UNIVERSIDADE NOVE DE JULHO – UNINOVE

DIRETORIA DE INFORMÁTICA

Projeto de Conectividade em Redes Locais

SÃO PAULO

2022

Projeto de Conectividade em Redes Locais

Guilherme Alves Lisboa	RA: 922102476
Tiago Freire de Luna	RA: 922101953
Vinicius de Azevedo Barbosa	RA: 2222104131
Vinicius Divino da Silva	RA: 2222107405
Rafael Silva Queiroz Miranda	RA: 2222200129
Erick Pereira Cavalcante	RA: 2222106236
Nilson Felipe Rodrigues	RA: 2222201179
Henrique Brandão de Arruda	RA: 422101027
Filipe Francisco de Oliveira	RA: 2221202070

Trabalho apresentado ao curso de tecnologia em Segurança da Informação da Universidade Nove de Julho, como parte dos requisitos para a obtenção do Grau de Tecnólogo em Segurança da Informação.

Orientador: Prof. Edson Melo De Souza Unidade:
Campus: MM, SA, VP, VG, VM
Curso: Tecnologia em Segurança da Informação.

São Paulo

2022

FOLHA DE APROVAÇÃO

Guilherme Alves Lisboa	RA: 922102476
Tiago Freire de Luna	RA: 922101953
Vinicius de Azevedo Barbosa	RA: 2222104131
Vinicius Divino da Silva	RA: 2222107405
Rafael Silva Queiroz Miranda	RA: 2222200129
Erick Pereira Cavalcante	RA: 2222106236
Nilson Felipe Rodrigues	RA: 2222201179
Henrique Brandão de Arruda	RA: 422101027
Filipe Francisco de Oliveira	RA: 2221202070

Projeto de Conectividade em Redes Locais

Trabalho de conclusão aprovado como requisito parcial para a obtenção do grau de Tecnólogo do curso de Tecnologia em Segurança da Informação, da Universidade Nove de Julho, pelo professor orientador abaixo mencionado.

São Paulo, 28 de novembro de 2022

_____

Prof. Edson Melo De Souza

RESUMO:

Neste projeto abordaremos temas voltados a “Redes”, através de vários tópicos mencionados, iremos abordar a rede como um todo desde a sua infraestrutura até sua parte lógica.

Em exemplos como telecomunicações, infraestrutura de tecnologia da informação; e na engenharia de software, escalabilidade é uma característica desejável em todo sistema, rede ou processo, que indica a habilidade de manipular uma porção crescente de trabalho de forma uniforme, ou estar preparado para crescer. Por exemplo, isso pode se referir à capacidade de um sistema em suportar um aumento de carga total quando os recursos (normalmente de hardware) são requeridos.

A escalabilidade é assunto extremamente importante em sistemas eletrônicos, bancos de dados, roteadores, redes de computadores etc. como nosso foco aqui será em redes iremos abranger mais sobre isso; como por exemplo: Hardwares necessários, Infraestrutura física, Certificação de rede, Layout entre outros.
Sinta-se à vontade para degustar do conteúdo aqui mencionado, onde o foco não foi apenas mais um projeto, mas sim, contribuir no avanço intelectual de cada indivíduo que tiver acesso a esse material, promovendo assim uma orientação, ou capacitação, com ênfase em redes.

Palavras-chaves: Hackers, Vulnerabilidade, Segurança da Informação, Testes de penetração, Invasão, Pentest, Ética, Legislação

LISTA DE FIGURAS

FIGURA 1 - VALORES DE DISPONIBILIDADE 16
FIGURA 2 - 34 SETORES 21
FIGURA 3 - 34 SETORES II 22
FIGURA 4 - TOPOLOGIA BARRAMENTO 23
FIGURA 5 - TOPOLOGIA ESTRELA 23
FIGURA 6 - TOPOLOGIA ANEL 23
FIGURA 7 - TOPOLOGIA PONTO A PONTO 23
FIGURA 8 - BACKBONE 24
FIGURA 9 - ESTRELA HIERÁRQUICA 24
FIGURA 10 - MALHA (MESH) 24
FIGURA 11 - WIRELESS 24
FIGURA 12 - TOPOLOGIA HIBRIDA 25
FIGURA 13 - TOPOLOGIA UTILIZADA 26
FIGURA 14 - CATEGORIZAÇÃO CABO UTP 27
FIGURA 15 - PARAFUSO PORCA GAIOLA 29
FIGURA 16 - ELETROCALHAS 29
FIGURA 17 - ESTRUTURA PREDIAL 30
FIGURA 18 - ABERTURA CMD 34
FIGURA 19 - CMD IPCONFIG 34
FIGURA 20 - SERVIDORES DE REDE 37
FIGURA 21 - SERVIDORES DE NUVEM 38
FIGURA 22 - SERVIDOR DE ARQUIVOS 38
FIGURA 23 - SERVIDOR WEB 40
FIGURA 24 - SERVIDOR DE EMAIL 40
FIGURA 25 - SERVIDOR PROXY 41
FIGURA 26 - COMPUTAÇÃO EM NUVEM 42
FIGURA 27 - AMBIENTE DE COMPUTAÇÃO EM NUVEM 43
FIGURA 28 - MODELO DE SERVIÇOS 45
FIGURA 29 - PAPEIS NA COMPUTAÇÃO EM NUVEM 46
FIGURA 30 - ARQUITETURA DA COMPUTAÇÃO EM NUVEM 48
FIGURA 31 - AMAZON EC2 49
FIGURA 32 - PLATAFORMA MICROSOFT AZURE 49
FIGURA 33 - ARQUITETURA DO ANEKA 50
FIGURA 34 - ARQUITETURA DO CLOUDAV 51
FIGURA 35 - DIVERSOS TIPOS DE SISTEMAS OPERACIONAIS 52
FIGURA 36 - RELAÇÃO USUÁRIO AO HARDWARE 53

SUMÁRIO

INTRODUÇÃO 8
CAPITULO 01 - SALA DE EQUIPAMENTOS 9
1.1 - Piso Elevado 9
1.2 – Climatização 9
1.3 – Restrição de Acesso a sala de equipamentos 9
CAPITULO 02 - INFRAESTRUTURA FÍSICA DA REDE LOCAL 11
2.1 - Hardwares e Softwares frequentemente utilizados. 11
2.2 Disponibilidade Da Rede Local Para Os Usuários 14
2.3 – Wireless 17
CAPITULO 03 – CERTIFICAÇÃO DE REDE 19
3.1 – Testes passivos 19
3.2 – Testes ativos 19
3.3 - Benefícios da certificação de rede 20
CAPITULO 04 – LAYOUT DE REDE 21
4.1- Topologias de rede 22
4.2 - Escolha do Material 26
4.3 - Implantação do Projeto 30
4.4 - Escalabilidade 31
5.1 – Básico de redes: endereço MAC e endereçamento IP 34
5.2 - Endereço lógico e físico no sistema operacional 35
*5.3 - C*ontrole de acesso à internet 35
CAPITULO 6 - Sistema operacional dos servidores 37
6.1 - Servidores mais conhecidos 38
6.2 - Monitoramento de aplicações em servidores em nuvem 41
CAPITULO 07 - Sistemas Operacional Das Estações de Trabalho 52
CAPITULO 7.1 - Sistemas Operacionais 52
7.2 - Unix 53
7.3 - Linux 54
7.4 - Familia Windows 54
CAPÍTULO 08 – ANTIVÍRUS 56
8.1 – O que é um vírus de computador? 56
8.2 – Malwares 56
8.3 – Principais Antivírus 57
CAPITULO 09 - SISTEMA DE BACKUP 59

09.1 - Exemplos de backup: 59
CAPITULO 10 - SERVIÇOS DE REDE 61
10.1 - Como Funciona? 61
10.2 - Exemplos de algumas portas padrões usados no TCP/IP: 61
CAPITULO 11 - ESTRUTURA DE ACESSO 64
11.1 Gerenciar o acesso a pastas do servidor 64
11.2 Definir Permissões Para Pastas De Servidor 65
11. 3 Adicionar Ou Mover Uma Pasta De Servidor 66
11.4 Estrutura da comunicação interna 67
11.5 Comunicação Interna 67
REFERÊNCIAS BIBLIOGRAFICAS: 69

INTRODUÇÃO

Concluímos que não é tão básico como muitas vezes se imagina, desde sua infraestrutura até sua Qos (qualidade de serviço) demanda de uma excelente conectividade e estratégia, para atender as altas demandas que surgem ao longo desse processo, e posteriormente com o avanço e o aumento da rede como um todo. Todo esse processo aconteceu devido a necessidade de comunicação onde seriam informados dados, na onde a definição da palavra é; Segundo (FOROUZAN, Behrouz A, 2008), apalavra dados se refere a informações apresentadas em qualquer forma que seja acordada entre as partes que criam e usam os dados. No caso da comunicação de dados que nada mais é do que a comunicação entre dois, ou mais dispositivos, onde a intermediação será feita pela estrutura dos meios de produção, como por exemplo: Cabos Fibra Óptica (Feitos de fibras de Vidro ou Polímeros), Cabos Coaxiais (Núcleos de Cobre, Blindagem Eletromagnética, Revestimento de Plástico) e Cabos Par – Trançado (cat 5, cat 5e).

A comunicação sempre foi essencial ao ser humano, com as dificuldades encontradas no meio da trajetória levaram a obrigatoriedade de se desenvolver, levando assim, o aprimoramento e evolução aos meios de comunicação dando ênfase as melhorias feitas nas técnicas e elementos constituintes do sistema de comunicação. Apesar da evolução todos os meios ainda hoje utilizam de elementos básicos exemplo: Transmissão (é o dispositivo que envia os dados), Receptor (é o dispositivo que recebe os dados), Meio de Comunicação (também conhecido como canal, o caminho utilizado), Protocolo (constitui de um conjunto de regras que proporciona a comunicação), Mensagem (é a informação propriamente dita que se deseja transmitir).

Durante a história a comunicação de dados foi dívida em quatro grupos de sistemas:

• Telefonia (Telefones, Orelhões, Celulares...)

• Radiodifusão (Telegrafo, Microfones, Rádio...)

• Televisão (Tvs, Telões, Projetores...)

• Redes de Computadores (Computadores, Notebooks, Desktops...)

A Internet evoluiu e tornou-se um ambiente dinâmico que constantemente oferece novos protocolos, serviços e aplicações. Os Firewalls são claramente uma parte essencial de quaisquer soluções de segurança de redes, embora ele não consiga garantir a segurança total. Para que o Firewall funcione, deve fazer parte de uma arquitetura consistente de segurança, com políticas realistas e conscientização por parte de todos os utilizadores.

CAPITULO 01 - SALA DE EQUIPAMENTOS

1.1 - Piso Elevado

Ao criar uma sala de equipamentos ou área de trabalho, deve-se levar em consideração a fragilidade de computadores, cabos, roteadores e eletrônicos em geral, organizando a área de forma a minimizar os danos, como combustão, umidade e erro humano.

Para isso, são criados vãos – às vezes no teto, às vezes no chão – para a passagem e fácil localização de cabos, dutos de ar-condicionado, tubos hidráulicos, dentre outros. Esses vãos são chamados de “piso elevado”.

O piso elevado deve ser montado após o término das outras etapas da obra, inclusive a pintura. Também é necessário marcar previamente em qual superfície o piso será instalado, para evitar que outros equipamentos sejam instalados no lugar ou que não haja espaço para a instalação do piso. A superfície também deve ser fixa e regular, para evitar umidade, entulho etc.

Em seguida, instale os pedestais, preferencialmente de PVC ou metal, e coloque as placas do piso nos locais anteriormente escolhidos, sem inclinações em relação à primeira.

Se a área for propensa à umidade, é necessário usar da impermeabilização de laje, como, por exemplo, colocar uma manta de PVC.

Apesar do alto custo e complexidade de instalar, um piso elevado é beneficial em longo prazo, pois todos os componentes estarão em um lugar seguro e conveniente.

1.2 – Climatização

Devido à baixa tolerância de aparelhos eletrônicos à umidade, é altamente recomendado manter estabilidade de temperatura no escritório.

Para evitar umidade e, consequentemente, a destruição de discos rígidos, muitos pensam que diminuir drasticamente a temperatura do escritório (para, por exemplo, 10 graus Celsius) é a forma mais viável de resolver o problema, no entanto, isso se torna problemático em longo prazo, pois quanto menor a temperatura, maior o consumo de energia, não leva os funcionários em consideração, que podem não conseguir trabalhar nessas condições, além de ser uma medida extrema.

De acordo com a ASHRAE (American Society of Heating, Refrigeratiing and Air Conditioning Engineers), órgão que trata das condições térmicas de ambientações humanas, a temperatura ideal na entrada de ar de equipamentos como ar-condicionado é entre 18 e 27 graus Celsius, com umidade relativa entre 40 e 55% dependendo da estação.

1.3 – Restrição de Acesso a sala de equipamentos

MEDIDAS DE PROTEÇÃO COLETIVA:

Em todos os serviços executados em instalações elétricas devem ser previstas e adotadas, prioritariamente, medidas de proteção coletiva aplicáveis, mediante procedimentos, às atividades a serem desenvolvidas, de forma a garantir a segurança e a saúde dos trabalhadores.

MEDIDAS DE PROTEÇÃO INDIVIDUAL:

Nos trabalhos em instalações elétricas, quando as medidas de proteção coletiva forem tecnicamente inviáveis ou insuficientes para controlar os riscos, devem ser adotados equipamentos de proteção individual específicos e adequados às atividades desenvolvidas, as roupas de trabalho devem ser adequadas às atividades, devendo contemplar a conduta, inflamabilidade e influências eletromagnéticas.

SEGURANÇA EM PROJETOS:

É obrigatório que os projetos de instalações elétricas especifiquem dispositivos de desligamento de circuitos que possuam recursos para impedimento de reenergização, para sinalização de advertência com indicação da condição operativa, todo projeto deve prever condições para a adoção de aterramento temporário.

SEGURANÇA EM INSTALAÇÕES ELÉTRICAS ENERGIZADAS:

As operações elementares como ligar e desligar circuitos elétricos, realizadas em baixa tensão, com materiais e equipamentos elétricos em perfeito estado de conservação, adequados para operação, podem ser realizadas por qualquer pessoa não advertida, os serviços em instalações energizadas, ou em suas proximidades devem ser suspensos de imediato na iminência de ocorrência que possa colocar os trabalhadores em perigo.

TRABALHOS ENVOLVENDO ALTA TENSÃO:

Os serviços em instalações elétricas energizadas em alta tensão, bem como aqueles executados no Sistema Elétrico de Potência não podem ser realizados individualmente, Antes de iniciar trabalhos em circuitos energizados em alta tensão, o superior imediato e a equipe, responsáveis pela execução do serviço, devem realizar uma avaliação prévia, estudar e planejar as atividades e ações a serem desenvolvidas de forma a atender os princípios técnicos básicos e as melhores técnicas de segurança em eletricidade aplicáveis ao serviço.

NR 10 - SEGURANÇA EM INSTALAÇÕES E SERVIÇOS EM ELETRICIDADE:

A NR 10 é a norma regulamentadora que trata da segurança e saúde dos serviços em eletricidade, ela se aplica a quatro fases, que são: geração, transmissão, distribuição e consumo, Isso também inclui todas as etapas do projeto, construção, montagem, operações e, até mesmo, as instalações elétricas de quaisquer trabalhos que envolvam eletricidade e suas proximidades, a norma deve ser adotada em todas as intervenções de instalações elétricas, mediante a técnicas de análise de risco, garantindo sempre a saúde e a segurança do profissional.

Importância da NR 10

A NR 10 é de suma importância para os trabalhadores que atuam em áreas de extremo risco elétrico, ela possui um sistema de resguardo e segurança para os trabalhadores, deixando o ambiente mais seguro, garantindo o bom funcionamento empresarial.

CAPITULO 02 - INFRAESTRUTURA FÍSICA DA REDE LOCAL

Antes de mais nada para que seja possível adentrarmos dentro das questões físicas e lógicas da rede, primeiro, vamos analisar qual é sua finalidade e os variados modelos existente atualmente. Antes de tudo, o que seria infraestrutura? A origem da palavra é: Infraestrutura é o conjunto de serviços fundamentais para o desenvolvimento socioeconômico, ou seja, na nossa situação é, tudo aquilo que é idealizado e aplicado para o funcionamento da rede, desde sua arquitetura até sua aplicação.

Todo esse processo aconteceu devido a necessidade de comunicação onde seriam informados dados na onde a definição da palavra é; Segundo (FOROUZAN, Behrouz A, 2008), a palavra **dados** se refere a informações apresentadas em qualquer forma que seja acordada entre as partes que criam e usam os dados. No caso da comunicação de dados que nada mais é do que a comunicação entre dois, ou mais dispositivos, onde a intermediação será feita pela estrutura dos meios de produção, como por exemplo: Cabos Fibra Óptica (Feitos de fibras de Vidro ou Polímeros), Cabos Coaxiais (Núcleos de Cobre, Blindagem Eletromagnética, Revestimento de Plástico) e Cabos Par – Trançado (cat 5, cat 5e).

A comunicação sempre foi essencial ao ser humano, com as dificuldades encontradas no meio da trajetória levaram a obrigatoriedade de se desenvolver, levando assim, o aprimoramento e evolução aos meios de comunicação dando ênfase as melhorias feitas nas técnicas e elementos constituintes do sistema de comunicação. Apesar da evolução todos os meios ainda hoje utilizam de elementos básicos exemplo: Transmissão (é o dispositivo que envia os dados), Receptor (é o dispositivo que recebe os dados), Meio de Comunicação (também conhecido como canal, o caminho utilizado), Protocolo (constitui de um conjunto de regras que proporciona a comunicação), Mensagem (é a informação propriamente dita que se deseja transmitir).

Durante a história a comunicação de dados foi dívida em quatro grupos de sistemas:

- Telefonia (Telefones, Orelhões, Celulares...)
- Radiodifusão (Telegrafo, Microfones, Rádio...)
- Televisão (Tvs, Telões, Projetores...)
- Redes de Computadores (Computadores, Notebooks, Desktops...)

Telefonia se deu em meados do século XIX (19) de 1801 a 1900, Radiodifusão entre os anos de 1844 e 2002, Televisão de 1842 a 1967 e por fim Redes de Computadores dos anos de 1961 a 1973. Todos esses acontecimentos foram de máxima importância para o desenvolvimento não só da comunicação de dados, mas também, ao desenvolvimento a Infraestrutura utilizada hoje em dia, como veremos a seguir sobre os Hardwares e Softwares.

2.1 - Hardwares e Softwares frequentemente utilizados.

