam utilizar um computador central para execução de tarefas simultâneas por intermédio de linhas dedicadas de transmissão de dados. Nessa mesma década foi realizada a primeira pesquisa encomendada pelo Departamento de Defesa dos Estados Unidos sobre a elaboração de uma rede de transmissão de dados, de forma que em caso de ataque nuclear, os militares pudessem manter o comando dos seus mísseis e aviões bombardeiros (FREUND, 2009, p. 18).

A IBM em 1971, lançou o IBM 3270 *Information Display System*, que foi projetado para estender a capacidade de processamento do computador que estava dentro do *Data Center*, para localidades remotas, essa técnica foi denominada de *time-sharing*. Também na década de 1970, o desenvolvimento tecnológico reduziu os custos de produção dos

computadores o que possibilitou o crescimento do número de máquinas nas empresas, consequentemente as demandas por maior capacidade de processamento e armazenamento também aumentaram, fazendo com que os usuários compartilhassem dados, dispositivos de armazenamento e periféricos entre as áreas das empresas (FREUND, 2009, p. 18).

Em 1981, a IBM lançou o IBM PC que possibilitava a utilização dos recursos computacionais locais, além de permitir acesso aos mainframes por intermédio de uma rede de cabos metálicos (FREUND, 2009, p. 20).

A partir do surgimento o computador pessoal a utilização dos recursos de tecnologia da informação aumentou substancialmente, inclusive com a utilização cada vez maior das redes de dados locais, mas foi a partir do início da década de 1990, após a criação dos protocolos HTTP e HTML que o crescimento da rede foi exponencial (FREUND, 2009, p. 20).

Nos dias atuais as redes de dados fazem parte naturalmente das vidas das pessoas em praticamente todos os momentos. Estão em constante e irreversível movimento de expansão territorial, buscando reduzir cada vez mais, as distâncias físicas por intermédio de processos mais ágeis e confiáveis de comunicação.

1.2 Topologias

Interessante esclarecer que, de acordo com o vocabulário utilizado na área da Tecnologia da Informação, o termo topologia denota a forma como os dispositivos das redes de dados são conectados, corroborado com o que cita Silva (2010, p. 35) quando define a topologia como sendo a estrutura física da rede de computadores, ou seja, o tipo de conexão dos equipamentos (nós) na rede.

As redes de dados podem ser estruturadas em topologia física, conforme as conexões dos cabos e nós são realizadas e topologia lógica, que corresponde ao fluxo que os dados seguem dentro da estrutura física, atendendo às configurações preestabelecidas (FREUND, 2009, p. 176).

A seguir serão citados os diversos tipos de topologia física existente e as formas de configuração mais comuns para as topologias lógicas.

1.1.1 Topologias Físicas

Segundo Freund (2009, p. 176), topologia física de uma rede refere-se à forma que os dispositivos estão organizados, sendo os tipos mais comuns em barramento, em anel, em estrela e em estrela estendida. Reiter (2006, p. 121) cita a topologia hierárquica e a

topologia em malha como outros tipos possíveis de serem empregados, enquanto Silva (2010, p. 38) ainda soma o tipo de topologia híbrida às demais, como sendo mais uma forma de desenhar o ambiente computacional.

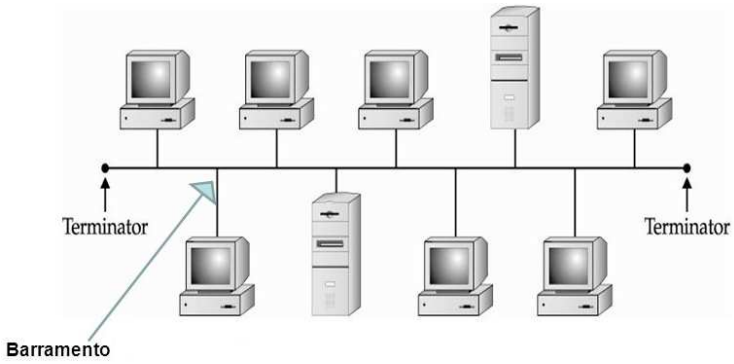
Barramento

Nessa topologia os nós são conectados a um cabo principal, também conhecido como *backbone*, que conduz os dados a todos os dispositivos que estão dentro do domínio delimitado pelos terminadores (dispositivos fixados no início e no final do *backbone*) (FREUND, 2009, p. 176).

É uma topologia barata e fácil de instalar, pois são empregados apenas cabos e conectores. Nela não existe um nó central, quando um nó é desconectado ou sofre alguma pane os demais permanecem funcionando e, de acordo com Reiter (2006, p. 119) o que um computador transmite é recebido por todos os demais. Trata-se de uma topologia não-determinística.

Contudo, se ocorrer algum problema com o barramento (*backbone*) toda a rede fica comprometida (FREUND, 2009, p. 176), além de ser uma topologia limitada na quantidade de dispositivos conectados e de possibilitar grande incidência de colisões de pacotes, já que não há controle quanto à ordem de transmissão por parte dos nós da rede.

Figura 1 – Exemplo de Topologia em Barramento.



Fonte – http://slideplayer.com.br/slide/327066/

Anel

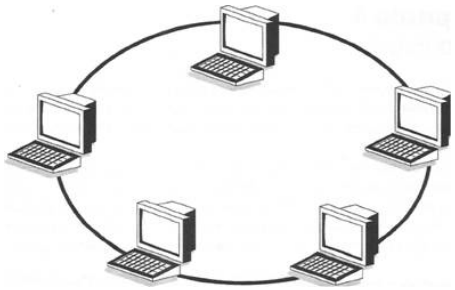
Neste caso os nós são conectados uns aos outros fazendo com que o barramento tome forma de um anel (FREUND, 2009, p. 178).

É uma estrutura que pode ser facilmente expandida apenas inserindo novos nós. O desempenho da rede não depende da quantidade de máquinas conectadas, e também não há

problema de atenuação, pois cada nó funciona como regenerador de dados (SILVA, 2010, p. 36).

Qualquer problema na ligação entre os nós pode comprometer toda a rede, mas para evitar esse problema pode ser empregado um hub concentrador que gerencia a conexão e a unidirecionalidade dos dados (SILVA, 2010, p. 36).

Figura 2 – Exemplo de Topologia em Anel.



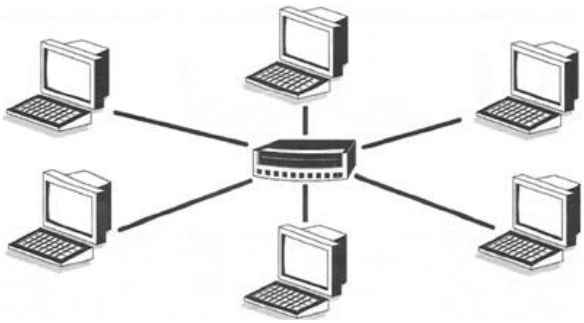
Fonte – http://www.fazerfacil.com.br/rede/topologia.htm

Estrela

Conforme Reiter (2006, p. 120) essa topologia se caracteriza pela existência de um nó central que exerce o papel de concentrador de conexões, assim para Freund (2009, p. 177) toda confiabilidade da rede fica depositada sobre esse ponto que, se sofrer algum dano acaba por comprometer todo o seu funcionamento. A expansão fica limitada à capacidade desse ponto central que pode ser um *hub*, *switch* ou roteador.

Silva (2010, p. 37) destaca que esse formato é mais oneroso para ser implantado, porém possibilita uma taxa de transmissão maior, facilita a identificação de falhas em cabos e a origem de outras falhas, a distribuição física dos nós e, se ocorrer um problema que interrompa o funcionamento de um nó, esse não interfere nos demais integrantes da rede.

Figura 3 – Exemplo de topologia em estrela.



Fonte – http://www.fazerfacil.com.br/rede/topologia.htm

Estrela Estendida

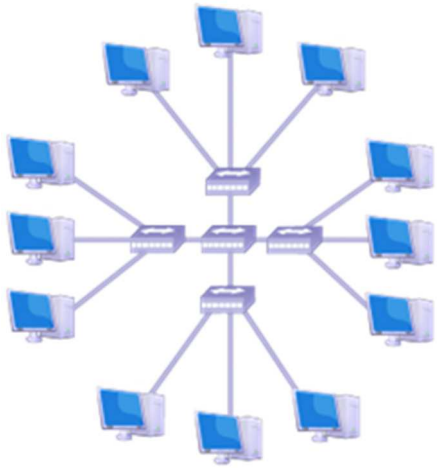
Para Reiter (2006, p. 120) essa é uma variante da topologia em estrela que, invés de conectar todos os computadores a um único nó central, conecta os computadores a nós interligados a um nó central.

Freund (2009, p. 177) cita que forma uma topologia em estrela central, sendo que cada nó terminal dessa estrela central é o nó central de outra topologia em estrela, além de ser empregada para expandir uma rede de forma fácil e ágil.

Contudo essa prática submete a rede ao problema do “cascateamento” do sinal o que pode reduzi-lo nos nós mais externos, diminuindo a capacidade produtiva dos usuários que utiliza esse equipamento.

Freund (2009, p. 177) sugere empregar *switches* nas estrelas centrais e *hubs* nas estrelas secundárias para otimizar os recursos dos dispositivos de uma rede estruturada nessa topologia, pois os *switches* utilizam comutação de circuitos para encaminhar as informações, consequentemente filtram o tráfego e na ocorrência de algum problema em alguma das portas, comprometerá somente a rede ligada a ela.

Figura 4 – Exemplo de topologia em estrela estendida.



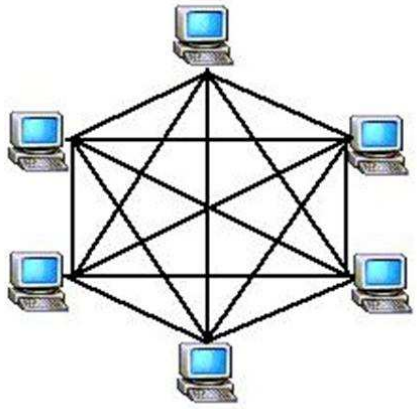
Fonte – https://glendasnotepad.wordpress.com/2008/08/10/159/

Malha

Nessa topologia não há um nó central, todos os nós estão conectados entre si, dessa forma os dados podem trafegar da origem ao destino por vários caminhos, garantindo que sejam entregues no caso de falhas em um ou mais nós da rede, por isso, conforme Reiter (2006, p. 121) é usada nos locais em que se necessita de uma grande confiabilidade na interligação dos nós da rede.

É uma topologia rápida e segura, pois são muitas as possibilidades de entrega das informações, mas é dispendiosa e de difícil instalação, pois como cita Silva (2010, p. 38) cada nó deve possuir a uma quantidade equivalente de placas de rede à quantidade de nós da parte da rede que ele está inserido.

Figura 5 – Exemplo de topologia em malha.



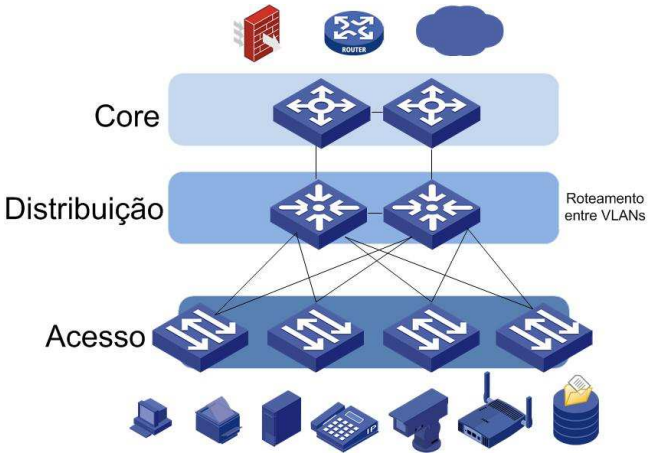
Fonte – http://si10m.webnode.pt/tipologias-fisicas-das-redes-de-computadores/

Hierárquica

É uma variante da topologia estendida, mas com a particularidade de expansão em somente uma direção, mantendo um ponto de recebimento de dados superior e não mais centralizado, evidenciando a hierarquia entre os nós de interligação (REITER, 2006, p. 121).

Evidencia ainda mais o “cascateamento” do sinal dentro da rede, com isso acentua-se a redução deste nas extremidades da mesma.

Figura 6 – Exemplo de topologia hierárquica.

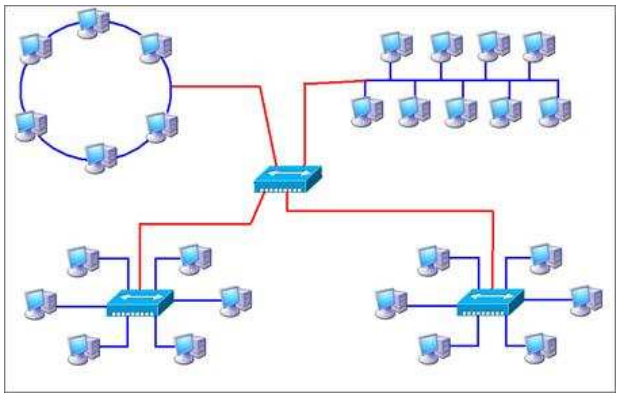


Fonte – http://www.comutadores.com.br/modelo-de-rede-hierarquica-parte-1-de-2/

Híbrida ou Mista

É a forma que se caracteriza pelo emprego de mais de uma topologia ao mesmo tempo na mesma rede, explorando o quê de melhor cada topologia apresentada anteriormente tem para cada ambiente da estrutura física onde será instalada. Essa topologia foi desenvolvida para solucionar necessidades específicas (SILVA, 2010, p. 38).

Figura 7 – Exemplo de topologia híbrida ou mista.



Fonte – http://www.teleco.com.br/tutoriais/tutorialrcompam/pagina_2.asp

1.1.2 Topologias Lógicas

Para Freund (2009, p. 179) existem dois tipos mais comuns de topologia lógica que são em barramento e em anel. As topologias lógicas se diferenciam uma da outra pela forma que os protocolos de comunicação agem dentro da estrutura física na orientação do tráfego dos dados.

Importante destacar que uma rede pode estar fisicamente estruturada com uma topologia e logicamente com outra.

Barramento

Nessa topologia lógica o nó que desejar transmitir dados pela rede, simplesmente o faz, e todos os nós recebem os dados transmitidos, mas somente aquele a quem o pacote for destinado terá acesso ao seu conteúdo. Esse envio de dados para toda a rede é conhecido como *broadcast*, não é uma boa prática manter esse fluxo descontrolado de dados pela rede, sob pena de congestionar a estrutura.

No barramento lógico não há ordem nem sequência para a transmissão, o nó deseja transmitir e executa, essa prática gera problemas de tráfego e frequentemente colisões de pacotes. Para diminuir a incidência de colisões de pacotes é utilizado um método de transmissão chamado de CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) (FREUND, 2009, p. 179).

Anel

O funcionamento dessa topologia está baseado na posse do *token*, que é um sinal que circula pela rede de maneira a permitir a transmissão de dados somente do nó que o detém naquele momento.

Quando o nó recebe o *token* ele transmite o pacote para a rede com o endereço do nó de destino, o pacote passa por todos os nós até chegar à máquina endereçada, então com o pacote entregue o *token* é liberado e passa para outro nó poder transmitir. Com essa topologia lógica não ocorrem colisões de pacotes (FREUND, 2009, p. 181).

