UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ
TECNÓLOGO EM REDES DE COMPUTADORES

TALLIS DEYVIDE MAIA RUBENS

PROJETO DE REDE DE COMPUTADORES PARA O CENTRO ADMINISTRATIVO DA PREFEITURA MUNICIPAL DE IBICUITINGA

QUIXADÁ
2013

TALLIS DEYVIDE MAIA RUBENS

PROJETO DE REDE DE COMPUTADORES PARA O CENTRO ADMINISTRATIVO DA PREFEITURA MUNICIPAL DE IBICUITINGA

Trabalho de Conclusão de Curso submetido à Coordenação do Curso Tecnólogo em Redes de Computadores da Universidade Federal do Ceará como requisito parcial para obtenção do grau de Tecnólogo.

Área de concentração: computação

Orientador Prof.º Dr. Arthur de Castro Callado

QUIXADÁ
2013

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Campus de Quixadá

R83p Rubens, Tallis Deyvide Maia
Projeto de rede de computadores para o Centro Administrativo da Prefeitura Municipal de Ibicuitinga / Tallis Deyvide Maia Rubens – 2013.
68f. : il. color., enc. ; 30 cm.

Monografia (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso Superior de Tecnologia em Redes de Computadores, Quixadá, 2013.
Orientação: Prof. Dr. Arthur de Castro Callado
Área de concentração: Computação

1. Redes de computadores 2. Informações eletrônicas governamentais 3. Redes locais (Computadores) I. Título.

CDD 004.6

TALLIS DEYVIDE MAIA RUBENS

TALLIS DEYVIDE MAIA RUBENS

PROJETO DE REDE DE COMPUTADORES PARA O CENTRO ADMINISTRATIVO DA PREFEITURA MUNICIPAL DE IBICUITINGA

Trabalho de Conclusão de Curso submetido à Coordenação do Curso Tecnólogo em Redes de Computadores da Universidade Federal do Ceará como requisito parcial para obtenção do grau de Tecnólogo.

Área de concentração: computação

Aprovado em: _____ / dezembro / 2013.

BANCA EXAMINADORA

_____
Prof°. Dr. Arthur de Castro Callado (Orientador)
Universidade Federal do Ceará - UFC

_____
Profª. Dra. Atslands Rego da Rocha
Universidade Federal do Ceará - UFC

_____
Profª. Dra. Paulyne Matthews Jucá
Universidade Federal do Ceará - UFC

A minha formação como tecnólogo não poderia ter sido concretizada sem a ajuda de meus amáveis e eternos pais Aldemir e Eliene, que, no decorrer da minha vida, proporcionaram-me, além de extenso carinho e amor, os conhecimentos da integridade, da perseverança e de procurar sempre em Deus a força maior para o meu desenvolvimento como ser humano. Por essa razão, gostaria de dedicar e reconhecer a vocês, minha imensa gratidão e sempre amor.

AGRADECIMENTOS

Ao prof. Dr. Arthur de Casto Callado, pela orientação deste de trabalho de conclusão de curso e seu grande desprendimento em ajudar-me.

À profª. Dra. Tânia Saraiva de Melo Pinheiro, pela sua eficiente supervisão metodológica e materiais fornecidos.

Aos professores do curso, Dr. Alberto Sampaio Lima, Dra. Atslands Rego da Rocha, Dr. David Sena, Oliveira, Me. Diana Braga Nogueira, Me. Enyo José Tavares Gonçalves, Dr. Flávio Rubens de Carvalho Sousa, Me. Jeandro de Mesquita Bezerra, Me. Jefferson de Carvalho Silva, Me. João Ferreira de Lavor, Me. João Marcelo Uchôa de Alencar, Dr. Marcos Antônio de Oliveira e Me. Marcos Dantas Ortiz.

Aos colegas e amigos do curso, Carlos Bruno, Adonai Filho, Evelyne Avelino, Joel Pereira, Sebastião Nogueira, Jammes Wilker, Glailton Costa, Francisco Nobre, Egberto Barreto, Paulo Victor Estevam, Thiago Torres, Rafael Pinheiro, Júlio César, Aline Oliveira, Felipe Alex, Otacílio Aguiar, Marcelo Miranda, João Faustino, Maicon Camurça, Everton Monteiro, Atrícia Sabino e Iranildo Fidelis.

Ao meu irmão Tayrisson e familiares.

Aos amigos Jayny Myrelle, Danielle Lima, Aurilene Damasceno, Max Well, Gabriel Henrique, Beatriz Sousa, Eduardo Henrique, Luiz Rodrigues, Jardel Freitas, Alan Sousa, Lidiano Oliveira, Vanessa Bezerra, Sadan Maia, Felipe Élison, Anderson Portela, Janayna Freitas, Jamilly Paz, Wilker Darly, Paulina Mota, Áurea Moura e Ana Crys pelo incentivo e amizade.

À Prefeitura Municipal de Ibicuitinga, em nome do Secretário James Dias e do Gerente de TI Wendell Bandeira pelo apoio prestado no decorrer do desenvolvimento do projeto.

"O sucesso nasce do querer, da determinação e persistência em se chegar a um objetivo. Mesmo não atingindo o alvo, quem busca e vence obstáculos, no mínimo fará coisas admiráveis."

(José de Alencar)

RESUMO

O uso das redes de computadores tem proporcionado grandes avanços no meio pessoal, científico, empresarial e industrial. Tais conquistas contribuem para o crescente e eficaz desenvolvimento dessas áreas. Visando essa colaboração, este trabalho de conclusão de curso tem como objetivo desenvolver um projeto de redes de computadores para o Centro administrativo da Prefeitura Municipal de Ibicuitinga-CE. O levantamento dos requisitos do Centro foram primordiais para a concepção deste trabalho, cuja vertente é tecnológica. Partindo desses dados, houve a criação das topologias física e lógica, do desenvolvimento de estratégias e mecanismos para as áreas de segurança e gerenciamento e do orçamento dos equipamentos. Pensando em segurança, foi criado um documento contendo as Políticas de Segurança da Informação para o Centro administrativo, que inclui normas e diretrizes que asseguram o manuseio dos dados que transitam na rede. Tal projeto é de grande relevância, pois contribuirá no desempenho das atividades e da melhor disponibilização do serviço público.

Palavras chave: Projeto de redes de computadores, Centro administrativo, Políticas de segurança, Topologias.

ABSTRACT

The use of computer networks has provided great advances in personal, scientific, business and industrial areas. Such achievements contribute to the growth and effective development of these areas. In order do address this collaboration, this work aims to develop a project of computer networks for the Administrative Center of the municipality of Ibicuitinga-CE. The surveyed requirements of the Center were crucial for the design of this study in the technological side. Based on these data, the physical and logical topologies were created, some strategies and mechanisms were developed to address the security and management of the network and the equipment budget was listed. Thinking about security, a document containing Policies on Information Security for the Administrative Center, which includes standards and guidelines that ensure the handling of data circulating on the network was created. This project is very important, as it will contribute to the performance of activities and better provision of public services.

Keywords: Design of computer networks, Administrative Center, Security Policies, Topologies.

SUMÁRIO

INTRODUÇÃO

A informática cada vez mais vem adquirindo relevância na vida das pessoas e nas empresas. E sua utilização é vista como meio de aprendizagem pessoal, crescimento e desenvolvimento empresarial. Contemporaneamente é muito relevante a presença de um computador nas residências, devido ao alto índice de desenvolvimento mental e abrangência de vivências com o resto do globo. A vontade de conhecer e se viver em constante interação com outros internautas faz essa ferramenta ganhar, cada vez mais, novos adeptos pelo mundo todo, cada um da sua forma e do seu jeito.

De acordo com Donahue (2008, p. 3), uma rede de computadores pode ser definida como “dois ou mais computadores conectados por algum meio através do qual são capazes de compartilhar informações”. Outrora, esses computadores eram conectados através de cabos, mas há alguns anos, com o progresso da tecnologia, tornou a conexão sem fio: a ausência da conexão física e a utilização de ondas de rádio, possível.

Hoje, com um considerável avanço em todas as áreas da informática, as redes de computadores estão inseridas em todas as partes, tais como empresas de pequeno porte até grandes organizações multinacionais, com novas funcionalidades e propósitos que são: proporcionar mais agilidade nos processos, comunicação entre locais remotos, segurança e processamento de dados, comodidade e entretenimento para os usuários, sejam eles usuários comuns ou grandes organizações. Para que as finalidades de uma de rede de computadores funcionem adequadamente, torna-se essencial a projeção e administração dessa rede, que inclui o levantamento e análise de requisitos, elaboração de projetos físicos e lógicos a aquisição de dispositivos, a configuração e teste da rede projetada. Portanto, também torna evidente e inevitável o estudo e desenvolvimento correto de um projeto que engloba e atenda todos os pontos supracitados.

Dada a importância da rede de computadores nas empresas e nas instituições, e a proeminente necessidade da construção de um projeto de redes que garanta o melhor funcionamento dos elementos constituintes, atualmente várias entidades, sejam públicas ou privadas, optam por aderir a padronização de seus cabos, a segurança e gerenciamento de seus dados. Em um recente trabalho realizado na Universidade Jean Piaget de Cabo Verde, a autora ressalta a importância de um projeto de redes, que segue:

> Segundo alguns dados, estudos recentes revelam que 70% dos problemas encontrados em redes locais estão relacionados com ao cabeamento. Esse fato é só um dos vários motivos pelo desenvolvimento de um projeto de rede de computadores nas organizações. Por mais que as organizações estejam atualizadas ao novo mundo da era tecnológica, apropriando das melhores tecnologias e equipamentos, para que tenham um melhor aproveitamento da rede, terão a necessidade de desenvolver um projeto de rede bem estrutura e ter especial atenção na escolha da cablagem. (MORENO, 2012, p. 99).

Realmente, a não disposição normatizada e padronizada do cabeamento pode gerar danos significativos ao funcionamento da rede, retendo muito da operacionalidade e afetando as atividades exercidas pelos usuários. Para ajudar a solucionar problemas como esse, existem organizações de padronização que possibilitam que as empresas produzam equipamentos que possam se intercomunicar. As principais organizações internacionais são a *International Standards Organization* (ISO), a *American National Standards Institute* (ANSI), a *Eletronics Industry Association* (EIA) e a Telecommunications Industry Association (TIA). Nacionalmente, existe a Associação brasileira de normas técnicas (ABNT).

Assim, conforme Carvalho (1998 *apud* FILHO, 2007, p. 41): "[...] o sistema de cabeamento estruturado visa suportar as necessidades tanto atuais quanto futuras, de comunicações para dados, voz e imagem. Para assegurar um perfeito sistema de cabeamento estruturado, alguns requisitos são de suma importância, entre eles, a prática adequada de instalação e a documentação do projeto físico". Então, o desenvolvimento de um projeto de redes incluindo a padronização de suas interfaces e meios de transmissão contribui para o bom funcionamento da rede.

Este trabalho visa desenvolver um projeto de redes de computadores para o Centro Administrativo do município de Ibicuitinga, localizado no Sertão Central do Estado do Ceará, aproximadamente a 190 km da capital Fortaleza (Apêndice A). Está incluso nesse projeto, um documento contendo as Políticas de Segurança da Informação – PSI (Apêndice C), desenvolvidas exclusivamente para o Centro administrativo, que tem como objetivo estabelecer normas e diretrizes a fim de orientar, implementar e melhorar a gestão de segurança da informação, garantindo a integridade, a disponibilidade e a confidencialidade dos dados que transitam na rede do centro. Comumente esse documento não é abordado em projeto de redes de computadores, mas é de grande importância para a proteção das informações e que toda organização deve seguir, como discorre a RFC 2196, que segue.

> "Uma política de segurança é uma declaração formal das regras que as pessoas a

> quem é dado acesso a tecnologia e ativos da informação de uma organização devem respeitar.” (RFC 2196, 1997).[1]

O trabalho desenvolvido no bloco D do prédio da UniPiaget, localizado no campus universitário da Cidade da Praia, Santiago, Cabo Verde, teve como propósito desenvolver uma rede de computadores. Com isso, houve significativa contribuição do projeto da universidade para a criação e planejamento do projeto do centro administrativo da prefeitura municipal de Ibicuitinga, devido às características de arquitetura, tipo de rede e infraestrutura serem bastante similares.

Este trabalho se enquadra na vertente tecnológica. Vale ressaltar que a ausência de uma infraestrutura de rede de computadores padronizada e adequada às necessidades do Centro Administrativo contribui negativamente para a administração dos processos e a comunicação entre as partes constituintes. Com a existência dessa infraestrutura serão atendidos diretamente todos os departamentos do Centro Administrativo, bem como os funcionários que prestam serviços e que utilizam ferramentas ligadas à rede. De forma indireta o projeto beneficiará os munícipes de Ibicuitinga que receberão um atendimento mais ágil e eficaz por parte da administração.

O projeto dessa rede é de considerável relevância, pois visa assegurar a proteção de dados sigilosos, como dados pessoais, jurídicos e empresariais que estão armazenados nos computadores da prefeitura. É nesse pensamento que esse trabalho pretende contribuir positivamente na busca da excelência em gestão de dados e na disponibilização de um melhor serviço público.

OBJETIVOS

2.1. Objetivo geral

Projetar uma rede de computadores para o Centro administrativo do município de Ibicuitinga, localizado no Sertão Central do Estado do Ceará.