Antes de tudo começaremos falando da estrutura física, ou seja, o Hardware necessário e frequentemente usado na elaboração da Rede. Tudo na verdade irá variar de acordo com a demanda do cliente como por exemplo: Local, largura da Banda, Alcance e outros detalhes importantes para compor a estrutura física da rede. Atualmente nas empresas independente da arquitetura da rede se usa; Switches, Roteadores e Cabos Par – Trançados, Servidores, Máquinas Clientes entre outros. Tudo isso nos leva as topologias, que seria a forma como os

dispositivos estão interligados na rede, em questões lógicas e físicas, as topologias físicas consistem nos recursos necessários para interligar os usuários na rede através de equipamentos e as formas de interligar esses equipamentos entre si, como por exemplo as topologias em: Barramento, Estrela, Anel, hierárquica, mista ou Hibrida e Malha ou Mesh.

Barramento

Neste tipo de topologia consiste em ligar todos os dispositivos na rede através de uma "barra", ou em algum meio de transmissão, como por exemplo o cabo coaxial. Esse tipo de topologia parou de ser usado devido ao baixo desempenho quando o tráfego da rede era intenso, já que todos os dispositivos ligados nela compartilhavam e disputava o mesmo meio de transmissão. Nesse esquema apenas um dispositivo pode enviar e receber por vez, quando uma máquina deseja enviar dados na rede, ela deve "escutar" o meio de transmissão, caso ele esteja liberado, os dados são transmitidos da origem para o destino, e nessa situação nenhum outro dispositivo pode transmitir na rede enquanto esse processo estiver em andamento.

Estrela

Na topologia estrela utiliza-se de um dispositivo central geralmente conhecido como concentradores (podendo ser chamado também de comutador), mas geralmente chamados de Hubs ou Switches, atualmente não se usam mais os Hubs por limitação no gerenciamento da rede. São conectados por cabos par – trançados ou fibra óptica, essa topologia costuma ser a mais utilizada pelo fato do dispositivo comutador (Hub ou Switches) costuma controlar o envio dos dados na origem e levando até o destino, permitindo que qualquer dispositivo na rede possa enviar e receber dados quando necessário.

A vantagem desse tipo de topologia é que, caso um nó ou dispositivo falhem a rede continua funcionando. Até porque quem estabelece a velocidade da rede é o dispositivo comutador (Hubs ou Switches). Porém o lado ruim desse esquema é justamente o dispositivo que comuta ela, ou gerencia ela, pois caso ele pare de funcionar a rede toda se perde.

Anel

Nesse esquema a rede os dispositivos ligados em um caminho fechado em série. Ao serem enviados os dados na rede eles passam por cada nó (Hosts, Máquinas) na rede, operando como repetidores até que o nó de origem e destino os retire da rede. Geralmente esse tipo de topologia é unidirecional, ou seja, possui uma única direção fazendo com que os dados sigam por um único caminho, mas dependendo do protocolo existem alguns casos em que poderão funcionar de forma Bidirecional, trafegando por mais de um caminho, caso um caminho apresente falhas, terá mais de uma opção.

Hierárquica

A topologia Hierárquica costuma ser dívida em três camadas, esse tipo e topologia usa geralmente um conjunto de redes em estrela de forma hierárquica. Os nós (hosts ou máquinas)

se comunicam por meio de dispositivos intermediários geralmente os Switches. As três camadas são:

Camada de Acesso:

Conecta os últimos dispositivos como por exemplo: computador, celular, tablets, telefone, conectados por meio dos Switches e pontos de acesso.

Camada de Distribuição:

Faz a conexão com a camada de acesso e no núcleo (servidor) da rede. Normalmente utiliza-se Switches de alto desempenho que segmentam o tráfego da rede, criando sub- redes separadas.

Camada Núcleo:

Costuma ser formada por equipamentos de alto desempenho que proporcionam uma conexão entre as camadas de distribuição. Dispositivos como Switches ou Roteadores costuma ser capazes de manusear grandes quantidades de dados.

Topologia Mista ou Hibrida

A topologia Mista ou Hibrida consiste na utilização de duas ou mais arquiteturas ao mesmo tempo. Essa topologia geralmente é utilizada para atender altas demandas, atendendo algumas necessidades especificas como, grandes redes, custo, flexibilidade e o crescimento da rede.

Topologia Malha ou Mesh

Geralmente se utiliza a topologia Malha ou Mesh quando se deseja um uso desnecessário na rede, pois cada nó (host ou máquina) estará conectado a todos os dispositivos na rede, formando uma teia com mais de um caminho até o destino. Costuma se usar roteadores para formar esse tipo de arquitetura, que fica responsável por encontrar o melhor trajeto por meio dos diferentes nós (host ou máquina). Mesmo tendo um nível de uso desnecessário, a topologia em Malha tem uma desvantagem em seu custo, e na dificuldade de configuração. A internet por exemplo seria um bom exemplo de uma rede do tipo Malha.

Topologia Lógica

Como já mencionado as topologias lógicas determinam como os sinais trafega através das redes e qual será método de acesso aos meios de transmissão. Conseguimos dividir essas topologias em dois métodos, sendo eles:

- Barramento ou Não – determinística;

- Anel ou Determinística;

Barramento ou não – determinística

Nós (hosts ou máquinas) que compõem uma rede do tipo não – determinística possuem o "poder" de enviar quando quiser, por exemplo, não contém um dispositivo concentrador que vai determinar quem vai enviar na rede. As redes do tipo Ethernet usam esse conceito, os nós da rede podem enviar a qualquer momento, desde que o canal de transmissão esteja disponível. Esses tipos de topologias lógicas são conhecidos como Topologias em Barramento (não podemos confundir com topologias físicas em barramento).

Anel ou Determinística

Diferente da topologia anterior aqui mencionada, as redes do tipo Determinística movimentam apenas um quadro na rede que atua controlando o acesso ao meio de transmissão. Redes Token Ring utilizam um dispositivo concentrador chamado de Mau (Multistation Access Unit, unidade de acesso de estação). Esse dispositivo concentra os demais que fazem parte do anel lógico, e por meio do token ou bastão, é realizado o controle do acesso ao meio de transmissão. Somente o nó (host máquina) que possui o bastão poderá enviar na rede por um período. O bastão contém a mensagem que circula pela rede até alcançar o dispositivo de destino, que copia a mensagem para processar, durante isso, o bastão volta a circular pelo anel. Apesar desse tipo de topologia não apresentar colisão dentro da rede, já que, somente quem está com o bastão pode enviar, atualmente, este tipo de rede não é muito comum de se encontrar, pois apresenta os seguintes fatores que geram desvantagem:

- A rede pode ficar ociosa caso o bastão esteja com um nó (host ou máquina) que possuí dados a serem enviados;

- Não tem compatibilidade com as redes Ethernet;

- Possui um custo elevado;

- Baixa banda.

2.2 Disponibilidade Da Rede Local Para Os Usuários

Quando se ouve sobre disponibilidade imagina que se tenha uma boa comunicação entre o usuário e a rede. Em uma empresa disponibilidade poderia abordar vários sentidos, um deles seria sobre as permissões dos usuários a rede segundo as suas hierarquias, porém, nosso intuito aqui é descrever sobre a disponibilidade da rede para o usuário final.

Segundo Tanenbaum (2005) "uma vez que uma rede é instalada, esperar-se que ela funcione continuamente durante anos sem apresentar falhas no sistema." Então uma QoS (Qualidade De Serviço) em redes de comunicação costuma ser um detalhe muito importante, principalmente no âmbito operacional que remete ao desempenho fim-a-fim de cada aplicação. Obter uma qualidade de serviço adequada se torna imprescindível na operação da rede e seus componentes, tornar viável a operação com qualidade.

Disponibilidade costuma se referir ao tempo que uma rede ou serviço está disponível para o usuário, seja por conexões via Lan ou Wlan. A disponibilidade geralmente está vinculada a redundância, confiabilidade (precisão, taxa de erros, estabilidade e período entre as falhas),

capacidade de lidar com as falhas (resiliência) e à recuperação do serviço em caso de interrupções.

Disponibilidade oferta a probabilidade de que um sistema estará funcionando e pronto para ser operado em um dado instante de tempo. Ela pode se enquadrar e três classes, de acordo com a faixa de valores desta probabilidade: Disponibilidade Básica, Alta Disponibilidade e Disponibilidade Continua.

Disponibilidade Básica

Geralmente encontrada em sistemas mais comuns, sem nenhum método especial, baseando em Softwares ou Hardwares, que procure de alguma forma encobrir as possíveis falhas. Geralmente ouve-se dizer que redes desta classe costumam apresentar uma disponibilidade de 99% a 99,9%. Estes valores são metódicos e os tempos não levam em consideração os tempos de parada planejada, porém são aceitas de forma comum na área.

Alta Disponibilidade

Se adicionados mecanismos especializados de detecção, recuperação e mascaramento de falhas, isso pode ocasionar em um aumento da disponibilidade do sistema, ao ponto que este venha se encaixar na classe e Alta Disponibilidade. Nesta classe as redes apresentam uma taxa de disponibilidade 99,99% a 99,999%, podendo ficar indisponíveis por um período geralmente entre 5 minutos e uma hora em um ano de operação.

O objetivo principal da Alta Disponibilidade é buscar uma forma dos serviços prestados, mesmo que o sistema em si venha a se alterar internamente por questões de falha. Nesta situação está implícito o conceito de mascaramento de falhas, através de redundância ou replicação.

Disponibilidade Continua

Com a adição dos noves se obtém uma disponibilidade cada vez mais próxima a casa dos 100%, reduzindo o tempo de inoperância do sistema de forma que este venha a ser desprezível ou mesmo inexistente. O que nos traz a disponibilidade continua, o que significa que todas as paradas planejadas e não planejadas são mascaradas, o sistema está sempre disponível.

A figura a seguir apresenta os valores de disponibilidade anual para as três classes apresentadas.

	Disponibilidade Anual (%)	Indisponibilidade Anual	Indisponibilidade Mensal
Disponibilidade Contínua	99,9999999	0,03 segundos	0,003 segundos
	99,999999	0,32 segundos	0,026 segundos
	99,99999	3,15 segundos	0,259 segundos
Alta Disponibilidade	99,9999	31,54 segundos	2,592 segundos
	99,999	5,26 minutos	25,92 segundos
	99,99	52,56 minutos	4,32 minutos
Disponibilidade Básica	99,9	8,76 horas	43,20 minutos
	99,5	43,80 horas	3,60 horas
	99,0	3,65 dias	7,20 horas
1 ano = 365 dias = 8.760 horas = 525.600 minutos = 31.536.000 segundos; 1 mês = 30 dias = 720 horas = 43.200 minutos = 2.592.000 segundos.			

Figura 1 - Valores de Disponibilidade

Tolerância A Falhas

De acordo com Garcia et al. (2003), "na maioria dos casos, a eficiência de diversos serviços prestados está associada ao bom desempenho da rede." Para se entender corretamente do que se está falando quando se discute disponibilidade em redes de comunicação devem-se conhecer os conceitos envolvidos. Antes de tudo, deve-se entender o que é falha, erro e defeito. Estas palavras, que parecem tão próximas, na verdade designam a ocorrência de algo anormal em três universos diferentes de uma rede de comunicação.

Falhas

Uma falha acontece no universo físico, ou seja, no nível dos equipamentos. Uma flutuação da fonte de alimentação, por exemplo, é uma falha. Uma interferência eletromagnética também. Estes são dois eventos indesejados, que acontecem no universo físico e afetam o funcionamento do sistema como um todo ou de partes dela. Conforme destacam Lopes, Sauvé e Nicolletti (2003) "Infelizmente, mesmo o melhor sistema de gerência de redes não pode evitar todas as falhas. Precisamos localizar e solucionar o problema o mais rapidamente possível".

Erro

A ocorrência de uma falha pode acarretar um erro, que é a representação da falha no universo informacional. Por exemplo, um computador trabalha com bits, cada um podendo conter 0 ou 1. Uma falha pode fazer com que um (ou mais de um) bit troque de valor inesperadamente, o que certamente afetará o funcionamento normal do sistema. Uma falha, portanto, pode gerar um erro em alguma informação.

Defeito

A informação errônea, se não for percebida e tratada, poderá gerar o que se conhece por defeito. O sistema simplesmente trava, mostra mensagem de erro, ou ainda perde os dados do usuário sem maiores avisos. Isto é percebido no universo do usuário. Lopes, Sauvé e Nicolletti (2003) afirmam que "Seja qual for a razão pela qual problemas graves estão sendo descobertos através de usuários, algo deve ser feito para reverter esta situação."

Recapitulando, uma falha no universo físico pode causar um erro no universo informacional, que por sua vez pode causar um defeito percebido no universo do usuário. A tolerância a falhas visa exatamente acabar com as falhas, ou tratá-las enquanto ainda são erros. Para que uma máquina assume o lugar de outra, é necessário que descubra de alguma forma que a outra falhou. Isso é feito através de testes periódicos, cujo período deve ser configurável, nos quais a máquina secundária testa não apenas se a outra está ativa, mas também fornecendo respostas adequadas a requisições de serviço.

Um mecanismo de gerenciamento e detecção de falhas equivocado pode causar instabilidade no sistema. Como ressalta Garcia et al. (2003) "é imprescindível a utilização de recursos computacionais que proporcionem um maior dinamismo e precisão no levantamento dos dados necessários à formatação dos diagnósticos".

2.3 – Wireless

A rede wireless é uma tecnologia que transmite dados entre dois ou mais pontos distantes, através da conexão à internet, sem precisar usar fios. Essa solução compreende uma série de outras, a depender da aplicação. A mais comum e popular delas é o Wi-Fi.

Dessa forma, a rede wireless é destinada principalmente a dispositivos móveis, como notebook, smartphones e acesso a Bluetooth. Ela também permite a transmissão de dados via satélite e a eficiência de outros meios de distribuição de sinal.

O primeiro fato a se considerar na infraestrutura wireless é o custo de ausência de recurso. Muitas vezes levamos em consideração apenas o investimento em ter a comodidade X ou Y, e nos esquecemos de todo o gasto gerado por não a ter. Assim, ficar sem wireless é perder produtividade, além de correr o risco de deixar informações incompletas.

Mobilidade

Essa talvez seja o maior benefício da rede sem fio. Afinal, ela é capaz de levar conexão para qualquer terminal e espaço físico.

Em outras palavras, você não precisa estar necessariamente no escritório para buscar informações do servidor corporativo, mas pode fazer isso de casa, na rua e até em outro país, que vai conseguir mandar sua mensagem, desde que haja um sinal Wi-Fi.

Gerenciamento

A ferramenta é gerenciada a partir de um painel via internet, muito importante para a infraestrutura de TI empresarial. A partir dele é possível detectar informações cruciais para a

gestão de conexões, como o status da rede, os pontos de acesso e pessoas conectadas em tempo real. Além disso, o painel também permite a identificação de problemas com mais agilidade.

Rastreabilidade

Com uma rede wireless, a TI consegue rastrear o comportamento dos usuários e suas redes sem fio, evitando atitudes que possam ferir a segurança.

Além destas vantagens apresentadas temos outras como: Criptografia, escalabilidade, relatórios, hotspot para visitantes etc. Mas tambem existe desvantagens como: a perca na velocidade e a segurança, pois as redes sem fio estão vulneráveis a interferências de sinais de rádio ou qualquer outro dispositivo eletrônico que opere na mesma frequência. Trocando em miúdos, elas podem ser interceptadas por usuários não autorizados, e para evitar que isso ocorra a gestão necessita de um excelente protocolo de segurança, incluindo tanto as ações de prevenção como recuperação de desastres.

CAPITULO 03 – CERTIFICAÇÃO DE REDE

A certificação de rede são testes realizados para se obter uma comprovação de qualidade e funcionamento dos cabos. Basicamente, eles mostram se a rede está disponível para uso ou não e avalia a qualidade do cabeamento para definir se está dentro dos parâmetros desejados.

Para realizar estes testes são usados equipamentos específicos adequadamente calibrados para identificar falhas, conforme a regulamentação das normas TIA/EIA 568B (A norma TIA/EIA 568B especifica os requerimentos mínimos para os componentes de fibra óptica utilizados no sistema de cabeamento como: cabos, conectores, hardware de conexão, patch cords e equipamentos de teste e medição em campo). Após os testes de certificação, gera-se um relatório com o registro de toda a analise realizada. Esse é um documento importante que deve ser anexado ao projeto da instalação. Dessa forma os dados poderão ser usados futuramente com comparativos com novos testes, que podem incluir:

- Atenuação
- Comprimento do cabo
- Pinagem dos cabos
- Resistencia dos cabos
- Perda e retorno de dados
- Atraso de propagação
- Mapeamento dos condutores

Os testes podem ser passivos e ativos, de acordo com o objetivo em questão.

3.1 – Testes passivos

Estes testes são realizados mesmo que a rede não apresente nenhum tipo de problema. Assim, eles funcionam de modo preventivo e felizmente são muito praticados. Os passivos podem ser estáticos ou dinâmicos:

- **Estáticos:** Seguem parâmetros extremamente rígidos que não aceitam nenhum tipo de reprovação, pois precisam atender a padrões exigidos em laboratórios, institutos de pesquisas, fabricas, instituições de ensino etc., e esses padrões são muito elevados.
- **Dinâmicos:** Incluem cerca de 16 testes de campo obrigatórios segundo a norma EIA/TIA 568B.1, tais como wiremap, attenuation, return loss e propagation delay.

3.2 – Testes ativos

Os testes ativos são realizados quando se deseja descobrir as causas de um mau funcionamento, como lentidão na rede. Com redes cada vez melhores e profissionais mais capacitados, esse tipo de teste passa a ser menos frequente.

Assim, quaisquer aspectos internos ou externos à instalação que podem afetar a qualidade da rede são identificados e corrigidos para garantir a eficiência operacional da infraestrutura de TI. Mas será que esses testes são mesmo necessários? Entenda os benefícios!

3.3 - Benefícios da certificação de rede

- **Agilidade no diagnóstico**
  Ao surgirem falhas, a certificação de rede pode checar todos os pontos de a infraestrutura e, de modo rápido e eficiente, detectar onde está o problema. Dessa forma, os chamados do departamento de TI são prontamente atendidos e de modo muito mais eficaz.

- **Respaldo documental de qualidade**
  Como vimos, os testes de certificação de rede são capazes de gerar relatórios detalhados que constituem uma parte importante dos documentos que acompanham as instalações.
  São dados que servirão de base para a tomada de decisão.

- **Possibilidade de ampliar a garantia ao cliente**
  Com a facilidade de diagnosticar a origem das falhas e assegurar a qualidade das instalações, é possível proporcionar ao cliente um prazo maior de garantia. Assim, a empresa se torna mais competitiva e o cliente ganha com um período de suporte mais interessante.

