



UNIVERSIDADE
EDUARDO
MONDLANE

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

CURSO DE LICENCIATURA EM ENGENHARIA INFORMÁTICA

**CONCEPÇÃO DE UMA INFRA-ESTRUTURA DE ADMINISTRAÇÃO DE SISTEMAS
DE COMPUTADORES**

Caso de Estudo: **Ordem dos Engenheiros de Moçambique(OrdEM)**

Autora:

MASSICAME, Fátima Francisco

Supervisores:

Eng.º Délcio Chadreca

Supervisor da Instituição

Eng.º Elton Pedro Sixpence.

Maputo, Agosto de 2022



UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

CURSO DE LICENCIATURA EM ENGENHARIA INFORMÁTICA

**CONCEPÇÃO DE UMA INFRA-ESTRUTURA DE ADMINISTRAÇÃO DE SISTEMAS
DE COMPUTADORES**

Caso de Estudo: **Ordem dos Engenheiros de Moçambique(OrdEM)**

Autora:

MASSICAME, Fátima Francisco

Supervisor da Faculdade

Eng.º Délcio Chadreca

Supervisor da Instituição

Eng.º Elton Pedro Sixpence

Maputo, Agosto de 2022



FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

TERMO DE ENTREGA DO RELATÓRIO DE ESTÁGIO PROFISSIONAL

Declaro que a estudante **Fátima Francisco Massicame** entregou no dia ___/___/2022, as 02 cópias do relatório do seu Estágio Profissional com referência **2022EIEPD218**, intitulado: Concepção de uma Infra-estrutura de Administração de Sistemas Informáticos.

Maputo, aos 15 de Agosto de 2022

A Chefe da Secretaria



FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

DECLARAÇÃO DE HONRA

Declaro sob compromisso de honra que o presente trabalho é resultado da minha investigação e que foi concebido para ser submetido apenas para a obtenção do grau de Licenciatura em Engenharia Informática na Faculdade de Engenharia da Universidade Eduardo Mondlane.

Maputo, aos 15 de Agosto de 2022

A Autora

(Fátima Francisco Massicame)

Dedicatória

Aos meus pais, Francisco Massicame e Virgínia Mondlane Massicame

Aos meus irmãos Gerson, Tânia Isabel e Leopoldina Massicame

À minha irmã mais velha, Nilza Cossa

À minha melhor amiga Mimi

Ao meu namorado, Pedro Madabula

À minha tia chará, Fátima Massicame

À minha avó, vovó Batata

Agradecimentos

Em primeiro lugar agradeço à Deus, pela dádiva da vida, por ter permitido que eu chegasse aqui, por ter me dado forças sempre que ficava desanimada e por ter sempre estado com a minha família.

O meu grande Khanimambo é dedicado aos meus pais, Francisco e Virgínia Massicame por terem me ensinado, de forma exemplar, boa parte do que sei hoje, por terem me dado amor incondicional, por terem persistido na minha educação mesmo quando, às vezes, eu pensava que era castigo, pela paciência e aos meus irmãos Gerson, Leopoldina, Tânia Isabel, Felizarda e Nilza por terem sempre acreditado em mim e pela força que eles depositam em mim.

Agradeço ao professor Velasco, meu professor de Matemática do ensino secundário, pelos conselhos e por ter me proporcionado o amor pela Matemática e pela Engenharia.

Agradeço à família que a faculdade me deu, meus *Mazzas*, pelos quatro anos de experiência, por terem estado comigo, me apoiando em todo o meu percurso na faculdade, especialmente à minha amiga Sara Tivana, Fortunato Jalane, Alexandre Chavane, Tomás Mondlane, Gilvaldo Massunguine, Cany Chicanequisso, Luís Macuvele, Henriques Chigumane, Michel Bisquê, António Cossa, Ricardo Manhice, Patrícia Paúnde, Hélio Chaúque e Manuel Novela.