---

1 A security policy is a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide.

2.2. Objetivos específicos

- Levantar e analisar necessidades;
- Criar projeto lógico e físico da rede;
- Propor mecanismos e estratégias de segurança;
- Elaborar estratégias de gerenciamento da rede;
- Elaborar políticas de segurança.

REVISÃO BIBLIOGRÁFICA

3.1. Rede de computadores

Devido à crescente necessidade de comunicação entre os computadores e outros dispositivos é que há algumas décadas, o termo *rede de computadores* vem ganhando relevância no meio tecnológico e sofrendo melhorias na sua definição com o passar dos anos. Com o intuito de clarificar esses acréscimos, estão elencados nesse tópico a visão de dois autores em momentos diferentes, que segue:

> […] utilizaremos a expressão "rede de computadores" quando quisermos mencionar um conjunto de computadores autônomos interconectados por uma única tecnologia. (TANENBAUM, 2003, p. 2).

Conforme visto, Tanenbaum conceituou de forma sintética. Já em uma visão da nova década e de acordo com o evolucionismo das tecnologias, Kurose e Ross detalhadamente definem o mesmo termo, que segue:

> […] uma rede consiste em muitas peças complexas de hardware e software que interagem umas com as outras – desde os enlaces, comutadores, roteadores, hospedeiros e outros dispositivos, que são componentes físicos da rede, até os muitos protocolos (tanto em hardware quanto em software) que controlam e coordenam esses componentes. (KUROSE; ROSS, 2010, p. 553).

Portanto, o termo *rede de computadores* consiste na interação e integração de um aglomerado de componentes físicos e lógicos dispostos de forma coordenada e administrada

por protocolos e por pessoas objetivando a realização de uma atividade. No decorrer desse trabalho será utilizada a definição proposta por Kurose e Ross, por ser a mais atualizada e condizente com os padrões contemporâneos.

3.1.1. Tipos de rede

De acordo com Mendes (2007, p. 31), "Uma rede existe quando é feita a interligação de computadores de forma local ou remota. Para fazer essa interligação, são necessários os componentes que formam a rede, tais como placas, cabos, conectores e outros aparelhos".

Considerando que as redes podem estar fisicamente no mesmo local ou em locais diferentes, as mesmas podem ser classificadas pelos tipos: *Local Area Network* (LAN), *Wide Area Network* (WAN), *Metropolitan Area Network* (MAN), entre outras.

A LAN caracteriza-se por ser uma rede localizada em um mesmo local físico, podendo ser um prédio, uma sala ou um conjunto de salas, acolhendo um aglomerado de computadores interligados por cabos, ondas de rádio ou infravermelho. Dentre diversas tenologias possíveis para interconectar computadores nesse tipo de rede, a mais usada é a *Ethernet*. A *Ethernet* é um padrão de transmissão de dados que permite a comunicação entre os computadores e outros componentes da rede. Tem como principais vantagens a simplicidade de instalação e o baixo custo.

Um conjunto de redes LAN e/ou MAN interligadas formam uma *Wide Area Network* ou WAN. A WAN tem dimensões maiores que as dos outros tipos de redes, que pode corresponder a países e até mesmo continentes. Um exemplo bem conhecido de uma rede desse tipo é a "Internet". As tecnologias usadas para interligar as diversas LANs que constituem uma WAN podem ser feitas por meio de linhas telefônicas, fibras ópticas ou ondas de rádio.

E a *Metropolitan Area Network* (MAN), que pode ser comparada a uma WAN com uma dimensão reduzida, também interliga redes locais, abrangendo uma área de uma cidade grande ou região metropolitana, sendo possível atender vários edifícios através da arquitetura ponto-a-ponto.

3.1.1.1. Tecnologia de LAN *Ethernet*

Tratando de tecnologia de transmissão de dados em redes locais com fio, a *Ethernet* de longe é o padrão dominante no mercado e é bem provável que essa superioridade continue em um futuro próximo (KUROSE, ROSS, 2010).

A *Ethernet* superou outras tecnologias de LAN com fio existentes nas décadas de 80 e 90 pelas características de velocidade, simplicidade e baixo custo. Esses foram os principais motivos que fizeram as empresas e instituições a não migrarem para outras tecnologias, tais como *token ring*, FDDI e ATM. Essa superioridade foi cada vez mais evidente com a criação da Ethernet comutada, possibilitando ainda mais altas velocidades de transmissão de dados.

A tecnologia *Ethernet* encontra-se nas versões de 10 Mbps, 100 Mbps, 1000 Mbps e 10 Gbps, conhecidos também através dos acrônimos relacionados abaixo às versões mais usadas da norma:

- Padrão 10 Mbps *Ethernet*
  - 10BASE-T e 10BASE-F, onde T e F, especifica o uso em cabos de par trançado e fibra óptica, respectivamente.
- Padrão *Fast Ethernet* (100 Mbps)
  - 100BASE-T, incluindo os padrões 100BASE-TX, 100BASE-T4 e 100BASE-T2, todos operando sobre cabo de par trançado;
  - 100BASE-FX, usando fibra óptica multimodo.
- Padrão Gigabit *Ethernet*
  - 1Gigabit *Ethernet* (1000 Mbps)
    - 1000BASE-T, sobre cabeamento de par trançado nas categorias 5e ou 6;
    - 1000BASE-SX e 1000BASE-LX, sobre fibra óptica.
  - 10 Gigabit *Ethernet* (10 Gbps)
    - 10BASE-SR, sobre fibra óptica multimodo suportando distâncias entre 26 a 82 metros;
    - 10BASE-LX4, sobre fibra óptica multimodo suportando distâncias entre 240 a 300 metros;
    - 10BASE-LR e 10BASE-ER, sobre fibra óptica monomodo suportando

distâncias de 10 Km a 40 Km.

3.1.2. Arquiteturas de aplicação

As arquiteturas mais conhecidas e comumente utilizadas, dependendo das necessidades de cada um, são os modelos cliente/servidor e o *peer-to-peer* ou par-a-par (P2P).

O modelo cliente/servidor é constituído por dois elementos, o cliente, que pode ser um computador, e tem como papel requisitar algum serviço ao servidor; e o servidor, que por outro lado tem a responsabilidade de receber essa solicitação e responder com um resultado. Geralmente os clientes e servidores se comunicam através de uma rede de computadores, mas podem também ser programas diferentes em um mesmo computador. Em síntese, esse modelo sempre terá um cliente que solicita e um servidor que responde aos pedidos.

Já no modelo P2P, seus dispositivos pertencem a um grupo livre e todos eles podem servir uns aos outros e solicitar serviços uns dos outros, com as mesmas capacidades e responsabilidades.

A sentença a seguir, mostra algumas aplicações que são baseadas nas arquiteturas P2P.

> Muitas das aplicações de hoje mais populares e de intenso tráfego são baseadas nas arquiteturas P2P, incluindo distribuição de arquivos (por exemplo, BitTorrent), compartilhamento de arquivo (por exemplo, eMule e LimeWire), telefonia por Internet (por exemplo, Skype) e IPTV (por exemplo, PPLive) (KUROSE; ROSS, 2010, p. 63).

3.2. Projeto de redes de computadores

Nesta seção descrevemos os conceitos usados em projetos de redes de computadores.

3.2.1. Topologia física

O termo topologia designa a interconexão física. Refere-se à organização ou layout físico dos computadores (COELHO, 2003). Apesar de tratar da estrutura física, a topologia pode ser usada para representar tanto o meio físico com o lógico. Em um projeto de redes, a topologia física indica a posição e extensão dos cabos, os dispositivos (computadores, impressoras, *switches*, roteadores) e as interligações entre eles, além de informações sobre a

estrutura do local. E é a partir do conhecimento da topologia física que é pensado o cabeamento estruturado para o projeto.

A topologia física de uma rede pode ser compreendida também como descreve Oppenheimer:

> Nesta fase do projeto de redes, decide-se que cabeamento, os protocolos de camada física e de enlaces de dados, e dispositivos de interconexão (como *switches*, roteadores e pontos de acesso) usar. (OPPENHEIMER, 2011, p. 283, tradução nossa)[2]

Existem alguns tipos de topologia física, as principais são: barramento, estrela e anel. O tipo barramento utiliza um cabo único no qual todos os dispositivos estão conectados a ele. A topologia estrela utiliza um dispositivo central, i.e. um *hub*, onde todos os outros dispositivos da rede se conectam. Já no tipo anel, cada computador está diretamente conectado a outro construindo uma espécie de anel físico.

3.2.1.1. Componentes da rede

Na sentença abaixo Kurose e Ross destacam quais os componentes (dispositivos ou equipamentos) que compõe atualmente a grande rede, a Internet. Apresenta ainda a modernização dos sistemas finais conectados à rede, que segue.

> A Internet é uma rede de computadores que interconecta milhares de dispositivos computacionais ao redor do mundo. Há pouco tempo, esses dispositivos eram basicamente computadores de mesa, estações de trabalho Linux, e os assim chamados servidores que armazenam e transmitem informações, como páginas da Web e mensagens de e-mail. No entanto, cada vez mais sistemas finais modernos da Internet, como TVs, laptops, consoles para jogos, telefones celulares, webcams, automóveis, dispositivos de sensoriamento ambiental, quadros de imagens, e sistemas internos elétricos e de segurança, estão sendo conectados à rede. (KUROSE; ROSS, 2010, p. 2).

Além dos dispositivos finais considerados acima, existem outros componentes que realizam o trabalho de receber e encaminhar as informações aos seus destinos finais, são eles chamados de roteadores e comutadores de camada de enlace (*switches*). Geralmente os roteadores trabalham no núcleo da rede (formado pela malha de roteadores que interligam as redes entre si) e os comutadores de camada de enlace são tipicamente utilizados em redes de acesso (redes residenciais ou corporativas).

---

2 During this phase of the top-down network design process, choices are made regarding cabling, physical and data link layer protocols, and internetworking devices (such as switches, routers, and wireless access points).

3.2.1.2. Enlace de rede

O caminho por onde são transmitidas as informações de um dispositivo para outro é chamado de enlace. Esses dispositivos podem ser computadores, servidores, roteadores, *switches* ou qualquer outro que compartilhe informação. Os enlaces podem ser de dois tipos: enlace com fio (conexão por cabo) ou enlace sem fio (*wireless*). São considerados enlaces do tipo com fio os cabos de par trançado, coaxiais, fibra óptica e outros. Já no enlace sem fio encontramos as tecnologias 802.11 (wi-fi), o *Bluetooth* (802.15.1, para distâncias mais curtas) e o WiMAX (802.16 para distâncias mais longas).

3.2.1.2.1. Cabo de par trançado

O cabo de par trançado é composto por pares de fios, enrolados em espiral com o intuito de reduzir o ruído e manter as suas propriedades elétricas. Existem dois tipos de cabos par trançados, o *Unshielded Twisted Pair – UTP* e o *Shielded Twister Pair – STP*. A principal diferença entre os dois tipos é a existência ou não de blindagem.

Os cabos de pares trançados não blindados, corresponde ao tipo UTP, que utiliza uma capa plástica sem blindagem. O UTP está dividido em seis categorias (Cat) diferenciando-se uma da outra pela frequência e taxa de transmissão de dados. Abaixo as categorias e suas especificações.

- Categoria 3: Reconhecida pela TIA/ABNT; largura de banda de 16 MHz e taxa de transmissão de até 10 Mbps;
- Categoria 4: Sem reconhecimento, substituída pela categoria 5.
- Categoria 5: Sem reconhecimento; largura de banda de até 100 MHz, é a mais utilizada, pois é compatível com qualquer placa de rede, e taxa de transmissão de até 100 Mbps;
    - Categoria 5e: Reconhecida pela TIA/ABNT; largura de banda de até 125 MHz e com taxa de transmissão de até 155 Mpbs, operando aplicações Ethernet a 10 e 100Mbps.
- Categoria 6: Reconhecida pela TIA/ABNT; Largura de banda de até 250 MHz e

taxa de transmissão de até 1 Gbps, tendo alcance de 55 metros;

- Categoria 6A: Reconhecida pela TIA; Largura de banda de até 500 MHz, com alcance de 100 metros, e alcance de 55 metros para redes de até 10 Gbps.

Existem também as categorias 7 e 7A, ambas atendendo somente os cabos de par trançado com blindagem ou STP. A categoria 7 tem norma brasileira publicada e suportada largura de banda de até 600 MHz (para redes de 40 Gbps). Já a categoria 7A ainda está em desenvolvimento, com largura de banda por par de 1000 MHz (rede de 100 Gbps) (MARIN 2011).

O STP como já visto, é constituído de blindagem externa e proteção do entrelaçamentos dos fios, suportando grandes interferências.

3.2.1.2.2. Cabo coaxial

O cabo coaxial é um um cabo constituído por um fio de cobre condutor central para transmissão de sinal, revestido por um material isolante que é rodeado por uma blindagem de plástico. O uso da blindagem e dos isolantes torna o cabo coaxial vantajoso em relação aos outros cabos, pelo fato de proteger bem o sinal transmitido de interferências elétricas e até mesmo de magnéticas.

A velocidade atingida pelo cabo coaxial depende do tipo de material da malha externa do cabo. Quando a malha externa for de cobre, o cabo pode alcançar taxas de transmissão de 10 Mbps à uma frequência de 2 Ghz. Quando a malha for de alumínio ou cabo grosso, transmitirá dados a uma velocidade de até 10 Mbps com uma frequência de 10 Ghz.