- **Redução de custos**
  Realizar testes para monitorar a qualidade da rede e prevenir a ocorrência de falhas graves é melhor do que remediar com reparos muito mais onerosos para o negócio.
  Além disso, o tempo em que a rede fica indisponível ou em mal funcionamento reduz substancialmente a produtividade. O resultado é queda de eficiência operacional e de receita. Sem falar na perda de credibilidade aos olhos dos clientes.
  As vantagens da certificação de rede são inúmeras. Sem dúvida ela é indispensável para o setor de TI garantir maior disponibilidade dos serviços e eficiência nas demais operações do negócio.

CAPITULO 04 – LAYOUT DE REDE

O layout tem como objetivo amplia a qualidade e eficiência de um processo produtivo, que está relacionado à maneira como os equipamentos que as pessoas distribuem em um espaço físico.

Ter um layout bem-elaborado é uma condição imprescindível para se alcançar bons resultados, ampliando o potencial de produção e reduzindo gastos desnecessários.

PROJETO LÓGICO

Para garantir um bom fluxo de trabalho, optou-se então pela passagem das eletrocalhas em uma altura que permitisse que qualquer alteração feita não prejudicasse a disposição de passagem dos cabos de redes. 34 setores distribuídos em uma planta baixa, conforme mostra a (figura 01). Para o desempenho de variadas funções possui vários dispositivos finais entre computadores, impressoras, câmeras de videomonitoramento etc.

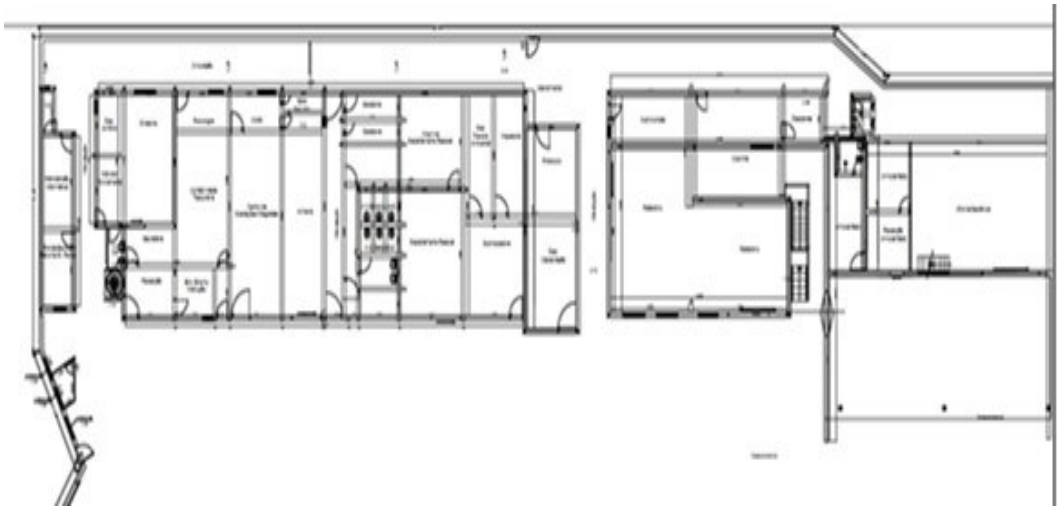


Figura 2 - 34 Setores

Diante disso, com o objetivo de facilitar eventual manutenção e proximidade dos switches de 16 portas em relação ao switch de 48 portas e ainda de forma a atender todos os departamentos eles foram então distribuídos conforme a figura abaixo.

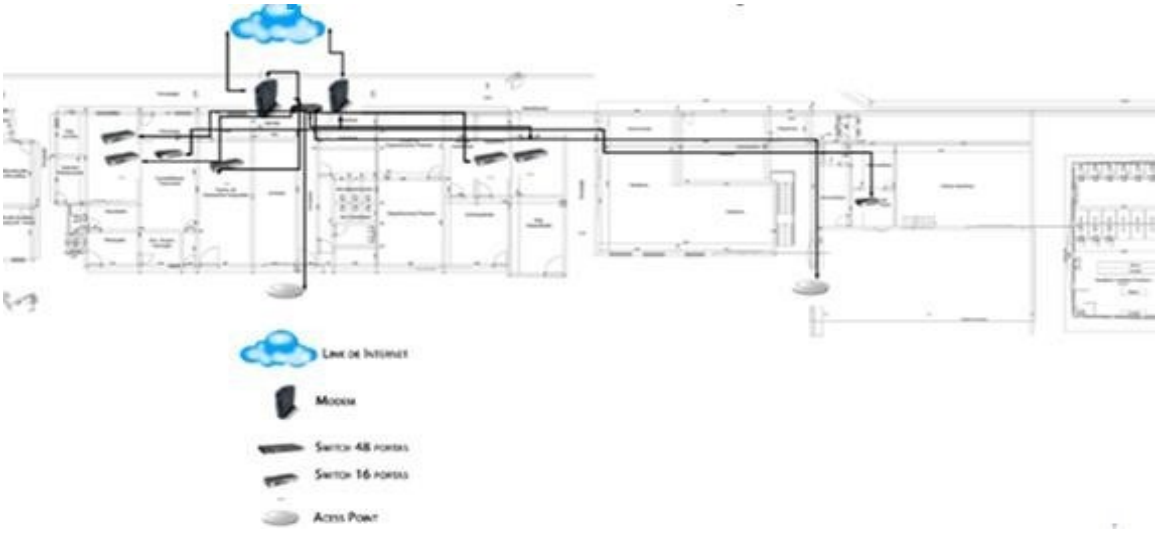


Figura 3 - 34 Setores II

4.1- Topologias de rede

Topologia utilizada

Uma rede é um conjunto de equipamentos interligados por um sistema de comunicação. Esses aparelhos são orientados por regras para o compartilhamento de dados e recursos, tanto físicos como lógicos, entre si.

A configuração de um computador a uma determinada rede dependerá da noção de como ela é organizada. Para isso, a topologia de rede funciona como um mapa que indica os fluxos de informação organizados em uma rede.

Topologia de rede física

A topologia física trabalha o layout de distribuição da rede. Ela inclui toda a descrição da estrutura física, como a posição das máquinas, roteadores os hubs e os switches, bem como a forma que os cabos serão conectados. Há várias opções de topologia física, confira cada uma delas a seguir.

Definindo a topologia de rede estruturada

Outro aspecto fundamental do projeto de cabeamento estruturado é a escolha da topologia. Ou seja, do layout ou forma de organização dos cabos e equipamentos que a rede terá.
Normas brasileiras e internacionais determinam os requisitos ideais para diferentes topologias de rede estruturada. Os layouts de cabeamento estruturado mais conhecidas são:

1.Topologia Barramento: é uma rede com vários pontos, onde os dispositivos (computadores, impressoras, máquinas etc.) são conectados por um cabo comum ou por links de comunicação.

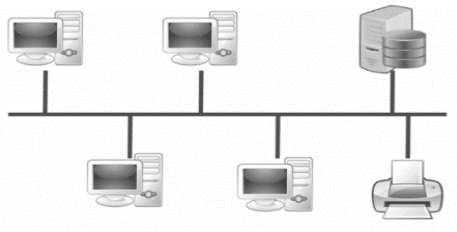
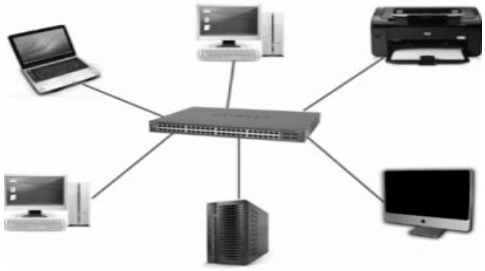


Figura 4 - Topologia Barramento



2.Topologia Estrela: neste *layout* todos os dispositivos de uma rede de cabeamento estruturado são conectados a um único controlador: um servidor com um *switch* distribuidor do sinal de informação.

Figura 5 - Topologia Estrela

3. Topologia Anel: os computadores e outros dispositivos são conectados entre si, formando um circuito fechado. Cada estação de trabalho tem que processar o sinal e repeti-lo ao computador seguinte.

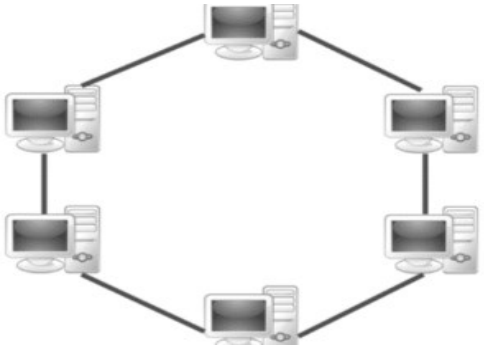


Figura 6 - Topologia Anel

4. Topologia Ponto a ponto (Peer to Peer): esse layout interliga apenas dois computadores por meio de um cabo crossover. O crossover é um par metálico específico para essa finalidade. Ele deve possuir uma ponta no padrão EIA/TIA 568 A e outra no padrão EIA/TIA 568 B.

Figura 7 - Topologia Ponto a Ponto

5. Backbone (Espinha Dorsal): a rede é dividida em vários segmentos conectados a servidores. Esses servidores são interligados a backbones. Pode haver vários backbones, e somente os servidores se ligam a eles, enquanto os computadores se ligam aos servidores. É a topografia utilizada em redes grandes e complexas, como a de uma universidade, órgão público ou grande empresa.

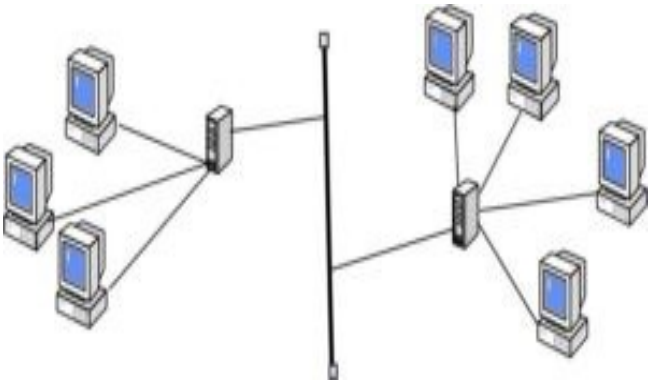


Figura 8 - Backbone

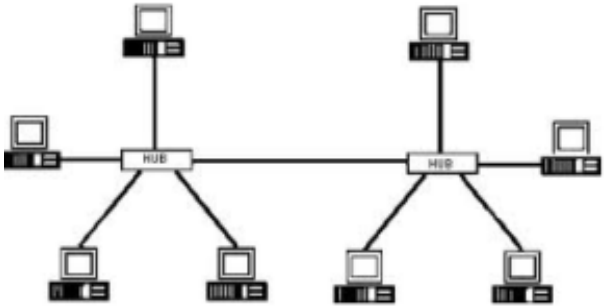


Figura 9 - Estrela Hierárquica

6. Estrela hierárquica (árvore): é uma interligação de várias redes com sub-redes. As sub-redes são conectadas por concentradores. E os vários concentradores se ligam a um concentrador central. Comum em edifícios com grandes redes comerciais.

7. Malha (Mesh): na topologia, os cabos interligam todos os pontos ou nós. Todos se comunicam entre si e há boa tolerância a falhas.

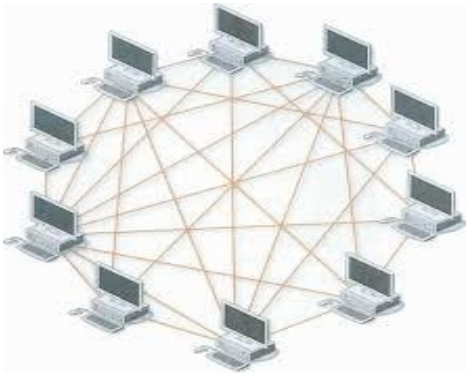


Figura 10 - Malha (Mesh)

Figura 11 - Wireless

8. Wireless (sem cabos): os dispositivos enviam sinais entre si sem a presença de cabos.

9. **Topologia Híbrida:** combinação de dois ou mais tipos de rede. É útil, por exemplo, em casos de *retrofit*, ou seja, adequação da rede a uma infraestrutura já existente. Ou para a ampliação de uma rede.

Figura 12 - Topologia Hibrida

Topologia utilizada

Nesse sentido, para garantir uma melhor gerenciabilidade da rede, foi empregada a topologia denominada árvore, conforme mostra a figura 6, nomenclatura adotada pelos autores, que explicam se tratar de uma variação da topologia estrela.

Topologia em árvore ou Topologia Hierárquica, ou Rede em Árvore ou Rede Hierárquica é uma topologia física baseada em uma estrutura hierárquica de várias redes e sub-redes. O nível mais alto, está ligado a vários módulos do nível inferior da hierarquia. Estes módulos podem ser eles mesmos conectados a vários módulos do nível inferior em um esquema semelhante ao desenho de uma árvore. Esta topologia facilita a manutenção do sistema e permite detectar avarias com mais facilidade, em comparação às topologias em Barramento e Anel. É mais utilizada em Redes Locais (LAN) e em Redes Campus.

São basicamente barras interconectadas, onde ramos menores são conectados a uma barra central, por um ou mais Hub's, switch e repetidores que interconectam outras redes. No geral, as redes em árvore, irão trabalhar com uma taxa de transmissão menor do que as redes em barra comum. Há cuidados que devem ser tomados, pois a cada ramificação irá propagar-se a dois caminhos distintos, exceto se os caminhos estejam perfeitamente casados; as velocidades de propagação e os sinais refletidos serão distintos uns dos outros. A topologia em árvore é baseada em uma estrutura hierárquica de várias redes e sub-redes.

A distância máxima sem amplificação é de apenas 100m (dependendo do cabo usado). Tem Dependência do nó central, se esta falha, a rede fica inoperante, o número de portas de um concentrador é limitado e quando for atingido o limite de portas disponíveis é necessário adquirir outro e interligá-lo com o existente, contando com um ou mais concentradores que ligam cada rede local e existente a outro concentrador que interliga todos os outros concentradores.

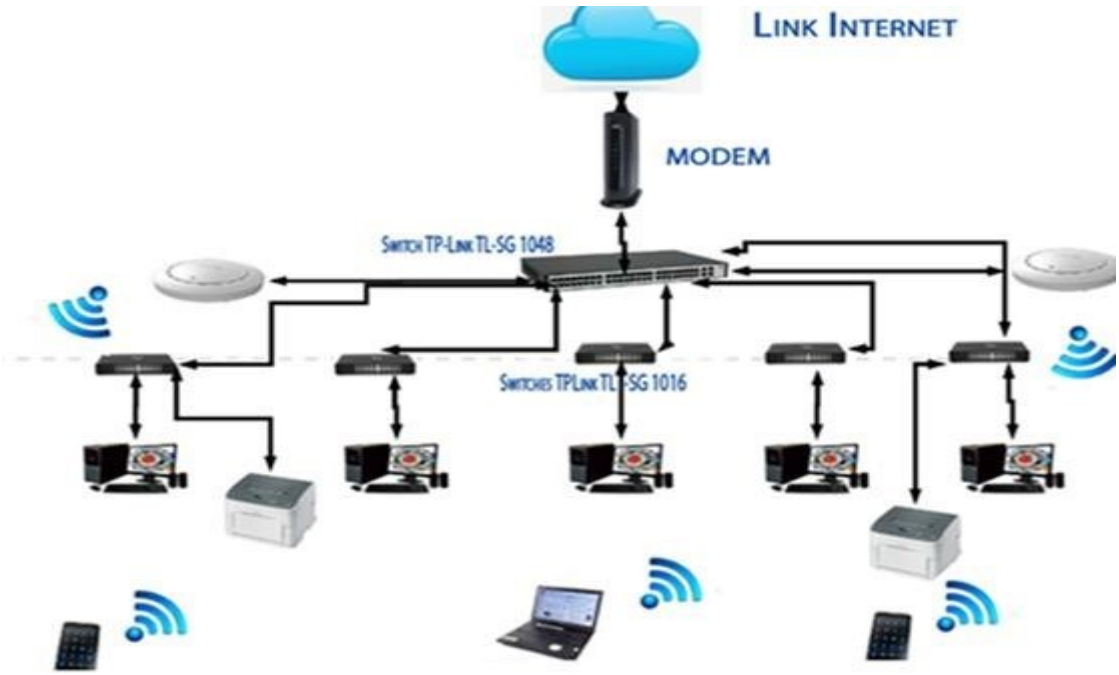


Figura 13 - Topologia Utilizada

Assim ao analisar o ganho de confiabilidade, já que permite que o administrador possa identificar rapidamente uma eventual falha no tráfego de dados, permitindo ainda um isolamento daquele setor inoperante, sem prejudicar os demais até que seja feito o devido reparo, tal como a substituição de um switch, por exemplo.

"A vantagem principal desse tipo de rede é a confiabilidade, pois se um desses segmentos 'ponto a ponto' tiver uma falha, afetará só os dois nós naquele enlace físico. Outros usuários de computador na rede continuam operando como se aquele segmento fosse inexistente." Fato esse, já percebido na prática.

4.2 - Escolha do Material

Com o objetivo de definir o material a ser empregado, obviamente foi considerado o valor deles, pois se trata de uma empresa de porte alto.

Dessa forma, após vários orçamentos realizados, verificou-se quais os mais vantajosos em vários requisitos, inclusive o financeiro, para aquisição. Contudo, sem renunciar à qualidade deles, já que de nada adiantaria investir em utilizar materiais que de fato, pouca (ou nenhuma) mudança iria trazer, efetivamente na prática. Assim, a escolha dos materiais foi resultado de uma equação que envolveu os custos que se teria e a qualidade esperada, para então garantir o interesse da empresa. Nesse sentido, apresenta-se os materiais, dentre outros, utilizados no projeto.

Cabo de Rede

Para a nova rede no prédio foram empregados cabos de rede UTP.

O cabo UTP (*Unshielded Twisted Pair*) - par trançado sem blindagem é atualmente o cabo mais utilizado em redes de computadores. O cabo UTP tem como vantagens ser de fácil manuseio e instalação, além de permitir taxas de transmissão elevadas. O alto desempenho alcançado em termos de qualidade pelos cabos UTP, aliado ao baixo custo de aquisição e instalação deles nas redes de computadores, motivou a padronização tanto por parte dos projetistas quanto dos fabricantes que os utilizam em seus projetos e precisam garantir a confiabilidade e o desempenho do cabeamento.

Com o objetivo de obter uma taxa de transmissão de dados satisfatória optou-se pelo emprego de cabos de rede categoria Cat6, já que ele possui taxa de transferência melhor que o cat5. Para utilização do cabo categoria 6 verifica-se a preferência do mesmo em substituição do cabo de rede cat5.

Obs. Os cabos UTP foram evoluindo nas últimas décadas, a partir do final dos anos 1980, e ganha uma classificação baseada na categorização desses cabos. quanto maior a categoria, maior a qualidade do cabo, suportando maior taxa de dados (*bits* por segundo), em consequência de possuir uma maior largura de banda (*Hertz*).