1.3 Tecnologias

Durante os estudos para implantação das redes de dados nos mais diversos ambientes, é importante considerar, além da topologia, qual tecnologia deve ser empregada para melhor atender às demandas e oferecer o melhor serviço ao usuário final, para elucidar essas considerações serão apresentadas algumas tecnologias disponíveis, além de relacionar com as suas indicações de uso.

Ethernet

É a tecnologia de rede mais empregada em redes locais (LAN), praticamente dominando totalmente esse mercado, o que conforme Reiter (2006, p. 121), a ethernet e suas variantes mais velozes ultrapassam a marca de 80%.

Conhecida também como norma IEEE 802.3, é um padrão de transmissão de dados em pacotes por meio físico utilizando fibra óptica, cabo de par trançado ou cabo coaxial fino ou grosso, embora o emprego desses últimos seja mais difícil de ser visto atualmente (SILVA, 2010, p. 97).

A transmissão é feita em pacotes que podem conter até 1500 *bytes* de dados por *frame*, além das informações do cabeçalho (REITER, 2006, p. 153).

Embora possa ser utilizada qualquer topologia física na sua implementação, seu funcionamento é feito na topologia lógica de barramento, mesmo que sejam utilizados dispositivos de concentração de sinal ou segmentação de domínio de colisão (FREUND, 2009, p.183).

Emprega o protocolo CSMA/CD para manter a incidência de colisões de pacotes em níveis aceitáveis. Esse protocolo monitora o ambiente de forma que apenas um nó por vez transmita dados pela rede, se por algum motivo dois ou mais nós transmitirem dados simultaneamente, o CSMA/CD detecta, mantém a transmissão de um e interrompe a dos

outros nós, fazendo com que esses aguardem uma fração de tempo aleatória para retransmitirem (SILVA, 2010, p. 97).

Essa tecnologia inicialmente chamada de *Ethernet* original operava à velocidade de 10 Mbps. Evoluiu e passou a ser chamada de *Fast Ethernet* com velocidade de 100 Mbps e padrão IEEE 802.3u. Seguindo a evolução passou para *Gigabit Ethernet*, com banda de 1 Gbps e chamada IEEE 802.3z. Em março de 2002 foi aprovado o padrão IEEE 802.3ae, com velocidade de 10 Gbps, a 10 *Gigabit Ethernet* que pode ser implementada em redes LAN, MAN e WAM, por intermédio de cabos de fibra óptica ou cabo de par trançado Cat 6a e Cat 7 (SILVA, 2010, p. 98).

Token Ring

Nessa tecnologia não existe colisão de pacotes e é empregada principalmente em ambientes que necessitem de robustez e precisão na entrega das informações, por exemplo, em redes de dispositivos de automação industriais.

Sua estrutura física pode ser semelhante à topologia em estrela, pois pode utilizar um ativo de nome MAU (*Multistation Access Unit*), que é fisicamente semelhante a um *switch*, como concentrador de conexões, porém o seu funcionamento lógico é em anel.

O que caracteriza a formação do anel nessa rede é a presença de um quadro chamado de *token* que fica circulando de nó em nó pela rede. Quando um nó deseja transmitir dados na rede ele mantém o *token* consigo, inseri nele um *bit* de sinal que informa que aquele quadro é de transmissão, anexa o pacote de dados nesse quadro e o envia para a rede com destino registrado no cabeçalho do pacote. Esse pacote passa por todos os nós da rede até chegar ao seu destino, que o devolve ao nó de origem confirmando a transmissão dos dados. Em seguida se o nó não for mais transmitir dados ele retira o *bit* do *token* e o libera na rede para que outro nó possa transmitir.

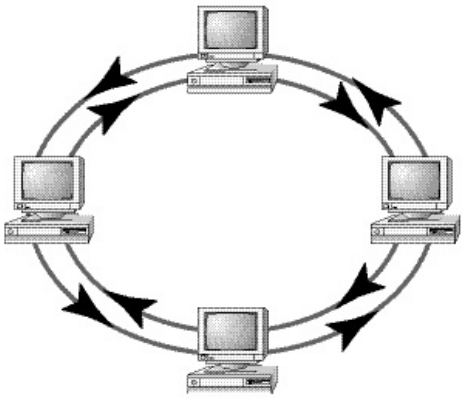
Como somente uma estação por vez tem autorização para transmitir dados na rede não há perda de sinal por colisão de pacotes, o que credita a essa tecnologia a certeza da entrega dos dados (FREUND, 2009, p. 184).

FDDI (*Fiber Distributed Data Interface*)

Outra tecnologia de redes de transmissão de dados de alto desempenho, com uso de fibra óptica, que pode ser utilizada em LANs ou na interligação dessas formando uma MAN com extensão de até 200 Km.

Assim como a *Token Ring*, sua topologia lógica é em anel, porém a topologia física é em anel duplo, com emprego do *token* para aumentar a confiabilidade na transmissão dos dados (REITER, 2006, p. 138).

Figura 8 – Exemplo da topologia de rede com tecnologia FDDI.



Fonte – http://daryalytayamm12.blogspot.com.br/2012/11/tipologias-de-redes-02112012.html

ATM

Uma rede ATM (*Asynchronous Transfer Mode*) é empregada para comunicação de redes LAN, MAN e WAN com alta velocidade, permitindo o tráfego de dados, voz e vídeo.

Por se tratar de uma tecnologia de alto desempenho é largamente utilizada nos núcleos (*cores*) das operadoras de telefonia.

Assim como a rede *ethernet*, também divide os dados em pacotes para serem transmitidos, porém os chama de células, as quais possuem tamanho fixo de 53 *bytes*, sendo 5 *bytes* para o cabeçalho e 48 *bytes* para dados (REITER, 2006, p. 241).

Frame-Relay

É uma tecnologia de transmissão de dados rápida, barata e que é aplicada em muitas redes para interligar aplicações do tipo LAN, SNA, dados e voz, porém o emprego de redes ATM e TCP/IP, além de serviços de acesso como *cable modem*, DSL e a utilização de VPN estão reduzindo o seu uso.

Por oferecer custos menores, ainda pode ser empregada onde as outras tecnologias mais caras não atendam à relação custo *versus* benefício, por exemplo, na zona rural.

Em uma rede *Frame-Relay* os dados são transmitidos em quadros (*frames*) com baixo retardo e sem controle de erros (REITER, 2006, p. 238).

ADSL

Essa tecnologia utiliza a mesma estrutura de uma operadora de telefonia para transmitir voz e dados dividindo em três as frequências de uma linha convencional, porém com a diferença que quando o sinal é de voz segue para o PSTN (*Public Switched Telephone Network*), que é a rede de comutação de circuitos de uma operadora, mas quando o acesso é para a *internet* é direcionado ao DSLAN (*Digital Subscriber Line Acces Multiplexer*).

A divisão da frequência foi uma oportunidade encontrada para utilizar a mesma estrutura já existente para fazer ligações de voz, já que uma linha telefônica utiliza frequências entre 300 e 4000 Hz. Assim as demais bandas seriam utilizadas para *uploads* e *downloads* de dados, sem que o usuário fosse obrigado a se desconectar da *internet* para fazer uma ligação telefônica (SILVA, 2010, p. 92).

1.4 Classificação das Redes

Silva (2010, p. 23) classifica as redes de duas formas, conforme sua abrangência geográfica e de acordo com a sua hierarquia.

Abrangência Geográfica

Essa é a forma de classificar uma rede de dados conforme a sua extensão geográfica, que pode estar restrita a uma casa, pequena empresa, um *campus* universitário, uma grande empresa, uma cidade ou todas se conectando tomando proporções estaduais, nacionais, continentais e mundiais.

A LAN (*Local Area Network*) é uma rede de pequenas proporções que atende a pequenas empresas, residências, escolas etc. Ela é composta por dispositivos conectados por cabos, placas de rede, pequenos *switches* ou *hubs*, que possibilitam a troca direta informações ou recursos entre os componentes da rede sem reencaminhamento (*forward*) dos pacotes, ou seja, sem passar por um roteador (FREUND, 2009, p. 138).

A MAN (*Metropolitan Area Network*) como o seu nome sugere é uma rede que atende a áreas de proporções metropolitanas possui características semelhantes à LAN, porém com capacidade de empregar velocidades maiores. Outra diferença é com relação à sua instalação, por sua dimensão ela utiliza espaços púbicos, sendo assim só pode ser instalada por empresas autorizadas e licenciadas pelos órgãos públicos (SILVA, 2010, p. 24).

A WAN (*Wide Area Network*) é rede a que abrange as maiores distâncias, chegando a cobrir todo o planeta, ela pode ser nomeada como rede geograficamente distribuída. É composta por redes e sub-redes, normalmente de operadoras de telefonia e

provedores de internet que se interconectam com as máquinas dos usuários utilizando roteadores e formas de transmissão de dados que podem ser por cabos de cobre, fibra óptica ou ondas de rádio (SILVA, 2010, p. 25).

Hierarquia

Esse é mais um modo de classificar as redes, porém não mais pela amplitude da área ocupada, mas sim pela hierarquia que os dispositivos ocupam dentro da rede.

Ponto-a-ponto é uma forma de classificar uma rede pequena com no máximo 6 estações e que não possui servidor, assim os dispositivos estão conectados entre si para compartilhar recursos e informações armazenadas em cada um dos equipamentos da rede. Todos os dispositivos podem utilizar *softwares* instalados nos outros micros, mas isso pode acarretar aumento de fluxo causando lentidão, neste caso sugere-se instalar os *softwares* em cada uma das máquinas. Outras características desse tipo de rede são o baixo custo de instalação e cabeamento simples, mas está relacionada a baixa segurança e dificuldade em gerenciar os serviços (SILVA, 2010, p. 25).

Cliente-Servidor é uma rede onde existe a figura de pelo menos um computador servidor que centraliza as operações solicitadas pelos micros dos usuários, denominados clientes. É uma rede que oferece maior desempenho, controle, organização e segurança, uma vez que os serviços são oferecidos por computadores mais robustos, com maior poder de processamento. O interessante é empregar um servidor para cada serviço de rede, assim um problema em um desses dispositivos não interrompe completamente o funcionamento da rede (SILVA, 2010, p. 26).

1.5 Componentes de uma Rede de Dados

Uma rede de dados é composta por diversos componentes, entre eles estão os físicos e os lógicos.

Os componentes físicos compõem a infra-estrutura por onde vão trafegar os dados, se esses componentes possuírem a capacidade de interferir nos dados que passam por eles são classificados como ativos de rede e, quando não possuem essa característica são classificados como passivos de rede.

Os componentes lógicos são os protocolos de rede e *softwares* de gerenciamento que orientam os dados distribuídos em pacotes, dando-lhes endereços e mostrando os melhores caminhos a serem percorridos.

1.5.1 Ativos de rede

Como ativos de redes podem-se citar aqueles que fazem parte da infra-estrutura da rede que são os *switches*, os roteadores, as placas de rede, as *bridges*, pois são equipamentos utilizam protocolos como ARP, RIP, OSPF entre outros, que interferem nos dados criando domínios de colisão, montando listas de endereços, enfim facilitando o fluxo, a segurança e orientando o caminho para ser percorrido pelos dados. Outro grupo de ativos de redes compõe a parte dos serviços a serem entregues para a rede, que são os servidores (DHCP, *Firewall*, PROXY etc) e aqueles que vão se beneficiar desses serviços que são os computadores e demais nós da rede (FREUND, 2009, p. 149).

1.5.2 Passivos de rede

Os passivos de redes são componentes que servem exclusivamente de caminho ou passagem para os dados sem que esses sejam orientados ou modificados. Os exemplos são os cabos (coaxial, fibra óptica, par trançado etc), *hubs*, *patch panels*, conectores e terminais, enfim são basicamente os componentes de camada 1 (física) dos modelos OSI ou TCP/IP (SILVA, 2010, p. 65).

2 SEGURANÇA DA INFORMAÇÃO

A definição de segurança da informação não é algo complexo, porém aplicá-la é uma tarefa das mais difíceis, pois interfere nos paradigmas atuais, além de parecer extremamente paradoxal e ser aplicada com base em probabilidades.

Segundo a ISO/IEC 27000:2014, segurança da informação é a preservação da confidencialidade, integridade e disponibilidade da informação. Para Lento (2011, p. 17) a segurança computacional (ou segurança da informação) é um serviço que consiste em tornar o computador livre de ameaças. Já a ABNT NBR ISO/IEC 17799:2005, diz que segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. Assim é possível observar que os diversos autores têm visões parecidas e complementares sobre a segurança da informação.

McCarthy (2014, p. 164) cita a “nova conscientização sobre o ataque do dia zero, a necessidade de uma diligência prévia transparente”, a “segurança da informação baseada em consequências”, o “constante desafio da mudança” e “enquanto estamos preocupados com os sistemas baseados em silício, os criminosos se voltam para os baseados em carbono”, como cinco paradigmas básicos sobre a segurança da informação que devem ser considerados se houver interesse em conquistar vitórias contra indivíduos e organizações mal-intencionados.

O interessante e intrigante nesse cenário é perceber que um único investimento em segurança, mesmo que alto, não retirará todos os riscos existentes nem tampouco imunizará a estrutura de ameaças futuras, portanto o paradoxo desse universo é trabalhar para prover segurança sem conseguir oferecê-la totalmente, é estar seguro até que algo aconteça, pois a segurança é um estado de momento.

2.1 Normas e Padrões

Muito embora não sejam exigidos nos contratos de serviços é uma boa prática utilizar alguma norma ou padrão, de preferência reconhecido internacionalmente, para estabelecer requisitos específicos de proteção das informações, assim como os procedimentos de controle dos métodos empregados.

A *International Organization for Standartization* (ISO) e a *International Electrotechnical Commission* (IEC) publicaram a série de padrões ISO/IEC 27000, que oferece uma visão geral de requisitos para serem aplicados em sistemas de gestão da segurança da informação, abordando entre outras, as seguintes áreas:

- 27001 – Sistemas de gestão de segurança da informação – requisitos

- 27002 – Código de práticas de gestão de segurança da informação

- 27003 – Guia de implementação do sistema de gestão de segurança da informação

- 27004 – Gestão de segurança da informação - avaliação

- 27005 – Gestão de riscos à segurança da informação

- 27006 – Requisitos para organização que fornecem auditoria e certificação de sistemas de gestão de segurança da informação

Outra organização internacional que fornece princípios, padrões e formulários de relatórios para investigação e, por conseguinte padronização de procedimentos é o *Federal Financial Institutions Examination Council* (FFIEC). Contudo, esses padrões são mais direcionados às instituições financeiras, o que não impede de serem empregados em outras situações, desde que sejam tomados os devidos cuidados de adaptação ao ambiente a ser utilizado. Esse conselho publicou uma série de documentos para inspeção de tecnologia da informação, inclusive para a segurança da informação como complemento ao *Gramm–Leach–Bliley Act* (GLBA), conhecida como a Lei de Modernização do Sistema Financeiro dos Estados Unidos, de 1999.