O cabo coaxial têm aplicações em equipamentos de áudio, em redes do tipo LAN e em descidas de antenas para dados, voz ou imagem.

3.2.1.2.3. Fibra óptica

Diferentemente dos cabos coaxiais e de par trançado que tem como condutor de sinal elétrico um fio de cobre, a fibra óptica é constituída de revestimento plástico e fibra de vidro, que transmite luz, ficando imune a interferências eletromagnéticas.

O sinal nas fibras podem ser transmitidas por duas fontes, a LED (Diodo emissor de

luz) e o *laser*. E podem ser de dois tipos conforme a fonte e a quantidades de sinais emitidos dentro da fibra, são o monomodo e o multimodo.

A monomodo (SM, *singlemode*) é assim classificada por apenas transmitir no interior da fibra um único caminho de luz, pois a fibra possui um núcleo reduzido. Essas características possibilitam duas vantagens no uso da fibra monomodo que são, uma maior largura de banda e transmissão de sinal a grandes distâncias. Apesar de vantajosas em transmissão, as fibras monomodo tem uma fabricação cara.

Diferente da monomodo, a multimodo (MM, *multimode*) apresenta vários caminhos para a propagação da luz no interior da fibra. A fibra MM pode ser classificada como índice degrau e índice gradual. Na MM índice degrau, o sinal é mais atenuado (enfraquecido) e distorcido que nas fibras MM índice gradual. Em contraste com as fibras SM, as multimodo são mais usadas em comunicações a curta distâncias.

3.2.1.2.4. 802.11 (Wi-fi)

O 802.11 ou *Wireless Fidelity* (Wi-Fi), é um padrão internacional que especifica e descreve as características de uma rede sem fios. Com essa tecnologia é possível conectar computadores e outros dispositivos compatíveis (impressoras, *tablets*, *smartfones* e outros) que estejam próximos geograficamente. Tudo isso ocorre sem a utilização de cabos e só é possível usando radiofrequência (ondas de rádio). Deve-se compreender que nem sempre uma rede sem fio é uma rede móvel, nesse caso existe a impossibilidade de ser móvel, por exemplo, um usuário possui um notebook e está em sua residência que é atendida por uma rede sem fio, mas precisa ir ao escritório que possui uma LAN cabeada, e que para fazer esse deslocamento, deve desligar a sua máquina e chegando em seu escritório precisa se conectar à rede cabeada. Nesse exemplo, o usuário é sem fio enquanto estava em sua residência, mas não móvel. A mobilidade existe quando um usuário não perde a conectividade enquanto se desloca por grandes distâncias independente de velocidade ou meio de transporte. Essa tecnologia torna viável essa funcionalidade, o uso de computadores, *smartfones* e *tablets* ligados à rede sem cabeamento em qualquer ponto dentro dos limites da área de atuação das ondas de rádio, além de não interferir na infraestrutura de prédios e casas.

Durante anos o padrão inicial 802.11 foi revisado e recebeu diferentes atualizações a fim de otimizar os valores em transferência de dados e alcance do sinal. Abaixo seguem

alguns padrões e seus valores.

- 802.11a – Taxas variando de 6 a 54 Mbps e alcance de até 70 metros;
- 802.11b – Taxas variando de 1 a 11 Mbps e alcance de até 150 (ambiente fechado) e 500 metros (ambiente aberto);
- 802.11g – Taxas variando de 6 a 54 Mbps e alcance de até 90 (ambiente fechado) e 400 metros (ambiente aberto) (KUROSE; ROSS, 2010).

3.2.2. Topologia lógica

"A topologia lógica é o caminho real que um sinal percorre em uma rede". (SOARES, 1995 *apud* MORENO, 2007, p. 34). Utilizou-se essa sentença resumida e obsoleta para que em comparação às definições atuais, seja esclarecido que o entendimento sobre determinados conceitos são aperfeiçoados. Partindo de uma visão mais atual, Oppenheimer define a topologia lógica como:

> É um mapa de uma rede interna que indica segmentos de rede, pontos de interconexão e comunidades de usuários. Embora a localização geográfica possa aparecer no mapa, o objetivo é mostrar a geometria da rede, e não a geografia física ou implementação técnica. (OPPENHEIMER, 2011, p. 119, tradução nossa).[3]

A topologia lógica também pode ser do tipo barramento, onde o sinal é gerado e enviado a todos os computadores independente de sua localização. Ou do tipo anel, onde o sinal é propagado por um caminho específico de única direção passando por todos os dispositivos.

3.2.2.1. Protocolo de rede

Em uma analogia humana o protocolo está vinculado à forma com que as pessoas precisam se comportar em determinado local, ou a maneira de comunicação (ordem e intensidade das falas) entre duas ou mais pessoas, por exemplo. Esse seria um protocolo humano, que não difere muito de um protocolo de rede. A única diferença é que os

3 A topology is a map of an internetwork that indicates network segments, interconnection points, and user communities. Although geographical sites can appear on the map, the purpose of the map is to show the geometry of the network, not the physical geography or technical implementation.

componentes no caso do protocolo humano são as pessoas, e já no protocolo de rede, os componentes são componentes de *hardware* e *software* de algum dispositivo (computador, *notebook*, roteador, *switch*).

Em síntese e de acordo com Kurose e Ross, “um protocolo define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na transmissão e/ou no recebimento de uma mensagem ou outro evento”.

3.2.2.2. Endereçamento IP

Em um sistema de comunicação global existe a necessidade de um método de identificação de seus componentes. No caso da grande rede (Internet) ou mesmo em uma rede local, os dispositivos (computadores, impressoras, *smartphones* e outros) precisam de uma identificação para se comunicar. Nesse caso, usam o *Internet Protocol*, ou somente IP, como identificador, ou seja, um endereço. Vale lembrar que esse endereço tem o objetivo de identificar, de forma única, cada conexão de rede. Na versão 4 o mesmo consiste em um número de 32 bits (unidade de informação), escrito com quatros octetos representados na forma decimal, cada octeto é representado por um número decimal e separados por um ponto, por exemplo, “192.168.1.10”. O endereço IP é composto por duas partes: a primeira identifica uma rede específica e a segunda parte identifica um dispositivo dentro dessa rede.

O crescimento da rede em âmbito global ocasionou na escassez dos endereços IP de versão 4 (32 bits). Para atender a necessidade de maior espaço para endereços IP, foi desenvolvido o IPv6, a 6ª versão do protocolo IP. Uma das principais contribuições do IPv6 foi justamente a expansão da capacidade de endereçamento, aumentando o tamanho do endereço IP de 32 para 128 bits, com isso, garantindo a disponibilidade de IPs mesmo com um crescimento exorbitante de número de dispositivos conectados à rede global.

3.2.2.3. Software

O software pode ser considerado como uma ferramenta lógica constituída de uma sequência de instruções, ou popularmente conhecido como um programa de computador. Os softwares podem ser de três tipos: sistema, aplicativo e/ou embarcados (embutidos). Um software de sistema dá ao usuário uma interface de alto nível, escondendo detalhes da

programação, por exemplo, sistemas operacionais e *drivers* de dispositivos. Um software de aplicação permite ao usuário realizar várias tarefas específicas a uma determinada área, é o caso dos *softwares* educacionais, vídeo games e aplicações administrativas e industriais. Já *softwares* que trabalham dentro de dispositivos como *smartphones*, *tablets* e outros de funcionalidade específica se enquadram na categoria de software embarcado ou embutido.

3.2.3. Cabeamento estruturado

Segundo Filho (2007), o cabeamento estruturado pode ser definido como um sistema baseado na padronização das interfaces e meios de transmissão, de modo a tornar o cabeamento independente da aplicação e do *layout* (distribuição dos equipamentos).

Essas padronizações devem ser exercidas levando em consideração as normas de algumas organizações padronizadoras, tais como: a *American National Standards Institute* (ANSI), a *Eletronics Industry Association* (EIA) e a *Telecommunications Industry Association* (TIA) que normatizam todas as implantações que compreendem um projeto de cabeamento estruturado. A aplicação dessas normas visa não somente atender as necessidades atuais como as futuras, precavendo-se de eventuais alterações e expansões do sistema. Essas mudanças são possibilitadas pela documentação do esquema de disposição do cabeamento e outros elementos no local a ser implantado, tais como: os cabos, a posição, a origem e o destino, as tomadas e o tipo de pavimento são informações que facilitam uma futura manutenção ou implementação de forma segura e rápida.

3.2.4. Segurança de redes

Durante as primeiras décadas de funcionamento, as tímidas funcionalidades das redes de computadores atendiam principalmente a professores universitários e a funcionários de empresas, com a finalidade de troca de mensagens através do correio eletrônico e compartilhamento de recursos. Devido à elevada utilização da rede em transições bancárias, compras, arquivamento e troca de dados sigilosos é que a segurança das redes atualmente é um assunto de grande preocupação na sociedade tecnológica e civil.

De acordo com Tanenbaum (2003, p. 767), “a segurança se preocupa em garantir que pessoas mal-intencionadas não leiam ou, pior ainda, modifiquem secretamente mensagens

enviadas a outros destinatários". Além de impedir a leitura e a alteração de dados por terceiros, a comunicação segura aspira que, por exemplo, em uma troca de mensagens, ambos, tanto o remetente quanto o destinatário tenham a certeza de estar se comunicando verdadeiramente com as pessoas desejadas.

Dadas as considerações supracitadas, segundo Kurose e Ross é possível identificar que as propriedades de uma comunicação segura são: confidencialidade, autenticação do ponto final, integridade de mensagem e segurança operacional. (KUROSE, ROSS, 2010). A segurança operacional está relacionada às empresas e organizações que estabelecem conexão com a rede pública, internet. E que a proteção é realizada pelos mecanismos de segurança ou operacionais, tais como *firewall*, filtros de pacotes e/ou sistemas de detecção de invasão, visando deter ataques contras as redes das organizações. Outra forma de contribuir com a rede segura de uma organização, é a criação de políticas de segurança. Das políticas, Comer descreve:

> A política não especifica como obter proteção, mas declara claramente e de forma não ambígua os itens que devem ser protegidos. […] são complexas porque envolvem comportamento humano tanto quanto computador e facilidades de rede (isto é, um visitante que transporta um disquete de fora da organização, uma rede sem fio que pode ser detectada de fora do edifício ou funcionários que trabalham em casa). (COMER, 2007, p. 547).

3.2.4.1. Mecanismos e estratégias de segurança

Entende-se por mecanismos de segurança um conjunto de medidas que tem como objetivo proteger a rede de ameaças que venham a comprometer a segurança dos dados e a operacionalidade do sistema. Os mecanismos podem ser recursos computacionais e a implantação de medidas de segurança física.

Um eficiente sistema de segurança monitora todas as atividades da rede, sinalizando comportamentos estranhos e tomando as medidas mais apropriadas de acordo com o problema. Refere-se a recursos computacionais de segurança, o *Firewall* e seus tipos de filtros, que é uma junção de *hardware* (dispositivo ou ferramenta física) e software que isola a rede interna da Internet, realizando o bloqueio de pacotes indesejáveis, maliciosos e não autorizados, e permitindo a passagem de pacotes autorizados.

Outros recursos utilizados são a autenticação, a autorização e a auditoria. A autenticação é o processo de verificar se a identidade de um determinado usuário é válida.

Normalmente a autenticidade do usuário é testada no acesso de algum programa ou computador, por exemplo, por meio da requisição de *log in* ou simplesmente *login* (Nome do utilizador) e senha. A autorização é um termo que se relaciona com a autenticação, já que autenticar é provar a identidade de uma pessoa, a autorização verifica se o usuário autenticado possui permissão para realizar determinadas operações. Já a auditoria é uma ferramenta que visa identificar por meio de dados coletados sobre o uso da rede e dispositivos possíveis tentativas de intrusão ou mal uso dos recursos. A auditoria também exerce o papel de validação dos mecanismos de proteção de acordo com as políticas de segurança.

A segurança física objetiva a proteção dos equipamentos e informações localizadas em salas de acesso restrito contra usuários não autorizados. Essa proteção pode ser instituída através do atendimento a algumas recomendações, como exemplo, temos: formas de identificação (crachás), controle de entrada e saída de materiais, equipamentos e pessoal, estabelecimento de horários de acesso e utilizar mecanismos de controle de acesso físico (fechaduras eletrônicas, alarmes, câmeras de vídeo). A estratégia preocupa-se com a correta implementação dos mecanismos e da segurança física, visando assegurar os recursos e os dados. Nesse planejamento cabe também a realização de treinamentos e palestras sobre segurança da informação com pessoal diretamente ligado a essa área.

3.2.4.2. Políticas de segurança

Em síntese, as políticas de segurança em redes de computadores estabelecem uma série de direitos, responsabilidades e procedimentos às pessoas que utilizam os recursos computacionais. Essa normatização tem como principal propósito informar aos funcionários, administradores e gestores as suas obrigações inerentes à utilização e proteção dos recursos e do acesso à informação. As políticas de segurança são divididas em políticas de acesso, de autenticação, de aquisição de tecnologia de computadores e de responsabilidades. Abaixo segue as definições de cada política.

- Política de acesso: define os direitos de acesso e regras para a adição de novos dispositivos e *softwares* à rede;
- Política de autenticação: define a política de uso de senhas e formas de autenticação;

- Política de aquisição de tecnologia de computadores: refere-se a regras de aquisição, auditoria e configuração de dispositivos e da rede, prevenindo a integridade dos recursos da rede;
- Política de responsabilidades: atribuição de responsabilidades às pessoas e equipes.