Em seguida, apresentam a categorização do cabo UTP, conforme a figura abaixo

Cat 5	até 100 Mbps	100Base-T (FastEthernet)
Cat 5e	até 1 Gbps	1000Base-T (GigaEthernet)
Cat 6	até 1 Gbps	Cabos Blindados (Alguns Modelos)
Cat 6a	até 10 Gbps	Cabos Blindados
Cat 7	até 10 Gbps	Cabos Blindados
Cat 7a	até 40 Gbps	Cabos Blindados
Cat 8	até 40 Gbps	Em análise para definição

Figura 14 - Categorização Cabo UTP

Switches

Não há definição clara dos tipos de *switches,* já que essa definição varia de acordo com o fabricante do equipamento, mas é possível, ainda observar as seguintes características que auxiliam na classificação deles: "Velocidade do barramento interno (*backplane*), Velocidade e tipo de portas, tamanho do *buffer* interno para pacotes, Mecanismos de *forwarding* e uso de VLAN".
Com a utilização de cabos UTP Cat6, permite uma maior transferência de dados, consequentemente deve-se utilizar *switch* que possa suportar essa vazão. Nesse sentido, necessário utilização de *switch* com padrão *Giga Ethernet*: "Na atualidade o padrão *Giga Ethernet* está se tornando comum em redes locais utilizando o cabo de par trançado (UTP) categoria 5 ou superior.
Isso possibilita que o segmento do *switch* possa funcionar a 1 Gbps."

Dessa maneira, foi utilizado no projeto um *switch* de 48 portas modelo **Switch Hp 48 Portas 10/100/1000 + 4 Jl814a** na sala do servidor, e nos departamentos do prédio o *switch* modelo TP-Link TL – SG1016d que, de acordo com o fabricante, apresentam as características que vão ao encontro do objetivo do projeto que é dar uma maior vazão na taxa de transferência de dados, permitindo uma rápida resposta após a análise deles. Assim, as características são:

Switch de 48 portas **Switch Hp 48 Portas 10/100/1000 + 4 Jl814a**: não possui complexidade no gerenciamento sem necessidade de configuração, o equipamento detecta automaticamente a velocidade do *link* do dispositivo de rede (10, 100 ou 1000Mbps) e se ajusta para melhorar o desempenho assegurando assim uma transmissão de dados confiável.

Switch Gigabit de **16 portas TP-Link TL – SG1016d**: além de possuir a configuração de autoajuste descrita no modelo anterior, possui também uma inovação na tecnologia que de acordo com o fabricante ajuda a economizar em até 15% de consumo de energia elétrica.

Racks

Os *switches* antigos no textel estavam dispostos sem proteção alguma sobre a laje do prédio contribuindo ainda mais para uma rede ineficaz. Para sanar esse problema foram adquiridos *racks* para acomodação dos referidos *switches*, com as seguintes medidas:

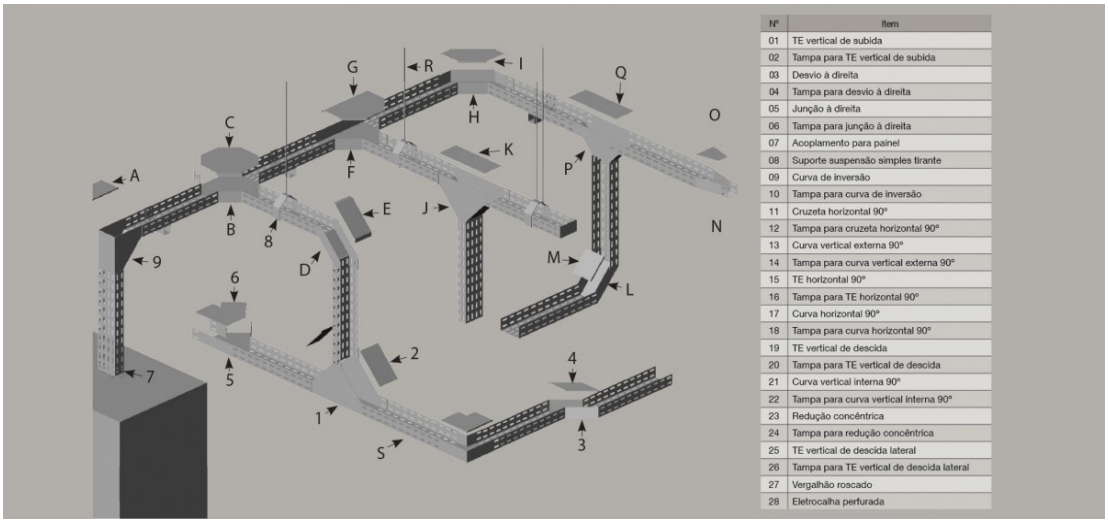
01 *Rack* de piso; 01 *Rack* de 19U; 05 *Racks* de 5U.

A norma mencionada trata exclusivamente da padronização dos *racks* (gabinetes), painéis e periféricos utilizados internamente em um cabeamento estruturado; os equipamentos contemplados na norma são: *patch panel*, guia de cabo, *rack* torre, *rack* fechado, bandeja frontal, bandeja deslizante, parafuso porca gaiola e *switches*.

A figura abaixo apresenta a imagem de um parafuso porca gaiola citado.

Figura 15 - Parafuso Porca Gaiola

Eletrocalhas



Nº	Item
01	TE vertical de subida
02	Tampa para TE vertical de subida
03	Desvio à direita
04	Tampa para desvio à direita
05	Junção à direita
06	Tampa para junção à direita
07	Acoplamento para painel
08	Suporte suspensão simples tirante
09	Curva de inversão
10	Tampa para curva de inversão
11	Cruzeta horizontal 90°
12	Tampa para cruzeta horizontal 90°
13	Curva vertical externa 90°
14	Tampa para curva vertical externa 90°
15	TE horizontal 90°
16	Tampa para TE horizontal 90°
17	Curva horizontal 90°
18	Tampa para curva horizontal 90°
19	TE vertical de descida
20	Tampa para TE vertical de descida
21	Curva vertical interna 90°
22	Tampa para curva vertical interna 90°
23	Redução concêntrica
24	Tampa para redução concêntrica
25	TE vertical de descida lateral
26	Tampa para TE vertical de descida lateral
27	Vergalhão roscado
28	Eletrocalha perfurada

Figura 16 - Eletrocalhas

A quantidade de cabos de rede cat5 utilizada no prédio cresceu exponencialmente e de forma desordenada haja vista o aumento significativo de dispositivos finais pelos usuários. Diante desse aumento, houve a distribuição de cabos de forma a atender rapidamente as necessidades, contudo a falta de planejamento, a falta de um local adequado para disposição dos referidos cabos resultou em um emaranhado de cabos que prejudicou até mesmo uma simples identificação deles, não permitindo assim, uma eficiente manutenção.

Visando eliminar essa situação, foi instalado eletrocalhas metálicas ao longo da coluna principal, para uma correta distribuição nos respectivos departamentos e com o intuito de não se deixar cabos expostos também foram utilizadas canaletas plásticas nos setores.

Dessa forma, a eletrocalha, foi então fixada na viga principal da estrutura predial com o objetivo de melhor distribuição dos cabos conforme figura abaixo.

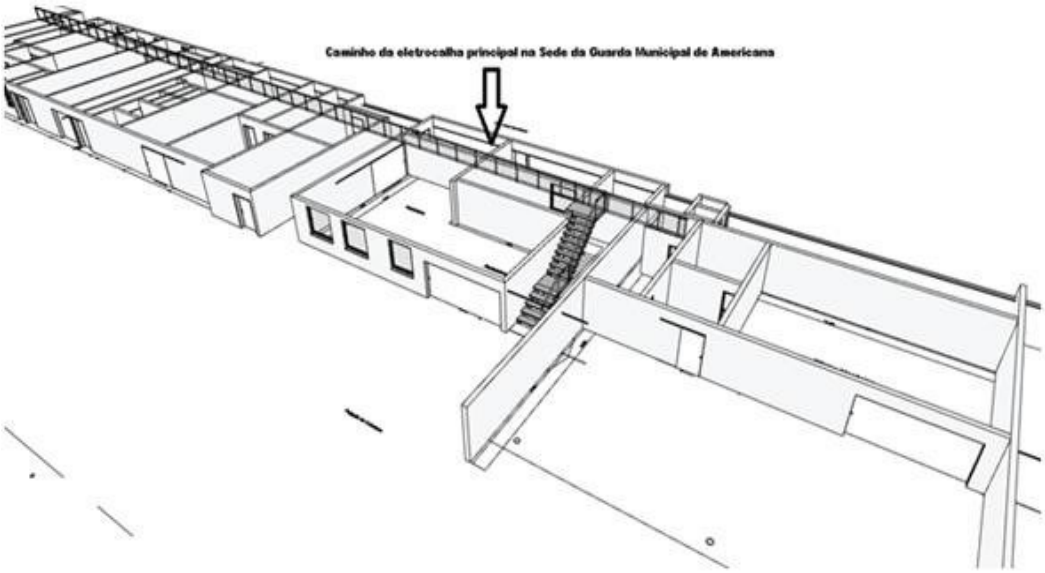


Figura 17 - Estrutura Predial

4.3 - Implantação do Projeto

Houve a fixação das eletrocalhas, conforme já descrito, na viga principal utilizando suporte tipo "mão francesa" para suportar a estrutura sem que haja o risco de envergadura com o peso, fixado então com parafusos.

Após a fixação iniciou-se a passagem do cabo de rede Cat6 pelas mesmas de modo que eles ficaram estendidos no interior da eletrocalha sem sofrer qualquer tipo de torção, que poderia resultar no rompimento dos mesmos e consequente perda de sinal.

Na sala do servidor foi fixado o rack de 19 U com a instalação do switch de 48 portas **Switch Hp 48 Portas 10/100/1000 + 4 Jl814a**. Dessa sala, os cabos de rede Cat6 seguem pelas eletrocalhas e descem pelo perfilado perfurado até as respectivas salas, sendo os mesmos conectados aos switches de 16 portas **TP-Link TL – SG1016d**, que foram fixados em miniracks de 5U. Dos miniracks o cabo de rede segue por canaleta de PVC até o equipamento.

Após a crimpagem dos cabos de rede Cat6 com a utilização de conectores RJ-45 Cat6, foi efetuado o devido teste para verificação de crimpagem utilizando um testador de cabos para prevenir qualquer tipo de mau funcionamento deles. Feito esses procedimentos, os dispositivos finais (*desktops*/impressoras) foram conectados à nova rede e a seguir houve a retirada de todos os cabos de categoria Cat5, retirando dessa forma o aspecto até então apresentado de uma infraestrutura desordenada com cabeamento exposto e instalado sem observância de qualquer tipo de norma, pois, em muitas das vezes, a antiga rede estava instalada juntamente com cabos de energia, ocasionando o chamado ruído, que causam danos significativos a transmissão de dados, vários tipos de ruídos que prejudicam o desempenho da rede, tais como térmicos, impulsos etc. No caso da antiga rede, o que se verificava comumente era o ruído por impulso, "O ruído por impulso é um pico (um sinal com grande energia em um curtíssimo espaço de tempo) proveniente de cabos de força, relâmpagos e assim por diante."

Verifica-se então que esse tipo de ruído prejudica demasiadamente o desempenho da rede, que sofria constantes interrupções na transmissão de dados ocasionando em muitas das vezes a interrupção total dos serviços que necessitavam de uma rede estável e funcionando.
Outro problema enfrentado na antiga rede estava relacionado à disposição dos *switches* utilizados que além de não suportar a transmissão de dados *gigabit*, estavam colocados sem qualquer proteção e em qualquer lugar em quantidade desconhecida que, até mesmo, surpreendeu a existência de *switch* conectados em outros *switches* causando o efeito de cascateamento.
É a simples interconexão de dois ou mais *switches* em série. Para estas conexões entre os *switches*, são empregadas portas ou interfaces convencionais; as mesmas portas/interfaces que são utilizadas para conectar qualquer dispositivo cliente (ex: computadores, *laptops*, roteadores, *firewalls*, pontos de acesso etc.).
Obviamente que essa conexão prejudica o desempenho de transmissão com vem se enfrentados, "o maior problema com relação ao cascateamento está justamente relacionado ao desempenho das conexões entre os *switches* envolvidos. Quanto maior for a quantidade de *switches* em uma conexão em paralelo, maior será o problema de escalabilidade."

4.4 - Escalabilidade

Uma infraestrutura de rede deve possuir uma característica que permita um aumento em dispositivos finais sem que influencie negativamente no desempenho dos já existentes.

Escalabilidade: Em telecomunicações, infraestrutura de tecnologia da informação; e na engenharia de *software*, escalabilidade é uma característica desejável em todo sistema, rede ou processo, que indica a habilidade de manipular uma porção crescente de trabalho de forma uniforme, ou estar preparado para crescer. Por exemplo, isso pode se referir à capacidade de um sistema em suportar um aumento de carga total quando os recursos (normalmente de *hardware*) são requeridos. A escalabilidade é assunto extremamente importante em sistemas eletrônicos, bancos de dados, roteadores, redes de computadores etc. Um sistema cujo desempenho aumenta com o acréscimo de *hardware*, proporcionalmente à capacidade acrescida, é chamado "sistema escalável".

Observando essa característica foi desenvolvida então a infraestrutura, com a utilização de *switches* capazes de suportar a inclusão de novos equipamentos permitindo que os já existentes continuem com o desempenho inicial ou que pelo menos tenha o mínimo de impacto sofrido.

Essa medida além de desejável, é por obvio necessária, pois uma reestruturação demanda investimento e não tem sentido em montar uma rede que atenda somente as necessidades atuais.

Assim, visando a agregação de novos equipamentos para um melhor atendimento dos colaboradores foi desenvolvida a rede implantada com o objetivo de evitar o mínimo de desperdício de tempo, custos, mão de obras etc. Aliás, nesse aspecto é preciosa. "Escalabilidade O *software* que suporta o *Data Warehouse* deve ser capaz de manipular o crescimento do uso e a mudança na forma de usar. A habilidade de escalabilidade significa proteger o investimento em pessoas, aplicações e *software*."

Partindo então dessa premissa, qual seja, na proteção do investimento feito para a implantação dessa nova rede, projetou-se a mesma com capacidade deste aumento sem que haja impacto negativo significativo na existente, pois do contrário, ou seja, se assim não fosse, de nada adiantaria ter um investimento atual e em um curto espaço de tempo ter que trocar toda a rede, como aconteceu com a atual, para que novos equipamentos fossem instalados para que entrassem em funcionamento, teria aí um desperdício do dinheiro, que é algo inadmissível quando se trata do orçamento.

CAPÍTULO 5 – Endereçamento Lógico da Rede Local

Você já se perguntou como as informações que vem da Internet, chegam ao seu computador ou celular?

Para isso, precisamos entender um pouco sobre os endereços de rede!

Para explicar o que são endereços de rede, vamos fazer a seguinte comparação:

Imagina que um amigo seu queira te enviar uma carta, e para isto, ele precisa incluir informações como o nome dele, endereço dele e depois, o seu nome e o seu endereço. Com essas quatro informações, a carta vai conseguir chegar até você.

Talvez você se pergunte, qual a relação disso com o que ocorre na Internet?

Vamos imaginar que o Google esteja te mandando o resultado de uma pesquisa para o seu celular e da mesma forma que o exemplo anterior, para você receber uma mensagem do Google é preciso colocar endereço nessa mensagem.

Ao contrário da situação da carta, em que precisamos incluir nome dos envolvidos e os endereços das ruas, para receber uma mensagem da Internet, ela precisa conter dois endereços:

1º Endereço lógico - Também conhecido como IP.

2º Endereço físico – Também chamado de MAC, que funciona como se fosse o "RG" do seu celular.

Vale lembrar que o Google vai utilizar apenas o seu endereço IP para encaminhar a mensagem até você, já o endereço MAC vai ser utilizado pelo seu roteador para encaminhar a mensagem até o seu celular.

Voltando ao exemplo da carta, a mensagem ela é encaminhada até o Correio para chegar na porta da sua casa e de forma similar, na Internet a mensagem é encaminhada por diversos roteadores até chegar no seu roteador usando o endereço IP. Com a carta na porta da sua casa, o entregador toca a campainha e entrega a carta para alguém da casa, se essa pessoa não conhecer o destinatário, ela avisa a todos que chegou uma carta e consequentemente, todos da casa verificam se a carta é para algum deles e se for, a carta é aceita.

Da mesma forma, quando a mensagem do Google chega no seu roteador e ele não souber qual o MAC do seu celular, ele faz uma pergunta – também chamada de Broadcast – que é emitida para todos os dispositivos conectados ao roteador, para descobrir qual o MAC corresponde ao IP do destino da mensagem.

Sabendo qual o MAC do seu celular, seu roteador irá finalmente encaminhar a mensagem até seu celular, utilizando seu endereço IP e o endereço MAC.

Vamos agora descobrir qual que é o endereço MAC e o endereço IP de um computador usando o Windows!

Bom, para descobrir seu endereço IP ou seu endereço MAC é bem simples. A primeira coisa que você vai fazer na barra de pesquisa é digitar “CMD” ou “*Prompt de Comando*”,

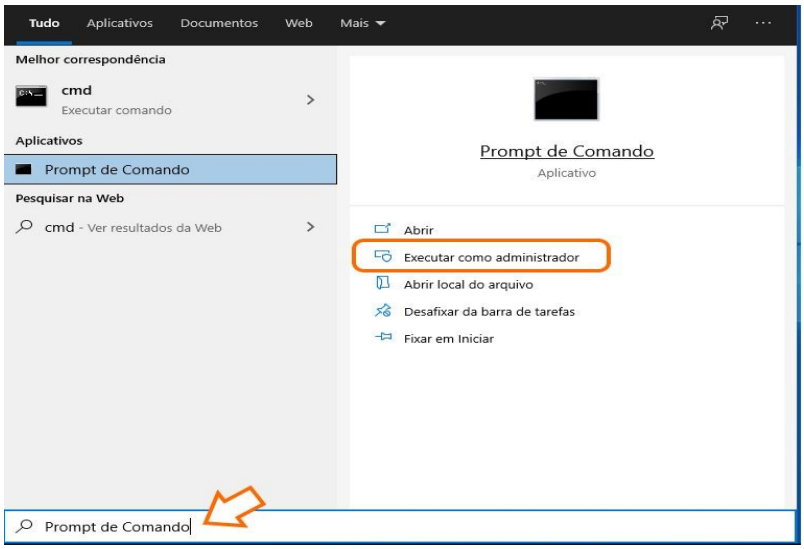


Figura 18 - Abertura CMD

em seguida, vai aparecer uma tela preta e você vai digitar o seguinte comando > config/all e depois pressionar “*Enter*”.