Agradeço especialmente ao meu namorado Pedro Madabula pelo suporte, apoio incondicional e por ter estado comigo em todos os momentos nos últimos dois anos, com ele ao meu lado, pude viver momentos maravilhosos na faculdade.

Agradeço à todos os meus docentes, especialmente às Engenheiras Ivone Cipriano e Roxan Cadir, ao Engenheiro Délcio Chadreca pela supervisão e apoio, ao Engenheiro Rúben Manhiça e ao Dr. Timóteo Sambo.

E por fim, o meu agradecimento é direcionado à Engenheira Carlota pela oportunidade de colocar em prática os fundamentos aprendidos na faculdade, ao Engenheiro Sixpence pela supervisão e apoio e ao Edon Tandana pela força e troca de experiência.

Epígrafe

“A Vida não é fácil para nenhum de nós. Mas e daí? Devemos ter persistência e acima de tudo, confiança em si mesmo. É preciso sentir confiança para fazer algo e alcançar os objectivos, custe o que custar. ”

Marie Curie

Resumo

Vive-se numa era de avanços tecnológicos, que nos remetem à criação de produtos e serviços com tecnologias inteligentes que são lançadas constantemente para servir como base em busca do conhecimento. Pensando nisso, deve-se analisar e identificar que as organizações precisam de profissionais especializados em sistemas de computadores para tornar todos os processos organizacionais mais eficientes, dinâmicos e rentáveis de forma sistematizada. Administração de sistemas é um tipo de actividade que envolve integrar os sistemas de computadores com as necessidades da comunidade usuária, de forma efectiva e eficiente, com o objectivo de viabilizar o funcionamento de uma rede de computadores, realizando a instalação, configuração e manutenção dos dispositivos e serviços que fazem parte de uma rede de computadores.

A Ordem dos Engenheiros de Moçambique é uma pessoa colectiva representativa de todos os engenheiros em exercício em Moçambique. O presente trabalho está directamente ligado às actividades dadas à autora pela entidade que ofereceu o estágio profissional, entre elas tem-se a implementação de rotinas de actualização da página *web* da Ordem dos Engenheiros de Moçambique, documentação da rede e implementação de rotinas de *backups*. Tendo isso em conta, foi proposta uma arquitectura centralizada de redes de computadores composta pelo router, um *firewall* para a gestão da rede e dos activos, um servidor de virtualização que fornecerá vários serviços aos clientes, um servidor NAS que funcionará como *storage* de *backup* de arquivos e estação de trabalho, que são os computadores clientes.

Palavras-chave: Sistemas de informação, redes de computadores, Ordem dos Engenheiros de Moçambique, *backup*, *firewall*, documentação da rede.

Abstract

We live in an era of technological advances, which lead us to the creation of products and services with intelligent technologies that are constantly launched to serve as a base in the search for knowledge. With this in mind, it must be analyzed and identified that organizations need professionals specialized in computer systems to make all organizational processes more efficient, dynamic and profitable in a systematic way. Systems administration is a type of activity that involves integrating computer systems with the needs of the user community, effectively and efficiently, with the aim of making a computer network viable, performing the installation, configuration and maintenance of devices and services that are part of a computer network.

The Order of Engineers of Mozambique is a legal person representing all engineers working in Mozambique. The present work is directly linked to the activities given to the author by the entity that offered the professional internship, among them there is the implementation of routines for updating the website of The Order of Engineers of Mozambique, network documentation and implementation of backup routines. Bearing this in mind, a centralized architecture of computer networks was proposed, comprising a router, a firewall for managing the network and assets, a virtualization server that will provide various services to clients, a NAS server that will function as a backup storage files and workstation, which are the client computers

Key words: Information systems, computer network, Order of Engineers of Mozambique, backup, firewall, network documentation.