O *Payment Card Industry Security Standards Council* (PCI SSC) é mais uma organização, um conselho na verdade, criado pelas principais operadoras de cartão de crédito para desenvolver normas e padrões a serem aplicados na segurança das transações financeiras realizadas com cartões de crédito. Anteriormente a esse conselho, os dispositivos empregados por essas operadoras eram independentes, ou seja, cada entidade utilizava as suas máquinas e processos, além das suas próprias medidas de segurança, o que tornavam os procedimentos individualizados. Visando a padronização dos procedimentos o PCI SSC elaborou o *Payment Card Industry - Data Security Standard* (PCI-DSS), que é um conjunto de documentos e diretrizes com orientações para serem aplicados exclusivamente nas áreas afetas à tecnologia da informação e ajudarem as empresas a permanecerem em conformidade com o padrão, aumentarem a segurança e manterem a interoperabilidade.

Ao longo do tempo e evolução dos negócios empresariais foi vislumbrada a possibilidade de repassar a outras empresas especializadas parte das obrigações administrativas, as chamadas terceirizações de serviços. Mas realizando esse repasse de tarefas a alta administração ficaria sem o controle dessas atividades, o que poderia gerar problemas futuros. Então foram criados os padrões *Statement on Audit Standarts* (SAS) para essas empresas terceirizadas seguirem, os quais seriam empregados no caso de uma auditoria. Os serviços de processamento de dados, por exemplo, eram regulados pelo *Statement on*

Audit Standarts nº 70 (SAS-70), que posteriormente seria substituído pelo *Service Organization Controls* nº 1 (SOC 1), assim como o *Systrust*, sistema contábil desenvolvido por americanos e canadenses para testar a disponibilidade, a segurança e a integridade de sistemas específicos, dando mais comodidade na administração dos negócios, foi substituído pelos SOC 2 e SOC 3. Os SOC são uma série de relatórios padronizados que são entregues por um contador certificado e auditado, a numeração que se segue à sigla é relativa às diversas áreas que os controles abrangem. Os SOC 2 e SOC 3 "tem por objetivo atender às necessidades de um amplo conjunto de usuários que precisem conhecer informações e as garantias de controles dos prestadores de serviços" e podem abranger um ou mais entre os cinco princípios (segurança, disponibilidade, integridade de processamento, confidencialidade e/ou privacidade), de acordo com McCarthy (2014, p. 22).

As instituições financeiras são as maiores investidoras em segurança da informação. Sempre preocupadas com a melhoria e padronização dos serviços desenvolveram, juntamente com firmas de contabilidade outro padrão para avaliação coerente dos prestadores de serviços. O *Shared Assessments Program* fornece o Questionário de Coleta de Informações Padronizadas (SIG, *Standardized Information Gathering*) e os Procedimentos Acordados (AUP, *Agreed Upon Procedures*), desenvolvidos e mantidos de acordo com os padrões da série ISO/IEC 27000, PCI DSS e o FFIEC. O SIG e o AUP possuem ferramentas que são empregadas pelas entidades para avaliarem os riscos dos seus prestadores de serviços e os seus próprios riscos, respectivamente.

2.2 Segurança da Informação nas Organizações

No início da informatização das organizações já existia preocupação com a segurança da informação, mas ainda eram tempos que poucas pessoas possuíam conhecimento para operar os grandes *mainframes*, portanto as estratégias de proteção eram basicamente limitar o acesso físico de pessoas não autorizadas às áreas computacionais das empresas e gerar usuário e senha para os poucos operadores.

Atualmente quando se trata de segurança dentro das organizações, seja indústria, comércio, ensino, entre outros é preciso entender onde essa organização está inserida no processo produtivo, saber que prover segurança é prevenir, monitorar e responder no mais curto prazo de tempo a ocorrência de um incidente e que, como afirmam Nakamura e Geus (2007, p. 43), é impossível ter uma rede totalmente segura.

Entende-se que uma pequena empresa que adquiri matéria prima, produz e vende o seu bem terá certa preocupação com segurança, mas aceitará muitos riscos, não

necessitando de um nível de segurança tão grande quanto uma instituição financeira, uma grande empresa que gera muito valor ou uma empresa que integra um ambiente cooperativo com filiais, fornecedores, prestadores de serviços etc. A necessidade de ser mais competitivo, produzir mais, com mais eficiência e rapidez, exigiu que, ao longo do tempo, a tecnologia da informação encontrasse meios para entregar o que as empresas necessitavam sem perder o foco na segurança.

Uma tecnologia facilitadora das relações funcionais e que é largamente utilizada para atender às exigências modernas é a rede de dados, assim a segurança não poderia ser negligenciada nesse ambiente. Seus elementos ativos e passivos, lógicos e físicos devem oferecer integridade, confidencialidade e disponibilidade a toda estrutura organizacional para garantir o bom funcionamento e a proteção dos bens, assegurando os seus diferenciais competitivos.

Como as conexões de rede permeiam todas as áreas, passando pelos servidores, *websites*, bancos de dados, sistemas financeiros, pagamento etc, sua flexibilidade e facilidade de operação resultam em maior produtividade, mais agilidade e consequentemente mais lucro, contudo, se não houver preocupação em manter essa estrutura a salvo de invasões, os prejuízos podem ser incalculáveis.

Organizações como bancos operam conquistando e mantendo uma relação de confiança entre eles e seus clientes, então se houver o rompimento dessa condição, muitos deixaram de usar os serviços e procurarão outras instituições ou passarão a realizar as transações de outra forma. Por esse motivo as instituições financeiras investem grandes quantias na manutenção, qualidade e confiabilidade dos serviços prestados por elas.

Nakamura e Geus (2007, p. 44) destacam cinco aspectos que devem ser considerados dentro de uma estratégia de segurança em ambientes cooperativos, que são: aspectos tecnológicos, aspectos humanos, aspectos processuais, aspectos jurídicos e aspectos de negócios. Neste trabalho o foco será nos aspectos tecnológicos.

2.3 Vulnerabilidades

Conforme a definição da ISO/IEC 27000:2014, vulnerabilidade é uma fraqueza de um ativo ou de controle que pode ser explorada por uma ou mais ameaças. Em um ambiente de rede existem diversas dessas fraquezas umas que já foram identificadas e corrigidas, outras que foram somente identificadas e possivelmente outra quantidade igual ou superior que ainda nem foi descoberta.

Assim como a força de uma corrente é igual à força do seu elo mais fraco, a segurança de uma estrutura de tecnologia da informação é tão robusta quanto às vulnerabilidades existentes. Essas fraquezas podem estar em cada um dos aspectos citados no item anterior, ou em todos, mas como o foco é o aspecto tecnológico podem-se citar algumas vulnerabilidades comuns existentes, tais como: falta de servidor de redundância, falta de *nobreak*, falta de antivírus, sistemas operacionais desatualizados, senhas fracas entre outras.

2.4 Dispositivos de Segurança Física

No meio da tecnologia da informação, a segurança física é feita por dispositivos que controlam e monitoram o acesso de pessoas a determinadas áreas das organizações, que possuam algo de valor e por isso precisam de maior atenção. Esse tipo de segurança é empregado criando perímetros de segurança, nos quais são determinadas quais pessoas terão permissão para transitar em cada área da organização. Há também as fortificações que apesar de não serem de tecnologia da informação, colaboram com a manutenção dos serviços computacionais.

Como cita Lento (2011, p. 21), a segurança física preocupa-se em proteger espaços ou dispositivos críticos ou sensíveis ao negócio, os quais devem ser mantidos em ares seguras, protegidos por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso.

Dentro desse cenário existem dispositivos que controlam ou impedem o acesso como: salas cofre, salas seguras, portas e catracas que são acionadas com identificação biométrica (impressões digitais, iris, identificação facial, voz etc), por cartões de identificação com código de barras e *chips*; câmeras de monitoramento com centrais inteligentes dotadas de monitores e que gravam as imagens em *storages* de grande capacidade, alarmes entre outros.

Assim como há controle no acesso de pessoas, há também os dispositivos de tecnologia da informação que executam as mesmas funções ou muito semelhantes dentro da estrutura da rede de dados, como os *firewalls*, os *intrusion prevention system* (IPS), os *intrusion detection system* (IDS), que apesar de possuírem *softwares* algumas empresas oferecem o *hardware* no qual somente o seu *software* funciona corretamente, então é possível classificá-los como dispositivos físicos de proteção e identificação de acesso.

Outros elementos que também podem ser englobados como dispositivos de segurança são os *nobreaks* e geradores que mantêm os serviços em produção durante eventuais falhas na alimentação de energia, *storages* e servidores de *backup* que possibilitam a recuperação de dados em casos de *crash* dos sistemas, aparelhos de ar condicionado

redundante para manter a temperatura ideal de funcionamento dos dispositivos, extintores de incêndio, enfim qualquer dispositivo físico que possibilite ou facilite a manutenção da disponibilidade, integridade ou confidencialidade dos dados pode ser classificado nesse meio.

2.5 Dispositivos de Segurança Lógica

Essa classificação de segurança está relacionada ao conjunto de medidas, procedimentos, *softwares* e protocolos que podem ser utilizados para controlar, dificultar ou impedir o acesso a sistemas ou arquivos por usuários ou *softwares* não autorizados, colaborando assim com a manutenção dos princípios da segurança da informação citados anteriormente. Segundo Lento (2011, p. 21), a segurança lógica segue a mesma premissa da segurança física, contudo a preocupação relaciona-se aos dispositivos lógicos do sistema computacional.

Algumas medidas para controle de acesso lógico são a criação de uma *demilitarized zone* (DMZ), configurada no *firewall*, que secciona a rede em uma área que pode ser acessada pela *internet* e outra de acesso exclusivo de dentro da rede organizacional e o cadastro de usuários, pelo menos com um nome para *login* e uma senha. Alguns procedimentos podem atuar juntamente com o cadastro para fortalecer a segurança, por exemplo, determinar na política de segurança quão forte deverá ser a senha, número mínimo de dígitos, emprego de caracteres especiais, alternando letras maiúsculas e minúsculas com numerais. Outro procedimento interessante é limitar o acesso somente às áreas afetas àquele usuário cadastrado, que é o princípio do privilégio mínimo.

Os antivírus ou anti *malwares, firewalls* que são comercializados ou encontrados gratuitamente exclusivamente em *softwares*, cadastro usuários, *softwares* para a execução de *backups* e controle de acesso agregam mais segurança à rede. Além dos dispositivos citados até o momento, Lento (2011, p. 64) destaca a utilização de protocolos como *Internet Protocol Security* (IPSec), *Domain Name Server Security* (DNSSec), Secure *Socket Layer* (SSL) etc, criptografia, a criação de uma autoridade certificadora interna e a *Virtual Private Network* (VPN), como outras medidas adotadas para incrementar a segurança organizacional.

2.6 Ameaças

Os sistemas computacionais assim como as redes de dados estão expostos a diversas formas de ameaças ao seu funcionamento. Segundo Lento (2011, p. 26), ameaça pode ser vista como um risco, e este risco pode ser uma pessoa, algo (um dispositivo

defeituoso), ou um evento (incêndio, terremoto etc) que venha explorar uma vulnerabilidade do sistema causando danos.

Interessante destacar que ao iniciar o tratamento da segurança da organização, não é funcional levantar as ameaças para depois providenciar as medidas de segurança. Primeiramente levantam-se as vulnerabilidades dos seus sistemas, depois são identificadas as ameaças que podem usar essas vulnerabilidades, em seguida providenciam-se tratamentos adequados, e por último aceitam-se alguns riscos, que por ventura, permaneçam.

2.6.1 Ameaças Internas

Essa divisão das ameaças está relacionada aos fatores internos às organizações. Assim é possível elencar diversas existentes dentro das empresas com potencial para causar danos aos sistemas de forma intencional ou não.

Segundo Lento (2011, p. 27) as ameaças não intencionais são provenientes da ignorância de operacionalidade do sistema (ex: erro involuntário de um administrador de rede inexperiente), e as intencionais são provenientes de atos programados por pessoas como um funcionário descontente ou desonesto que pode provocar danos deliberadamente.

2.6.2 Ameaças Externas

Quando se pensa em fatores externos que possam causar danos dentro das organizações, deve-se raciocinar também com fatores intencionais ou não e naturais ou não. Dessa forma, as ameaças externas são provenientes de qualquer fator, evento ou circunstância que esteja fora do ambiente organizacional que possa causar algum dano.

Fenômenos da natureza como vendavais, chuvas torrenciais, descargas elétricas, inundações, terremoto e maremoto (embora esses últimos não sejam realidade no território brasileiro) constituem os fatores naturais, portanto não intencionais que ameaçam a operação dos sistemas de informática.

Acidente de trânsito, exemplo quando um veículo abalroa um poste de transmissão de energia e interrompe o abastecimento da empresa, não é natural e também não é intencional.

Pessoas mal-intencionadas que podem utilizar seus conhecimentos de informática para tentar burlar os sistemas de segurança, os chamados *hackers*, eles podem provocar danos, inserir *softwares* espiões, desconfigurar sistemas e *sites*, extrair informações, como dados de clientes, arquivos de senhas e *logs* etc, esse tipo de ameaça é intencional.

Enfim, as ameaças são muitas cabendo aos gestores de segurança a elaboração de sistemas de proteção adequados às realidades de cada organização, para minimizar as possibilidades dessas ameaças interferirem nas atividades das empresas.

3 SEGURANÇA x PRODUTIVIDADE

Este assunto não é exclusivo da área de tecnologia da informação, ao contrário, ele foi adaptado à informática, pois em todos os ramos de trabalho existe a preocupação com esse binômio, tamanha é a sua influência sobre os resultados esperados.

As empresas devem garantir a segurança nas operações para que não sejam penalizadas com redução da produção ou paralisação completa das atividades. No caso da tecnologia da informação a segurança e a produtividade estão relacionadas à manutenção da disponibilidade dos serviços e infra-estrutura de informática (*sites*, rede de dados, bancos de dados etc), além das entregas realizadas pelos colaboradores, de acordo com que determina e/ou deseja a alta direção e os seus projetos estratégicos.

Para Nakamura e Geus (2007, p. 63), a administração da segurança de uma organização é uma tarefa complexa, na medida em que ela deve ser dimensionada, sem que a produtividade dos usuários seja afetada. Caso a empresa tenha interesse na manutenção dos serviços ativos em frequência de 24x7, ou seja, 24 horas por dia durante os 7 dias da semana, deverá investir muitos recursos para manter a estrutura, elaborando um eficiente sistema que passa pelo suprimento de energia elétrica, proteção dos dispositivos e consequentemente dos dados, substituição de servidores, treinamento dos funcionários até a recuperação dos dados que por ventura tenham sido danificados ou perdidos, *disaster recovery*.