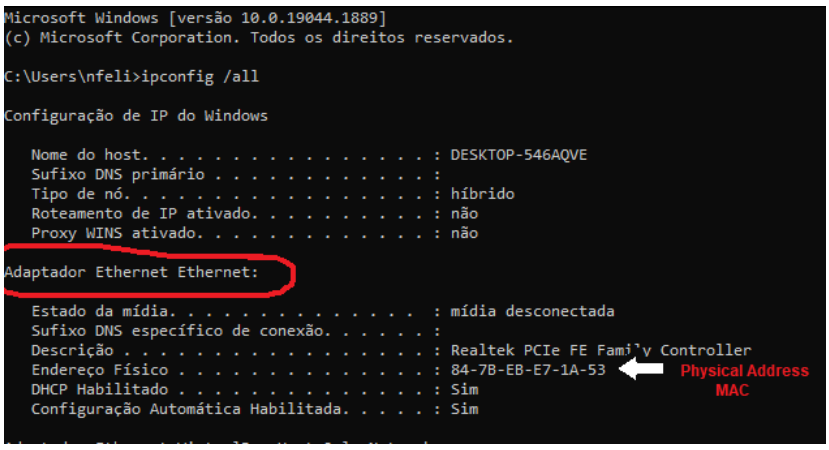


Figura 19 - CMD ipconfig

Observe que aparece várias informações sobre a sua rede, mas o que vai importar para nós, são as informações que estão no “*Ethernet adapter Ethernet*”. Teremos também o “Physical Address” que é o endereço MAC e você vai ter o “*IPv4 Address*” que é o IP rede local.

Desta forma, é assim que você descobre o endereço MAC e endereço IP!

5.1 – Básico de redes: endereço MAC e endereçamento IP

Dentro do básico de redes, existe uma forma de entender os conceitos para situações mais comuns do dia a dia. Por exemplo, temos o endereçamento MAC e o endereçamento IP. O endereço MAC cuja sigla significa Media Access Control, traduzindo para o português é Controle de Acesso de Mídia, pode ser considerado como o documento de identificação de um dispositivo de rede como NVRs, câmeras, switches, computadores, roteadores, smartphones, tablets, impressoras de rede e diversos outros equipamentos que usam comunicação em rede. O

MAC é uma identificação permanente, seria como uma impressão digital de uma pessoa. Cada dispositivo de rede possui um endereço MAC com 12 caracteres. Eles serão usados “pelo resto da vida”:

Exemplo: 00:1e:c2:9e:28:6b, os três primeiros pares são emitidos pelo fabricante e, por isso, são permanentes. São conhecimentos como Identificador organizacionalmente exclusivo (OUI) e é possível que o fornecedor possua mais de um identificador. Os três últimos pares fazem parte do próprio dispositivo.

O endereço MAC é usado para permitir e identificar os dispositivos da rede, justamente por ser estático, mesmo o endereço IP não é conhecido. O que funciona para detectar a localização de um equipamento específico. Também pode ser utilizado para conectar ou restringir endereços e outras variáveis.

Endereço IP é um endereço exclusivo feito para identificar um dispositivo na Internet ou em uma rede local. Em uma rede, informações são enviadas para os dispositivos, elas contêm as informações de localização e torna o dispositivo acessível para comunicação. IP vem do inglês "Internet Protocol" (protocolo de rede) que consiste em um conjunto de regras que regem o formato de dados enviados pela Internet ou por uma rede local.

A Internet precisa de um meio de distinguir diferentes computadores, roteadores e sites. O endereço IP providencia isso, além de ser uma parte essencial do funcionamento da Internet.

5.2 - Endereço lógico e físico no sistema operacional

O **endereço lógico** é criado pela Unidade Central Processamento (CPU) durante a execução de um programa. O endereço lógico não existe fisicamente, mas também é conhecido como Endereço Virtual. Este endereço é usado como referência para acessar o local da memória física pela CPU. A um termo chamado Espaço de Endereço Lógico que é usado para o conjunto de todos os endereços lógicos gerados por uma perspectiva de um programa. Para mapear o endereço lógico existe um hardware chamado Memory Management Unit (MMU).

Endereço físico serve para identificar uma localização física dos dados necessários em uma memória. O usuário nunca irar lidar diretamente com o endereço físico, mas pode acessá-lo por meio de seu endereço lógico correspondente. O programa que está rodando neste endereço lógico precisa de memória física para sua execução, portanto, o endereço lógico deve ser mapeado para o endereço físico pela Memory Management Unit (MMU) antes de serem usados. O termo Espaço de endereço físico é usado para todos os endereços físicos correspondentes aos endereços lógicos em um espaço de endereço lógico.

*5.3 - C*ontrole de acesso à internet

“O controle de acesso à internet permite que uma empresa restrinja o acesso a sites, conteúdo impróprios ou o uso de programas suspeitos, que possam representar riscos para a sua infraestrutura de TI. É uma medida de segurança mais restritiva que deve ser desenvolvida tomando todos os cuidados necessários para não atrapalhar o desenvolvimento das atividades na empresa.” (Microcity, 2020)

A internet está presente em todos os lugares e no mundo corporativo contemporâneo. O acesso mundial de computadores vem sendo usado para inúmeras funções em diversos setores. E para assegurar que o melhor da internet seja aproveitado sem que o pior prejudique o seu negócio, é importante investir em uma segurança de sua rede e estabelecer um controle de acesso à internet.

Sendo uma empresa pequena ou de grande porte, é impossível imaginar um negócio que não precise da internet em seus processos. Desde responder clientes por e-mails, Whatsapp, Telegram, ou usar a maquininha de cartão ao armazenamento de dados em nuvem e IoT, a internet está presente.

Mas ao mesmo tempo que a internet é o meio para grandes soluções corporativas, se usado de forma errada ou descontrolada pode tornar toda a rede corporativa vulnerável, tornando a principal porta de entrada de ameaças à segurança da informação de uma empresa. E-mails fraudulentos, downloads de arquivos com origem não confiável e acessos a sites suspeitos ou indevidos são alguns dos caminhos mais usados por criminosos para ataques cibernéticos.

O controle de acesso à internet vem se tornando uma das ferramentas mais utilizadas para combater alguns riscos oferecidos por essas ameaças, que deve ter também outros recursos como aliado na área de segurança da informação.

Caso a empresa tenha uma política mais restritiva, o controle de acesso à internet também ajuda a diminuir o acesso a contas de e-mails pessoais, redes sociais como Facebook e LinkedIn, sites de comércios eletrônicos, entretenimento e esportes ou mesmo de conteúdo ilegal durante o período de trabalho.

Gestores acreditam que o uso excessivo da internet para assuntos pessoais pode atrapalhar e diminuir o rendimento, dificultando a concentração das pessoas em suas devidas tarefas. Esses acessos não relacionados ao trabalho podem ocupar uma capacidade da banda larga da internet, importante para assegurar a velocidade dos processos da empresa. Ou seja, o acesso irregular à internet desperdiça recursos e aumenta os riscos de ciberataques, gerando assim ataques efetuados através da internet, no qual são violados sistemas informáticos, com o objetivo de espiar, provocar danos, roubar dados etc.

O controle de acesso, por sua vez, ainda promove compliance com a LGPD, que tem como função de regular o tratamento de dados sensíveis de clientes e usuários.

Por isso, medidas devem ser tomadas para evitar que o controle de acessa à internet seja eficaz em sua empresa. Além das ferramentas de bloqueio de acesso, é possível monitorar a navegação. Desta forma permite que o profissional responsável junto com a ferramenta tenha um controle minucioso de sites que estão sendo acessados, tempo gasto e tentativas de acesso a sites bloqueados para empresas com políticas mais restritivas.

Pode parecer uma medida extremamente invasiva, mas pode ser uma ótima solução caso ocorra acessos indesejados e tentativas de fraudar o sistema de segurança. Esse tipo de monitoramento pode ser feito pela empresa, desde que seus profissionais sejam explicitamente comunicados. Por fim, a empresa deve comunicar aos seus usuários todos os recursos usados para controle de acesso à internet e para segurança da informação. Além de ter a obrigação de explicitar o uso desse tipo de controle, e é fundamental que todos compreendam a importância dessas ferramentas, que respeitem as regras e adotem as boas práticas.

CAPITULO 6 - Sistema operacional dos servidores

"Sistema operacional dos servidores" Trata-se do software básico que gerenciará o sistema e que deve ser definido de acordo com cada aplicação. Dentre esses principais sistemas operacionais estão distribuições Linux como Red Hat, Unix, Solaris e versões do Windows Server da Microsoft.

Características de um servidor

Os componentes internos (hardware) que compõem cada servidor diferem de acordo o poder de processamento, capacidade de armazenamento, portas de comunicação, nível de segurança e de proteção do sistema contra desastres. Além disso, cada aplicação possui diferentes níveis de exigência em termos de disponibilidade, performance e segurança, por isso o hardware e software que compõe cada servidor também é definido de acordo com cada projeto. Instalações profissionais como datacenters geralmente possuem diversos servidores redundantes, funcionando agrupados com outros equipamentos (em cluster) e equipados com uma série de ferramentas para manter o funcionamento contínuo.

Servidores de rede

Apesar de vago, o termo "servidor de rede" geralmente refere-se a um computador ou sistema de uma infraestrutura de TI ou datacenter capaz de executar aplicações como softwares corporativos para atender diversos usuários localmente ou via internet. Esses servidores geralmente são capazes de executar aplicativos corporativos como gerenciar bancos de dados, fazer backup, montar um ambiente de virtualização ou controlar o acesso aos dados através da criação de contas e senhas, inclusive atribuindo privilégios para grupos específicos de usuários.

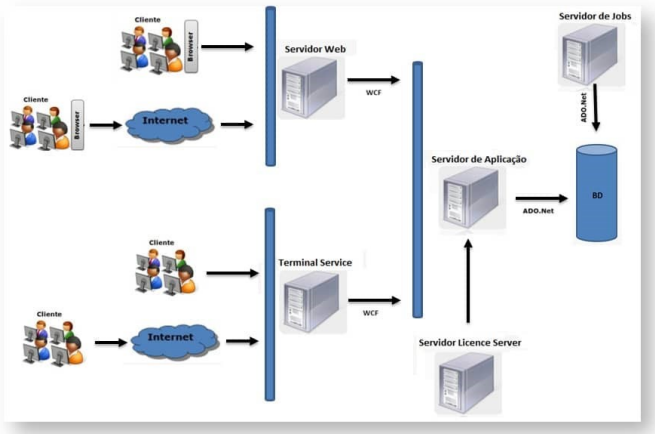


Figura 20 - Servidores de Rede

Servidores de nuvem

Com hardware similar aos servidores encontrados em nossas redes LAN, os computadores que prestam serviços via internet geralmente são instalados em infraestruturas de TI como datacenters e prestam serviços como a hospedagem de sites, distribuição de e-mails e outros serviços o streaming de áudio e vídeo. Empresas como provedores de internet podem vender "áreas" de sistemas virtuais pela capacidade de processamento, espaço na nuvem ou ainda comercializar todo o hardware de um ou mais servidores físicos para que o usuário defina seu

próprio ambiente. Também conhecidos como servidores dedicados, essas soluções existem fisicamente, porém também podem ser parte de grandes ambientes clusterizados e virtualizados, quase sempre à prova de falhas. Nesses casos, apesar da máquina existir, a métrica comercializada pode definida pelo uso, capacidade de processamento e/ou de armazenamento do sistema.

Figura 21 - Servidores de Nuvem

6.1 - Servidores mais conhecidos

Servidor de Arquivos

Um servidor de arquivos é um sistema capaz de armazenar e compartilhar uma grande quantidade de informações em rede, mantendo o gerenciamento centralizado. Qualquer computador pode ser configurado para esse fim, porém equipamentos como storages NAS cumprem muito melhor essa função.

Figura 22 - Servidor de Arquivos

Servidores de aplicação

Servidores de aplicação são sistemas utilizados para executar aplicações corporativas e atender diversas estações de trabalho (usuários) de forma simultânea dentro da mesma rede. Com poder de processamento maior que as estações de trabalho dos usuários, um servidor de aplicação pode executar várias aplicações corporativas e atender diversos usuários, mantendo as respectivas bases de dados sempre centralizadas, atualizadas e armazenadas.

Servidor de armazenamento

Um servidor de armazenamento em rede geralmente possui vários hard disks que trabalham em conjunto e disponibilizam espaço de armazenamento para aplicações em rede (NAS) ou para trabalho conjunto com um servidor de aplicação (DAS). Os novos servidores de armazenamento podem também integrar módulos de memória flash, trabalhando em conjunto com os hard disks (hybrid servers) ou possuírem suas matrizes de armazenamento totalmente formada por memórias flash (server all flash).

Servidores de banco de dados

Alguns servidores são configurados dar eficiência, de forma dedicada, ao processamento e a transferência de dados entre os sistemas computacionais dentro da infraestrutura de TI. Essas soluções são conhecidas como servidores de banco de dados, e proporcionam um ambiente para instalar e processar bases de dados que recebem muitas requisições. Associar servidores de aplicação a sistemas de armazenamento através da montagem de um servidor de dados, seja ela por hardware ou software, traz benefícios como liberar processamento do servidor de aplicação, centralizar as bases de dados de forma organizada e proporcionar mais segurança.

Media server

Media servers são servidores para armazenar e transmitir conteúdo de áudio ou vídeo localmente ou via internet, através de um processo conhecido como streaming. Youtube, Netflix e Amazon são empresas que comercializam conteúdo por assinatura e de hard users desse tipo de tecnologia. Graças a ferramentas como protocolo DLNA, pequenos sistemas de armazenamento domésticos como storages NAS também podem ser considerados servidores de mídia, pois centralizam e compartilham conteúdo como filmes e músicas através de redes locais com TVs de tela grande e sistemas de áudio.

Servidor Web

Apesar de abrangente, o termo servidor web geralmente é designado para sistemas que fornecem serviços como disponibilizar conteúdo (sites) que são acessados através de programas navegadores como Internet Explorer, Google Chrome ou Safari, via protocolo HTTP (Hypertext Transfer Protocol). Um servidor web pode ser um sistema montado exclusivamente para esse fim (hardware + software) ou uma ser apenas aplicação (instância) de um sistema maior, sendo caracterizado por hospedar e executar aplicações escritas em HTML. Esses servidores geralmente são seguros e disponibilizam uma série de ferramentas para criação, gerenciamento e publicação de sites. A maioria dos servidores web utilizam em seus hosts físicos sistemas operacionais baseados em Linux como o Apache e o Nginx, ou ainda sistemas como o IIS Microsoft e o OHS Oracle.

Figura 23 - Servidor WEB

Servidor de email

Um servidor de email é um equipamento configurado para armazenar e transferir e-mails através de redes locais ou via internet. Esses sistemas podem ser montados exclusivamente para esse fim ou ser apenas uma instância num sistema maior. Servidores de email utilizam os protocolos SMTP, IMAP e POP3 para enviar e receber as correspondências. Diversos aplicativos podem ser instalados para esse fim, suportando a maioria dos sistemas operacionais, como os softwares Outlook (Windows), Apple Mail (Mac), Thunderbolt (Linux), Gmail (Android) e Spark (iOS).

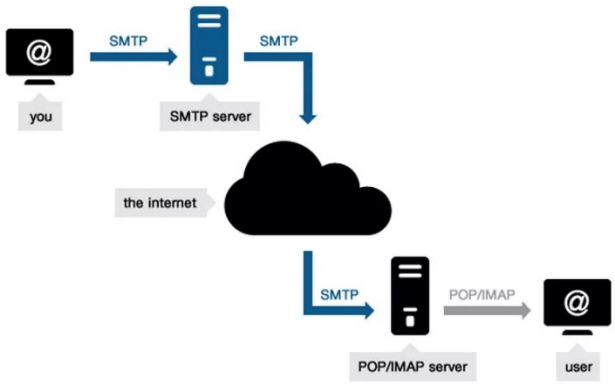


Figura 24 - Servidor de email

Servidor FTP

Muito usado em ambientes de nuvem, o servidor FTP é utilizado para armazenamento e troca de arquivos, permitindo melhor controle das transferências realizadas, proporcionando um ambiente seguro para troca de informações entre computadores e outros dispositivos. O conjunto de protocolos TCP/IP permite download e upload de arquivos via conexão com protocolo FTP (File Transfer Protocol). Ferramentas como essa possibilitam a criação de servidores de armazenamento com serviços de segurança como a autenticação por login e senha, criptografia, uso de SSL (FTPS) e o uso da tecnologia SSH (SFTP).

Servidor Proxy

Atuando como mediador dos computadores clientes que buscam serviços e recursos de outros servidores, um servidor proxy é o intermediário entre a comunicação de dois dispositivos. Ele

gerencia requisições como acesso aos arquivos, páginas web e outros serviços, filtrando todas as solicitações e determinando como as mesmas devem ser manejadas. Um servidor proxy é, por exemplo, o intermediário entre um acesso feito por uma estação de trabalho a um servidor web, filtrando e gerenciando cada requisição, verificando ainda se existe algum acesso anterior gravado (cache) para melhorar o desempenho do sistema.

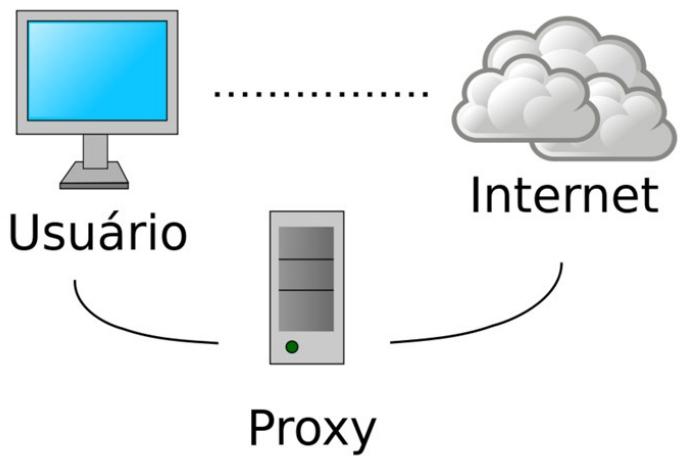


Figura 25 - Servidor Proxy

Outros tipos de servidores

Além dos servidores já mencionados, uma série de sistemas podem ser classificados como servidores. Servidores NAS, servidores dns, telnet e servidores de impressão, além de outros já em desuso como "servidor de fax", são apenas algumas formas para definir sistemas centrais baseados na estrutura cliente-servidor.A internet, a programação orientada a objetos e tecnologias como a virtualização e o clustering descaracterizaram o conceito de que servidor é apenas um recurso de hardware. Assim, uma boa definição para o termo é um sistema computacional dedicado, baseado num ou mais computadores, aliado à um conjunto de softwares e capaz de prestar serviços para outros dispositivos, clientes ou processos.