Índice

| | |
|---|----|
| 1. Capítulo I – Introdução..... | 1 |
| 1.1. Contextualização..... | 1 |
| 1.2. Definição do Problema..... | 2 |
| 1.3. Motivação..... | 3 |
| 1.4. Objectivos..... | 3 |
| 1.4.1. Objectivo Geral..... | 3 |
| 1.4.2. Objectivos Específicos..... | 3 |
| 1.5. Metodologia..... | 4 |
| 1.5.1. Classificação da Pesquisa..... | 4 |
| 1.5.2. Técnicas de Colecta de Dados e Tecnologias utilizadas..... | 7 |
| 1.6. Estrutura do Trabalho..... | 7 |
| 2. Capítulo II – Revisão da Literatura..... | 9 |
| 2.1. Sistemas de Informação..... | 9 |
| 2.1.1. Conceito de Sistema..... | 10 |
| 2.1.1.1. Sistemas de Informação..... | 10 |
| 2.1.2. Classificação dos Sistemas de Informação..... | 11 |
| 2.2. Redes de Computadores..... | 13 |
| 2.2.1. Aplicações das Redes de Computadores..... | 14 |
| 2.2.1.1. Aplicações Comerciais..... | 14 |
| 2.2.1.2. Aplicações Domésticas..... | 15 |
| 2.2.1.3. Mobilidade..... | 16 |
| 2.2.2. Classificação das Redes de Computadores..... | 17 |
| 2.2.2.1. Classificação das redes de computadores quanto à extensão geográfica | 17 |
| 2.2.2.2. Classificação das redes de computadores quanto à hierarquia..... | 19 |
| 2.2.3. Principais Componentes de uma Rede de Computadores..... | 21 |
| 2.2.3.1. Servidores..... | 21 |

| | | |
|----------|--|----|
| 2.2.3.2. | Sistemas Operacionais de Servidores | 23 |
| 2.2.3.3. | Principais dispositivos da rede de computadores..... | 24 |
| 2.2.3.4. | Principais conceitos relacionados às redes de computadores | 25 |
| 2.2.4. | Topologias de Redes de Computadores..... | 26 |
| 2.2.4.1. | Barramento..... | 26 |
| 2.2.4.2. | Anel | 27 |
| 2.2.4.3. | Estrela | 28 |
| 2.2.4.4. | Malha..... | 29 |
| 2.2.4.5. | Árvore..... | 29 |
| 2.2.4.6. | Híbrida..... | 30 |
| 2.3. | <i>Firewall</i> | 30 |
| 2.3.1. | Tipos de <i>Firewall</i> | 31 |
| 2.3.1.1. | <i>Firewall Proxy</i> | 31 |
| 2.3.1.2. | <i>Firewall</i> de Inspeção com estado | 32 |
| 2.3.1.3. | <i>Firewall</i> de filtro de pacotes..... | 33 |
| 2.3.1.4. | <i>Firewall</i> de Gerenciamento Unificado de Ameaças (UTM)..... | 33 |
| 2.3.1.5. | <i>Firewall</i> de Última Geração (NGFW)..... | 34 |
| 2.3.1.6. | NGFW focado em ameaças | 34 |
| 2.3.1.7. | <i>Firewall</i> virtual | 34 |
| 2.3.2. | Arquitecturas de implementação de <i>firewall</i> | 35 |
| 2.3.2.1. | Arquitetura <i>Dual-Homed Host</i> | 35 |
| 2.3.2.2. | Arquitetura <i>Screened Host</i> | 36 |
| 2.3.2.3. | Arquitetura <i>Screened Subnet</i> | 36 |
| 2.3.3. | Políticas de <i>Firewall</i> | 37 |
| 2.3.4. | Zonas em <i>Firewall</i> | 38 |
| 2.4. | Rotinas de <i>Backups</i> | 39 |
| 2.4.1. | Tipos de <i>Backup</i> | 39 |
| 2.4.1.1. | <i>Backup</i> Normal ou Completo..... | 39 |