No que tange ao desempenho dos colaboradores, deve ser considerada qual a real necessidade de cada funcionário acessar sistemas internos e *internet*. O que é destacado por Nakamura e Geus (2007, p. 62) quando citam que a segurança é inversamente proporcional às funcionalidades, ou seja, quanto maiores são as funcionalidades, como serviços, aplicativos e demais facilidades, menor é a segurança desse ambiente. Por exemplo, quando se aplica uma política de segurança muito rígida pode ocorrer de o funcionário que possuir um pouco mais de conhecimento em informática, empenhar muito tempo buscando formas de burlar a segurança e assim diminuir sua produtividade, neste caso, verifica-se a expressão que diz que segurança é inversamente proporcional a produtividade. Por outro lado, se a segurança for muito permissiva, os funcionários poderão acessar todos os sistemas internos, *sites* de bate-papo e relacionamento, comunidades virtuais etc, os quais não contribuirão para o aumento da produção empresarial, além de serem portas abertas para ataques de vírus e *worms*, engenharia social e tantos outros que tenham a possibilidade de causar danos a partir de acessos incorretos à *internet*. Nesta situação pode-se citar outra expressão que diz que segurança é inversamente proporcional às funcionalidades.

Dentro do que foi exposto, acredita-se que o melhor a ser aplicado é uma segurança proativa com controle de acesso, funcionalidades e permissões adequadas, mas de forma a buscar o equilíbrio entre a segurança e a produtividade, para que a empresa possa extrair o máximo do colaborador e dos sistemas, protegendo seus valores, mantendo seus serviços e assumindo alguns riscos.

3.1 Produtividade Empresarial

Quando se trata de produtividade empresarial pode-se relacionar ao segmento industrial e citar uma expressão matemática que descreve adequadamente o que se espera de uma organização: a produtividade é igual à diferença entre o que é produzido e os custos que foram aplicados para alcançar essa produção. De acordo com Longenecker, Moore e Petty (1997, p. 484 *apud* MARINO, 2006, p. 2), produtividade é a eficiência com a qual os insumos são transformados em produção.

Para produzir um automóvel ou construir um edifício, as empresas investem em contratação de funcionários, em elaboração de projetos, aquisição de matérias primas, construção de ambientes adequados para os fins que se destinam, entre outras coisas, tudo isso para vencer cada etapa entregando os resultados esperados, essa também é uma visão sobre produtividade empresarial, porém mais prática.

Contudo, também há nesse meio a preocupação com segurança, uma vez que nenhuma montadora de automóvel gostaria de ter seu novo projeto sendo lançado pelo concorrente, ou ter atrasos por falta de operacionalidade dos meios informatizados. Da mesma forma que nenhuma construtora gostaria de iniciar a construção de um novo empreendimento que já fora lançado por outra construtora. Por isso, também existe a preocupação com a manutenção dos segredos empresarias e onde são empregadas as ferramentas de segurança adequadas a cada ambiente e fase do ciclo produtivo.

3.2 Impacto da Segurança na Produtividade

Nakamura e Geus (2007, p. 62) destacam duas associações que não podem deixar de serem consideradas quando se trata do impacto da segurança na produtividade dos usuários, a primeira cita que a segurança é inversamente proporcional à produtividade dos usuários, ou seja, quanto maiores forem as preocupações, os investimentos e os equipamentos de segurança da informação, menor será a produtividade obtida do colaborador, e a segunda diz que a segurança é inversamente proporcional às funcionalidades, então quanto maiores as funcionalidades, como serviços, aplicativos e demais facilidades, como acesso às redes

sociais, *softwares* de bate-papo etc, menor será a segurança desse ambiente, pois nessas funcionalidades estão diversas vulnerabilidades que podem ser exploradas. Diante dessas duas expressões busca-se o equilíbrio entre a segurança, as funcionalidades e a produtividade.

É notório que quanto maior for a segurança, menor será a produtividade dos funcionários, contudo se for observado pelo lado da manutenção dos serviços ativos, quanto maior a preocupação com a segurança, maior será a quantidade de tempo que os ativos, serviços e a estrutura estarão em produção para corresponder às expectativas das organizações.

Sendo assim, deve-se observar a segurança por vários ângulos, iniciando pela proteção aos meios de informática que o colaborador utiliza para desempenhar suas tarefas, como o cabeamento que deverá estar conforme as normas ANSI/TIA/EIA 568B - Requerimentos gerais de Cabeamento Estruturado e especificação dos componentes para cabos e fibras; esta norma define os principais conceitos do cabeamento estruturado, seus elementos, a topologia, tipos de cabos e tomadas, distâncias e testes de certificação. Os computadores devem estar conectados à rede e monitorados de forma que não seja permitido ao usuário empregá-lo para outros fins que não os de interesse da organização. Os sistemas e demais aplicativos que serão instalados nos computadores devem ser somente aqueles afetos à área de trabalho dos usuários, de forma a reduzir os riscos de as vulnerabilidades serem exploradas e causarem danos que podem reduzir a operação ou paralisar todo o ambiente. Pode-se considerar também, que produção no caso da informática é a permanência dos serviços e sistemas em atividade, diferente da produção empresarial que pode ser apresentada por uma expressão matemática de fácil mensuração.

A informática embora nos dias atuais esteja diretamente relacionada ao sucesso ou fracasso de muitas empresas, sendo inclusive o próprio negócio de outras tantas, em muitas ainda é uma atividade meio, ou seja, que dá suporte à atividade principal, assim, como foi dito, para a informática, a produção pode ser considerada alta ou baixa de acordo com a manutenção dos sistemas ativos que apoiam as atividades de produção das organizações, não gerando recursos diretos, mas sendo o suporte para toda a cadeia produtiva.

4 PROPOSTA DE AMBIENTE PRODUTIVO COM SEGURANÇA

Neste capítulo será apresentada uma proposta de infra-estrutura de rede de dados que possa manter o ambiente de informática produtivo, adequando a segurança da informação a níveis aceitáveis, de forma a facilitar a gerência, com bom desempenho e com o mínimo de investimento financeiro.

4.1 Topologia

De acordo com Silva (2010 p. 35), topologia é a estrutura física da rede de computadores, ou seja, o tipo de conexão dos equipamentos (nós) na rede e como eles são conectados. Para este projeto o desenho da rede que será apresentado é uma topologia de estrela estendida, de classificação cliente-servidor, onde será possível identificar algumas redes em estrela isoladas e conectadas por intermédio de dois dispositivos de *firewalls*, que poderão se for o caso, atuar como roteadores. O primeiro estará na extremidade e será o *gateway* da *internet*. Esse dispositivo fechará as portas virtuais de acesso à rede interna, permitindo acesso exclusivamente aos serviços que estiverem na DMZ (*site, e-mail*, ou outro serviço qualquer que seja necessário), e o segundo será o que controlará e conectará os seguimentos internos, que serão a rede dos administradores, a rede dos usuários, a rede dos serviços internos (*intranet*, ldap, samba etc) e a saída para a *internet*, passando pelo primeiro *firewall*. Assim o *firewall* externo terá três placas de rede e o interno terá quatro placas de rede.

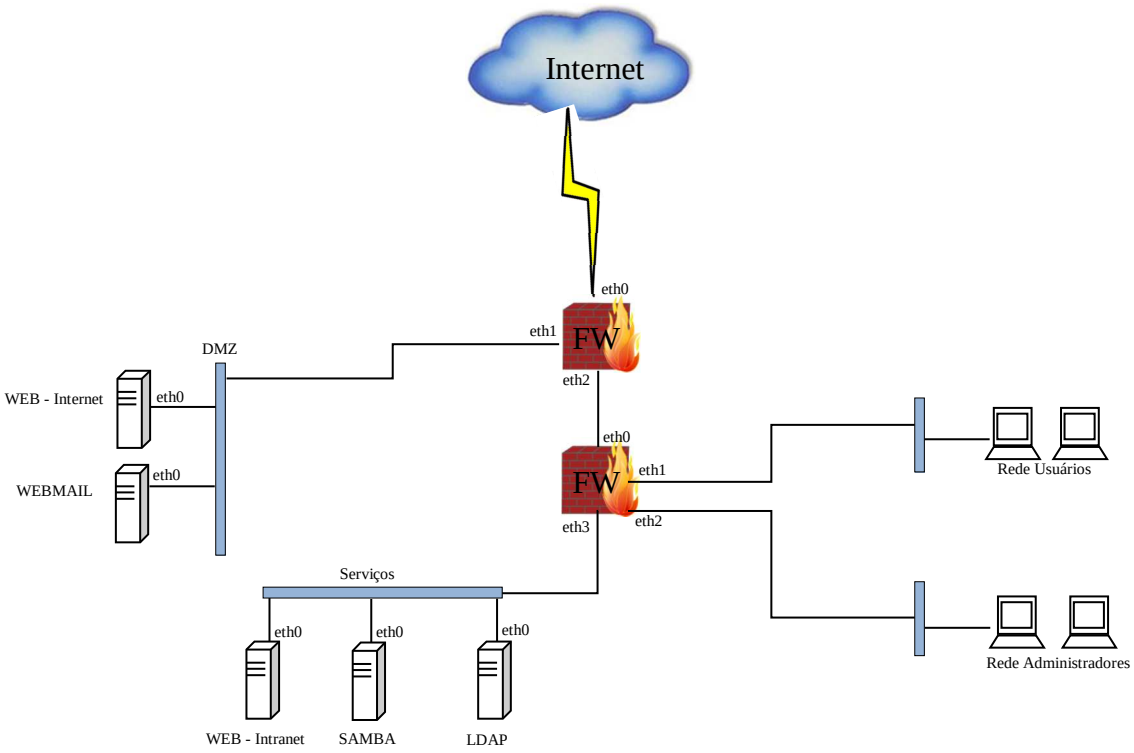
Para facilitar a administração e gerenciamento dos recursos, as redes ou as placas de rede poderão ser identificadas pela área que atenderão dentro a organização, ou seja, rede dos administradores da rede, rede dos usuários, rede dos serviços e acesso à *internet*.

Na rede dos usuários, dependendo das dimensões da empresa, será interessante segmentar em Vlans (*Virtual Local Area Network*), para facilitar a administração e reduzir os domínios de colisão. Para isso serão empregados *switches* de camada 3, os quais admitem essa segmentação além de servirem como roteadores se for necessário para algumas situações específicas, como por exemplo, no caso de criar uma rede exclusiva para o setor de desenvolvimento de novos projetos ou para o setor financeiro.

Entendendo que atualmente as redes são cabeamentos estruturados, nos quais são aplicadas as redes de voz, dados e energia elétrica no mesmo projeto, será interessante a designação e identificação de portas dos *switches* para a Vlan dos computadores (quantas forem necessárias, lembrando que não é aconselhável que uma Vlan tenha mais que 254 IPs), Vlan para as impressoras, Vlan para câmeras de vídeo (segurança das instalações), Vlan para

tráfego de voz (caso de telefonia VoIP) e quantas mais sejam necessárias para a adequação do ambiente.

Figura 9 – Proposta de topologia.



Fonte – Produzido pelo autor do trabalho.

A figura acima é meramente ilustrativa, na qual estão listados alguns serviços na DMZ e na rede interna de serviços, todavia, em uma rede não são somente esses componentes, a ideia é oferecer uma visão da distribuição e segmentação, com o intuito de facilitar o entendimento. A seguir serão apresentados todos os componentes que farão parte da rede.

4.2 Componentes

Como foi citado acima, uma rede de dados é composta por diversos elementos físicos e lógicos, os quais foram elencados durante a exposição dos capítulos anteriores. Além desses dispositivos serão listados também alguns equipamentos de suporte de energia elétrica e sugestões de conexões elétricas que podem aumentar a sua disponibilidade.

4.2.1 *Firewall*

Uma rede de dados necessita de toda a proteção possível, e uma das medidas mais básicas é a instalação de um *firewall*. Esse dispositivo é definido por Zwicky, Cooper e Chapman (2000 *apud* LENTO, 2011, p. 89) como sendo barreiras interpostas entre a rede privada e a rede externa com a finalidade de evitar intrusos (ataques); isto é, são mecanismos (dispositivos) de segurança que protegem os recursos de *hardware* e *software*, da empresa, dos perigos (ameaças) aos quais o sistema está exposto. Então, pode ser um *software* ou um *hardware* e é normalmente a primeira barreira externa da rede. Existem diversos fabricantes como a *McAfee*, *WatchGuard*, *Huawei* etc e distribuições gratuitas, como o *Endian*, *Pfsense* entre outros, o mais importante, no entanto é empregar um dispositivo que seja adequado às necessidades da organização.

A primeira providência a ser tomada quando se trata de aplicação de um *firewall* é realizar um estudo para buscar um dispositivo adequado às dimensões da organização. Para isso existe um guia o *Firewall Buyer's Guide* da ICSA, que ajuda a estabelecer quais dispositivos devem ser adquiridos, proprietários ou não, de forma a atender às necessidades das empresas.

Um *firewall* funciona fechando muitas portas lógicas de acesso à rede, permitindo a entrada apenas naquelas que são utilizadas pela organização, por exemplo, quando é utilizado um servidor de correio eletrônico, a porta 25 do protocolo SMTP, utilizada para a transmissão, a porta 109 do protocolo POP ou a porta 110 do protocolo POP3, para o recebimento dos *e-mails* ficam abertas, de acordo com a versão a ser empregada. Uma observação muito importante é que o *firewall* não impede a infestação por *malwares*, isso é função de *softwares* como os antivírus.

A visão a ser utilizada durante a configuração do *firewall* será sempre de dentro da ferramenta, ou seja, se posicionando no interior do dispositivo será possível identificar e desenhar o caminho que os dados deverão percorrer tanto na saída da rede para a *internet* quanto no caminho inverso. Utilizando o exemplo do correio eletrônico, quando um *e-mail* chega ao *gateway* da rede ele está entrando no *firewall*, e quando ele é destinado ao servidor de correio eletrônico está saindo do *firewall*, assim fica fácil entender o que deve ser feito em cada porta que será utilizada, umas portas somente deixam os dados saírem, enquanto outras somente permitem que os dados entrem.

Diversas empresas desenvolvem *softwares firewalls* que são instalados em *hardwares* adquiridos pelas organizações separadamente, e outras produzem o *hardware* com o seu sistema pronto para ser configurado para os clientes. Esses dispositivos proprietários

possuem custos altos de aquisição e manutenção, o que inviabiliza muitos projetos para pequenas empresas, mas existem soluções gratuitas muito eficientes, de fácil instalação e configuração.

Com intuito de reduzir custos e oferecer um bom serviço, dois *softwares* gratuitos podem ser utilizados, o *Endian* que é um SOHO (*Small Office and Home Office*) para as pequenas empresas e o *pfSense* que é um SMB (*Small and Midsize Business*) para pequenas e médias empresas. Ambos podem ser instalados em servidores que não possuem alto desempenho, já que a função principal é fechar portas, mas também não deve ser uma máquina que comprometa o "roteamento" dos pacotes de dados, como já foi citado anteriormente, sempre que houver a necessidade de implantar um serviço, um sistema, ou adquirir um produto, deve ser realizada uma avaliação buscando o equilíbrio entre o custo, o emprego do recurso e o resultado esperado, assim é possível reduzir as possibilidades de superestimar ou subestimar a ferramenta que será implantada.

4.2.2 NAT

Segundo Lento (2011, p. 101), o NAT (*Network Address Translation*) por ele mesmo, não provê segurança, mas ajuda a esconder o *layout* da rede interna e força que todas as conexões sejam realizadas via um único ponto de passagem. Sob o ponto de vista da segurança, para Nakamura e Geus (2007, p. 227), o NAT pode esconder os endereços dos equipamentos da rede interna e, consequentemente, sua topologia de rede, dificultando os eventuais ataques externos.