6.2 - Monitoramento de aplicações em servidores em nuvem

Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafios

Computação em nuvem é uma tendência recente de tecnologia cujo objetivo é proporcionar serviços de Tecnologia da Informação (TI) sob demanda com pagamento baseado no uso. Tendências anteriores à computação em nuvem foram limitadas a uma determinada classe de usuários ou focadas em tornar disponível uma demanda específica de recursos de TI, principalmente de informática. Computação em nuvem pretende ser global e prover serviços para as massas que vão desde o usuário final que hospeda seus documentos pessoais na internet até empresas que terceirizam toda infraestrutura de TI para outras empresas. Nunca uma abordagem para a utilização real foi tão global e completa: não apenas recursos de computação

e armazenamento são entregues sob demanda, mas toda a pilha de computação pode ser aproveitada na nuvem.

Exemplo de Visão geral de uma nuvem computacional:

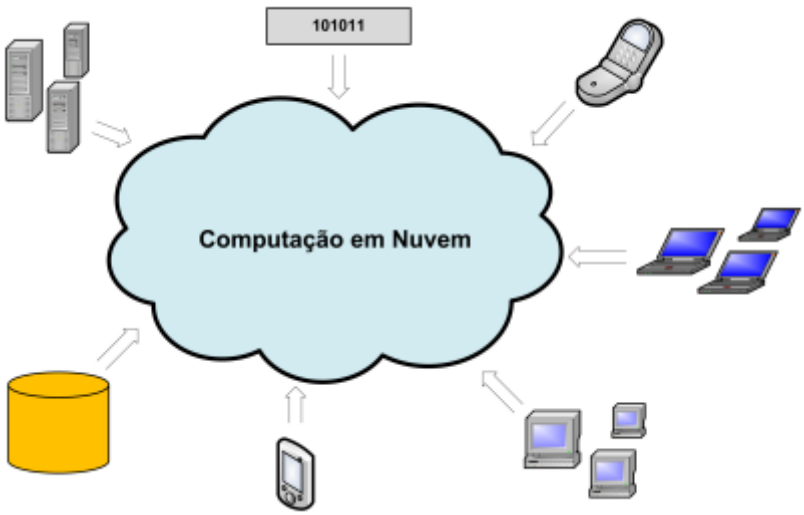


Figura 26 - Computação em Nuvem

Com isso, os usuários estão movendo seus dados e aplicações para a nuvem e assim acessá-los de forma simples e de qualquer local sendo um caso de utilização de processamento centralizado.

Na computação em nuvem, os recursos de TI são fornecidos como um serviço, permitindo aos usuários acessarem os serviços sem a necessidade de conhecimento sobre a tecnologia utilizada. Assim, os usuários e empresas passaram a acessar os serviços sob demanda e independentemente da localização, o que aumentou a quantidade de serviços disponíveis. Este trabalho aborda a computação em nuvem.

Computação em Nuvem

A computação em nuvem está se tornando uma das palavras chaves da indústria de TI. A nuvem é uma metáfora para a Internet ou infraestrutura de comunicação entre os componentes arquiteturais, baseada em uma abstração que oculta à complexibilidade de infraestrutura. Cada parte desta infraestrutura é provida como um serviço e, estes são normalmente alocados em centros de dados, utilizando hardware compartilhado para computação e armazenamento.

Para utilizarem os serviços, os usuários necessitam apenas ter em suas máquinas um sistema operacional, um navegador e acesso à Internet. Todos os recursos computacionais, diminuindo

o custo na aquisição de máquinas. Todo hardware pode ser utilizado para realizar alguma tarefa que seja adequada a fim de aumentar o poder de processamento e cooperar com os recursos existentes.

A infraestrutura do ambiente de computação em nuvem normalmente é composta por um grande número, centenas ou milhares de máquinas físicas ou nós físicos de baixo custo, conectadas por meio de uma rede. Cada máquina física tem as mesmas configurações de software, mas pode ter variação na capacidade de hardware em termos de CPU, memória e armazenamento em disco. Dentro de cada m´quina física existe um número de variável de máquinas (VM) ou nós virtuais em execução, de acordo com a capacidade do hardware disponível na máquina física.

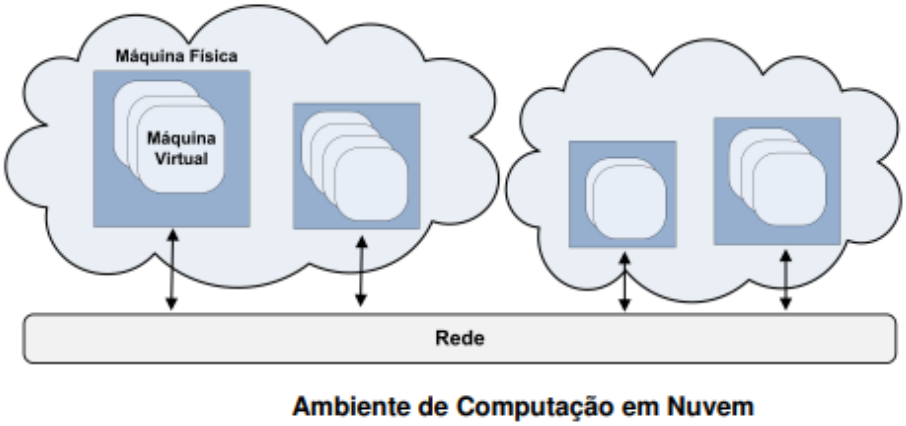


Figura 27 - Ambiente de computação em nuvem

O modelo de computação em nuvem foi desenvolvido com o objetivo de fornecer serviços de fácil acesso, baixo custo e com garantias de disponibilidade e escalabilidade. Este modelo visa fornecer, basicamente, três benefícios. O primeiro benefício é reduzir o custo na aquisição e composição de toda infraestrutura requerida para atender as necessidades das empresas, podendo essa infraestrutura ser composta sob demanda e com recursos heterogêneos e de menor custo. O segundo é a flexibilidade que esse modelo oferece no que diz respeito à adição e substituição de recursos computacionais, podendo escalar tanto em nível de recursos de hardware quanto software para atender as necessidades das empresas e usuários. O último benefício é prover uma abstração e facilidade de acesso aos usuários destes serviços. Neste sentido, os usuários dos serviços não precisam conhecer aspectos de localização física e de entrega dos resultados destes serviços.

Características Essenciais

As características essenciais são vantagens que as soluções de computação em nuvem oferecem. Algumas destas características, em conjunto, definem exclusivamente a computação em nuvem e faz a distinção com outros paradigmas.

Self-service sob demanda

O usuário pode adquirir unilateralmente recurso computacional, como tempo de processamento no servidor ou armazenamento na rede, na medida em que necessite e sem precisar de interação humana com os provedores de cada serviço. O hardware e o software dentro de uma nuvem podem ser automaticamente reconfigurados, orquestrados e estas modificações são apresentadas de forma transparente para os usuários, que possuem perfis diferentes e assim podem personalizar os seus ambientes computacionais , por exemplo, instalação de software e configuração de rede para definição de determinados privilégios.

Amplo acesso

Recursos são disponibilizados por meio da rede e acessados através de mecanismo padronizados que possibilitam o uso por plataformas **Thin ou thin cliente**, tais como celulares, laptops e PDAs. A interface de acesso à nuvem não obriga os usuários a mudar suas condições e ambientes de trabalho, como por exemplo, linguagem de programação e sistema operacional. Já os sistemas de software clientes e instalados localmente para o acesso à nuvem são leves, como um navegador de Internet.

Pooling de recursos

Os recursos computacionais do provedor são organizados em um Pool para servir múltiplos usuários usando um modelo Multi-tenant ou Multi-unquilino, com diferentes recursos físicos e virtuais, podendo somente especificar a localização em um nível mais alto de abstração, tais como país, estado ou centro de dados.

Elasticidade rápida

Recursos podem ser adquiridos de forma rápida e elástica, alguns casos automaticamente, caso haja a necessidade de escalar com o aumento da demanda, e liberados, na retração dessa demanda. Para os usuários, os recursos disponíveis para uso parecem ser ilimitados e podem ser adquiridos em qualquer quantidade e a qualquer momento. A virtualização auxilia a elasticidade rápida na computação nuvem, criando várias instâncias de recursos requisitados utilizando um único recurso real. Além disso., a Virtualização é uma maneira de abstrair características físicas de uma plataforma computacional dos usuários, exibindo outro hardware virtual e emulando um ou maus ambientes que podem ser independentes ou não.

Serviço medido

Sistemas em nuvem automaticamente controlam e otimizam o uso de recursos por meio de uma capacidade de medição. A automação é realizada em algum nível de abstração apropriado para o tipo de serviço, tais como armazenamento, processamento, largura de banda e contas dos usuários ativos. O uso de recurso pode ser monitorado e controlado, possibilitando transparência para o provedor e o usuário do serviço utilizado. Para garantir a quantidade do serviço, pode-se utilizar a abordagem baseada em acordo de nível de disponibilidade, funcionalidade, desempenho ou outros atributos do serviço como faturamento e até mesmo penalidade em caso de violação destes níveis.

Modelo de serviços

O ambiente de computação em nuvem é composto de três modelos de serviços. Estes modelos são importantes, pois eles definem um padrão arquitetural para soluções de computação em nuvem.

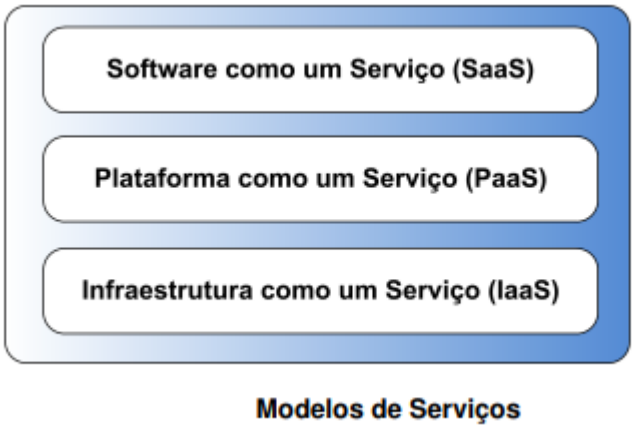


Figura 28 - Modelo de Serviços

Software como um serviço (SaaS)

O modelo de SaaS proporciona sistemas de software com propósitos específicos que estão disponíveis para os usuários através da Internet. Os sistemas de software são acessíveis a partir de vários dispositivos do usuário por meio de uma interface **Thin client** como um navegador Web. No SaaS, o usuário não administra ou controla a infraestrutura subjacente, incluindo rede, servidores, sistemas operacionais, armazenamento ou mesmo as características individuais da aplicação, exceto configurações especificas. Com isso, os desenvolvedores se concentram em inovação e não na infraestrutura, levando ao desenvolvimento rápido de sistemas de software.

Como o software está na Web, ele pode ser acessado pelos usuários de qualquer lugar e a qualquer momento, permitindo maior interação entre unidades de uma mesma empresa ou outros serviços de software. Assim , novos recursos podem ser incorporados automaticamente aos sistemas de software sem que os usuários percebam estas ações tornando transparente a evolução e atualização dos sistemas. O SaaS reduz os custos, pois é dispensada a aquisição de

licenças de sistemas de software. Como exemplos de SaaS podemos destacar os serviços de **Customer Relationship** Management (CRM) da salesforce.

Papéis na Computação em Nuvem

Os papéis são importantes para definir responsabilidades, acesso e perfil para diferentes usuários que fazem parte e estão envolvidos em uma solução de computação em nuvem. Para entender melhor a computação em nuvem, pode-se classificar os atores dos modelos de acordo com os papéis desempenhados.

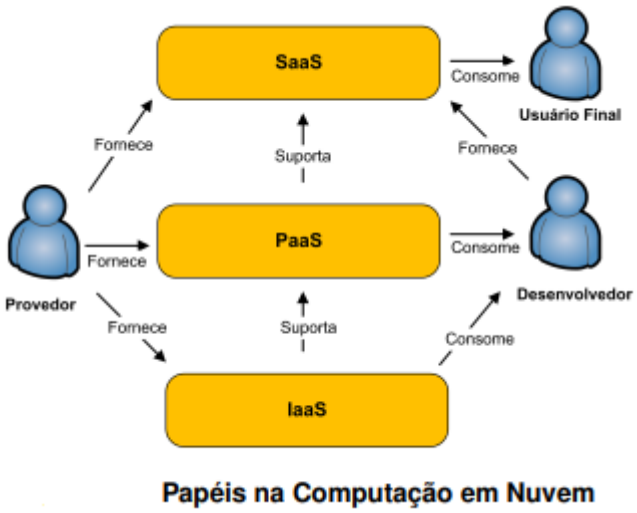


Figura 29 - Papeis na computação em nuvem

O provedor é responsável por disponibilizar, gerenciar e monitorar toda a estrutura para a solução de computação em nuvem, deixando o desenvolvimento e o usuário final sem esse tipo de responsabilidade e fornecendo serviços nos três modelos de serviços. Os desenvolvedores utilizam os recursos fornecidos e disponibilizam serviços para os usuários finais. Estas organizações em papéis ajudam a definir os atores e os seus diferentes interesses, sendo que apenas o provedor fornece suporte a todos os modelos de serviços.

Nuvem privada

No modelo de implantação de nuvem privada, a infraestrutura de nuvem é utilizada exclusivamente para uma organização, sendo esta nuvem local ou remota e administrada pela própria empresa ou por terceiros. Neste modelo de implantação são empregados políticas de acesso aos serviços. As técnicas utilizadas para prover tais características podem ser em nível de gerenciamento de redes, configurações dos provedores de serviços e a utilização de tecnologias de autenticação e autorização.

Nuvem pública

No modelo de implantação de nuvem pública, a infraestrutura de nuvens é disponibilizada para o público em geral, sendo acessado por qualquer usuário que conheça a localização do serviço. Neste modelo de implantação no podem ser aplicadas restrições de acesso quanto ao gerenciamento de redes, e menos ainda, utilizar técnicas para autenticação e autorização.

Nuvem comunidade

No modelo de implantação de nuvem comunidade ocorre o compartilhamento por diversas empresas de uma nuvem, sendo esta suportada por uma comunidade especifica que partilhou seus interesses, tais como a missão. Os requisitos de segurança, política e considerações sobre flexibilidade. Este tipo de modelo de implantação pode existir localmente ou remotamente e geralmente é administrado por alguma empresa da comunidade ou por terceiros. ´

Nuvem Hibrida

No modelo de implantação de nuvem hibrida, existe uma composição de duas ou mais nuvens, que podem ser privadas, comunidade ou pública e que permanecem como entidades únicas, ligadas por umas tecnologias padronizadas ou proprietária que permite a portabilidade de dados e aplicações.

Arquitetura da Computação em Nuvem

Arquitetura da Computação em Nuvem A arquitetura de computação em nuvem é baseada em camadas, sendo que cada uma destas trata de uma particularidade na disponibilização de recursos para as aplicações [Buyya et al. 2009b]. Uma camada é uma divisão lógica de componentes de hardware e software. Alguns destes recursos computacionais podem ser agrupados e organizados para realizar uma determinada tarefa do sistema como um todo. Cada camada pode ter seu gerenciamento ou monitoramento de forma independente das outras camadas, melhorando a flexibilidade, reuso e escalabilidade no tocante a substituição ou adição de recursos computacionais sem afetar as outras camadas. A Figura 7.5 exibe essas camadas e suas respectivas associações.

A camada de mais baixo nível é a de infraestrutura física, que contêm centros de dados, clusters, desktops e outros recursos de hardware, podendo ter recursos heterogêneos. Com isso, fornece certa flexibilidade e facilidade de agregação de novos recursos à medida que se tornem necessários. Uma camada de middleware é responsável por gerenciar a infraestrutura física e

tem por objetivo fornecer um núcleo lógico de uma nuvem. Estes serviços contêm negociações de QoS, gerenciamento dos SLAs, serviços de cobrança, serviços para verificar aceitação de requisições baseado no QoS e preço, serviços

Figura 30 - Arquitetura da Computação em nuvem

Amazon Web Services (AWS)

O Amazon AWS é um ambiente de computação em nuvem com características de escalabilidade, disponibilidade, elasticidade e desempenho para aplicações executadas neste ambiente O Amazon AWS disponibiliza uma infraestrutura completa para computação em diversos níveis de processamento, desde tarefas simples até de alto desempenho e possui uma gerência eficaz dos recursos. O Amazon Web Services é composto por um conjunto de sistemas, dentre os quais podemos destacar:

• Execução: Elastic Compute Cloud (EC2).

• Armazenamento: Simple Storage Service (S3), SimpleDB e Relational Database Service (RDS). • Programação: Simple Queue Service (SQS) e Elastic MapReduce.

• Monitorização: Cloudfront.

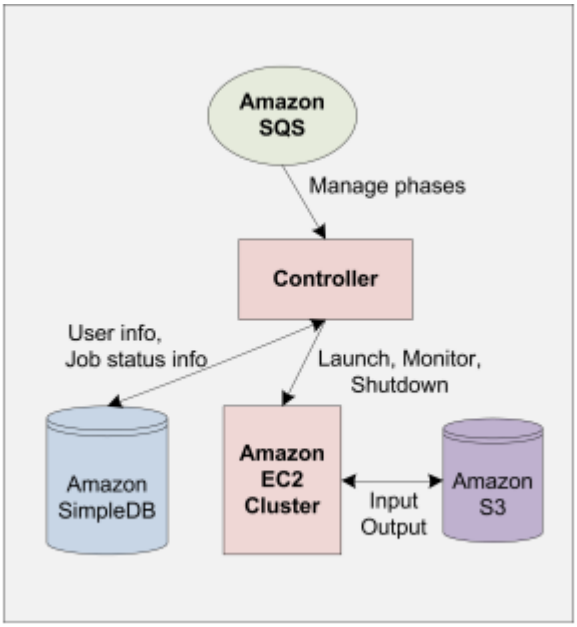


Figura 31 - Amazon EC2

Microsoft Azure

O Microsoft Azure é uma plataforma para a implementação de computação em nuvem que oferece um conjunto específico de serviços para desenvolvedores [Azure 2010]. Esta plataforma pode ser usada por aplicações em execução em nuvem ou fora desta. A plataforma Azure é formada pelo sistema operacional Windows Azure e um conjunto de serviços: Live Services, .NET Services, SQL Services, SharePoint Services e Dynamics CRM Services. O Windows Azure é um sistema operacional para serviços na nuvem que é utilizado para o desenvolvimento, hospedagem e gerenciamento dos serviços dentro do ambiente Azure. Microsoft .NET Services é um conjunto de serviços escaláveis, orientados.