Para que as políticas de segurança tenham uma boa aplicação faz-se necessário a implementação de mecanismos de segurança que atendam os requisitos da rede e a concordância dessas políticas com os procedimentos administrativos.

3.2.5. Gerenciamento de redes

O gerenciamento de redes consiste em controlar e monitorar os sistemas de *hardware* e *software* que compreendem uma rede. A detecção e a correção de problemas que causam a ineficiência na comunicação é o principal trabalho de um administrador de redes. Todavia, além de identificar e corrigir, deve-se eliminar as condições que poderão levar ao retorno do problema. Na maioria dos casos, gerenciar uma rede não é uma tarefa fácil, devido a heterogeneidade de *hardware*, *software* e inter-redes que por vezes são incompatíveis. Todas essas ações contribuem para um bom desempenho e qualidade de serviço, conforme descreve Saydam:

> Gerenciamento de rede inclui o oferecimento, a integração e a coordenação de elementos de hardware, software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer às exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável. (1996 *apud* KUROSE, ROSS, 2010, p. 556).

Apesar de longa, essa sentença evidencia a importância do gerenciamento da rede que atenta em preparar um ambiente que satisfaça as exigências operacionais, sejam em qualquer âmbito organizacional, contribuindo dessa forma com o desempenho e qualidade de serviço.

3.2.5.1. SNMP

O SNMP (Simple Network Management Protocol – Protocolo Simples de Gerência de Rede), é um protocolo da camada de aplicação que gerencia tipicamente redes IP. O SNMP possibilita aos administradores de rede gerenciar o desempenho da rede, identificando e

combatendo eventuais falhas e/ou problemas, além de fornecer informações direcionadas ao planejamento de expansão da rede. O SNMP oferece suporte a múltiplas versões, tipicamente SNMPv1, SNMPv2 e SNMPv3. Utilizaremos na rede da prefeitura a versão 3, devido ao adicionamento de melhorias em segurança ao protocolo como privacidade, autenticação e controle de acesso.

3.2.5.2. Estratégias de gerenciamento

O gerenciamento eficiente da rede, contribui significativamente para um bom desempenho e qualidade nos serviços prestados. O conhecimento da rede, seus componentes, suas funções e objetivos norteiam o administrador a escolher protocolos e *softwares* de gerência que exerçam o gerenciamento correto da rede. A estratégia de gerenciamento trata justamente desse levantamento de funcionalidades e objetivos para selecionar as tecnologias de gerência mais adequadas às necessidades da rede.

3.3. Centro administrativo da Prefeitura municipal de Ibicuitinga

O município de Ibicuitinga está localizado na região nordeste do estado do Ceará, precisamente na região do Baixo Jaguaribe, atingindo a zona do Sertão Central cearense, distante de Fortaleza cerca de 190 km. O município conta hoje com uma população estimada em 11.335 habitantes, constituído de 50,7% de sua população urbana e 49,3% rural.

Um centro administrativo municipal pode ser considerado como um local (edifício) onde estão instaladas entidades administrativas como prefeituras, secretarias e/ou departamentos. Nesses órgãos concentram-se grandes quantidades de dados confidenciais e de grande valia, por isso, a existência da preocupação com o desempenho da comunicação e segurança das informações.

PROCEDIMENTOS METODOLÓGICOS

Este projeto abrange o Centro administrativo do município de Ibicuitinga-CE. O projeto contém as seguintes etapas: o levantamento de requisitos, a caracterização da rede atual, o projeto lógico, físico, de segurança e de gerenciamento e o orçamento dos componentes da rede.

4.1. Levantamento de requisitos

Para dar-se início ao desenvolvimento do projeto é necessário conhecer as necessidades do cliente. Os requisitos são as necessidades e preferências do cliente que são relevantes para iniciar a construção do projeto, pois norteiam o projetista ou o administrador a escolher tecnologias e dispositivos almejando o bom funcionamento da rede ao final dos trabalhos. Essas necessidades foram levantadas por meio de uma entrevista com o secretário de finanças e o gerente de tecnologia da informação do centro administrativo. A entrevista foi realizada no dia 26 de junho de 2013 e foi registrada em um diário de campo, onde foram anotadas todas as respostas de um questionário, elaborado anteriormente através de um roteiro de entrevista (Apêndice B).

Após a coleta dos requisitos foi realizada a análise dos mesmos. Eles devem ser claros, realistas e mensuráveis. Na análise, foram sugeridas soluções para as necessidades dos clientes, i.e., se o cliente solicitou que fosse realizado o *backup* dos dados semanalmente, o objetivo do desenvolvedor foi, para essa solicitação, escolher um software de *backup* que se adeque à rede e realize a guarda dos dados semanalmente.

4.2. Caracterização da rede atual

Com a análise de requisitos a próxima etapa foi caracterizar o estado da rede atual. Conhecer o estado atual da rede é importante, pois relaciona os requisitos com os prováveis problemas existentes, confirmando assim, a real necessidade de alcançar os objetivos do

trabalho. Essa etapa foi acompanhada pelo gerente de TI, onde foi possível identificar quais dispositivos, cabos, tecnologias, sistemas, formas de segurança são e como estão sendo utilizadas. Além de fazer o conhecimento desses elementos, o estudo propiciou a realização das medições e identificação das instalações do prédio. Conhecer as medidas, como: altura, largura e comprimento das salas do prédio, bem como, a posição das instalações elétricas e hidráulicas são importantes para a criação do projeto físico e do cabeamento estruturado. Todos esses dados foram registrados no diário de campo juntamente com os requisitos.

4.3. Projeto lógico

Em seguida, inicia-se a criação do projeto lógico da rede. A topologia lógica, a escolha dos *softwares*, o endereçamento são partes que constituem essa fase.

A disposição lógica da rede e suas tecnologias (*softwares*, protocolos) servem de insumo para a elaboração de estratégias de gerenciamento e segurança, e também para a escolha de mecanismos de segurança, que são duas etapas que sucedem a anterior e são relevantes para o desempenho da rede.

4.4. Projeto físico

Posteriormente, elabora-se o projeto físico. Nessa fase, temos a topologia física (mapa da rede com a organização do cabeamento e componentes), o cabeamento estruturado, as tecnologias de LAN e componentes da rede (*switches*, *access points*, roteadores).

4.5. Plano de Manutenção

Após as etapas anteriores elabora-se o conjunto de medidas e procedimentos necessários à manutenção da rede, como políticas de segurança, *backup*, verificação de necessidades de atualização de *software*, enlaces e equipamentos etc.

4.6. Orçamento

Após todas as etapas e consequentemente com a escolha dos equipamentos,

ferramentas, cabos, e outros dispositivos, ficará disponível a tabela orçamentária contendo todos os gastos com esses itens incluindo a sua implantação (mão-de-obra). Ao final dessa etapas fica concluído o projeto de redes de computadores do Centro administrativo de Ibicuitinga.

CONCLUSÃO E LIÇÕES APRENDIDAS

O projeto foi considerado eficaz pelos responsáveis pelo centro administrativo, que entenderam a importância de projetar a sua rede de computadores e formalizar os processos na área de informática. Nos encontros e reuniões essa importância e interesse ficaram mais evidentes. Durante todo o processo de construção do projeto as necessidades ficaram mais claras, comprovando a considerável relevância que o trabalho tinha. Contrariando a necessidade de reestruturação da rede de computadores do centro, a indisponibilidade de verbas para essa causa dificultou a escolha de equipamentos mais avançados e a aquisição de cabeamento mais compatível com os contidos no orçamento. A falta de disponibilidade de alguns membros da gestão do centro administrativo para comparecimento às reuniões causou atrasos nas tomadas de decisão. Mesmo diante de todos esses problemas o projeto ganhou forma e atendeu a todas as grandes necessidades apresentadas pela gestão, tais como: segurança, disponibilidade de conexão e gerenciamento dos dados e usuários. As contribuições foram visíveis, quando comparado com a precária infraestrutura encontrada no início do projeto. As topologias lógica e física foram totalmente repensadas e readequadas para atender aos novos serviços e à demanda apresentada. A aquisição de novos equipamentos de interconexão e de servidores repaginou a rede, que hoje pode ser considerada uma rede segura, organizada e disponível. Analisando a convivência com a gestão do centro, os desafios, as soluções e os problemas, ficou aprendido que sempre se deve planejar um projeto levando em consideração as fragilidades financeiras da empresa, e tentar ao máximo reutilizar os equipamentos e pessoal existentes. Diante dos fatos, o centro administrativo teve um significativo ganho com o desenvolvimento do projeto.

REFERÊNCIAS

CARVALHO, Gustavo de Oliveira. **Gerência de conectividade**. Campinas, 1998.

COELHO, Paulo Eustáquio. **Projetos de redes locais com cabeamento estruturado**. 1ª ed. Belo Horizonte: Instituto Online, 2003.

COMER, Douglas E. **Redes de computadores e internet**. Porto Alegre: Bookman, 2007.

DONAHUE, Gary A. **Redes Robustas**. Rio de Janiero: Alta Books, 2008.

FRASER, B. **RFC 2196. Site Security Handbook, 1997**. Disponível em: <http://www. faqs. org/rfcs/rfc2196.html>. Acesso em: 30 nov. 2013.

FILHO, Richard Gebara. **Ferramenta para Projeto físico e visualização de redes de computadores**. 140 f. Dissertação de Mestrado. (Mestrado em Ciência da computação) – Centro Universitário Eurípedes de Marília, Fundação de ensino Eurípedes Soares da Rocha, Marília, 2007.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet: uma abordagem top-down**. 5ª ed. São Paulo: Addison Wesley, 2010.

MARIN, Paulo Sérgio. **Cabeamento estruturado: desvendando cada passo: do projeto à instalação.** 3ª ed. São Paulo: Érica, 2011.

MENDES, Douglas Rocha. **Redes de computadores: Teoria e prática.** São Paulo: Novatec, 2007.

MORENO, Nilva K. S. G. **Projecto de rede de computadores edifício D da UniPiaget**. 2012. Monografia (Licenciatura em Engenharia de Sistema e Informática) – Universidade Jean Piaget de Cabo Verde, Santiago, 2012.

OPPENHEIMER, Priscilla. **Top-Down Network Design.** 3ª ed. Indianapolis: Cisco Press, 2011.

SOARES, Luiz Fernando Gomes et al. **Redes de computadores: das LANs, MANs, e WANs às redes ATM**. Rio de Janeiro: Campus, 1995.

TANENBAUM, Andrew S. **Redes de computadores**. 4ª ed. Rio de Janeiro: Campus, 2003.

APÊNDICE A – PROJETO DE REDES DE COMPUTADORES PARA O CENTRO ADMINISTRATIVO DA PREFEITURA MUNICIPAL DE IBICUITINGA.

PROJETO DE REDES DE COMPUTADORES PARA O CENTRO ADMINISTRATIVO DA PREFEITURA MUNICIPAL DE IBICUITINGA.

TALLIS DEYVIDE MAIA RUBENS

Ibicuitinga, dezembro de 2013.

1. SUMÁRIO EXECUTIVO

Com a grande necessidade de comunicação, compartilhamento de recursos, agilidade em processos e prestação de serviços de qualidade é que empresas e instituições estão investindo na otimização e padronização de suas redes de computadores, medidas que garantem e respondem às importantes necessidades supracitadas.

O constante tráfego de dados e informações pessoais e empresariais através das redes locais e pública, fomentou a segurança nessa área da tecnologia. Nos dias de hoje vários ataques ocorrem à redes vulneráveis e os resultados são os mais indesejáveis possíveis, que vão desde o acesso a informações confidenciais até transferência de quantias bancárias. Partindo dessa realidade administradores e desenvolvedores de rede visam assegurar a guarda dos dados utilizando mecanismos e políticas de segurança, além de treinar e capacitar os usuários finais de como agirem diante de ameaças e armadilhas digitais. Outro meio que garante a proteção das informações e satisfaz as exigências de desempenho, é o gerenciamento e monitoração dos componentes da rede. Por meio dessa medida, a rede e seus elementos podem ser controlados, monitorados, analisados e avaliados, certificando que haverá a rápida identificação de possíveis problemas e falhas, o que promove a ágil solução.

Visto que a rede de computadores concede ampla vantagem para as organizações, o desenvolvimento de projetos e a implementação de suas ações são cada vez mais requisitadas. O presente trabalho objetiva projetar uma rede de computadores para o Centro administrativo da Prefeitura municipal de Ibicuitinga, localizada no Sertão Central do Estado do Ceará, aproximadamente a 190 km da capital Fortaleza. As informações sobre as necessidades e aspectos gerais de infraestrutura e estado da rede atual foram disponibilizados pelo gerente de TI e o secretário de finanças, Wendell Bandeira e James Dias, respectivamente. Esse projeto cobre todos os departamentos do centro e a sua elaboração beneficiará os processos administrativos que disporão de mais agilidade, qualidade e proteção. A qualidade no atendimento prestado favorecerá os munícipes que procuram informações e serviços. Portanto, o projeto que tem em sua finalidade a rede de computadores, propiciará que a gestão administrativa da Prefeitura de Ibicuitinga flua de forma positiva.

2. OBJETIVO

Projetar uma rede de computadores para o Centro Administrativo da Prefeitura municipal de Ibicuitinga, localizado no Sertão Central do Estado do Ceará.