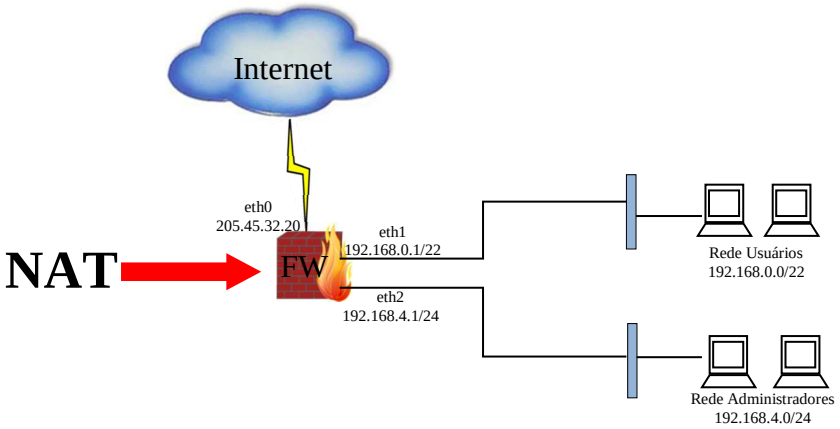
Lento (2011, p. 101) destaca que quando uma máquina de rede interna envia um pacote para fora da rede, o NAT modifica o seu endereço de origem, de forma que o pacote pareça ter vindo de um endereço válido para a *internet*. Quando uma máquina externa envia um pacote para dentro da rede, o NAT modifica o endereço de destino, visível externamente, em um endereço interno.

É sabido que endereços IPv4 válidos para serem utilizados na *internet* estão escassos, e os que ainda estão disponíveis são negociados pelos provedores a preços cada vez mais altos, o que inviabiliza a utilização de um endereço válido para cada *host* de uma rede local. Além disso, o sistema de endereçamento utilizando IPv6 ainda não está totalmente ativo, assim foram pensadas e aplicadas diversas formas de estender a utilização IPv4, entre elas o NAT, que é a forma de fazer com que uma rede interna máscara 22, com seus 1022 endereços IP para *hosts*, por exemplo, possa fazer conexão com a *internet* por intermédio de um único IP válido, reduzindo os custos junto ao provedor, sem comprometer o acesso.

Lento (2011, p. 92) cita que o NAT consiste em um procedimento no qual o roteador realiza mudanças nos endereços de rede do pacote. Porém com a evolução dos meios de informática, atualizações nos procedimentos, inclusive para redução de custos, a configuração do NAT é feita no *gateway* da rede, que nesta proposta é o *firewall* mais externo, o qual assume também a função de roteador.

No seu funcionamento básico, o NAT recebe o pacote de dados vindo do cliente com endereço IP interno e o converte para outro endereço IP, que pode ser encontrado pelos diversos servidores da *internet*. Da mesma forma, quando o NAT recebe um pacote vindo da *internet* destinado a um cliente interno, ele o converte para o endereço da rede interna.

Figura 10 – Exemplo de acesso à *internet* utilizando o NAT.



Fonte – Produzido pelo autor do trabalho.

4.2.3 DMZ

A DMZ (*Demilitarized Zone*, ou em português, Zona Desmilitarizada) é uma rede de servidores que fica posicionada logo após o *firewall gateway* da rede, nela estão localizados os serviços que a organização oferece ao púbico externo, como o *site*, servidor de *e-mail*, DNS (*Domain Name Server*) e, no caso de estabelecimentos de educacionais o servidor de Ensino a Distância, como o *Moodle* ou *Teleduc*, por exemplo, entre outras possibilidades.

Reiter (2006, p. 312) define DMZ como sendo um termo que designa uma área segura entre duas linhas, é a parte da rede que não pertence à rede interna, totalmente protegida por um *firewall*, e nem à *internet*, onde o outro *firewall* cuida da proteção.

Ao contrário do que possa parecer, devido ao nome dado a essa rede, é a parte que deverá ter a maior preocupação e aparato de segurança. Fazendo uma analogia com a geopolítica, quando há uma área desmilitarizada entre países, por exemplo, é em torno dessa

área que se posicionam as maiores forças de ambas as partes, pois no primeiro descuido de um lado, o outro poderá invadir e ocupar o espaço, para que isso não ocorra, a atenção é redobrada.

Da mesma forma, tratando-se de tecnologia da informação os serviços que estão acessíveis da *internet* são aqueles que estão expostos às maiores ameaças cibernéticas, por isso a preocupação deverá ser elevada e constante. Medidas de proteção e de contingência deverão ser testadas, aplicadas e atualizadas constantemente para evitar danos aos usuários e à imagem da organização.

A DMZ é configurada dentro do *firewall gateway* da rede, no qual serão estabelecidas as portas dos protocolos que poderão ser acessadas a partir da *internet* e as portas dos protocolos que serão oferecidas como caminho para esses acessos aos servidores de destino. Ou seja, um acesso externo ao *site* da organização busca a porta 80, do protocolo HTTP (*HiperText Transfer Protocol*), ao se deparar com o *firewall* essa solicitação será encaminhada somente para o endereço que corresponde ao servidor que hospeda o *site* daquela organização, evitando que o caminho possa ser utilizado para acesso às áreas internas da rede.

Essas regras de acessos externos são utilizadas como medidas de proteção às demais áreas da rede organizacional, pois se elas não existirem os serviços externos ficam no mesmo barramento de rede dos demais servidores internos, como banco de dados, computadores dos usuários e demais sistemas de gestão empresarias que, se forem invadidos poderão não só causar danos à imagem da organização, mas também, possibilitar furtos de dados de clientes, de projetos e, em casos extremos até ser determinante para a falência da empresa.

4.2.4 PROXY

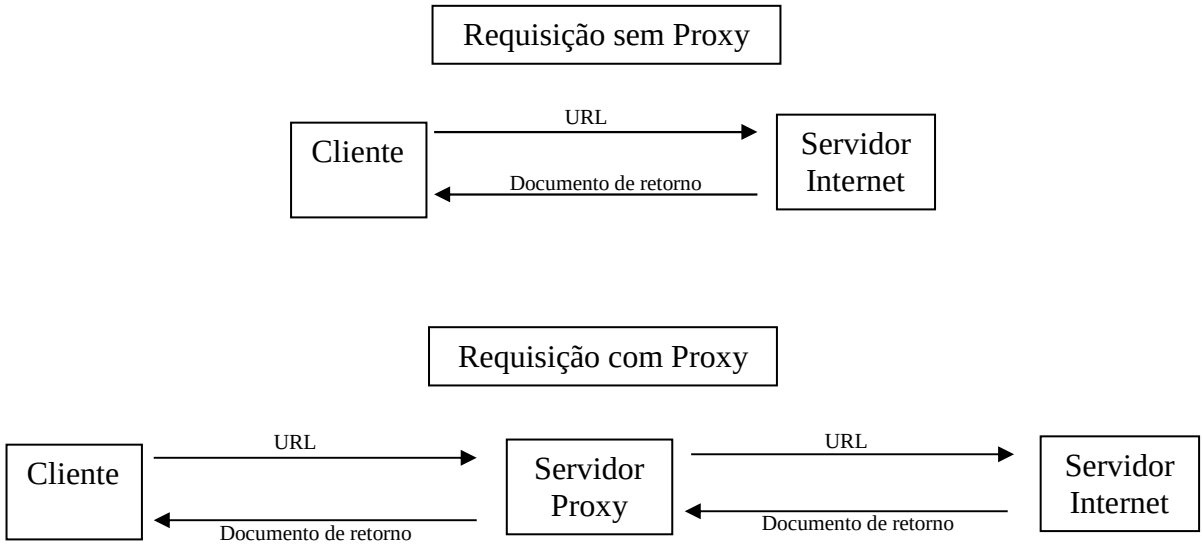
Para Reiter (2006, p. 326), um servidor PROXY é um programa que armazena localmente objetos na *internet* para posterior distribuição aos clientes. É um servidor que atua como um intermediário entre a estação de trabalho e a *internet*. Silva (2010, p. 265) define PROXY como um *firewall* de controle de aplicação que fica instalado geralmente em computadores servidores, trabalhando como intermediador entre a rede e a *internet*, ou a outra rede, ele primeiro avalia o número da sessão TCP dos pacotes para depois liberar a comunicação.

Serviços de PROXY são programas de aplicações especiais ou programas servidores que recebem solicitações de clientes para serviços de *internet*. Essas solicitações

são analisadas pelo PROXY que, de acordo com as suas regras permitirá ou não o acesso ao servidor da *internet*. Nesse processo o PROXY assume o papel do cliente fazendo a conexão com os serviços de *internet* desejados pelo cliente, porém sem que esse último fique diretamente ligado, mascarando e protegendo o cliente e a rede que ele está utilizando.

Sem o PROXY, o usuário digita no seu *browser* a URL do destino desejado e se conecta diretamente ao serviço de *internet*, sem qualquer tipo de filtro, o que pode proporcionar visita a *sites* que não são de interesse da empresa, ou que não são se quer afetos aos assuntos profissionais, o que pode proporcionar a entrada de *malwares* e ataques de engenharia social, que poderão interferir na disponibilidade, autenticidade e integridade da rede e dos dados. Mas com a utilização do PROXY, as conexões são controladas o que oferece maior segurança para a rede, além de manter os usuários focados em assuntos profissionais, aumentando a produtividade.

Figura 11 – Exemplo de acesso à *internet* com e sem o PROXY.



Fonte – Produzido pelo autor do trabalho.

O servidor PROXY, diferente do que se possa imaginar necessita de desempenho, ou seja, precisa ser instalado em uma máquina suficientemente robusta para que a análise que ele faz em cada pacote de solicitação dos clientes possa ser feita adequadamente, sem comprometer o desempenho da rede e dos demais acessos de outros usuários.

Uma boa aplicação de PROXY é o Squid, esse *software* é gratuito, baixado facilmente da *internet* ou instalado diretamente via *Shell* do *Linux* com o comando “#apt-get install squid3”, e pode ser configurado com diversas regras de acesso registradas nas suas

ACLs. Por exemplo, haverá necessidade de alguns usuários especiais possuírem acesso total à *internet*, para eles poderá ser criada uma ACL “acesso_total”, nela estarão todos os *logins* ou IPs das máquinas dos usuários com essa permissão. Da mesma forma poderá ser criada a ACL “acesso_limitado”, nesta ACL estarão todos os demais usuários que passarão pelas regras de bloqueio registradas em outra ACL, que pode ter o nome de “bloqueados”, nela estarão todas as palavras, expressões e siglas, por exemplo, que serão bloqueadas pelo PROXY, ou seja, se em uma URL estiver a palavra “sexo”, e essa palavra estiver listada na ACL “bloqueados”, o PROXY impedirá a passagem da requisição para a *internet*. Lembrando que o PROXY sempre lê as regras de cima para baixo, então assim que encontrar algo que combine com as suas regras ele age eliminando as regras listadas abaixo.

4.2.5 DHCP

O servidor DHCP (*Dinamic Host Configuration Protocol*) configurado em uma rede é outro dispositivo que não oferece segurança adicional à estrutura, mas possibilita maior rapidez na distribuição dos endereços IP internos, além de efetuar atualizações constantes, assegurando a identificação dos *hosts* ativos e redistribuindo os endereços IP que estão ociosos. Este protocolo, segundo Silva (2010, p. 54) é utilizado para gerar e administrar endereços IP, o qual junto com o servidor DHCP distribui os endereços, máscaras, *gateway*, entre outras configurações, para os equipamentos que compõem a rede, porém para que o servidor possa se comunicar com os equipamentos da rede, esses precisam ter o cliente DHCP instalado.

A ideia de utilizar o DHCP na rede e não fixar um IP para cada *host* é empregar o tempo de forma mais vantajosa para a organização, aumentando a produtividade do administrador da rede, que deixará de cadastrar os *hosts*, MACs e IPs, podendo se empenhar em outras atividades que aumentem o desempenho e/ou a segurança organizacional, além de não correr o risco de acabarem os endereços e ajudar a possibilitar o BYOD (*Bryng Your Own Device*) na empresa.

Como esta proposta contempla também a redução de custos, a configuração do Servidor DHCP no *Windows Server* não será abordada por ser proprietário. No *Linux Debian* é facilmente baixado, instalado e configurado. Basta executar o comando no *Shell* “#apt-get install dhcp”, configurar o arquivo “dhcpd” para estabelecer a prioridade do servidor com o comando “#vi /etc/init.d/dhcpd” para abrir o arquivo e editar para “run_dhcpd=1, depois efetuar a configuração do arquivo dhcpd.conf, com o comando “#vi /etc/dhcpd.conf” para

editar o arquivo com as informações da rede. Essas são as configurações básicas do DHCP *free*, sem custo de licenças.

4.2.6 Sistemas de *Backup*

Uma estrutura de tecnologia da informação em alguns casos é a atividade fim, ou seja, o próprio negócio da empresa, ou em outras situações suporta (apoia) toda a administração e produção como atividade meio, em ambos os casos é determinante para a continuidade das operações empresariais. Portanto, copiar e guardar os dados gerados, que é a criação de *backup*, definido por Reiter (2006, p. 308) como sendo à cópia dos dados de um dispositivo para outro com o objetivo de posteriormente os recuperar (os dados), caso haja algum problema, é um ponto muito importante e pode ser determinante para a manutenção das atividades da organização.

Uma empresa que possa investir em equipamentos *storage* como *NetAPP*, *Hauwer*, *Seagate*, HP, *Dell*, por exemplo, que são dispositivos com grande capacidade de armazenamento de dados, terão ótimo suporte quanto ao dimensionamento do espaço e no caso de descontinuidade dos serviços será prontamente atendida.

Contudo existem *softwares* que oferecem praticamente os mesmos serviços sem custos com licenças ou treinamentos longos. O Bacula é um desses *softwares*, ele pode ser instalado em um servidor físico ou virtual e configurado para realizar *backups* dos diretórios dos demais servidores, em conformidade com as especificações de segurança da organização.

4.2.7 Sistemas de Virtualização de Servidores

A virtualização embora não seja uma ideia recente está crescendo exponencialmente com as reflexões sobre a “TI Verde”. Essa expressão trata da preocupação no emprego dos meios de tecnologia da informação sem que para isso haja aumento no consumo dos recursos naturais. O custo de aquisição de equipamentos que acomodem os serviços utilizados pelas organizações é muito alto se forem feitos com a intenção de empregar um equipamento físico para cada serviço.

Há algum tempo os administradores de rede empenhavam um servidor para cada serviço, isso objetivava conseguir o melhor desempenho da máquina, porém com o aumento das organizações e a evolução da tecnologia da informação, aumentou também a quantidade de equipamentos consumindo energia e dissipando calor. Para tentar resolver ou minimizar esses problemas, começaram a surgir os servidores virtuais, que são segundo Silva (2010, p. 29) uma maneira de tentar utilizar um único servidor para realizar várias tarefas, sendo

possível por meio da instalação de um *software* que converte um servidor físico em várias máquinas virtuais.

Empregando um Sistema de Virtualização como o *XenServer* ou o *VMware*, que possuem distribuições gratuitas é possível utilizar os recursos de um equipamento físico para diversos servidores virtuais independentes, que podem ser substituídos rapidamente se houver necessidade, reduzindo custos e aumento a produtividade.