Figura 32 - Plataforma Microsoft Azure

Google App Engine

Google App Engine é uma plataforma para o desenvolvimento de aplicações Web escaláveis que são executados na infraestrutura do Google [Ciurana 2009]. Esta plataforma fornece um conjunto de APIs e um modelo de aplicação que permite aos desenvolvedores utilizarem serviços adicionais fornecidos pelo Google, como o e-mail, armazenamento, entre outros. De

acordo com o modelo de aplicação previsto, os desenvolvedores podem criar aplicações Java e Python e utilizar diversos recursos tais como armazenamento, transações, ajuste e balanceamento de carga automáticos, ambiente de desenvolvimento local e tarefas programadas. O Google App Engine possui um serviço de armazenamento baseado no BigTable [Chang et al. 2006], um sistema distribuído de armazenamento de dados em larga escala. As aplicações desenvolvidas para o App Engine serão executadas no Google, que realiza automaticamente, caso necessário, o dimensionamento.

Aneka

O Aneka é uma plataforma para a implementação de aplicações em computação em nuvem baseada em . O Aneka fornece serviços de persistência, segurança (autorização, autenticação e auditoria), comunicação e manipulação de mensagens. com isso, o Aneka proporciona flexibilidade e extensibilidade para orquestrar vários serviços. O objetivo central do Aneka é fornecer um ambiente que é implantado em infraestruturas físicas e virtuais e que permite a execução de aplicativos desenvolvidos com modelos de aplicações diferentes. O Aneka fornece aos desenvolvedores um conjunto de APIs para explorar esses recursos de forma transparente e expressar a lógica de negócio das aplicações usando abstrações de programação. Os desenvolvedores de sistema podem utilizar uma coleção de ferramentas para monitorar e controlar a infraestrutura implantada.

O Aneka possui um Software Development Kit (SDK) que permite aos desenvolvedores criarem aplicações no contexto de nuvens em qualquer linguagem suportada pelo .NET runtime e um conjunto de ferramentas para criação rápida de nuvens, estando disponível para o Windows e sistemas baseados em Linux.

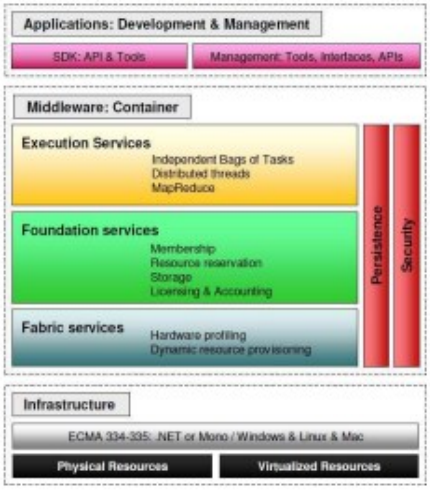


Figura 33 - Arquitetura do Aneka

CloudAV

Aplicativos antivírus são ferramentas muito utilizadas para detectar e bloquear arquivos maliciosos e indesejados. No entanto, a eficácia há longo prazo de antivírus tradicionais é questionável. As aplicações de antivírus podem falhar para detectar muitas ameaças modernas e sua crescente complexidade resulta em vulnerabilidades que estão sendo exploradas por certos vírus. O CloudAV é um novo modelo para detecção de vírus em máquinas baseado no fornecimento de um antivírus como um serviço de computação em nuvem [Oberheide et al. 2008]. Este modelo utiliza uma técnica chamada de N-version protection, que permite a

identificação de arquivos maliciosos e indesejados por múltiplos mecanismos de detecção em paralelo. Neste sentido, cada arquivo é analisado por diversos aplicativos antivírus, o que fornece uma melhor identificação de arquivos maliciosos. A Figura 7.11 ilustra a arquitetura proposta pelo CloudAV. O CloudAV possui dois componentes arquiteturais: um agente e um serviço de rede. O agente é hospedado na máquina dos usuários e tem por função verificar a existência de novos arquivos nesta máquina e enviá-los para o serviço de rede. Estes arquivos podem ser originados por diversos meios, tecnologias ou aplicações.

Quando um arquivo chega na máquina monitorada, o agente identifica este arquivo e o envia para o serviço de rede. O serviço de rede é composto por outros serviços: serviço de análise e serviço baseado em técnicas forenses. Este serviço de rede tem a responsabilidade de receber os arquivos enviados pelo agente e identificar os arquivos maliciosos ou que sejam dotados de conteúdos suspeitos. Para identificar estes arquivos, o serviço de rede utiliza o serviço de análise, sendo este composto por diversos aplicativos antivírus.

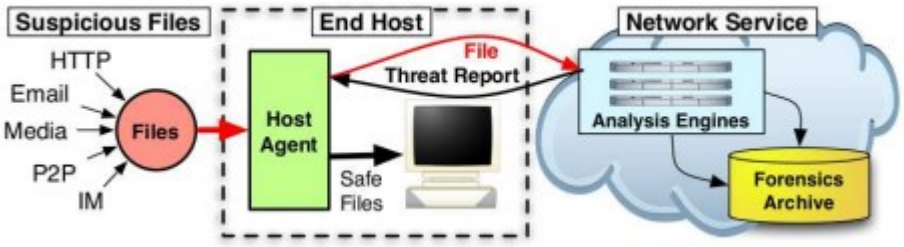


Figura 34 - Arquitetura do CloudAV

CAPITULO 07 - Sistemas Operacional Das Estações de Trabalho

Definição

O Sistema Operacional e um software essencial e mais importante dentre todos. ele funciona assíncrono, não tem começo meio e fim. Os Sistemas Operacionais servem como suporte de hardware para as aplicações dos usuários, e realiza intermediações com uma camada de software. Ele realiza todo o gerenciamento de software e hardware, serve como ponte para o usuário, e todo o gerenciamento de recursos no computador como teclado, mouse , memorias e os programas que o usuário deseja executar. Ele é uma aplicação que se nao existisse o usuário iria ter que ter conhecimentos aprofundados para realizar qualquer aplicação no computador. Existem vários tipos de sistemas operacionais para computadores tem o Windows, Linux e Mac iOS. Para smartfones temos o iOS criado pela Apple para seus smartfones, e o Android criado pela google para Samsung, LG ente outras marcas.

Figura 35 - Diversos tipos de sistemas operacionais

CAPITULO 7.1 - Sistemas Operacionais

Um conjunto de programas que se situa entre os softwares aplicativos e o hardware. Gerencia os recursos do computador (CPU, dispositivos periféricos).Estabelece uma interface com o usuário. Determina como o usuário interage com o sistema operacional. Provê e executa serviços para softwares aplicativos.

Figura 36 - Relação Usuário ao Hardware

Conversores de linguagem: Convertem código de programa para uma forma legível por máquina.

Programas utilitários: Executam tarefas secundárias.

Quando Surgiu: Criado por um grupo de desenvolvedores da AT&T ciaram o Unix em 1969, sendo o primeiro sistema operacional moderno da computação, nos primórdios da computação, os computadores não possuíam sistema operacional, apenas existindo o hardware do computador. Operador e programador da máquina eram uma só pessoa, ou seja, todas as instruções necessárias ao funcionamento do hardware eram realizadas manualmente.

Importância: O sistema operacional é o software básico para a utilização do computador, sem ele seria praticamente impossível um usuário comum utilizar o PC. Ele é o responsável por fazer a comunicação usuário/hardware.

Como seria um computador sem um Sistema Operacional: Se não existisse sistema operacional, o computador não teria os gráficos, as imagens, recursos e os gerenciamentos em que ele gerencia os hardwares do computador. Sem ele, o usuário iria ter que conhecer o micro mais a fundo fazendo com que ele demore mais para obter o resultado em algo, nós iriamos nos deparar com linguagem de programação. Teríamos que programar todos os componentes manualmente.

7.2 - Unix

O Unix foi um dos primeiros sistemas operacionais, e foi o primeiro sistema operacional portável, o primeiro a possuir suporte a multitarefas, multiusuário, recursos de rede, um sistema de arquivos eficiente e o famoso shell. Esses fatores fizeram com que o sistema tenha sido um pioneiro e um molde que serviu para vários outros sistemas operacionais. Um exemplo de sistema baseado no Unix é o Android, que roda no seu smartphone, ou (se você usa um celular da Apple) o IOS, que também é baseado no Unix.

Porque quem é usado: o Unix e usado para provedores cloud e servidores porque ele tem acesso simultâneo de usuários e multitarefa, eficiência, alta segurança e bom desempenho em tarefas de rede e não haver licença para o seu uso

7.3 - Linux

Usa interface de linha de comando. Muitas companhias criaram uma GUI para funcionar com o Linux. Conceito de fonte aberta. O código-fonte é livre. Usuários podem baixar (download), modificar e distribuir o software. Mais estável do que o Windows. Aplicativos relativamente escassos

Porque quem é usado: O Linux é considerado melhor opção para gerenciar os servidores pois nao há necessidade de uma interface gráfica para o usuário e com os benefícios: Estabilidade, Eficiência, Segurança, Rede, Flexibilidade, Suporte técnico, sem folgas e o código fonte distribuído livremente.

7.4 - Familia Windows

Windows 1.0
Windows 2.0
Windows 3.0

Mercado SOHO (Small Office Home Office)

Windows 95

Windows 98

Windows Millennium Edition (ME)

Mercado corporativo
Windows NT
Windows 2000

Mercado corporativo / SOHO

Windows XP

Windows XP 64bitsIII

Windows Vista

Windows 7

Windows 8

Windows 8.1

Windows 10

Windows 11

Porque quem é usado: O Windows e um dos sistemas operacionais mais usados no mundo e por ser compatível com vários fabricantes de computadores. E por facilitar o acesso do usuário ao computador com interfaces mais eficientes , atrativas e mais fáceis de usar além dos softwares mais eficazes e rápidos.

CAPÍTULO 08 – ANTIVÍRUS

Não é surpresa alguma que a internet evoluiu muito nesses últimos anos, essa evolução facilitou a vida de muitas pessoas, indústrias e empresas, imagine comparar uma empresa nos dias de hoje, adepta a tecnologia e uma empresa antiga, antes da internet. Essa evolução possibilitou fácil acesso à informação, fácil acesso a comunicação, gestão e gerou empregos para profissionais capacitados, porém nem tudo são as mil maravilhas, com todo esse avanço benigno também houve o avanço maligno da internet, com hackers mal-intencionados. Imagine um banco que tem um servidor com contas, saldos, senhas e informação privada, imagine o prejuízo se alguma dessas informações fossem vazadas. Uma das ferramentas utilizadas por esses hackers são os malwares, também conhecido como vírus, e nesse capítulo vamos abordar com cuidado suas origens, prevenções etc.

8.1 – O que é um vírus de computador?

Na informática, um vírus de computador é um software malicioso que é desenvolvido por programadores geralmente não hesitariam em usar de malefícios para benefício próprio. Igual um vírus biológico, o programa infecta o sistema, realiza copias de si mesmo e tenta se espalhar para outros sistemas e dispositivos de informática.

A maioria das contaminações por vírus ocorre por descuido do próprio usuário, um exemplo muito comum de como isso pode ocorrer se dá pelo meio do download de arquivos infectados que podem ser passados por anexos em e-mails ou mensagens de texto. A contaminação também pode ocorrer de outras formas, como o acesso de sites de origem duvidosa ou até por meio de arquivos maliciosos em pendrives, CDs, DVDs, HDs externos ou qualquer outro dispositivo de armazenamento de dados. Uma outra possibilidade de ser contaminado seria pelo descuido do usuário ao não atualizar o seu Sistema Operacional, sem as devidas correções de segurança que buscam barrar o acesso indevido desses softwares maliciosos que podem tentar a invasão via internet.

Existem vários tipos de vírus, alguns assim que alojados na sua máquina agem instantaneamente, e existem outros que só visam acesso a informações especificas e as buscam de forma oculta, sem chamar a atenção.

8.2 – Malwares

- **Vírus:** propaga-se infectando com cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução dos arquivos hospedeiros para que possa se tornar ativo e continuar o processo de infecção;

- **Worm:** é capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos, e não necessita ser executado para se propagar. A sua propagação dá-se através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

- **Trojan:** Trojan ou em português, Cavalo de Troia: passa-se por "presente"; cartões virtuais, álbum de fotos, protetor de tela, jogo etc.; que, além de executar funções às quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário

- **Keylogger:** captura e armazena as teclas digitadas pelo usuário no teclado do computador. Normalmente, a ativação é condicionada a uma ação prévia do usuário, por exemplo, após o acesso a um e-commerce ou Internet Banking, para captura de senhas bancárias e/ou números de cartões de crédito com o código de segurança.

- **Screenlogger:** forma avançada de keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado

- **Spyware:** tem objetivo de monitorar atividades de um sistema e enviar as informações a terceiros

- **Adware:** projetado para apresentar propagandas. É comum aparecerem na hora de instalar um programa

- **Backdoor:** Backdoor, ou em português, "Porta dos Fundos": permite a entrada de um invasor por meio das portas virtuais existentes no computador. Normalmente, este programa é colocado de forma a não ser notado.

- **Exploits:** projetado para explorar uma vulnerabilidade existente em um software de computador

- **Sniffers:** usados para capturar e armazenar dados trafegando em uma rede de computadores, principalmente onde não se faz uso de criptografia. Deixa a placa de rede em modo promíscuo

- **Port Scanners:** fazem varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente usados para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador

- **Bot:** além de incluir funcionalidades de worms, dispõem de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o bot, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar spam etc.

8.3 – Principais Antivírus

Como exemplificado acima, os vírus de computador são um perigo real para todos os sistemas operacionais, mesmos os mais sofisticados sistemas podem ser vulneráveis a esse tipo de ataque e não somente a este, mas a diversos ataques dos mais variáveis meios, e se torna de extrema importância uma proteção para esses ataques, utilizando antivírus e protocolos de segurança.

Alguns antivírus no mercado:

- **Firewall:** Para proteger o computador contra tentativas de invasão e ameaças oriundas da Internet e eventualmente de redes locais

  O firewall checa todos os pacotes de dados que trafegam pela rede, filtrando aqueles que não satisfazem as regras de segurança que foram estabelecidas em sua configuração e um firewall já vem pré-configurado, ou seja, vem com algumas regras de segurança básicas já definida, mas você pode alterar as regras pré-existentes e/ou acrescentar novas, de acordo com suas necessidades;

- **Sandbox:** O conceito do Sandbox é bem semelhante ao de criar uma máquina virtual – de fato, esse método é considerado um tipo de virtualização. São softwares que permitem que você faça testes em uma área especial, reservada do computador. De modo que não prejudique o SO e seus arquivos;

- **Anti-spyware:** É o software que tem por finalidade combater os vírus que, quando instalados, têm o objetivo de roubar senhas e/ou arquivos pessoais

- **Antivírus:** Para se proteger contra os diversos tipos de pragas virtuais existentes no mercado;

Alguns antivírus do mercado:

- Avast
- AVG
- Avira
- Bitdefender
- Kaspersky
- McAfee
- Norton
- Panda

CAPITULO 09 - SISTEMA DE BACKUP

Um sistema de backup é um termo utilizado para uma atividade que consiste em realizar cópias de segurança de dados digitais de um dispositivo, como fotos, documentos, softwares ou qualquer arquivo digital, com o intuito de recuperar em caso de perdas ou falhas no sistema em que os arquivos estão armazenados.

O backup dos dados corporativos é um processo fundamental para as empresas, seja **para o** bom funcionamento dos sistemas corporativos, como para garantir a proteção das informações, realizar cópias de segurança é a melhor solução para se recuperar dados em caso de falhas nos hardwares e softwares e, muitas vezes, a única alternativa para lidar com ataques.
É necessário definir um nível de prioridade para os backups realizados a partir da criticidade dos dados. Por exemplo, dados financeiros, de clientes e informações sobre novos projetos e tomadas de decisões precisam estar seguros e à disposição dos gestores para serem utilizados, um simples pane no sistema pode fazer uma empresa perder toda a sua base de cadastro de clientes, o que iria gerar grandes prejuízos financeiros**.**
O desempenho desse tipo de backup irá depender da conexão da internet utilizada, os dados podem ser salvos em tempo real, no entanto, em caso de quedas na conexão, o acesso pode ser prejudicado, além disso, a empresa precisa reforçar seus métodos de segurança para evitar que usuários sem autorização acessem as informações ou tente roubá-las. Portanto, é preciso criar uma estratégia de proteção voltada para a Nuvem.

09.1 - Exemplos de backup:

- **Backup de fotos e vídeos**
  A maneira mais simples de trabalhar com backup de fotos e vídeos no celular é usando o google foto, todas as fotos que você tira com a câmera do seu celular ficam salvas na sua conta do google. basta sincronizar e as alterações serão refletidas em todos os dispositivos.

- **Backup do Windows**
  O tipo de cópia de segurança que você vai fazer, vai depender da versão do Windows, O backup manual é recomendado no caso de versões mais recentes, nele, você escolhe e transfere arquivos e configurações em uma mídia removível ou um local de rede.

TEMOS 4 TIPOS DE METODO DE BACKUP

- **Backup completo:** Faz uma cópia de todos os arquivões que você tem no computador, esse processo, se você usa um sistema de automatização, é feita uma marcação nos dados copiados, de forma que tais copias não se dupliquem.

- **Backup incremental:** Esse tipo de backup serve para fazer copias apenas dos arquivos que foram alterados ou criados do zero após o backup normal.

- **Backup diferencial:** Faz a cópia dos arquivos criados ou modificados desde o backup anterior, ele recebe esse nome porque apenas o que é diferente da cópia anterior é armazenado.

- **Backup diário:** Diz respeito a cópias de segurança de todos os documentos feitas diariamente. Ele é importante para quem precisa ter a confiança da data de um arquivo.

Possiveis lugares para armazenar os backups são:

- **PEN DRIVE:** Os pendrives são pequenos dispositivos de entrada USB que permitem a gravação de dados, eles são muito uteis, já que permitem que os arquivos salvos sejam editados e dão a você a possibilidade de levar sempre com a pessoa para as informações de que precisa.
- **HD EXTERNO:** O HD é responsável por guardar todas as informações do seu computador, quanto ao HD externo, trata-se de um dispositivo que funciona com uma entrada USB e tem a mesma função daquele que está dentro do seu computador que armazena dados.

Nuvem: Backup em nuvem é o backup com cópia de segurança de dados digitais arquivos, sistemas entre outras, em estrutura de armazenamento computacional a nuvem, a estrutura de nuvem pode estar ou não em um local distinto da origem dos dados, podendo ser em datacenter externo ou interno na empresa.