3. ESCOPO

Este projeto abrange o Centro administrativo do município de Ibicuitinga-CE. O imóvel está localizado na Rua Edval Maia da Silva, 16 A. Essa rede servirá aos funcionários em suas atividades profissionais nos setores de contabilidade, finanças, tesouraria, recursos humanos, gabinete, arrecadação, licitação, jurídico, controle interno e secretaria administrativa.

4. REQUISITOS

São descritos abaixo os requisitos coletados por meio de uma entrevista com o gerente de TI Wendell Bandeira e o secretário de finanças James Dias do centro administrativo de Ibicuitinga.

4.1. Compartilhamento de arquivos

Disponibilizar pastas em um servidor de compartilhamento de arquivos visando atender os grupos de usuários. O compartilhamento de arquivos deverá estar ativo para os setores de contabilidade e licitação.

4.2. Gerenciamento da rede

Definir estratégias de gerenciamento da rede, monitorando e controlando os dispositivos afim de detectar e corrigir problemas. Requer também relatórios de acesso com as atividades de usuários. Utilizar o protocolo simples de gerenciamento de rede, o SNMP, para realizar essas ações.

4.3. Grupos de usuários

Gerenciar usuários e classificá-los em grupos, estabelecendo um controle de acesso sobre às informações, levando em consideração os departamentos existentes, que são: contabilidade, licitação, recursos humanos, tesouraria, arrecadação, gabinete, jurídico, controle interno, secretaria administrativa e finanças.

4.4. Mobilidade

Instalação e configuração de dois pontos de acesso provendo a mobilidade dentro do centro administrativo, limitando o sinal do rádio às dependências do prédio.

4.5. Backup

Realização de *backups* semanais (em uma cópia e guardadas em outro prédio) em todos os dispositivos do centro administrativo de forma a manter as informações resguardadas.

4.6. Largura de banda e redundância do *link* de comunicação

Escolha dos provedores de internet bem como a largura de banda adequada às atividades exercidas no centro. E atentando para a redundância do link de comunicação, resguardando-se de possíveis desconexões em um dos links contratados. Além da preocupação com o link, haverá também redundância nos *switches* da rede. A prefeitura tem preferência pelo provedor FortalNet.

4.7. Segurança

Definir mecanismos e elaborar estratégias de segurança, bem como realizar treinamentos e desenvolver políticas de segurança. Os departamentos com maior necessidade de segurança lógica e física são a contabilidade e licitação.

5. ESTADO DA REDE ATUAL

Essa seção aborda a caracterização da rede atual do centro administrativo, seus dispositivos, sistemas e softwares utilizados. A disposição desses dispositivos e o cabeamento estão apresentados topologicamente para uma melhor compreensão.

5.1. Dispositivos

A relação dos dispositivos instalados e em uso no centro e a sua quantidade são listados abaixo:

1. Rádio Bullet M5 do Provedor FortalNet (1);
2. Roteador Wireless D-Link DI-524 (1);
3. Switch IntelBras SF 1600 D 16 portas Ethernet (2);
4. Fonte PPPoE (1);
5. Impressora Samsung SCX 3200 (4);
6. Máquina de Xerox (1);
7. Computador desktop (15).

5.2. Sistemas Operacionais

Os computadores instalados no centro tem como sistema operacional o Windows, nas versões XP e 7.

5.3. Cabeamento

Todo o prédio têm cabeamento categoria 5, usando a tecnologia 10BASE-T e estão distribuídos em canaletas de parede.

5.4. Topologia física

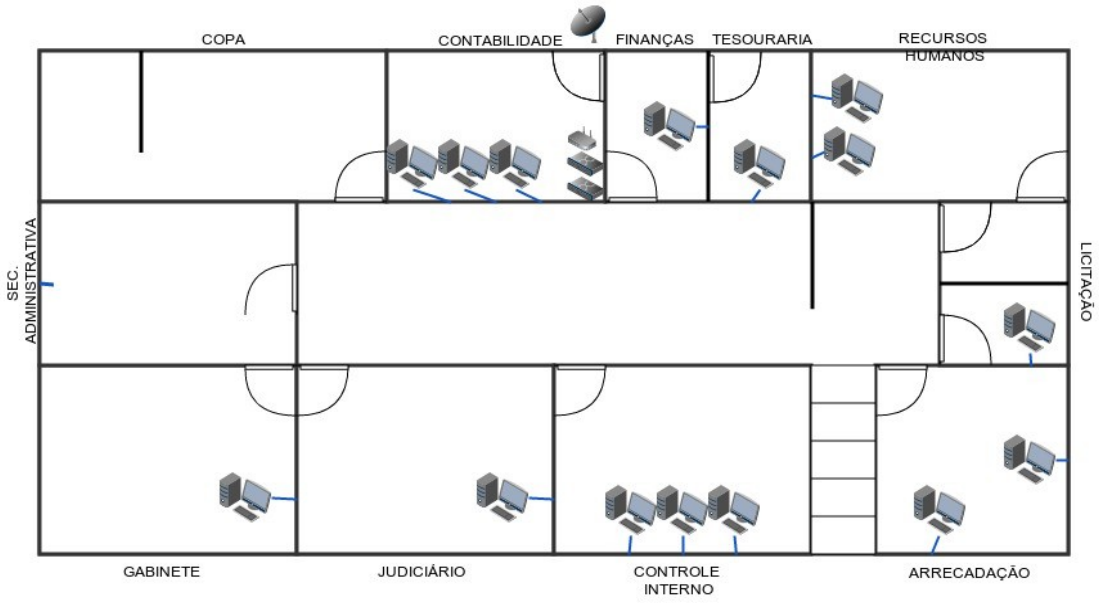

Figura 1: Topologia física atual

5.5. Topologia lógica

A topologia lógica atual, contém 1(um) ponto de acesso, dois (2) *switches* e 15 (quinze) computadores. O AP exerce o papel tradicional de ponto de acesso, mais a função de DHCP. Os *switches* fazem a comunicação entre os hospedeiros e o AP.

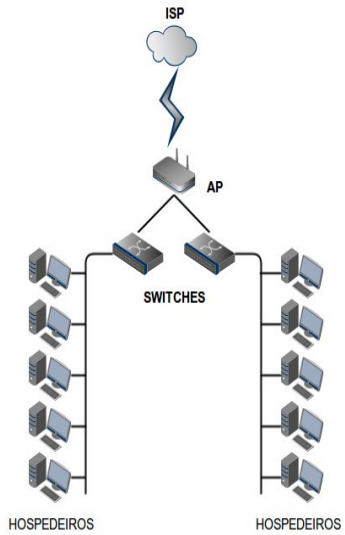

Figura 2: Topologia lógica atual

6. PROJETO LÓGICO

A rede do Centro Administrativo de Ibicuitinga estará topologicamente projetada como indica a figura abaixo.

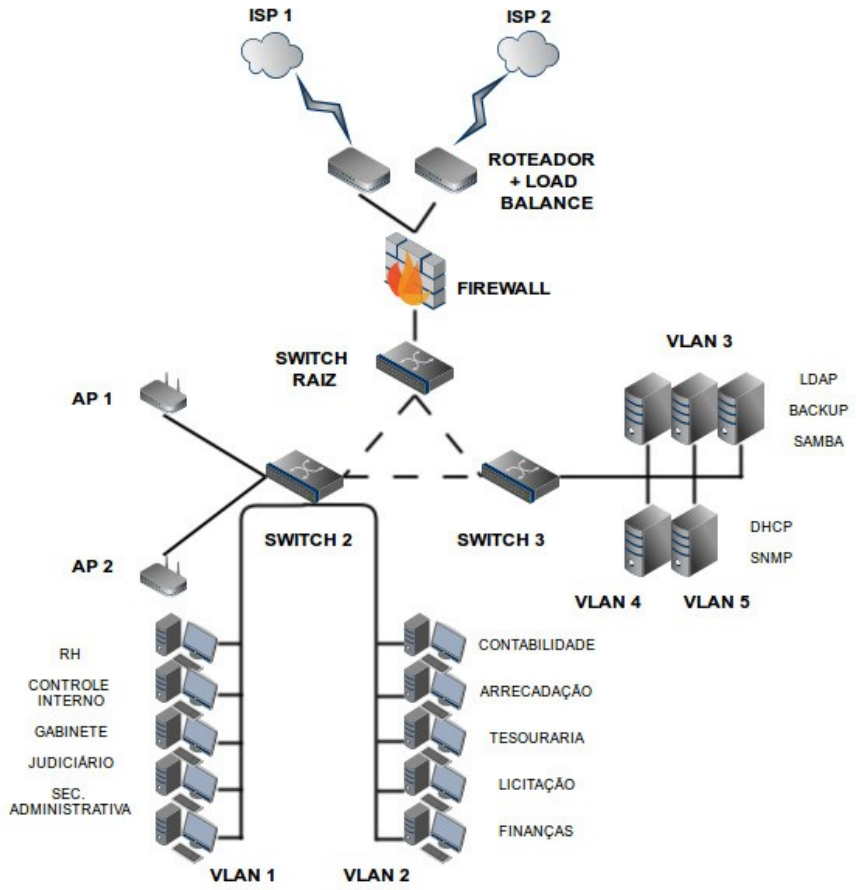

Figura 3: Topologia lógica projetada

Essa topologia é um mapa da rede que indica seus segmentos, pontos de interconexão e comunidades de usuários. A topologia acima, está utilizando o modelo hierárquico que facilita a compreensão e apresenta as partes da rede e seus objetivos.

Essa rede foi projetada levando em consideração os requisitos apresentados pelo cliente. As necessidades levantadas norteiam os projetistas a desenvolverem uma rede que atenda os princípios relevantes do Centro administrativo.

Além disso, a rede mostra-se hierarquizada em um modelo de três camadas lógicas:

Core Layer: é o servidor que vai rotear os dados da rede interna para a externa e vice-versa; *Distribution Layer*: são os *switches* que são capazes de rotear entre VLANs e há definição de domínios de *broadcast* e *multicast;* e por último a *Acces Layer*: controla o acesso de usuários aos recursos da rede, *switches* e APs da camada 2 e a criação de diferentes domínios de colisão. Com isso, facilitamos o entendimento de onde deve ser colocado cada recurso, como cada recurso se encaixa e interage com os outros e quais finalidades vão onde.

A topologia lógica apresentada, contém a existência de redundância de link de comunicação com a internet e 2 (dois) roteadores com balanceamento de carga garantindo a disponibilidade e o desempenho da conexão.

Para a criação das regras do *firewall*, será utilizada a ferramenta *Iptables*, que atua em nível de pacotes. O termo pacote o qual está sendo referido é bem generalizado, abrangendo todas as PDUs[1] (*Protocol Data Units*) das camadas TCP/IP[2]. Geralmente, quando desejamos tratar de camadas específicas, cada PDU é nomeada de acordo com a camada a que pertence. Porém, nesse caso, como o *Iptables* age nas camadas de rede (IPs) e de transporte (Portas), o termo utilizado será esse.

Em nível de aplicação, utilizaremos o Squid, que é um servidor proxy que suporta protocolos das camadas mais altas da pilha TCP/IP. Ele também reduz a utilização da conexão, melhorando o tempo de resposta dos usuários da rede, criando uma memória cache (em dispositivos voláteis e não-voláteis) de requisições frequentes de páginas web, por exemplo. Os bloqueios serão aplicados a determinadas páginas web não utilizadas pela prefeitura. Tais como sítios pornográficos e outros endereços eletrônicos que não estejam ligados aos objetivos da administração. Vale ressaltar que o bloqueio de sites e outras páginas web seguirão os critérios estabelecidos pelas normas e diretrizes contidas no documento de Políticas de Segurança do Centro Administrativo de Ibicuitinga.

O backup dos dados da rede do Centro administrativo será realizado semanalmente através do software Bacula, que é uma ferramenta de código aberto. As principais características desse software são a estrutura cliente/servidor (permitindo *backup* centralizado em uma máquina) e portabilidade (módulos para diferentes sistemas operacionais). A manutenção será realizada pela gerência de TI do centro administrativo.

1 Um bloco de dados que é transmitido entre duas instâncias da mesma camada TCP/IP.

2 Conjunto de protocolos de comunicação entre computadores em rede. O conjunto de protocolos pode ser visto como um modelo de camadas, onde cada camada é responsável por um grupo de tarefas. As camadas mais altas estão logicamente mais perto do usuário (chamada camada de aplicação).

O gerenciamento de arquivos será possibilitado pela aplicação da ferramenta SAMBA que propicia justamente o compartilhamento de arquivos referenciado pelos requisitos apresentados pela comissão da instituição.

O gerenciamento de usuários será possível através do protocolo LDAP que define o acesso aos serviços de diretórios e do OpenLDAP que é um pacote adicionado de recursos de software necessários para torná-lo funcional. Esse serviço é necessário para armazenar todos os dados da rede, como ID de usuários, nomes, senhas, além de outros, centralizando as consultas e pesquisas. Com o OpenLDAP instalado e com usuários com nomes e senhas configurados, será exequível a busca na base do LDAP de qualquer ponto da rede, e o usuário terá acesso aos que lhe forem permitidos, bem como a busca de informação em qualquer ponto da rede.

Com os *switches* serão criadas 5 (cinco) VLANs (LANs Virtuais) que farão a separação das comunidades da rede. Na tabela 1 consta os elementos e as VLANs associados a eles.