| | | |
|----------|--|----|
| 2.4.1.2. | <i>Backup</i> Incremental..... | 40 |
| 2.4.1.3. | <i>Backup</i> Diferencial ou Acumulativo | 40 |
| 2.4.2. | Armazenamento de dados | 40 |
| 2.4.2.1. | Armazenamento Directamente Conectado (DAS - <i>Direct Attached Storage</i>) | 41 |
| 2.4.2.2. | Armazenamento Conectado à Rede (NAS - <i>Network Attached Storage</i>) | 41 |
| 2.4.2.3. | Área de Armazenamento em Rede (SAN - <i>Storage Area Network</i>) | 41 |
| 2.4.2.4. | Sistema de agregação e protecção de disco..... | 42 |
| 3. | Capítulo III – Caso de Estudo | 44 |
| 3.1. | Ordem dos Engenheiros de Moçambique | 44 |
| 3.1.1. | Missão | 44 |
| 3.1.2. | Visão..... | 45 |
| 3.1.3. | Colégios de especialidade | 45 |
| 3.1.4. | Membro da Ordem dos Engenheiros de Moçambique..... | 46 |
| 3.2. | Situação actual..... | 47 |
| 3.2.1. | Constrangimentos Identificados..... | 48 |
| 4. | Capítulo IV – Desenvolvimento da solução proposta..... | 50 |
| 4.1. | Rotina de Actualização da Página <i>Web</i> da OrdEM | 50 |
| 4.2. | Documentação da rede LAN da OrdEM | 50 |
| 4.3. | Implementação de uma rotina de <i>Backups</i> | 51 |
| 4.4. | Proposta de solução..... | 53 |
| 4.4.1. | Princípio de funcionamento | 54 |
| 4.4.2. | Testes da solução..... | 55 |
| 5. | Capítulo V – Discussão de resultados | 56 |
| 5.1. | Definição do problema..... | 56 |
| 5.2. | Revisão da literatura..... | 56 |
| 5.3. | Caso de estudo | 56 |

| | |
|--|------|
| 5.4. Desenvolvimento da proposta de solução..... | 57 |
| 6. Capítulo VI – Considerações finais | 58 |
| 6.1. Constrangimentos | 58 |
| 6.2. Conclusões..... | 58 |
| 6.3. Recomendações..... | 59 |
| Bibliografias..... | 60 |
| Outras Bibliografias | 61 |
| Anexos | A1.1 |
| Anexo 1: Scan da rede local da OrdEM através do Nmap | A1.1 |
| Anexo 2: Scan da rede local da OrdEM através do Fing..... | A2.1 |
| Anexo 3: Plano Geral da Página Web da OrdEM..... | A3.1 |
| Anexo 4: Testes do Windows Server 2012 R2..... | A4.1 |

Lista de figuras

| | |
|--|------|
| Figura 1: Sistema de Informação baseado em computadores | 11 |
| Figura 2: Exemplo de uma rede PAN | 17 |
| Figura 3: Exemplo de uma rede LAN | 18 |
| Figura 4: Exemplo de uma MAN..... | 18 |
| Figura 5: Exemplo de uma WAN | 19 |
| Figura 6: Rede ponto-a-ponto..... | 20 |
| Figura 7: Rede Cliente-Servidor | 21 |
| Figura 8: Switch..... | 24 |
| Figura 9: Router..... | 25 |
| Figure 10: Access Point..... | 25 |
| Figura 11: Exemplo de uma topologia em barramento | 26 |
| Figura 12: Topologia anel..... | 27 |
| Figura 13: Topologia Estrela..... | 28 |
| Figura 14: Topologia em malha | 29 |
| Figura 15: Topologia em árvore..... | 30 |
| Figura 16: Topologia híbrida..... | 30 |
| Figura 17: Exemplo de Firewall | 31 |
| Figura 18: Firewall Proxy | 32 |
| Figura 19: Firewall de inspeção com estado..... | 33 |
| Figura 20: Firewall de filtro de pacotes..... | 33 |
| Figura 21: Arquitectura Dual-Homed Host..... | 35 |
| Figura 22: Arquitectura Screened Host | 36 |
| Figura 23: Arquitectura Screened Subnet..... | 37 |
| Figura 24: Zonas em firewall | 39 |
| Figura 25: Diagrama da rede LAN da OrdEM..... | 48 |
| Figura 26: Directório das pastas do Google Drive no file explorer..... | 52 |
| Figura 27: Pastas no Google Drive..... | 52 |
| Figure 28: Arquitectura da solução proposta | 53 |
| Figura 29: Scan da rede através do Nmap..... | A1.1 |
| Figura 30: Scan da rede a partir do Fing | A2.1 |
| Figura 31: Plano geral da página web da OrdEM..... | A3.2 |
| Figura 32: Configuração dos requisitos do Windows Server 2012 | A4.1 |
| Figura 33: Server Manager Dashboard | A4.1 |