CAPITULO 10 - SERVIÇOS DE REDE

Uma rede de serviços refere-se à maneira como o código de software de aplicativos hospedados na nuvem é aplicado em diferentes níveis do servidor da Web em camadas integradas. Em vez de funcionar em um tempo de execução isolado na camada superior de uma configuração de pilha de servidores da Web, o código de aplicativo hospedado na nuvem pode ser criado com APIs que facilitam chamadas para outros serviços controlados por software disponíveis no nível do sistema operacional, do servidor da Web, da rede ou do data center. Uma rede de serviços aumenta a funcionalidade potencial de aplicativos de software, ampliando os níveis de comunicação interoperável entre elementos de infraestrutura em produção.
Serviços de rede é o que está disponível para ser acessado pelo usuário. No TCP/IP, cada serviço é associado a um número chamado porta que é onde o servidor espera pelas conexões dos computadores clientes. Uma porta de rede pode se referenciada tanto pelo número como pelo nome do serviço.

10.1 - Como Funciona?

A Internet oferece uma grande quantidade de recursos e possibilidades de uso que vão do email e do acesso a páginas Web ao vídeo em tempo real e ao compartilhamento de arquivos em sistemas peer-to-peer. Todas essas possibilidades de uso são construídas a partir de um conceito relativamente simples: o de serviço de rede.
Um serviço de rede pode ser visto como uma aplicação distribuída, que executa em dois ou mais computadores conectados por uma rede. Cada serviço de rede é composto por ao menos quatro elementos:

Servidor: computador que realiza a parte principal do serviço, usando seus recursos locais e/ou outros serviços.

Cliente: computador que solicita o serviço através da rede; geralmente o cliente age a pedido de um ser humano, através de uma interface de usuário, mas ele também pode ser o representante de outro sistema computacional.

Protocolo: é a definição do serviço propriamente dito, ou seja, os passos, o conjunto de mensagens e os formatos de dados que definem o diálogo necessário entre o cliente e o servidor para a realização do serviço.

Middleware: é o suporte de execução e de comunicação que permite a construção do serviço. Em geral o middleware é composto por sistemas operacionais e protocolos de rede encarregados de encaminhar os pedidos do cliente para o servidor e as respostas de volta ao cliente.

10.2 - Exemplos de algumas portas padrões usados no TCP/IP:

- **21 - FTP** (transferência de arquivos)
  FTP significa File Transfer Protocol (protocolo de transferência de arquivos). Vamos explicar melhor. Essencialmente, um “protocolo” ou protocolo de internet é um conjunto de procedimentos ou regras que permitem que dispositivos eletrônicos se

comuniquem entre si. FTP é o conjunto de regras que os dispositivos em uma rede TCP/IP (a internet) usam para transferir arquivos. Quando você usa a Internet, está usando uma variedade de protocolos diferentes. Para navegar, você usa HTTP. Para enviar e receber mensagens instantâneas, você usa XMPP. FTP é simplesmente o protocolo usado para mover arquivos.

- **23 - Telnet** (terminal virtual remoto)
  O Telnet é um protocolo e aplicação, parte da família TCP/IP, para acesso e utilização de computadores remotos. Com Telnet podemos fazer "login" noutros computadores da Internet e utilizar os seus recursos. Por exemplo, executar aplicações e/ou aceder a serviços existentes nos computadores remotos., consultar bases de dados e catálogos bibliográficos (OPAC's), etc. O nosso computador passa a ser como que um terminal (não inteligente) diretamente ligado ao computador remoto (onde é executado todo o processamento).

- **25 - SMTP** (envio de e-mails)
  SMTP é a sigla para Simple Mail Transfer Protocol, que pode ser traduzido como protocolo simples de transferência de correio. Esse é um padrão utilizado com eficiência na transferência de emails pela internet. Ele é compatível com as grandes plataformas de email utilizadas atualmente, como o Gmail, o Hotmail e o Outlook. O SMTP é um protocolo de envio, sendo necessário um outro protocolo, como o POP3, para completar a transferência da mensagem eletrônica. Assim, o POP3 — ou outro protocolo com função similar — atua como servidor de entrada e o SMTP atua como servidor de saída.

- **53 - DNS** (resolvedor de nomes)
  Os servidores DNS (Domain Name System, ou Sistema de Nomes de Domínios) são os responsáveis por localizar e traduzir para números IP (Internet Protocol) os endereços dos sites que digitamos nos navegadores, assim, existem os registros de domínios e os servidores de DNS espalhados pelo mundo com a simples função de traduzir o que é digitado na barra de endereços. Assim, ele é capaz de entender que a URL específica só vai acessar um único endereço IP através dos bancos de dados.

- **79 - FINGER** (detalhes sobre usuários do sistema)
  Finger é um programa que você pode usar para encontrar informações sobre usuários de computador. Geralmente lista o nome de login, o nome completo e possivelmente outros detalhes sobre o usuário que você está digitando. Esses detalhes podem incluir a localização do escritório e o número de telefone (se conhecido), horário de login, tempo ocioso, horário em que o correio foi lido pela última vez e os arquivos de plano e projeto do usuário.

- **80 - HTTP** (protocolo www - transferência de páginas Internet)
  O HTTP é um protocolo que permite a manutenção de recursos, como documentos HTML. É uma base de qualquer troca de dados a cliente Web e um protocolo, o que significa que as requisições são iniciadas pelo destinatário, geralmente um navegador da Web. Um documento completo for reconstruído a partir de diferentes sub-documentos obtidos, como por exemplo texto, descrição do layout, imagens, vídeos, scripts e muito mais.

- **110 - Pop-3** (recebimento de mensagens)
  A principal função do POP3 é acessar e descarregar as mensagens do servidor de e-mail, de modo que elas possam ser acessadas off-line. Basicamente, esse processo é dividido em 4 fases: Conexão, Autenticação , Transação e Atualização.

- **119 - NNTP** (usado por programas de notícias)
  Os NNTP são as iniciais das palavras “Network News Transport Protocol” que se traduz em espanhol “protocolo para a transferência de notícias na rede” , que foi concebido para otimizar a ineficiência das notícias publicadas na Internet. Este protocolo funciona sob o controle de um servidor central , ou seja, todas as notícias publicadas devem primeiro passar por uma avaliação ditada pelo servidor. O cliente, que é o usuário com a intenção de querer publicar a notícia, além disso, o cliente faz uma conexão interativa que melhora ainda mais o sistema.

O arquivo padrão responsável pelo mapeamento do nome dos serviços e das portas mais utilizadas é o /etc/services.

Alguns serviços de rede podem fazer uso de suportes de comunicação mais sofisticados, construídos como camadas acima do TCP ou UDP. Esse é o caso dos serviços baseados em RPC (Remote Procedure Call), dos Web Services e dos ambientes de objetos distribuídos como Java RMI (Remote Method Invocation) e CORBA. Neste caso, as aplicações cliente e servidor se comunicam através de chamadas de procedimentos ou de métodos remotos, construídos por bibliotecas específicas sobre o TCP/IP. Nesse caso, vários processos podem estar envolvidos na construção do serviço, tanto do lado cliente quanto do lado servidor. Muitas vezes os números de portas usados não são padronizados e podem variar de uma execução para outra, o que pode dificultar a criação de regras de filtragem (firewall) para esses serviços.

CAPITULO 11 - ESTRUTURA DE ACESSO

Como administrador do servidor, você pode gerenciar o acesso a qualquer pasta de servidor (conhecidas como pastas compartilhadas quando acessadas no Launchpad, no Acesso via Web Remoto, no aplicativo My Server para Windows Phone ou no aplicativo My Server para Windows 8) no servidor usando as tarefas na guia Pastas do Servidor do Painel, permitindo aos usuários níveis variados de acesso a uma variedade de arquivos.

11.1 Gerenciar o acesso a pastas do servidor

Windows Server Essentials permite que você armazene arquivos que estão localizados nos computadores cliente para um local central usando pastas do servidor. Armazenar os arquivos em pastas do servidor garante que os arquivos estejam em um local que seja sempre acessível de uma maneira segura a partir de cada cliente.

Usar pastas do servidor para armazenar os arquivos permite que você:

Faça backup da pasta de servidor usando o Servidor de backup e restauração para ajudar na proteção contra falha total do servidor.

Acesse os arquivos que estão armazenados na pasta do servidor a partir de qualquer local usando um navegador da Internet por meio do Acesso via Web remoto ou por meio de aplicativos My Server para Windows Phone e Windows 8.

Acesse a nova pasta no servidor a partir de qualquer computador cliente.

Você pode gerenciar o acesso às pastas de qualquer servidor no servidor usando as tarefas da guia Pastas do servidor no Painel. A tabela a seguir lista as pastas do servidor que são criadas por padrão quando você instala o Windows Server Essentials ou ativa o streaming de mídia no seu servidor.

Nome de pasta do servidor e sua descrição

Backups do computador cliente: Por padrão, o Windows Server Essentials cria backups de computadores cliente que são armazenados nessa pasta. As configurações de Backups do computador cliente pode ser modificadas pelo administrador da rede.

Empresa: Usado para armazenar e acessar documentos relacionados à sua organização pelos usuários da rede.

Backups do histórico de arquivos: Por padrão, o Windows Server Essentials usa o histórico de arquivos para criar backups de arquivos que estão armazenados nesta pasta. Essas configurações do histórico de arquivos podem ser modificadas por administradores de rede.

Redirecionamento de pasta: Usado para armazenar e acessar pastas que estão configuradas para redirecionamento de pasta pelos usuários da rede.

Usuários: Usada para armazenar e acessar arquivos por usuários da rede. Uma pasta específica do usuário é gerada automaticamente na pasta Usuários do servidor para cada conta de usuário de rede que você criar.

Música: Usado para armazenar e acessar arquivos de música pelos usuários da rede. Esta pasta está disponível quando você ativa o compartilhamento de mídia.

Imagens: Usado para armazenar e acessar arquivos de imagem pelos usuários da rede. Esta pasta está disponível quando você ativa o compartilhamento de mídia.

TV gravada: Usada para armazenar e acessar programas de TV gravados pelos usuários da rede. Esta pasta está disponível quando você ativa o compartilhamento de mídia.

Vídeos: Usado para armazenar e acessar arquivos de vídeo pelos usuários da rede. Esta pasta está disponível quando você ativa o compartilhamento de mídia.

Ocultar pastas do servidor

Como administrador de rede, você pode optar por ocultar qualquer uma dessas pastas de servidor e impedir que elas sejam exibidas no site de Acesso Remoto via Web ou nos aplicativos de serviços Web (como o My Server).

11.2 Definir Permissões Para Pastas De Servidor

Para quaisquer pastas de servidor adicionais que adicionar ao servidor usando o Painel, você pode escolher três configurações diferentes de acesso:

Leitura/gravação

Escolha essa configuração se quiser permitir que a pessoa crie, altere ou exclua quaisquer arquivos na pasta do servidor.

Somente leitura

Escolha essa configuração se quiser permitir apenas que a pessoa leia os arquivos na pasta do servidor. Usuários com acesso somente leitura não podem criar, alterar ou excluir os arquivos na pasta do servidor.

Sem acesso

Escolha esta opção se você não quiser que a pessoa acesse os arquivos na pasta do servidor. As permissões que são exibidas nas propriedades da pasta representam apenas os usuários que

são gerenciados pelo Painel. Elas não incluem permissões de usuário como contas de serviço ou grupos, não incluem permissões que podem ser definidas na pasta usando outras ferramentas nativas, nem incluem usuários que não foram adicionados por meio do Painel.

11. 3 Adicionar Ou Mover Uma Pasta De Servidor

Você pode adicionar mais pastas do servidor para armazenar os arquivos no servidor, além de pastas do servidor padrão que são criadas durante a instalação. Você pode adicionar pastas do servidor no servidor primário ou em um servidor membro que executa o Windows Server Essentials.

Você pode mover uma pasta de servidor que está localizada no servidor primário que executa o Windows Server Essentials e é exibida na guia Pastas do servidor do Painel para outra unidade de disco rígido, quando necessário, usando o Assistente de Adição de Pasta. Você pode mover uma pasta de servidor para outro endereço local de unidade de disco rígido se:

- A unidade de disco rígido de dados não tiver espaço suficiente para armazenar dados.
- Você quiser alterar o local de armazenamento padrão. Para um movimento mais rápido, considere a possibilidade de mover a pasta do servidor enquanto ele não inclui nenhum dado.
- Você deseja remover o disco rígido existente sem perder as pastas do servidor que estão localizadas nele.

Antes de mover a pasta, verifique o seguinte:

- Certifique-se de que você faça backup do servidor.
- Certifique-se de que todos os backups do cliente foram interrompidos e não estão em andamento, se você planeja migrar a pasta de Backup do computador cliente. Ao mover a pasta de Backup do computador cliente, o servidor não poderá fazer backup de nenhum dos computadores cliente até que a movimentação de pasta esteja concluída.
- Certifique-se de que o servidor não está executando operações críticas do sistema. É recomendável que você conclua todas as atualizações ou backups que estiverem em andamento antes de uma movimentação de pasta, ou o processo pode levar mais tempo para ser concluído.

- Nenhum dos arquivos na pasta a ser movida estão em uso. Não será possível acessar a pasta do servidor enquanto ele é movido.
- Não é possível mover uma pasta do NTFS para ReFS se os arquivos nas pastas do servidor implementam as tecnologias a seguir:
- Fluxos de dados alternados
- Identificadores de objeto
- Nomes curtos (nomes 8.3)
- Compactação
- Criptografia EFS
- NTFS Transacional, TxF (introduzido com o Windows Vista
- Arquivos esparsos
- Links físicos
- Atributos estendidos
- Cotas

11.4 Estrutura da comunicação interna

A comunicação interna nem sempre é valorizada ou reconhecida como essencial para o crescimento e sobrevivência de organizações, negócios ou outras entidades.

A habilidade no processamento e conversão de dados em informações prontas para serem utilizadas na tomada de decisão representa uma oportunidade valiosa no aprimoramento do processo de comunicação no mundo dos negócios na era da informação e neste momento em que a tecnologia é prontamente disponível. A troca de informações só pode ocorrer por meio de uma comunicação interna eficaz.

11.5 Comunicação Interna

Sabemos que a comunicação é o processo de troca de informações entre duas ou mais pessoas. Desde os tempos mais remotos, a necessidade de nos comunicar é uma questão de sobrevivência. No mundo dos negócios não é diferente. A necessidade de tornar os funcionários influentes, integrados e informados do que acontece na empresa, fazendo-os sentir parte dela, fez surgir a comunicação interna, considerada hoje como algo imprescindível às organizações, merecendo, cada vez mais, maior atenção. Por meio da Comunicação Interna, torna-se possível estabelecer canais que possibilitem o relacionamento ágil e transparente da direção da organização com o seu público interno e entre os próprios

elementos que integram este público. Nesse sentido, entender a importância da Comunicação Interna em todos os meios hierárquicos, como um instrumento da administração estratégica é uma exigência para se atingir a eficácia organizacional. Compreender a importância desse processo de comunicação para que flua de forma eficiente, no momento oportuno, de forma que seja atingido o objetivo pretendido, é um desafio para as organizações. A comunicação efetiva só se estabelece em clima de verdade e autenticidade. Caso contrário, só haverá jogos de aparência, desperdício de tempo e, principalmente uma "anti-comunicação" no que é essencial/necessário. Porém não basta assegurar que a comunicação ocorra. É preciso fazer com que o conteúdo seja efetivamente aprendido para que as pessoas estejam em condições de usar o que é informado. (Alberto Ruggiero 2002)

Visando um processo de comunicação mais veloz e acessível aos colaboradores, com praticidade e custos mais baixos, as empresas apoiam suas ações de marketing interno nos canais de comunicação digitais. Entre eles:

E-mail: canal de comunicação comum, podendo vincular muitas informações, por meio do qual as mensagens podem ser originadas externas ou internamente.

Intranet: importante veículo interno, tendo como resultado o marketing para dentro, onde as diferentes áreas da empresa podem divulgar, para o todo, seus resultados, procedimentos adotados, informações de mercado. Além disso, as intranets hoje são utilizadas como canais de interatividade, onde se tornam comuns a publicação de jogos e atividades que proporcionarão melhorias nos processos, estimulando a busca de informações pelos colaboradores.

Pelo fato, a sua aplicação a todos os conceitos emprega-se à intranet, como, por exemplo, o paradigma de cliente-servidor. Para tal, a gama de endereços IP reservada para esse tipo de aplicação situa-se entre 192.168.0.0 até 192.168.255.255.

Mídias eletrônicas: canal para veiculação de imagens relacionadas com campanhas internas, por exemplo, a tela de descanso de computadores (BRUM, 2010).

REFERÊNCIAS BIBLIOGRAFICAS:

Básico de redes: o que você precisa entender sobre endereçamento de rede, disponível em: <https://blog.intelbras.com.br/basico-de-redes-o-que-voce-precisa-entender-sobre-enderecamento-de-rede/#:~:text=Dentro%20de%20uma%20LAN%20(Local,igual%2C%20mas%20de%20dispositivos%20diferentes.>

O que é endereço IP – definição e explicação, disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address>

Endereço lógico e físico no sistema operacional, disponível em: <https://acervolima.com/endereco-logico-e-fisico-no-sistema-operacional-1/>

Controle de acesso à internet: Entenda a importância para a segurança digital da sua empresa, disponível em: <https://www.microcity.com.br/controle-de-acesso-a-internet/>

Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro Prof. Edwar Saliba Júnior: <http://www.esj.eti.br/IFTM/Disciplinas/Grau02/OCS/OCS_Unidade_03.pdf>

Avast Software S.R.O. Malware. Disponível em: <https://www.avast.com/pt-br/c-malware>

AVAST SOFTWARE S.R.O. Vírus de Computador. Disponível em: <https://www.avast.com/pt-br/c-computer-virus>

Piso Elevado – Tipos, Execução e Preço disponível em: <https://carluc.com.br/projeto-arquitetonico/piso-elevado/>

Serviço de rede: o que são, para que servem e quais existem na atualidade? Disponível em: <https://www.informatique-mania.com/pt/linformatique/service-reseau/>

O que é uma rede de serviços? Disponível em: <https://www.vmware.com/br/topics/glossary/content/service-mesh.html>

Sistemas Operacionais Modernos, Andrew Stuart Tanenbaum

Estações de Trabalho, disponível em: <https://portal.unila.edu.br/proagi/ctic/sobre/catalogo-de-servicos/estacoes-de-trabalho>

Infraestrutura - O que é, quais os tipos, seus desafios e prioridades, disponível em: <https://www.portaldaindustria.com.br/industria-de-a-z/infraestrutura/>

Projeto de cabeamento estruturado, disponível em: <https://omsengenharia.com.br/blog/cabeamento-estruturado-projetos/>

Microsoft. Windows Server Essentials: Gerenciar Pastas do Servidor no Windows Server Essentials.

2022. Disponível em: <http:// learn.microsoft.com >

V Pontes Chaves de Melo - Tecitura, 2006 - academia.edu