VLANs	**Elementos**
VLAN 1	RH, Controle interno, Gabinete, Judiciário e Secretaria administrativa.
VLAN 2	Contabilidade, Arrecadação, Tesouraria, Licitação e Finanças.
VLAN 3	Servidores de Backup, Arquivos e Usuários.
VLAN 4	DHCP
VLAN 5	SNMP

Tabela 1: VLANs e seus elementos

A criação dessas VLANs dar-se devido a grande quantidade de informações confidenciais, como por exemplo os dados encontrados nos setores de contabilidade, arrecadação, tesouraria, licitação e finanças. Optou-se por incluir os setores citados em uma única VLAN, realizando a separação dos demais setores e resguardando as informações. Esse cenário impossibilita que um funcionário mal intencionado cause problemas em outro departamento que não seja o seu. Outro ponto relevante para a criação dessas VLANs é a redução de tráfego de *broadcast*. A limitação do alcance de cada *broadcast* contribui para que

não aja desperdício de banda.

Para que seja possível a alocação de IPs em todas as VLANs, a porta do servidor DHCP será “tageada” nas outras VLANs, com isso haverá a distribuição de IPs. O servidor DHCP e demais servidores terão duas interfaces físicas cada, uma para a VLAN do setor de contabilidade e a outra para o setor de RH.. Essa implementação fará com que as VLANs fiquem acessíveis e aja a distribuição de IPs.

Os *Access points* deverão operar em modo bridge. Portanto, não serão alocados IPs para eles. Somente os nós sem fio que se autenticarem receberão os IPs.

6.1. Endereçamento

Será utilizada a arquitetura TCP/IP, onde há um controle de tráfego mais apurado entre todos os setores da prefeitura, e a conexão é definida de forma prioritária, garantindo a integridade das informações.

Para essa rede, o esquema de endereçamento sugerido está indicado na Tabela 2.

Local/Setor	Endereço de Rede e máscara	Endereço(s)	Endereço de broadcast	Gateway
VLAN1 (recepção, gabinete, secretaria e RH)	192.168.1.0 255.255.255.0	192.168.1.10 - 192.168.1.254	192.168.1.255	192.168.1.1
VLAN2 (contabilidade, tesouraria, judiciário e arrecadação)	192.168.2.0 255.255.255.0	192.168.2.10 – 192.168.2.254	192.168.2.255	192.168.2.1
LDAP	Eth1 - 192.168.1.0 Eth2 – 192.168.2.0 255.255.255.0	Eth1 – 192.168.1.2 Eth2 – 192.168.2.2	Eth1 - 192.168.1.255 Eth2 - 192.168.2.255	Eth1 - 192.168.1.1 Eth2 - 192.168.2.1
DHCP	Eth1 - 192.168.1.0 Eth2 – 192.168.2.0 255.255.255.0	Eth1 – 192.168.1.3 Eth2 - 192.168.2.3	Eth1 - 192.168.1.255 Eth2 - 192.168.2.255	Eth1 - 192.168.1.1 Eth2 - 192.168.2.1
SNMP	Eth1 - 192.168.1.0 Eth2 – 192.168.2.0 255.255.255.0	Eth1 – 192.168.1.4 Eth2 - 192.168.2.4	Eth1 - 192.168.1.255 Eth2 - 192.168.2.255	Eth1 - 192.168.1.1 Eth2 - 192.168.2.1
Backup	Eth1 - 192.168.1.0 Eth2 – 192.168.2.0 255.255.255.0	Eth1 – 192.168.1.5 Eth2 - 192.168.2.5	Eth1 - 192.168.1.255 Eth2 - 192.168.2.255	Eth1 - 192.168.1.1 Eth2 - 192.168.2.1
Samba	Eth1 - 192.168.1.0 Eth2 – 192.168.2.0 255.255.255.0	Eth1 - 192.168.1.6 Eth2 – 192.168.2.6	Eth1 - 192.168.1.255 Eth2 - 192.168.2.255	Eth1 - 192.168.1.1 Eth2 - 192.168.2.1

Tabela 2 - Endereçamento

Para haver comunicação entre todos os elementos da rede, é preciso determinar os links entre os *switches* como *trunk.* Links como este são capazes de transportar informações sobre múltiplas VLANs.

O servidor de *proxy* e *firewall* terá quatro interfaces físicas de rede, duas que recebem o IP dos dois roteadores que operam como *bridge.* Ele, o servidor proxy, será o *gateway* padrão para todas as VLANs. Ou seja, para que os hosts possam se comunicar, terão que passar por suas regras.

6.2. Rotas

Considerando o roteamento estático, o esquema de roteamento a ser usado torna-se simples.

Basicamente:

- Servidor *firewall/proxy* tem como rota o switch raiz e os roteadores;
- *Switch* raiz tem como rota os *switches* não-raíz e o servidor *firewall/proxy*;
- Os *hosts* nas VLANs têm como rota seus respectivos gateways e *switches* das redes que fazem parte.

7. MECANISMOS E ESTRATÉGIAS DE SEGURANÇA

Segurança é um aspecto importante do projeto lógico de uma rede e omiti-lo poderá afetar a escalabilidade, o desempenho e a disponibilidade. Atualmente projetar redes seguras é desafiador pela complexidade e natureza das redes modernas. Com o intuito de tornar a rede do Centro administrativo segura foram desenvolvidas e implementadas políticas e mecanismos de segurança. Antes de idealizar as políticas e mecanismos de segurança foi necessário identificar os recursos da rede e analisar os possíveis riscos de segurança. Abaixo, foram elencados os recursos da rede, e posteriormente segue os riscos existentes.

Os recursos da rede do centro incluem:

- Hospedeiros (incluindo sistemas operacionais, aplicações, dados);
- Dispositivos de interconexão (roteadores, *switches*);
- Dados que transitam na rede.

Os riscos de segurança identificados podem ser intrusos e até usuários inexperientes que por falta de conhecimento e falta de capacitação baixam softwares da internet que possuem vírus. Com o levantamento e análise dos riscos foram desenvolvidas e escolhidos os mecanismos de segurança. Segue abaixo as políticas de segurança e os mecanismos escolhidos para atender os requisitos e proteger a rede projetada.

- Políticas de segurança:
  - Padrões mínimos de segurança de senhas;
  - Delimitação de horários para o uso da rede;
  - Regularizar a entrada de equipamentos não pertencentes a empresa, tais como: pen drives, notebooks e outros;
  - Backups frequentes;
  - Monitoramento de logs;
  - Definição de responsabilidades;
  - Somente os administradores e/ou empresa contratada poderá adicionar novos softwares ou aplicações aos hospedeiros;
  - Somente os administradores e/ou empresa contratada poderá configurar ou auditar os sistemas de computadores da rede, de forma a manter a integridade das políticas de segurança;
- Mecanismos de segurança:
  - Autenticação: utilização de mecanismo normal: nome de login e senha;
  - Autorização: permissões de acesso;
  - Auditoria: coleta de dados sobre o uso dos recursos, com o intuito de identificar possíveis tentativas de intrusão ou mal uso dos recursos;
  - Mecanismo de controle de acesso: *Firewall/Proxy.*
  - Segurança física.

Os procedimentos implementam as políticas. Portanto, proceder bem a um incidente é de extrema importância para que as políticas realizem com eficiência os seus papeis. Para que os usuários do Centro administrativo possam responder acertadamente a essas ocorrências será ministrado um curso de capacitação e treinamento de procedimentos de segurança a todos setores da instituição.

8. ESTRATÉGIAS DE GERENCIAMENTO DA REDE

A detecção e a correção de problemas que causam ineficiência na comunicação é o papel de um bom gerenciamento de redes de computadores. O monitoramento e o controle de sistemas realiza justamente esse trabalho de detectar e corrigir esses problemas e eliminar as condições que poderão levar a que o problema volte a surgir. Na maioria dos casos, gerenciar uma rede não é tarefa fácil, devido a heterogeneidade de hardware, software e de componentes de rede, que por vezes são incompatíveis. As falhas em uma rede, caso não detectadas podem interferir no desempenho da mesma. Para realizar esse monitoramento e controle dos componentes da rede, faz-se necessário a implantação de um software de gerência de redes.

A rede do Centro administrativo será gerenciada pelo protocolo de gerência de redes, o SNMP (Simple Network Management Protocol – Protocolo Simples de Gerência de Rede).

Os dispositivos geridos que farão a coleta e armazenamento das informações de gestão serão o *switches* raiz e a máquina que faz o papel de *Firewall/Proxy*. Os agentes SNMP instalados nesses dispositivos farão o conhecimento da gestão local e traduzirão estas informações para um formato compatível com o protocolo SNMP. O sistema NMS (*NetWare Management System*) é responsável por monitorar e controlar os dispositivos geridos, por meio das informações colhidas de todos os dispositivos da rede. Permite o administrador visualizar as informações de leitura SNMP, por meio de gráficos, tabelas, relatórios e alertas. São exemplos desse tipo de sistema, o MRTG, o Cacti, o Nagios, entre outros.

9. PROJETO FÍSICO

9.1. Topologia física

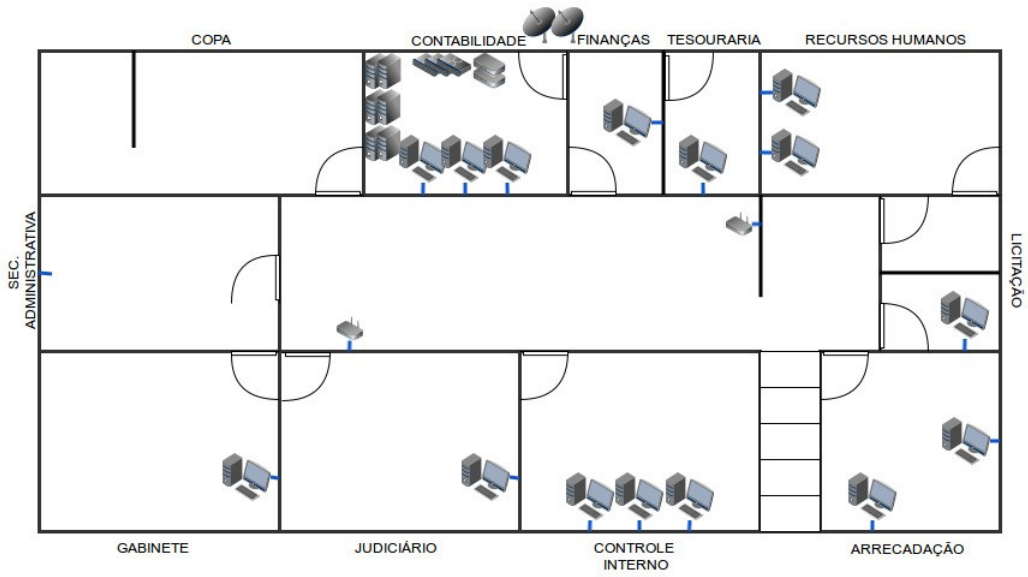

Figura 4: Topologia física projetada

A figura acima apresenta a topologia física projetada. Foram incluídos os 3 (três) *switches*, os 7 (sete) servidores e os 2 (dois) roteadores na sala da contabilidade. Os 2 (dois) pontos de acesso foram instalados nos extremos da sala principal do prédio. E no lado de fora do prédio foram instalados 2 (duas) antenas a rádio do provedor.

9.2. Tecnologias da LAN

Utilizando da tecnologia de LAN e cabeamento existentes na infraestrutura de rede do prédio, optou-se pela continuidade do padrão 10BASE-T e cabeamento UTP Cat5, decisão tomada devido ao entendimento de que a rede do Centro não tem tendência de crescimento significativo a curto e médio prazos.

9.3. Seleção de dispositivos de interconexão

O presente projeto contém 3 (três) *switches,* 2 (dois) *access points* e 2 (dois) modems. SEGUE EM ANEXO AS ESPECIFICAÇÕES.

9.4. Orçamento

São considerados no orçamento os equipamentos que precisam ser adquiridos. Os mesmos constam na tabela abaixo. A escolha da marca e modelo deu-se devido às especificações existentes em anexo, e também foram levados em consideração o respaldo e a qualidade dos produtos dessas marcas no mercado. Não foram incluídas as licenças de software, porque são utilizados somente softwares livres, ou seja, sem custo para o centro administrativo.

Item	**Recurso**	**Quant.**	**Descrição**	**Valor Unitário**	**Valor Total**
1	Switch	3	Switch L2 24 portas 1 GBE UTP SFP combo	1500,00	4500,00
2	Ponto de acesso	2	Access-Point sem-fios Lite-N TL-WA901ND	179,40	358,80
3	Servidor	7	Dell Power Edge T110 II	1949,00	13643,00
4	Roteador	2	4 Wan Roteador TP-Link TL-R470T+ Load Balance	156,99	313,98
5	Fechadura	3	Fechadura Elétrica C-90 Dupla HDL Inox	314,10	942,30
TOTAL					**19758,08**

Tabela 3: Orçamento

APÊNDICE B – ROTEIRO DE ENTREVISTA

Roteiro de entrevista

No presente roteiro consta um questionário que tem por finalidade o levantamento de requisitos para a elaboração de um projeto de rede de computadores para o Centro administrativo da Prefeitura municipal de Ibicuitinga-CE. Abaixo seguem o questionário e dados sobre a entrevista.

Data: 26 de junho de 2013;

Entrevistador: Tallis Deyvide Maia Rubens

Entrevistados: Wendell Bandeira e James Dias Gomes, gerente de TI e secretário de finanças, respectivamente;

Local: Centro administrativo de Ibicuitinga, situado na Rua Edval Maia da Silva, 16 A;

Questionário

1. Quais os motivos que levaram à administração da prefeitura de Ibicuitinga a optar pelo desenvolvimento de um projeto de rede de computadores para o seu centro administrativo?