| | |
|--|------|
| Figura 34: Atribuição de um IP fixo ao servidor | A4.2 |
| Figura 35: AD-DS | A4.2 |
| Figura 36: Serviços de impressão | A4.3 |
| Figura 37: Serviço DHCP | A4.3 |
| Figura 38: Tela inicial do Pfsense..... | A4.4 |
| Figura 39: Atribuição de um IP para o WebConnector do pfsense..... | A4.4 |

Lista de tabelas

| | |
|--|----|
| Tabela 1: Sistemas Operacionais em Servidores..... | 24 |
| Tabela 2: Documentação da rede LAN da OrdEM | 51 |

Lista de abreviações e acrónimos

| | |
|--------------|--|
| AWS | <i>Amazon Web Services</i> |
| DHCP | <i>Dynamic Host Configuration Protocol</i> |
| DNS | <i>Domain Name System</i> |
| EUA | Estados Unidos da América |
| HTML | <i>Hypertext Markup Language</i> (Linguagem de Marcação de Hipertexto) |
| IOT | <i>Internet of Things</i> (Internet das Coisas) |
| IP | <i>Internet Protocol</i> (Protocolo de Internet) |
| ISP | <i>Internet Service Provider</i> (Serviço Provedor de Internet) |
| LAN | <i>Local Area Network</i> |
| MAN | <i>Metropolitan Area Network</i> |
| Nmap | <i>Network mapper</i> |
| NGFW | <i>Next Generation Firewall</i> |
| OrdEM | Ordem dos Engenheiros de Moçambique |
| PAN | <i>Personal Area Network</i> |
| RAID | <i>Redundant Array of Independent Disks</i> |
| SI | Sistemas de Informação |
| TGS | Teoria Geral de Sistemas |
| TI | Tecnologias de Informação |
| UML | <i>Unified Modeling Language</i> (Linguagem de Modelagem Unificada) |
| UTM | <i>Unified Threat Management</i> (Gerenciamento Unificado a Ameaças) |
| VPN | <i>Virtual Private Network</i> (Rede Privada Virtual) |
| WAN | <i>Wide Area Network</i> |

Glossário de termos

Android é um sistema operacional baseado no núcleo Linux, com uma interface de usuário baseada na manipulação directa. É projectado principalmente para dispositivos móveis com tela sensível ao toque como *smartphones* e *tablets*.

Arpanet é uma rede de comunicação de dados criada pela Agência de Pesquisas em Projectos Avançados (ARPA) dos EUA, que inicialmente conectou algumas Universidades e centros de pesquisa, por volta de 1960.

Democratização definição de princípios de igualdade entre os membros de um grupo ou comunidade. Ou mesmo disponibilização (de algo) à todos.

E-commerce comércio eletrônico, refere-se à vendas de produtos e serviços pela Internet.

E-mail correio eletrônico, é um método ou sistema que permite compor, enviar e receber mensagens através de um sistema de computadores online de comunicação de forma assíncrona.

Estanque acto ou efeito de parar uma acção ou desenvolvimento de algo.

Fidedigno algo real, verdadeiro e autêntico.

Firewall é uma solução de segurança baseada em *hardware* e *software* que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

Smartphone é um celular que combina recursos de computadores pessoais com funcionalidades avançadas que podem ser estendidas através de aplicações executadas pelo sistema operacional.