Como citado antes, algum tempo atrás era costume instalar cada serviço em um computador servidor físico isolado para garantir o funcionamento da estrutura, dessa forma o PROXY rodava em um servidor, o DHCP em outro, o Banco de Dados em outro, e assim por diante. Além de onerar a empresa no momento da aquisição dos equipamentos, o consumo de energia elétrica também era elevado. Com o avanço dos sistemas de virtualização é possível criar diversas máquinas virtuais independentes que funcionam adequadamente, mantêm a produtividade em alto nível de desempenho, tudo dentro de um único equipamento físico.

Alguns servidores como o DHCP, DNS, Samba, PROXY, Banco de dados, entre outros, de acordo com a organização, poderiam ser instalados e configurados virtualmente sem redução significativa no desempenho.

4.2.8 Sistemas de Monitoramento

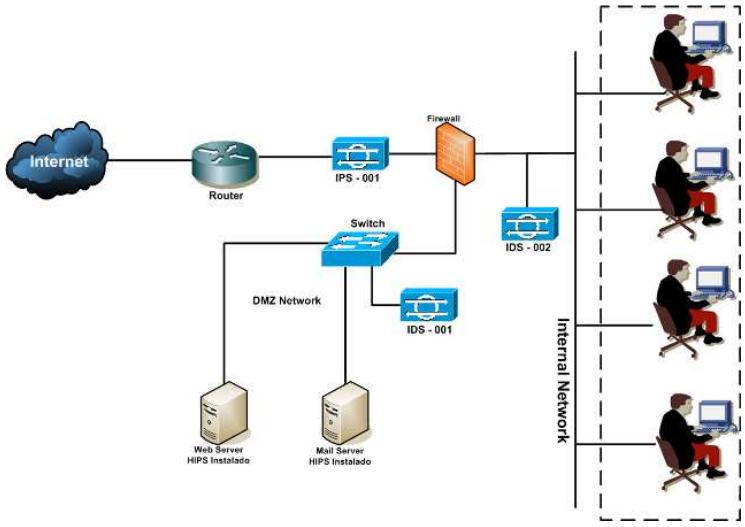
Um dos grandes óbices para os administradores das redes de dados é a ocorrência de problemas com computadores clientes ou servidores que somente são detectados quando esses param de funcionar. Outro problema é relativo aos ataques ou intrusões que provocam danos ou furtam informações valiosas, sem serem detectados por sistemas de segurança mais simples.

Para aumentar a pró-atividade na solução de problemas de funcionamento dos dispositivos internos é interessante que a rede conte com sistemas de monitoramento de desempenho e situação operacional. Como em outros sistemas, existem *softwares* proprietários como o *Network Performance Monitor* da *SolarWinds* e livres como o *Zabbix* e o *Nagios*, todos atendem às demandas relativas aos sinais de mau funcionamento dos componentes a serem monitorados, como o nível de processamento, utilização da memória, espaço em disco etc, facilitando a ação dos administradores das redes nas tomadas de decisão, quanto a recuperação ou substituição do equipamento com problema.

Quanto aos ataques e possíveis intrusões podem ser utilizados um IDS (*Intrusion Detection System*), que segundo Reiter (2006, p. 318) tem como um dos objetivos principais detectar se alguém está tentando entrar no seu sistema ou se algum usuário legítimo está

fazendo mau uso do mesmo, além de que para Nakamura e Geus (2007, p. 267) possuem as funções de coletar, analisar e armazenar as informações e responder às atividades suspeitas, ou um IPS (*Intrusion Prevention System*), que segundo Nakamura e Geus (2007, p. 293) pode ser um IDS operando *inline* com o *firewall*, dessa forma é caracterizado como um IPS baseado em rede, mas também existem os IPS baseados em *hosts*. O primeiro pode ser definido como sistemas de *software/hardware* que automatizam o processo de monitoramento de eventos que ocorrem em sistemas computacionais, analisando-os com base em assinaturas criadas a partir de problemas de segurança, que são as intrusões. O segundo pode ser visto como a evolução do primeiro, podendo agir como um IDS, além de possuir a capacidade de prevenir uma possível intrusão, rechaçando os ataques.

Figura 12 – Exemplo topologia de rede demonstrando a posição de dispositivos IDS/IPS.



Fonte – https://bitvoador.wordpress.com/2011/08/25/informatica-ips-e-ids/

No desenho da rede os dispositivos IDS são posicionados atrás do *firewall*, *inline* ou conectados a uma porta de *switch*, na primeira opção, como citado acima, todo o fluxo de entrada e saída da rede passa obrigatoriamente por ele, fazendo com que ele possa operar como um IPS, e na segunda situação o IDS recebe apenas uma cópia dos dados gerando relatórios, agindo de forma passiva apenas detectando intrusões. O grande problema desses dispositivos é a geração de uma quantidade muito grande de falsos positivos, o que sobrecarrega o analista de segurança.

Quanto ao IPS ele pode ficar à frente ou atrás do *firewall*, porém atrás ele poderá agir concentrando ações apenas nos ataques que passarem pelo *firewall*, reduzindo substancialmente o seu trabalho. Não há informações sobre IDS/IPS gratuitos, portanto

mesmo sendo facilitadores para a administração de rede de dados, principalmente quanto à segurança é muito possível que a maioria das organizações não aplique essas ferramentas, dados os custos de aquisição.

4.3 Atualização dos Sistemas Operacionais

Muitos problemas de intrusões em redes de dados e em sistemas informatizados têm origem na ausência de uma prática simples e que deveria ser realizada constantemente, a atualização dos sistemas operacionais.

Principalmente os sistemas operacionais e aplicativos recém lançados, possuem muitos *bugs*, então as atualizações constituem operações essenciais para a longevidade do ambiente de informática. Constantemente há comunicados como esse "Comunicado de Segurança da *Microsoft*: Atualização para vulnerabilidades no *Adobe Flash Player* no *Internet Explorer* 10", extraído de http://support.microsoft.com/kb/2770041/pt-br, que destacam a importância da atualização desses *softwares*.

Sistematicamente há discussões sobre a eficiência dos sistemas operacionais, quanto à segurança, desempenho, facilidade de operação etc. No que diz respeito à segurança, o grande mal é a falta de ação dos administradores das redes, que permitem que esses permaneçam desatualizados, mesmo após o lançamento de pacotes de atualização.

Tanto o *Windows* quanto o *Linux*, que são os mais utilizados atualmente são bastante seguros, desde que sejam atualizados conforme as orientações do fabricante ou do distribuidor, respectivamente, pois o sistema operacional mais vulnerável é aquele que está desatualizado.

Os indivíduos mal-intencionados que utilizam os meios cibernéticos para causar danos, os chamados "*Hackers*", buscam principalmente as vulnerabilidades existentes para explorá-las e vencer as barreiras de segurança. Portanto, devem-se aplicar constantemente as atualizações dos sistemas operacionais, pois se os "*Hackers*" buscam incessantemente novas vulnerabilidades para explorá-las, cabe aos administradores das redes, pelo menos instalarem as proteções desenvolvidas para aquelas que já foram encontradas.

Uma sugestão importante é escolher um servidor de cada sistema operacional para realizar as atualizações automáticas, pois há situações que os pacotes de atualizações interferem em alguns sistemas, provocando mau funcionamento, incompatibilidade e até paralisação do serviço. Assim, tendo redundância de servidores, pode-se manter um atualizando automaticamente e o outro não, dessa maneira os serviços permanecerão ativos e

possibilitará ao administrador tempo para solucionar o problema sem interferir na disponibilidade dos sistemas e serviços, mantendo a produtividade da rede.

4.4 Adequação das Instalações

As instalações para os equipamentos de tecnologia da informação não devem ser iguais às demais áreas da organização, pois são áreas muito sensíveis. Dificilmente, exceção feita às grandes empresas, bancos e organizações governamentais, encontra-se um local que foi pensado e projetado exclusivamente para a informática. Sem dúvida o reaproveitamento de salas e demais espaços constituem uma realidade na maioria das situações.

Mas é possível adequar um ambiente já existente à utilização por parte da informática. A reestruturação do espaço físico pode ser feita conforme a norma ABNT NBR ISO/IEC 27001:2013 (A.11.2.1 – Escolha de local e proteção do equipamento e A.11.1.1 Perímetro de segurança física), passando pela substituição de portas (A.11.1.2 - Controles de entrada física), retirada de janelas ou substituição por vidros mais espessos e resistentes (A.11.1.4 - Proteção contra ameaças externas e do meio ambiente), elevação do piso (A.11.1.5 – Trabalho em áreas seguras), e no caso de edifícios comerciais e *data centers*, utilizar a norma ABNT – NBR 14565:2012, para adequar o cabeamento (A.11.2.3 – Segurança do cabeamento), que normalmente não é dimensionado para a nova demanda e instalação de sistema de ar refrigerado (Padrão ASHRAE – Classe 1), por exemplo, são medidas que colaboram com a segurança da informação e a manutenção da produtividade da estrutura.

Para que um ambiente seja considerado fisicamente seguro é necessário a realização de um projeto adequado às expectativas e exigências da empresa, de acordo com o valor do bem que se deseja manter seguro. Partindo da escolha do local que será protegido, uma boa estratégia é montar um perímetro dividido em níveis com diversos dispositivos de segurança, como cercas, câmeras, portão de acesso único entre outros, que vão se sobrepondo até o local que se deseja proteger, como o CPD da organização.

Segundo Lento (2011, p. 23) as barreias de segurança visam desencorajar, objetivando fazer com o que o atacante perca o estímulo por tentar suplantar a segurança, pela presença de meios físicos, tecnológicos ou humanos (ex: vigilantes ou câmeras de vídeo); dificultar, empregando dispositivos complementares aos anteriores visando dificultar o acesso indevido (ex: catracas e detectores de metal); discriminar, estabelecendo perfis de acesso associando esses perfis com as áreas que eles podem circular dentro da organização (ex: o crachá azul estabelece a área azul da empresa como limite de circulação); detectar, apresentam soluções que sinalizam, alertam e instrumentam os gestores de segurança na

detecção de risco (ex: IDS, sistema de monitoramento – *Nessus*, *Nagios* ou *Zabbix*); deter, objetiva impedir que as ameaças físicas ou lógicas atinjam os ativos (ex: ações administrativas, punitivas e bloqueio de acessos físicos e lógicos, IPS); e diagnosticar, representa a continuidade do processo de gestão da segurança. É o caminho de retorno à primeira barreira que possibilita aplicar melhorias.

A sala onde será instalado o CPD deve possuir um sistema de refrigeração adequado e redundante, monitorado constantemente para manter os servidores operando em temperaturas e níveis de umidade apropriados. Dessa forma a ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers, Sociedade Americana de Engenheiros de Climatização), uma entidade norte-americana reconhecida internacionalmente na área de padronização de climatização, estabeleceu 4 classes de ambientes a serem considerados conforme quadro 1 e apresentou as conclusões dos estudos feitos acerca da temperatura e umidade permitidas e ideais para os ambientes, chegando às conclusões descritas no quadro 2, a seguir:

Quadro 1 – Classes de requisitos para os ambientes dos equipamentos.

CLASSES DE REQUISITOS PARA OS AMBIENTES DOS EQUIPAMENTOS			
Classes	Ar Condicionado	Controle do ambiente	Exemplo
1	Sim	Rígido	Equipamentos com Servidores e *Storages*
2	Sim	Frouxo	Equipamentos com Servidores e *Storages* fora do CPD
3	Sim	Não	Estações de Trabalho, PCs e impressoras
4	Não	Não	Pontos de venda de equipamentos

Fonte – Produzido pelo autor do trabalho, (adaptado e traduzido de http://searchdatacenter.techtarget.com/tip/Using-ASHRAE-specs-for-data-center-metrics)

Quadro 2 – Especificações de temperatura e umidade relativa.

ESPECIFICAÇÕES DO AMBIENTE				
Classe	Temperatura Permitida (°C)	Temperatura Recomendada (°C)	% umidade relativa permitida	% umidade relativa recomendada
1	15 até 32.2	20 até 25	20-80	40 -55

Fonte – Produzido pelo autor do trabalho, (adaptado e traduzido de http://searchdatacenter.techtarget.com/tip/Using-ASHRAE-specs-for-data-center-metrics)

As instalações elétricas devem ser estruturadas para suportar a demanda extra de energia, então é interessante a montagem de uma rede elétrica exclusiva desde a "Casa de Força" da organização para atender à demanda do CPD, de forma que essa não perca tensão e provoque perda de desempenho ou danos nos equipamentos. O *nobreak* é um dispositivo fundamental para a manutenção dos serviços ativos, e a aquisição dessa ferramenta deve ser

adequada ao consumo dos equipamentos que serão atendidos por ele. Existem *sites* de vendedores que fornecem calculadoras online para ajudarem na escolha dos equipamentos como: http://extreme.outervision.com/psucalculatorlite.jsp. Outra consideração é quanto ao histórico de quedas de energia constantes ou apagões longos na região. Neste caso pode ser instalado um *nobreak* com autonomia maior, dando maior tranquilidade para o administrador da rede aguardar o retorno da energia, apenas monitorando os serviços. Contudo, se for necessário que os serviços fiquem ativos no regime de 24/7, sob pena de perda de negócios ou credibilidade que possam impactar a organização, torna-se interessante reduzir o investimento no *nobreak*, adquirindo um menor, suficiente para manter os servidores em funcionamento, até que um gerador seja acionado e forneça energia elétrica ou que retorne a eletricidade da concessionária, para todos os equipamentos do CPD.