2. Dentre esses motivos, destaque o(os) principal(ais). Justifique.

3. Existe preferência por sistema operacional?

4. Em quantos e quais setores (departamentos) o centro administrativo está dividido?

5. Quais são os departamentos que necessitam de uma melhor segurança lógica de dados?

6. Há a necessidade de haver uma separação lógica entre esses setores?

7. Existem setores que necessitam compartilhar arquivos uns com os outros? Quais?

8. Havendo a necessidade de sub-redes, deverá também existir a preocupação em criar grupos de usuários?

9. Em relação a guarda dos dados. Será necessário a realização de backup dos arquivos? Se sim, diário, semanal ou mensal?

10. Atualmente é disponibilizado algum serviço (site, e-mail)?

11. Tratando de acesso à internet. Há preferência por provedores? Se sim. Quais?

12. Relativo a segurança física e lógica do centro existe algum sistema de políticas?

13. O gerenciamento e monitorização dos dados deverão ser levados em consideração no projeto?

14. Relativo a mobilidade, o centro administrativo disponibilizará redes sem fio para os funcionários e público?

15. Atualmente o governo municipal recebe algum recurso para a área das tecnologias de informações? Se sim, de que valor?

APÊNDICE C – POLÍTICAS DE SEGURANÇA DO CENTRO ADMINISTRATIVO DE IBICUITINGA

POLÍTICAS DE SEGURANÇA DO CENTRO ADMINISTRATIVO DE IBICUITINGA

1 Controle do documento

1.1 Armazenamento do documento

Título do documento	Políticas de segurança do Centro administrativo de Ibicuitinga
Localização do documento	Site da prefeitura na seção Documentos
Formato do documento	PDF

1.2 Histórico de versão

Versão	Data	Sumário de mudanças
1.0	12/12/2013	Primeira versão

1.3 Aprovações

Nome	Cargo	Data da aprovação	Versão aprovada
James Dias Gomes	Secretário de finanças	A avaliar	1.0
Gildenberg Gomes	Secretário administrativo	A avaliar	1.0
Nonato Saraiva	Chefe de gabinete	A avaliar	1.0
Wendell Bandeira	Gerente de tecnologia da informação - TI	A avaliar	1.0

2 Visão geral das Políticas de segurança – PSI

As informações, dados, sistemas e a rede de computadores são ativos de uma organização, ou seja, é algo que tem valor e importância para a mesma. E proteger a

integridade, a disponibilidade e a confidencialidade desses ativos é de considerável relevância para a boa execução das atividades administrativas, da disponibilidade de sistemas, do funcionamento da rede e da prestação de serviços ao público. Considerando que esses ativos podem ser dados e informações que transitam na rede de computadores, ou que podem estar guardados em seus dispositivos, bem como informações físicas impressas.

As políticas de segurança da informação, ou PSI, é um documento que tem como objetivo, orientar, estabelecer, implementar e melhorar a gestão de segurança da informação do Centro administrativo da Prefeitura municipal de Ibicuitinga - CAPI. As diretrizes contidas nesse documento referem-se à proteção dos ativos e estabelece responsabilidades para todo o quadro de funcionários do Centro. Essa PSI atende as recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005 que confere a boa gestão em segurança da informação, e condiz com as leis vigentes em nosso país.

Tal documento encontra-se disponível no site da Prefeitura municipal de Ibicuitinga, na seção Documentos.

3 Objetivo

O presente documento tem como objetivo estabelecer diretrizes e normas à gestão de segurança da informação com efeito de garantir a integridade, a disponibilidade e a confidencialidade dos ativos do CAPI, seguindo um padrão adequando às necessidades administrativas do Centro.

Esse documento consiste em garantir a proteção e a preservação adequada das informações e ativos quanto à:

- **Integridade:** Garantir o estado atual da informação, protegê-la na transmissão e contra alterações;
- **Disponibilidade:** Garantir o acesso à informação sempre que pessoas autorizadas requirirem;
- **Confidencialidade:** Acesso somente por pessoas autorizadas;

4 Aplicações e escopo da PSI

A presente PSI após a sua aprovação deverá ser seguida por todos os colaboradores, bem como contratados, prestadores de serviços e/ou temporários (com prévia autorização) que venham a utilizar equipamentos tecnológicos ou outra forma de obtenção de informação.

Todos os colaboradores em geral, serão informados previamente da existência desse documento, suas diretrizes e de que poderão ser monitorados e ter os registros de acesso gravados. Os mesmos deverão está constantemente atualizados, verificando qualquer mudança de versão dessa PSI.

5 Das responsabilidade e coordenação da segurança da informação

A gestão da segurança da informação será realizada por meio do gerente de TI, sendo de sua responsabilidade a revisão, a implantação e o acompanhamento do cumprimento das diretrizes contidas no presente documento.

O chefe de gabinete e os secretários serão responsáveis em estimular e fiscalizar o cumprimento da PSI, visando o comprometimento total de suas equipes. Todos os colaboradores deverão aceitar e cumprir as diretrizes e procedimentos da PSI. O não cumprimento da mesma acarretará em medidas punitivas legais e corretivas.

6 Princípios da PSI

Todas as informações manipuladas, geradas e recebidas pelos funcionários e prestadores de serviço dentro do CAPI e resultantes de atividades profissionais são pertencentes à organização.

Todos os ativos (sistemas, informações e equipamentos de informática e comunicação) deverão ser somente utilizados em atividades relacionadas ao Centro. O uso de equipamentos e recursos pessoais serão permitidos somente com avaliação prévia pela gestão de segurança da informação.

7 Revisão e aprovação da PSI

A revisão da PSI deverá ser realizada anualmente considerando o estado atual do CAPI, sua estrutura física, de redes de computadores e processos administrativos. As solicitações de mudanças na PSI deverão ser propostas no período de revisão da mesma.

A aprovação ou não do documento será decidida pelo gerente de TI, chefe de gabinete, secretário administrativo e de finanças. Sendo realizada a aprovação da nova versão, o conteúdo do documento deverá ser divulgado e disponibilizado no site da prefeitura, na seção Documentos.

8 Dos recursos e riscos tecnológicos

Os recursos da rede de computadores do CAPI incluem:

- Hospedeiros (Sistemas operacionais, aplicações);
- Dispositivos de interconexão (*Access points*, *switches*, *Firewall*);
- Dados que transitem na rede.

Intrusos externos que tentam penetrar na rede interna do Centro com o intuito de captar informação e dados confidenciais, vírus de *softwares* baixados da Internet, uso de equipamentos pessoais no ambiente de trabalho, usuários inexperientes e sem capacitação, são os riscos identificados, no decorrer desse documento serão elencados as decisões, dentre elas normas, procedimentos e mecanismos de segurança a fim de proteger e guardar os ativos.

9 Segurança física e do ambiente

9.1 Áreas seguras

Essas áreas são locais onde estão instalados equipamentos de processamento, roteamento e de segurança. Os ativos correspondentes ao CAPI estão instalados na sala da secretaria de finanças. Portanto, as normas contidas nessa seção são relacionadas a essa sala e

estão relacionadas às atividades exercidas pelos colaboradores, fornecedores, prestadores de serviço e terceiros.

9.1.1 Perímetro de segurança física

- Os servidores, *Firewall,* roteadores, *switches*, computadores e impressoras estão instalados e protegidos por uma sala com paredes convencionais e portas com trancas reforçadas, com entrada controlada por uma recepção única.

9.1.2 Controles de entrada física

- A entrada será permitida somente a funcionários, terceiros, visitantes e prestadores de serviços com autorização concedida previamente;
- A data e a hora de entrada e saída de visitantes devem ser registradas e as suas ações supervisionadas;
- Todos os funcionários, visitantes, terceiros e prestadores de serviços deverão possuir crachás de identificação, caso algum indivíduo não esteja portando a sua identificação, esse, deverá ser levado à recepção para que seja verificado se o seu registro/entrada foi aprovado;
- Todos e qualquer serviço prestado por suporte externo deverá ser monitorado pelo gerente de TI.

9.1.3 Proteção contra ameaças externas e do meio ambiente

- As instalações hidráulicas devem ser constantemente verificadas objetivando a prevenção de vazamentos nas tubulações;
- Suprimentos em grande volume como: documentos e papelaria em geral, deverão está em uma distância considerável e segura de materiais combustíveis;
- Os extintores deverão ser constantemente avaliados e posicionados em

locais estratégicos e de fácil acessibilidade.

9.1.4 Trabalhando em áreas seguras

- O conhecimento da área segura deverá ser repassado somente ao pessoal autorizado;
- Fica proibido a permanência de colaboradores e terceiros sem a supervisão do gerente de TI;
- As áreas seguras deverão estar trancadas e periodicamente verificadas quando nenhuma atividade esteja sendo realizada;
- É proibido a utilização de máquinas fotográficas, gravadores de áudio e vídeo na sala de área segura, salvo se for autorizado.

9.2 Segurança de equipamentos

Essa seção tem como objetivo impedir o dano, o furto e o comprometimento dos ativos, garantindo também a proteção contra ameaças físicas e ambientais.

Essas ações têm por finalidade proteger os equipamentos (incluindo os utilizados fora do CAPI, bem como a retirada de ativos) contra o acesso não autorizado às informações, evitando da mesma forma o dano e o furto desses. Observa-se também a inclusão e a remoção de equipamentos no Centro.

9.2.1 Instalação e proteção do equipamento

- Os equipamentos deverão estar em salas de paredes convencionais e protegidas por portas com trancas;
- Os computadores deverão estar posicionados de forma que o ângulo de visão seja restrito para que não haja o risco das informação sejam vistas por pessoal não autorizado;
- Não é permitido comer, beber e fumar nas salas onde estão localizados os

equipamentos de processamento (computadores, *switches*, servidores, roteadores);

- Deverá ser analisados periodicamente o estado dos ar condicionados com o objetivo de controlar a temperatura das salas para que não afetem negativamente no rendimento dos equipamentos de processamento.

9.2.2 Segurança do cabeamento

- As linhas de energia e de telecomunicações devem ser subterrâneas (ou fiquem abaixo do piso);
- O cabeamento de redes devem estar instalados em canaletas ou conduítes, e evitar que o trajeto passe por áreas públicas, evitando intercepção não autorizada e danos;
- Deverá haver segregação entre os cabos de energia e de redes, para evitar interferências;
- Identificar os cabos e os equipamentos com marcações claramente identificáveis com a finalidade de diminuir erros de manuseios, e registrar essas informações em um documento.

9.2.3 Manutenção dos equipamentos

- A manutenção dos equipamentos deverá ser realizada primeiramente pelo gerente de TI ou pessoal interno autorizado. Caso seja necessário a contratação de suporte externo, as atividades deverão ser acompanhadas pelo gerente de TI.

9.2.4 Remoção de propriedade

- Todos os ativos pertencentes ao CAPI não deverão ser removidos sem autorização prévia expedida pelo gerente de TI e com o consentimento do secretário administrativo;

- O controle de retirada e retorno dos ativos deverão ser registrados, informando hora, data, detalhes da remoção, destino e responsável;

9.3 Monitoramento e da Auditoria

Para garantir que as normas e procedimentos contidos nesse documento estejam sendo aplicadas e exercidas por todos os colaboradores deverá ser realizado o monitoramento diário por meio de sistema de gerenciamento e a auditoria em período bimestral, gerando relatórios de histórico do uso dos equipamentos, da rede interna, da Internet e incidentes de segurança. Portanto, o CAPI poderá:

- instalar sistemas de gerenciamento e monitoramento nos ativos (estações de trabalho, *Firewall,* servidores, dispositivos móveis e outros componentes da rede) com o objetivo de identificar acessos maliciosos e a indevida manipulação de dados;
- por solicitação da gerência de TI e gestão do CAPI, ou por exigência judicial, tornar públicas os dados e informações colhidas através do monitoramento e auditoria dos ativos;
- inspecionar fisicamente máquinas;
- instalar sistemas de proteção e detecção nos ativos, garantindo a segurança da informação.
- Monitorar o acesso à rede externa de todos os colaboradores, por exemplo: sites visitados, *download/upload* de arquivos, e-mails, entre outros.

10 Internet

A implantação das políticas de segurança no CAPI visa basicamente o desenvolvimento e o comportamento ético e profissional no uso dos ativos pertencentes ao Centro, bem como na utilização da Internet. Apesar de ser um meio de grande benefício, a

rede pública carrega consigo uma gama de riscos potenciais à segurança de uma rede local. Portanto, a presente PSI objetiva garantir um acesso seguro através de normas e procedimentos que estão elencados a seguir.