Software sequências de instruções escritas para serem interpretadas por um computador com o objectivo de executar tarefas específicas.

Stakeholders são todas as partes interessadas num negócio ou projecto.

Utilizador é o termo utilizado para referenciar a qualquer um que utiliza determinado serviço ou recurso.

Website conjunto de páginas na internet.

1. Capítulo I – Introdução

1.1. Contextualização

A informação é, hoje em dia, um dos motores da actividade humana. Uma Organização, independentemente do seu tamanho, natureza ou mesmo actividade, precisa da informação para executar, prosseguir a sua missão e cumprir os objectivos a que se propõe. Qualquer Organização moderna possui, na sua estrutura, sistemas, máquinas tecnológicas, equipamentos de informática, *softwares* e pessoas especialistas e recorre às Tecnologias de Informação e Comunicação como forma de melhorar a eficiência operacional e o processo de tomada de decisão, bem como para garantir a função dos sistemas de informação enquanto infra-estrutura de suporte ao fluxo de informação na Organização.

Sistema de Informação, segundo Mendes (2009), é um conjunto de componentes inter-relacionados que colecta (ou recupera) dados, processa, armazena e distribui informações destinadas a apoiar a tomada de decisões e controle numa Organização.

De acordo com Perry (2004), citado por Lampert & Badalotti (2015), actualmente os sistemas de informação têm participado de toda actividade de negócio de uma empresa que oferece um produto ou serviço – desde a concepção, planeamento e produção, até a comercialização, distribuição e suporte. Como resultado, os sistemas de informação têm se tornado um componente crítico do planeamento estratégico e da vantagem competitiva das organizações, levando os executivos a uma maior preocupação com a administração dos sistemas informáticos. Administração de sistemas informáticos é uma actividade que envolve a integração dos sistemas de computadores e as necessidades da comunidade usuária, de forma mais efectiva e eficiente. Isso inclui a instalação, suporte, manutenção de servidores e outros sistemas, planeamento de respostas à indisponibilidade de serviços, administração das redes de computadores, supervisão ou treinamento de técnicos de operação e apoio ao usuário, entre outras.

Durante o Estágio Profissional na Ordem dos Engenheiros de Moçambique (OrdEM) foram executadas várias tarefas como controlar o espaço *e-mail* no servidor da OrdEM, de modo que não haja congestionamento no processo de transmissão da informação, visto que é a base de comunicação entre os elementos internos e externos da OrdEM é a troca de *e-mails*. Implementar rotinas de actualização da página *web*, pois a ocorrência de eventos é muito frequente e sendo o web site um meio de comunicação constante entre os membros e a OrdEM, é necessário mantê-lo sempre actualizado de modo que

os membros estejam a par dos acontecimentos promovidos pela OrdEM. Documentar a rede de computadores da OrdEM e implementar uma rotina de *backups*, com o objectivo de garantir a possibilidade de restabelecer o ambiente em caso de ocorrência de incidentes ou desastres.

Todas as actividades anteriormente mencionadas constituem um conjunto de boas práticas de gestão de uma rede de computadores organizacional.

1.2. Definição do Problema

Lampert & Badalotti (2015), afirmam que todos os anos as empresas investem uma parte significativa do seu orçamento em Tecnologias de Informação (TI) de forma a garantir a disponibilidade da informação para a tomada de decisão. As TI são omnipresentes num mundo cada vez mais global e ligado, e as organizações públicas e privadas têm os seus processos de negócio cada vez mais dependentes do normal funcionamento das suas infra-estruturas de TI. As organizações devem tomar consciência que o conhecimento e utilização das TI pode ajudá-las a ter sucesso no seu processo de melhoria contínua e pode mesmo chegar a mudar a forma como os negócios são geridos. Estudos feitos por Gouveia & Ranito (2011), mostram fortes indícios que as TI afectam positivamente o desempenho das organizações e o “não-uso” das TI torna a informação desvalorizada, pois os dados não recebem o tratamento adequado.