5 TESTES E RESULTADOS ESPERADOS

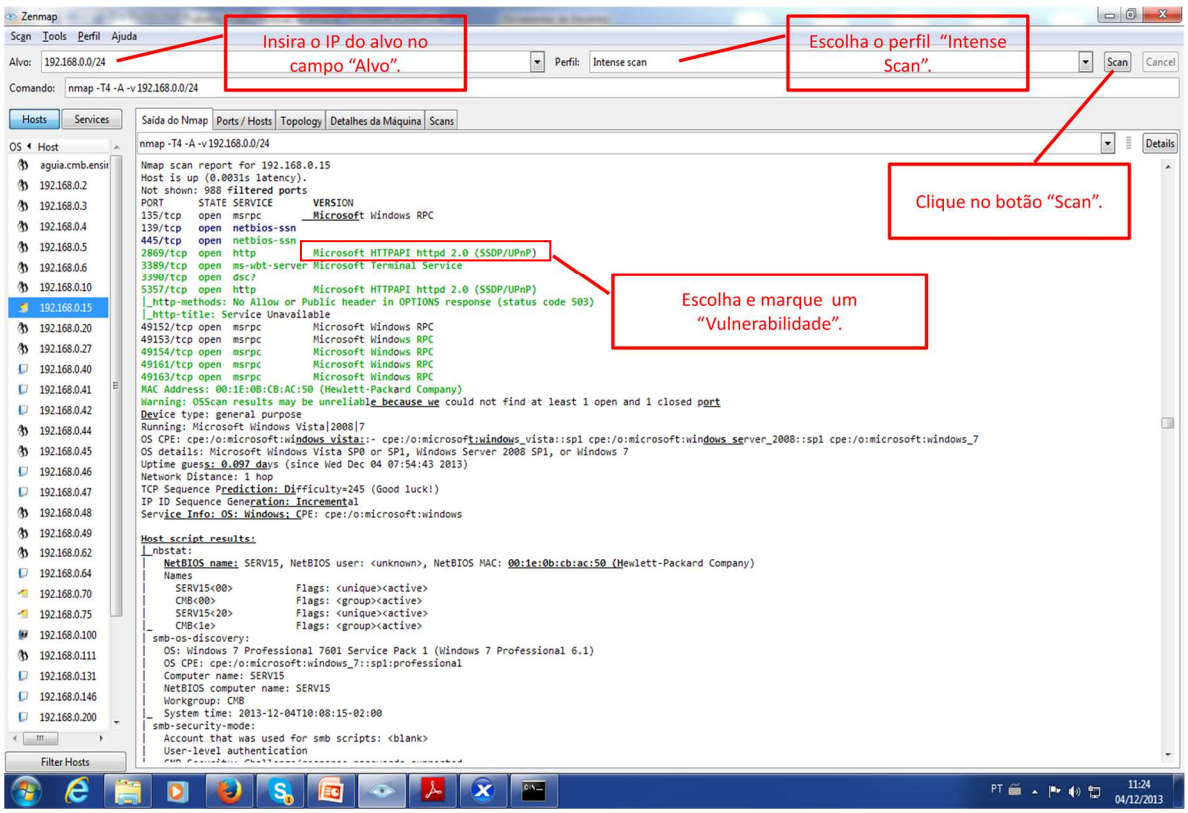
Os testes sugeridos são alguns simples, básicos e gratuitos dentre diversos outros, que poderão ajudar na gestão dos recursos de tecnologia da informação das organizações. Porém antes de executar os testes é importante verificar quem irá realizá-los, uma empresa contratada, um revendedor, o pessoal interno, os *hackers*, pois de acordo com Nakamura e Geus (2007, p. 258), todos têm suas vantagens e desvantagens, cabendo ao gestor de TI da organização escolher o que melhor lhe atender.

As atividades que seguem não são aplicadas somente no término do projeto, devem ser executadas sistematicamente, de preferência com prazos fixados e registrados na Política de Segurança, como parte do fechamento do ciclo PDCA.

5.1 Teste de vulnerabilidades.

Sugere-se utilizar o *software Nmap* ou o *Zenmap*, dada a sua facilidade de operação para fazer varreduras em busca de vulnerabilidades nos sistemas operacionais dos computadores e servidores da rede.

Figura 13 – Exemplo de resposta de teste de vulnerabilidade.

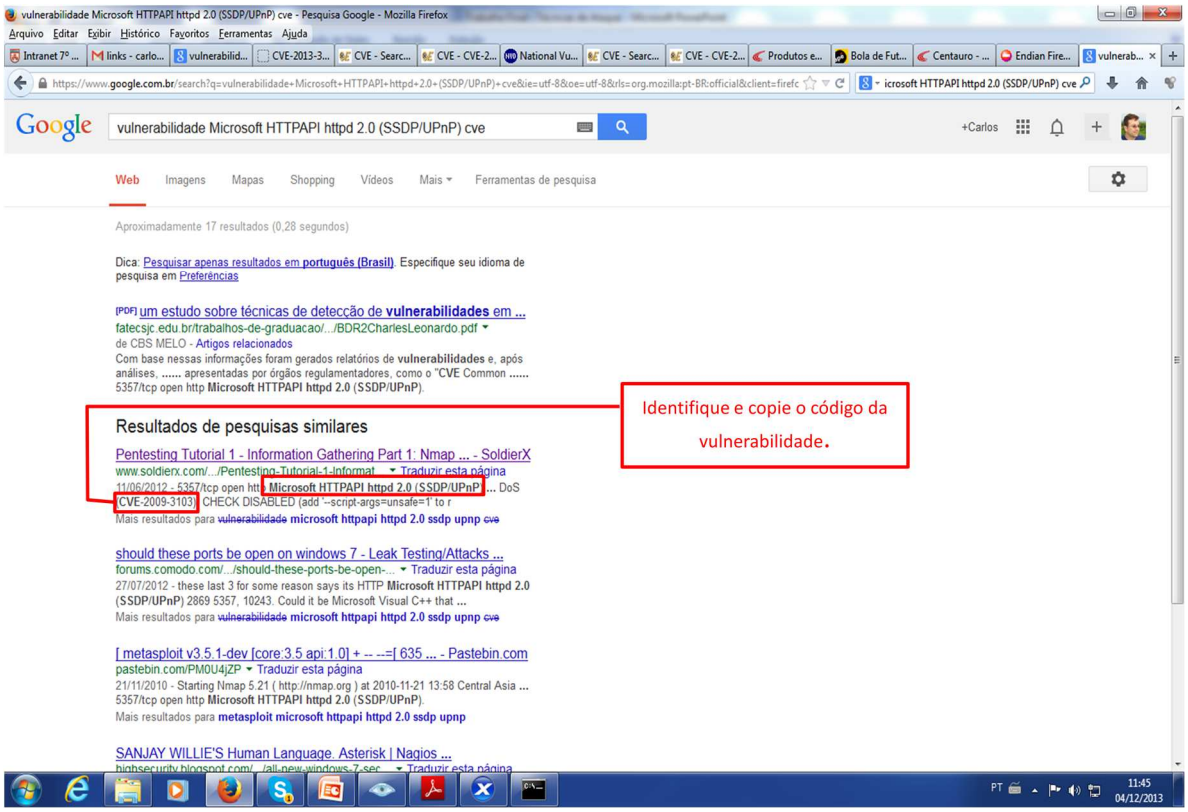


Fonte – Produzido pelo autor do trabalho.

Nos primeiros testes certamente serão encontrados muitos problemas os quais são até aceitáveis, desde que sejam tratados o mais rápido possível, objetivando a conformidade com as normas em vigor, por exemplo, as boas práticas citadas na ABNT NBR ISO/IEC 27002:2013.

Desta maneira, as vulnerabilidades encontradas após a varredura do *software* escolhido (*Zenmap* ou *Nmap*) são selecionadas e colocadas nos *sites* de busca para obtenção do seu código CVE.

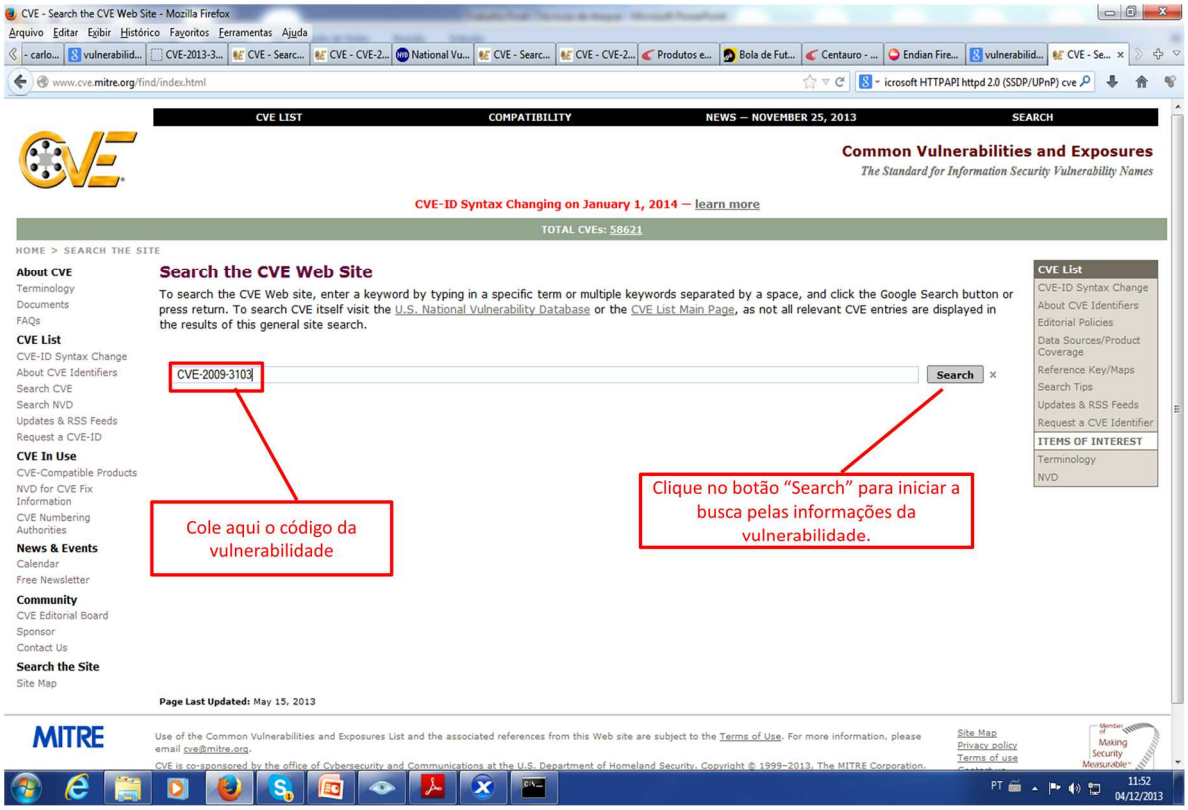
Figura 14 – Exemplo de pesquisa por código CVE em *sites* de busca.



Fonte – Produzido pelo autor do trabalho.

De posse do referido código são feitas buscas nos *sites* do *Common Vulnerabilities and Exposures* (www.cve.mitre.org) e do *National Vulnerability Database* (http://nvd.nist.gov), onde estão listadas e descritas todas as vulnerabilidades conhecidas, com os possíveis danos que podem causar e as soluções que a serem aplicadas para eliminá-las do sistema.

Figura 15 – Exemplo de pesquisa por descrição e solução de vulnerabilidade.

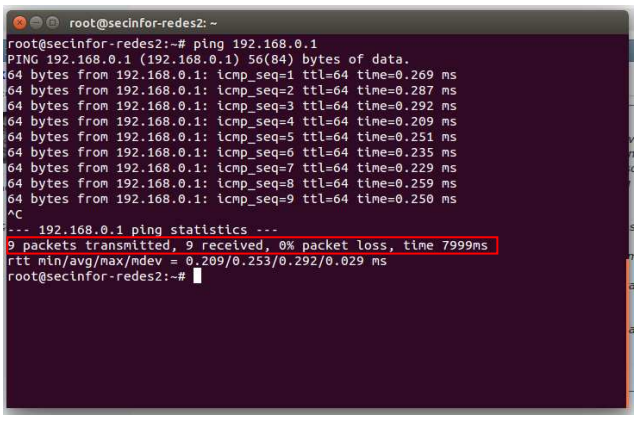


Fonte – Produzido pelo autor do trabalho.

5.2 Teste de estabilidade da rede.

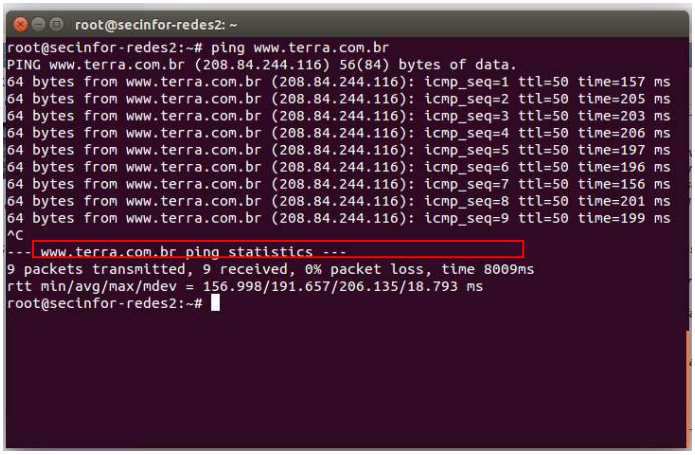
Como foi dito durante este trabalho, uma rede de dados é composta por diversos dispositivos os quais funcionam com suprimento de energia elétrica e sob condições adequadas de temperatura e umidade, por isso são aplicados diversos testes para verificar a estabilidade da rede, tanto na transmissão dos dados quanto no suprimento de energia pelos diversos meios, rede elétrica predial, *nobreak* e gerador, quando for o caso.

Figura 16 – Exemplo de teste de latência com "*ping*" em rede interna.



Fonte – Produzido pelo autor do trabalho.

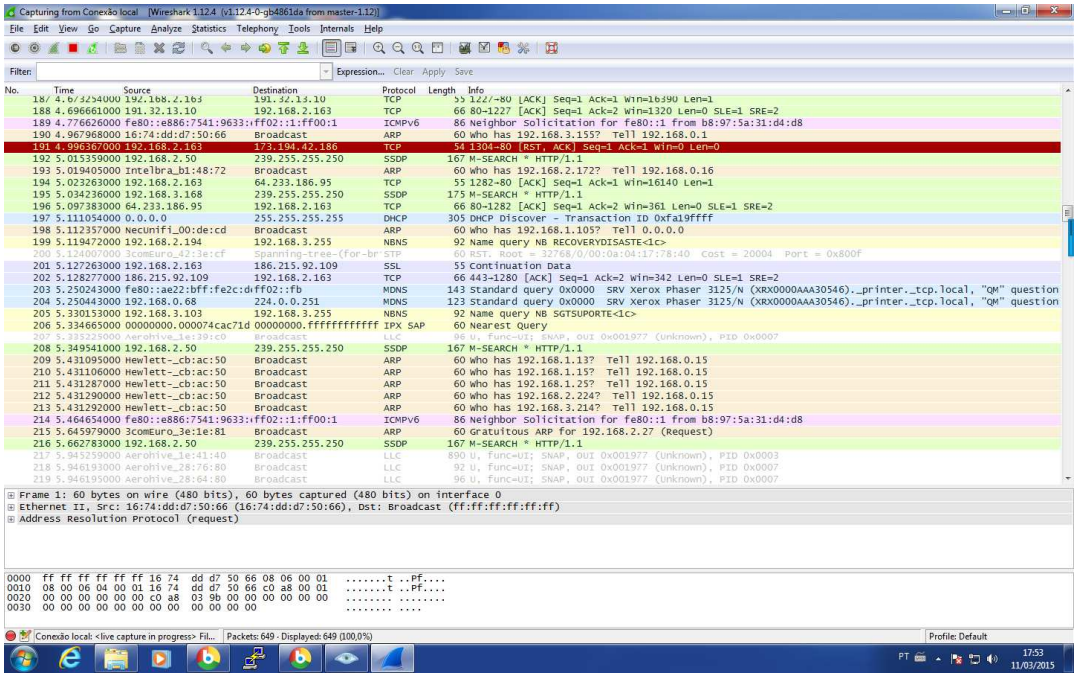
Figura 17 – Exemplo de teste de latência com “*ping*” para a *internet*.



Fonte – Produzido pelo autor do trabalho.

O teste de latência que mede o tempo necessário para uma mensagem ir a um destino e voltar dele, conhecido como “*ping*” é utilizado para verificar a estabilidade e a velocidade da rede conforme o tempo de resposta. As respostas devem estar em ms (milissegundos), são consideradas normais e não alarmantes respostas constantes em uma LAN de até 0,300ms. Nas imagens anteriores podem ser observadas outras entregas do teste que são a quantidade de pacotes transmitidos e recebidos, além dos pacotes perdidos. Caso a resposta do “*ping*” seja alta, significa que a rede está lenta por erros de configuração ou interferências na estrutura.