- O CAPI tem total liberdade de monitorar todos os acessos à rede pública. E toda e qualquer informação produzida, transmitida e recebida pela Internet está sujeita a divulgação e auditoria;
- Serão bloqueados por meio de controles (escolhidos pela gerência de TI, tais como: *Firewall,* antivírus) todos os sites e portais sem autorização de acesso em todas as estações de trabalho;
- É proibido qualquer tentativa de alteração e negação dos parâmetros de segurança usados nos equipamentos do CAPI por pessoas sem autorização para tal ação, e caso haja comprometimento e/ou exposição das informações, o colaborador será punido administrativamente, cabendo também penalidades civis e criminais;
- O uso pessoal da Internet disponibilizada pela instituição será permitida, contanto que não prejudique o desempenho do colaborador em suas atividades administrativas;
- Cabe somente aos colaboradores autorizados a divulgação de notas, notícias e qualquer informação produzida nos ativos da CAPI em sites, portais, lista de discussão, redes sociais, comunicadores instantâneos e via e-mails;
- É proibido o uso, a instalação e a distribuição não autorizada de programas baixados da internet com autoria e patente legal;
- É proibido o uso, a instalação e a distribuição de softwares pirateados;
- O *download* (baixa) de programas de entretenimento, jogos ou musicais está devidamente proibido;
- Nenhum arquivo de cunho sexual e/ou pornográfico deverá ser acessado, gravado ou transmitido pelos recursos tecnológicos do CAPI;
- Será penalizado o colaborador que produzir ou transmitir de forma consciente qualquer tipo de vírus, programas ilegais e outras perturbações

através dos recursos da CAPI;

- É proibida a utilização de *softwares peer-to-peer* (*BitTorrent*, Emule, Ares e afins);
- O acesso a sites de notícias, entretenimento, redes sociais, *blogs*, entre outros, serão permitidos somente em horários não comerciais a definir pela administração do CAPI.

11 Identificação

O uso de dispositivos de identificação e senhas são imprescindíveis para as mais variadas instituições e empresas que contém recursos tecnológicos e que necessitam de segurança. Cabe a esses, garantir a proteção dos ativos, evitar e prevenir o uso indevido da identidade de qualquer colaborador. Sendo que a utilização de dispositivos e/ou senhas de outras pessoas, constitui crime tipificado, conforme consta no artigo 307 do Código Penal Brasileiro, que se refere a falsa identidade.

As normas referentes a essa seção deverão ser seguidas e aplicadas a todos os colaboradores. Contrariando essa normatização o colaborador infrator estará sujeito a penalidades administrativas, civis e criminais. Referente a identificação física e lógica, segue.

- O dispositivo físico utilizado pelo CAPI será o crachá, e esse deve estar a associado a uma pessoa física e atrelado aos documentos oficiais do referido colaborador;
- O uso correto dos dispositivos identificadores estará na responsabilidade do colaborador, bem como o não compartilhamento dos mesmos;
- Não poderá existir o compartilhamento de logins, salvo, se com autorização prévia da gerência de TI;
- O departamento de Recursos humanos é o responsável pela confecção e distribuição dos crachás, como a devida identificação de função. Já a gerência de TI fará a identificação lógica dos colaboradores utilizando um serviço de contas de grupos e usuários;

- No primeiro acesso às estações de trabalho, o colaborador usará a senha *default* (informada pelo gerência de TI). Logo após a autenticação deverá estar configurada a opção de mudança de senha. E o usuário fará a alteração seguindo as orientações abaixo:
    - Usuário sem privilégios de administrador, deverá criar uma senha de tamanho variável com no mínimo 6 caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %), letras maiúsculas e minúsculas obrigatoriamente;
    - Usuário com privilégios de administrador, deverá criar uma senha de tamanho variável com no mínimo 10 caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %), letras maiúsculas e minúsculas obrigatoriamente;
    - Não poderão ser utilizadas combinações baseadas em dados pessoais como: data de nascimento, placa de automóvel, número telefônico e muito menos sequências óbvias tais como: “abcdefg” ou “1234567”;

- A memorização da senha é de responsabilidade do colaborador, bem como sua proteção e guarda. Sendo aconselhável a não gravação da senha em editores de texto ou blocos de anotações;
- O usuário que obtiver 3 (três) tentativas erradas em um mesmo acesso, terá sua conta bloqueada. O desbloqueio deverá ser solicitada a gerência de TI.
- A alteração da senha poderá ser feita pelo usuário a qualquer momento, caso o mesmo tenha esquecido, deverá solicitar a redefinição da senha a gerência de TI;
- Usuários normais terão um período máximo de 120 dias para efetuarem a troca de senhas, sendo proibido o uso da última senha cadastrada. Já usuários com privilégios de administração terão um prazo de 60 dias para a troca de senha, sendo proibido o uso das duas últimas senhas.

12 Computadores e recursos tecnológicos

Todos os equipamentos disponíveis aos colaboradores são de propriedade do CAPI, e devem ser utilizados e manuseados corretamente, exercendo sempre atividades relacionadas aos interesses da administração. Diante dessas recomendações fica proibido:

- Qualquer tipo de manutenção física e lógica, desinstalação, instalação, configuração ou alteração realizada por usuários. Essas ações devem ser solicitadas previamente e só podem ser feitas pela gerência de TI;
- A cópia e a inclusão de arquivos pessoais nos *drives* da rede, caso seja feita a identificação desses arquivos, os mesmos serão excluídos sem aviso prévio ao possuinte;
- O acesso não autorizado a outros computadores, a interrupção de serviços, servidores e da rede por meios ilícitos;
- Acessar informações confidenciais e bular o sistema de segurança;
- Utilizar *software* pirata;
- Hospedar pornografia ou outro conteúdo que infrinja quaisquer leis.

No uso dos computadores alguns procedimentos devem ser levados em consideração, como:

- Os computadores individuais devem ter senha de *Bios*;
- Qualquer dispositivo estranho conectado no computador sem o consentimento do usuário deverá ser informado a gerência de TI;
- As configurações de segurança dos computadores não deverão ser manipuladas e/ou alteradas por nenhum colaborador;
- Quando não utilizados, os computadores e impressoras devem estar desligados.

13 Backup

Das normas e procedimentos relacionados ao *backup*, devem ser atendidos os seguintes critérios.

- O servidor de *backup* deve ser configurado para que o serviço seja executado automaticamente fora dos horários comerciais, período em que o uso da rede e de seus componentes é mínimo;
- A gerência de TI deve constantemente verificar a disponibilidade de atualização e de novas versões do *software* que realiza o *backup*;
- As mídias de *backup* devem está guardadas em local que não seja o prédio do Centro administrativo, sendo seguro, seco e climatizado. E o tempo de vida das mídias deve ser monitorado e controlado periodicamente através do prazo de validade das mesmas;
- Em caso de erro de *backup*, o serviço deve ser retomado no próximo horário disponível.

14 Redes sem fio

O CAPI tem em sua infraestrutura de rede sem fio, 2 (dois) *access points,* fazendo a comunicação entre equipamentos compatíveis com essa tecnologia. Essa seção destina normas quanto à instalação e configuração dos pontos de acesso, que seguem elencados abaixo:

- O raio do sinal de cada ponto de acesso deve corresponder a 50 metros, limitando o acesso fora das dependências do prédio;
- Implementar a segurança utilizando o sistema de codificação AES (*Advanced Encryption Standard*);
- As senhas dos pontos de acesso devem seguir as mesmas normas e critérios contidos na seção Identificação.

15 Correio eletrônico

O objetivo dessa seção é definir normas relativas ao uso do correio eletrônico particular utilizando a rede de computadores do CAPI.

É expressamente proibido aos colaboradores do CAPI:

- enviar mensagens do tipo “corrente”;
- apagar mensagens pertinentes ao CAPI, quando o mesmo estiver passando por auditoria interna e/ou investigação administrativa;
- divulgar informações não autorizadas pertencentes ao CAPI;
- Produzir, difundir e divulgar mensagem que:
  - contenha: *spam*, vírus de computador e arquivos com códigos executáveis;
  - inclua conteúdo impróprio, ilegal ou obsceno;
  - seja de natureza difamatória, caluniosa, violenta, pornográfica, ameaçadora entre outras;
  - tenha finalidade preconceituosa de caráter sexual, racial e de incapacidade física ou mental.

As mensagens enviadas pelos colaboradores devem sempre conter o seguinte formato: nome do colaborador, nome da empresa, função, telefone e correio eletrônico.

16 Das disposições finais

O CAPI acredita no atendimento e na execução dessas normas e procedimentos por parte dos seus colaboradores, bem como a supervisão pelos secretários. A implantação e o desenvolvimento dessa PSI deve estar atrelada a ética, e deve ser compreendida como parte fundamental para o exercício da segurança das informações, da correta aplicação dos ativos e dos bons costumes adotado por todos que fazem essa administração.

ANEXO A – ESPECIFICAÇÕES DOS EQUIPAMENTOS

Abaixo segue as especificações dos equipamentos de rede que deverão ser adquiridos para a construção da rede local.

Equipamento 1 – Switch L2 24 portas 1 GBE UTP SFP combo

1. Características gerais

   a) Switch Ethernet de camada 2, compatível com as tecnologias Ethernet, Fast Ethernet e Gigabit Ethernet, com pelo menos 24 portas UTP. A unidade deverá permitir a expansão para 48 (quarenta e oito) portas UTP.

2. Protocolos e padrões requeridos

   a) Fast Ethernet 100BASE-TX (IEEE 802.3u);
   b) STP Spanning Tree Protocol (IEEE 802.1D);
   c) VLANs (IEEE 802.1Q);

3. Gerenciamento

   a) Protocolo de Gerenciamento SNMPv1, SNMPv2 e SNMPv3
   b) Suporte a 4 grupos de RMON (estatísticas, histórico, alarmes e eventos);
   c) Interface de gerenciamento baseada em WEB (HTTP) e/ou CLI;
   d) Porta do console para gerenciamento e configuração via linha de comando com conector

      RJ- 45 ou RS-232. (os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos);
   e) Permitir atualização de *firmware* via TFTP/FTP;
   f) Possuir suporte a espelhamento de portas para uma porta específica de modo a permitir a conexão de um analisador externo.

4. Desempenho

a) Possuir desempenho de no mínimo 65 Mbps considerando pacotes de 64 bytes;
b) Possuir matriz de comutação de pelo menos 10 Gbps;
c) Deve implementar no mínimo 30 VLANs segundo o protocolo IEEE 802.1Q;
d) Quantidade mínima de 8.000 endereços MAC.

5. Segurança

a) Filtros de camada 2 aplicáveis em interfaces físicas ou lógicas sem impacto no desempenho de encaminhamento de pacotes. A filtragem deve ser baseada em endereço MAC e IP, porta TCP/UDP, VLAN;
b) Possuir suporte a associação de um endereço MAC específico a uma dada porta do Switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão;
c) Suporte ao protocolo de autenticação, autorização e accounting (AAA) TACACS+ ou RADIUS para controle do acesso administrativo, por usuário, ao equipamento. Deve ser possível fazer a autenticação, autorização de comandos e "accounting" de comandos em qualquer acesso administrativo ao equipamento.

6. Generalidades

a) Deverá possuir estrutura apropriada para acondicionamento em armário de fiação (rack) padrão 19 polegadas e vir acompanhado do respectivo kit de suporte específico para montagem ;
b) A fonte alimentação deverá funcionar com tensão elétrica nominal de 110V~220V AC, 50~60Hz, de modo automático;
c) Deverá ser acompanhado de documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;
d) Deverá ser fornecido com todos os acessórios necessários para operacionalização do equipamento, tais como software, cabos lógicos, cabos de interface RS-232 e

cabos de energia elétrica.;

e) Deve possuir garantia e assistência técnica on-site por um período mínimo de 48 (quarenta e oito) meses conforme o procedimento indicado no item 7 deste anexo. Condições de Garantia, Suporte e Assistência Técnica.

Equipamento 2 – Access Point

1. Características gerais

a) Permite ligar dispositivos sem fios G (802.11g) ou B (802.11b);
b) Alcance do raio de no mínimo 50 metros.
c) Suportar modo de conexão infraestruturado;
d) Possuir indicadores LED Power, 10/100/1000 Mbps e 802.11a/b/g/n em atividade;
e) Possuir estrutura física que permita fixação do equipamento em teto e parede;
f) Deve possuir todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, cabos de console, kits para fixação, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação,configuração e operacionalização do equipamento.
g) Possuir certificação Wi-Fi Alliance para operar nos padrões 802.11a/b/g/n.
h) Permitir conexão simultânea de clientes nos padrões 802.11a/b/g/n.
i) Suportar a pilha de protocolos TCP/IP.
j) Suportar no mínimo 16 VLANs.

2. Protocolos e padrões requeridos

a) Padrão IEEE 802.3i – 10BASE-T;
b) Padrão IEEE 802.3u – 10BASE-TX
c) Protocolos: DHCP (modo cliente);
d) Permitir habilitar e desabilitar a divulgação do SSID.
e) Suporte a mudança dinâmica das taxas de operação.
f) Implementar detecção automática de interferências e realizar ajustes automáticos

para otimização da cobertura do sinal.

g) Possibilitar a comunicação sem fio entre outros APs via WDS, ou similar, de forma a aumentar a área de cobertura da rede.

3. Segurança

a) Implementar os seguintes padrões de criptografia:
   - WEP (64 e 128 bits);
   - WPA e WPA2 – IEEE 802.11i.;
   - TKIP;
   - AES 128 bits com CCMP.

4. Gerenciamento

a) Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – comand line interface) com conector RJ-45 ou USB;
b) Possuir compatibilidade com o protocolo de gerenciamento SNMP, versão 1, 2 e 3.

5. Garantias

Fornecer garantia de funcionamento pelo período de 48 (quarenta e oito) meses contada a partir do recebimento definitivo do equipamento, sem prejuízo de qualquer política de garantia adicional oferecida pelo fabricante. A Contratada deverá descrever, em sua proposta, os termos da garantia adicional oferecida pelo fabricante.