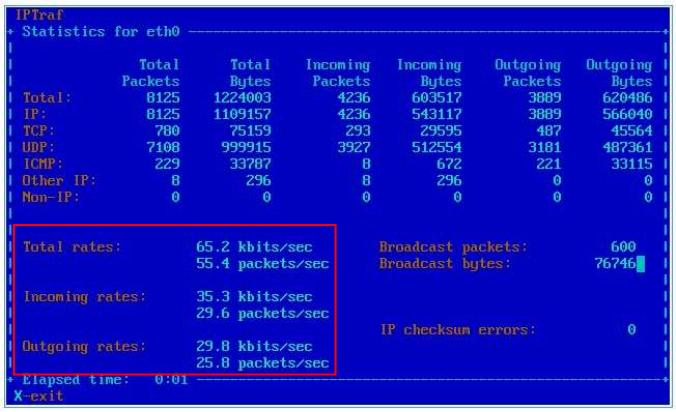
Figura 18 – Exemplo de teste de fluxo de pacotes com *Wireshark* em rede interna.



Fonte – Produzido pelo autor do trabalho.

Para efetuar os testes de transmissão dos dados é possível utilizar o *Wireshark* ou o IPTRAF que são *softwares* gratuitos de fácil instalação no *Linux* e/ou *Windows*, capazes de verificarem, em tempo real, o volume de Kbits/Seg e Pacotes/Seg que estão trafegando, assim estabelecer parâmetros de normalidade evitando “inundação” de dados que pode paralisar a rede.

Figura 19 – Exemplo de teste de fluxo de pacotes com IPTRAF em rede interna.



Fonte – Produzido pelo autor do trabalho.

Na imagem do *Wireshark*, é possível verificar o fluxo de pacotes com o endereço de origem e destino, o seu tamanho e seus protocolos, entre outras informações. No caso da imagem do IPTRAF, as informações são mais sucintas, mas não menos importantes como o total de fluxo de pacotes/seg e kbits/seg e o fluxo de entrada e saída. Esses dados são determinantes de acordo com as bandas das redes, portanto um fluxo total de 65.2 kbits/sec não provoca lentidão em uma rede com banda *gigabit/sec*, por exemplo.

Quanto ao suprimento de energia elétrica, no caso da rede predial é interessante que seja exclusiva para o CPD, para evitar ou diminuir a possibilidade de perda de tensão o que é prejudicial ao funcionamento dos equipamentos, muito embora as fontes, estabilizadores e *nobreaks* consigam transformar as tensões alternadas de 110w ou 220w em baixas tensões de correntes contínuas que circulam nos componentes dos computadores, mas as grandes variações para cima ou para baixo sobrecarregam esses dispositivos, podendo danificá-los. Neste caso, basta realizar a leitura da tensão elétrica para verificar a sua normalidade, e se for necessário adequá-la conforme as especificações técnicas.

Quanto aos testes do *nobreak* e do gerador, esse último quando for o caso, basta interromper o suprimento de energia que os alimenta para verificar se os dispositivos, os quais

deveriam se manter ativos estão sendo alimentados adequadamente e monitorar se o tempo de autonomia efetivo, corresponde ao que foi adquirido junto ao fornecedor.

5.3 Teste de *Firewall*

Segundo Nakamura e Geus (2007, p. 256), testar um *firewall* significa verificar se uma política de segurança foi bem desenvolvida, se foi implementada de modo correto e se o *firewall* realiza aquilo que declara realizar.

Para consolidar as funcionalidades do *firewall*, podem ser aplicados os testes de penetração utilizando, por exemplo, ferramentas gratuitas disponíveis no *Kali Linux* para efetuar esse tipo de teste, no qual se espera que, se as configurações do *firewall* estiverem corretas, a rede não será invadida por esse meio.

Para Raeny (1997 *apud* NAKAMURA; GEUS, 2007, p. 257), um teste de *firewall* pode ser estruturado em quatro etapas:

- Coleta de informações indiretas: informações que podem ser obtidas sem que o *firewall* faça registros ou bloqueie acessos.

- Coleta de informações diretas: são as informações protegidas e que, portanto, podem ter seu acesso detectado e registrado.

- Ataques externos: esses testes podem ser realizados utilizando-se ferramentas como *scanning* de vulnerabilidades, a partir de *hosts* confiáveis, ou por meio de IP *Spoofing*, que mascara a origem dos ataques.

- Ataques internos: estes testes têm como objetivo verificar se os usuários internos podem realizar ataques a *hosts* externos.

5.4 Auditoria de Informática

Uma auditoria pode ser interna quando é idealizada e realizada pelos próprios membros da organização, ou externa quando se contrata uma empresa especializada para atestar a conformidade da organização ou levantar inconformidades que deverão ser adequadas, de acordo com as normas vigentes.

Segundo Lento (2011, p. 210) uma auditoria consiste em estabelecer e executar procedimentos para a coleta de dados gerados pela atividade de um sistema computacional (uma rede, sistema de informação ou qualquer dispositivo de *hardware* ou *software*).

Dias (2000 *apud* LENTO, 2011, p. 210) destaca que a auditoria é dividida em três fases:

- Planejamento – identifica os instrumentos indispensáveis à sua realização;

- Execução – reúne as evidências teoricamente confiáveis, relevantes e úteis para a realização dos objetivos da auditoria;

- Relatório – são apresentados os resultados, análises e conclusões.

Mesmo não sendo propriamente um teste, uma auditoria é um “mal necessário”, pois realiza uma leitura profunda do que se deseja discutir e/ou adequar levantando inconformidades, o que nem sempre é bem-visto pelos gestores, que poderiam ser prejudiciais aos recursos de tecnologia da informação.

De posse do relatório da auditoria o gestor de TI poderá elaborar um plano de segurança ou de contingência para transformar as inconformidades em conformidades, estabelecendo regras e procedimentos que realimentarão o ciclo PDCA.

CONCLUSÃO

Para que uma rede de dados possa ser considerada produtiva e segura, é preciso inicialmente saber distinguir a produtividade empresarial da produtividade computacional, ou de informática. A produtividade empresarial é estabelecida por uma equação matemática na qual é verificado que a produtividade é a diferença entre o valor final do que foi produzido e o custo dessa produção. No caso de um sistema computacional ou uma rede de dados, a visão muda, pois para a informática, produtividade está relacionada ao tempo de permanência dos serviços ativos, assim busca-se a disponibilidade 24/7, 24 horas por dia durante os 7 dias da semana, essa seria a produtividade 100% dos sistemas de informática.

Contudo para chegar a esse nível de produtividade o investimento financeiro deverá ser proporcional ao alto nível de exigência, assim somente grandes empresas e principalmente grandes bancos investem somas correspondentes à imposição da disponibilidade 100%. As médias e pequenas empresas também se preocupam com a segurança e produtividade dos seus sistemas, mas assumem muito mais riscos do que aquelas que poderiam sofrer muito mais com a perda da credibilidade e/ou dos seus segredos industriais.

A busca pelo equilíbrio é constante, e assumir riscos faz parte dessa equação. Para atingir os resultados esperados de produção, uma rede de dados deve possuir diversos dispositivos que irão lhe proteger de ataques externos, de ataques internos (mau uso intencional ou não), da falta de energia elétrica, das intempéries etc, e mesmo assim deverá buscar sempre a atualização das rotinas e melhoria dos processos – PDCA (*Plan, Do, Check and Act*), pois a segurança é um estado de momento.

Para a proteção física dos meios de informática, as instalações devem ser adequadas, com controle de acesso, estabelecimento de perímetros de segurança, monitoramento por câmeras, salas seguras ou salas cofres, refrigeração, luzes de emergência, extintores de incêndios entre outras ferramentas.

Para a proteção lógica, vários dispositivos devem ser aplicados, como *firewalls*, servidores PROXY, IDS (*Intrusion Detection System*) ou IPS (*Intrusion Prevention System*), controle de usuários, privilégio mínimo, senhas diferentes e robustas para cada sistema etc.

No entanto, para atingir a proteção de todos os serviços e sistemas e assegurar a alta disponibilidade com grande produtividade é preciso, além dos dispositivos físicos e lógicos, um maciço trabalho de conscientização dos usuários, pois o elo mais fraco na corrente da segurança da informação é o fator humano.

Assim é sugerido que os sistemas operacionais dos servidores sejam distribuições *Linux* (*Debian*, *RedHat*, *Fedora* etc), pela experiência, prática e facilidade na operação sugere-se o *Debian7-Wheezy* ou a distribuição estável mais recente como padrão a ser empregado. A ideia para o desenho da rede de dados é a topologia estrela estendida, com utilização de *switches* de camada 2 ou 3, segmentada em VLANs, com classificação hierárquica cliente-servidor, tecnologia *Gigabit Ethernet* para ter maior longevidade e para que o custo do investimento inicial seja diluído pelo seu tempo de vida útil, destacando a relação custo *versus* benefício.

A sugestão relativa à proteção lógica é a utilização de dois *firewalls* gratuitos *pfSense* ou *Endian*, o primeiro "externo" que será o *gateway* e onde estarão as configurações de segmentação da DMZ e o NAT para acesso à *internet*. No segundo que poderá ser nomeado de "interno" serão configuradas as segmentações das redes dos administradores, dos usuários e dos serviços internos da rede, além do acesso ao *firewall gateway*. Essas medidas efetuadas no *firewall* "interno" visam diminuir os domínios de colisão e facilitar a identificação de possíveis falhas futuras, reduzindo o tempo de reação.

O acesso à *internet* deverá ser filtrado pelo *PROXY Squid*, que é gratuito e de fácil configuração, no qual estarão as ACLs de controle de conexões e exceções. Esse servidor deverá ser instalado e configurado na rede de serviços, assim como o DHCP.

Se houver necessidade de a rede se tornar híbrida, por causa de algum sistema legado ou aquisição de alguma ferramenta que seja exclusiva da plataforma *Windows*, e com isso obrigue a utilização simultânea de *Windows* e *Linux*, poderá ser configurado um Servidor Samba, que também é gratuito, para criar um domínio híbrido e integrar os serviços, compartilhar pastas (diretórios) e recursos desses dois sistemas operacionais.

Os usuários merecem atenção especial, por isso uma política de segurança clara e normas de utilização dos recursos de informática deverão ser criadas e distribuídas, além de sistematizar a promoção da sua leitura por parte dos colaboradores. O cadastro dos usuários poderá ser efetuado utilizando o protocolo LDAP (*Lightweight Directory Access Protocol*) e administrado pelo *software* LDAP Admin ou o GOSA, pois são gratuitos, de fácil instalação, configuração e administração.

O suprimento de energia deve ser adequado a cada empresa de acordo com a sua situação particular de negócios e dimensões. Sugere-se criar uma rede de suprimento de energia exclusiva para o CPD (Centro de Processamento de Dados), para que não haja perda de tensão e a instalação de um *nobreak* que suporte tempo suficiente, pelo menos para que os servidores sejam desligados corretamente. Caso seja necessário que os servidores

permaneçam ligados por tempo indeterminado, sob pena de perda de negócios, credibilidade, enfim, na situação de as perdas serem maiores que o investimento, então o interessante é instalar um *nobreak* que dê autonomia mínima até que um gerador de energia seja acionado e restabeleça o fluxo de energia elétrica, assim o investimento financeiro no *nobreak* será reduzido e redirecionando para a aquisição de um gerador mais robusto que ofereça maior autonomia.

No CPD, o ideal é que não haja janelas de vidros, para evitar fragmentação por choque de pássaros, chuvas de granizo, vendavais etc, além disso, deverá ser refrigerado adequadamente com a instalação de aparelhos de ar condicionado. De acordo com o tamanho do espaço calcula-se o porte dos aparelhos, os quais deverão ser no mínimo dois para redundância e rodízio na utilização, e também estarem conectados à rede elétrica atendida por um gerador de energia elétrica.

Sistemas de combate a incêndios também são propostos, no caso dos CPDs, o ideal é que sejam instalados extintores de incêndio de gás carbônico.

Os computadores que serão utilizados como servidores e a quantidade desses equipamentos são determinados pela dimensão da organização, inclusive podendo utilizar alguns Sistemas de Virtualização de Servidores, como o *VMware* e o *XenServer* que possuem distribuições gratuitas oferecendo serviços que podem atender às empresas reduzindo os custos com a aquisição de equipamentos. Outra vantagem da virtualização é quanto à redundância dos servidores, sempre é interessante possuir pelo menos dois de cada servidor em produção, contudo a aquisição de máquinas para esse fim onera o projeto e muitas vezes o inviabiliza, assim as empresas assumem os riscos que a falta desses dispositivos redundantes traz. No caso da virtualização esses custos não existem, já que os servidores podem ser exportados como arquivos e em alguma necessidade podem substituir rapidamente aquele que estava ativo.

Por fim, aconselha-se utilizar um sistema de monitoramento que fornecerá informações em tempo real da rede, servidores, computadores clientes, impressoras e demais dispositivos computacionais, para essa atividade existem, entre outros, dois *softwares* livres o *Zabbix* e o *Nagios*, cada um com suas particularidades e funcionalidades, mas ambos de alto desempenho.

A estrutura descrita acima retrata um sistema computacional básico de segurança e produtividade que estabelecerá a manutenção dos serviços ativos de acordo com as necessidades de cada organização.

REFERÊNCIAS

ABNT. NBR ISO/IEC 27002:2013

Comunicado de Segurança da *Microsoft*: Atualização para vulnerabilidades no *Adobe Flash Player* no *Internet Explorer* 10. Disponível em: <http://support.microsoft.com/kb/2770041/pt-br>. Acesso em: 2 mar. 2015. 21:00.

FREUND, Gislaine Parra. **Redes de Computadores I**. Palhoça: UnisulVirtual, 2009.

ICSA. 3rd Annual Firewall Buyer's Guide. ICSA 2003.

ISO/IEC 27000:2014, p. 4

LENTO, Luiz Otávio Botelho. **Segurança da Informação**. Palhoça: UnisulVirtual, 2011.

McCARTHY, N. K. **Resposta a Incidentes de Segurança em Computadores**: planos para proteção de informação em risco. Porto Alegre: Bookman, 2014.

MARINO, Lúcia Helena Fazzane de Castro. Gestão da qualidade e gestão do conhecimento: fatores-chave para produtividade e competitividade empresarial. In: **XIII SIMPEP** – Bauru, 2006, p 2. Disponível em: < http://www.simpep.feb.unesp.br/anais/anais_13/artigos/598.pdf>. Acesso em: 03 mar. 2015. 19:45.

Measure proper temperature and humidity using Ashrae's Thermal Guidelines for Data Processing Environments. Disponível em: <http://searchdatacenter.techtarget.com/tip/Using-ASHRAE-specs-for-data-center-metrics>. Acesso em: 12 fev. 2015. 23:00.

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

REITER, Cláudio César. **Redes de Computadores II**. Palhoça: UnisulVirtual, 2006.

SILVA, Camila Ceccatto. **Trabalhando com Redes de Computadores**: conceito e prática. Santa Cruz do Rio Pardo: Viena, 2010.