A OrdEM é uma associação pública representativa dos formados em cursos de engenharia. Todo o engenheiro inscrito nela é considerado membro da OrdEM. Ao longo da realização do Estágio Profissional foi notado que embora a OrdEM receba e processe um volume considerável de dados, não foi estabelecida alguma rotina de *backups*, então caso ocorra algum desastre que provoque perda total ou parcial da informação crítica, a OrdEM terá um grande problema pela frente. De uma forma geral foram identificados os seguintes problemas:

- Ausência de rotinas de *backup* de informação, o que pode originar a perda da informação, conseqüentemente uma pausa no trabalho;
- Ausência da documentação da LAN, o que dificulta o processo de comunicação e diagnóstico de problemas;
- Elevado nível de exposição ao vírus informático nos computadores da OrdEM.

O presente trabalho surge com a finalidade de resolver os problemas acima citados.

1.3. Motivação

De acordo com (Gouveia & Ranito, 2011), actualmente empresas de diversos sectores se apoiam na tecnologia, visto que a mesma proporciona uma comunicação mais flexível entre os *stakeholders*. A tecnologia também oferece vários outros benefícios, como maior agilidade na execução de tarefas, melhoria de funcionamento, maior retorno do valor investido, melhor organização da empresa, e conseqüentemente menor gasto com mão-de-obra humana. A implementação de um conjunto de boas práticas na administração de um sistema de informação organizacional garante a segurança e disponibilidade da informação na organização, que todos os serviços sejam concluídos dentro do prazo e que nenhuma solicitação do cliente seja perdida elevando a confiabilidade dos serviços prestados e tornando os processos mais dinâmicos e rentáveis.

O motivo da realização do presente trabalho é identificar uma forma de resolver os problemas anteriormente mencionados, como por exemplo, a implementação de rotinas de *backup* para que, em caso de algum incidente ou falhas humanas, os arquivos não sejam perdidos ou danificados, bem como a descentralização dos computadores da OrdEM.

1.4. Objectivos

1.4.1. Objectivo Geral

- Conceber e implementar um conjunto de boas práticas no âmbito da gestão da LAN da Ordem dos Engenheiros de Moçambique.

1.4.2. Objectivos Específicos

- Abordar os conceitos principais relacionados à administração de sistemas de computadores;
- Conceber e implementar rotinas de actualização da página *web* da OrdEM;
- Documentar a rede da OrdEM;
- Implementar e gerir uma rotina de *backups*;
- Propor uma arquitectura de rede de computadores centralizada.

1.5. Metodologia

1.5.1. Classificação da Pesquisa

Um dos pontos mais importantes num trabalho de pesquisa é a Metodologia de investigação. É onde são apresentados todos os métodos que foram utilizados para atingir o objectivo do trabalho. Existem várias classificações para a metodologia de investigação, contudo, o presente trabalho sustenta-se nas metodologias sugeridas por Gil (1999), Demo (1996), Turato (2004) e Lakatos e Marconi (1999). Uma pesquisa pode ser classificada quanto à natureza, abordagem metodológica, objectivos e procedimentos.

- **Quanto à natureza**

A pesquisa pode ser básica ou aplicada.

Segundo Thesaurus (2016) a pesquisa básica visa a construção de conhecimentos novos para o avanço da Ciência, busca gerar verdades de interesses universais e não prevê aplicação prática do resultado.

A pesquisa aplicada, de acordo com Thesaurus(2016), visa a construção de conhecimentos para a solução de problemas específicos, é dirigida à busca da verdade para determinada aplicação prática em situação particular.

O presente trabalho apresenta uma pesquisa de natureza aplicada, pois visa a construção de conhecimentos para a solução dos problemas na administração do sistema de computadores da OrdEM.

- **Quanto à abordagem metodológica**

A pesquisa pode ser quantitativa ou qualitativa.

A pesquisa quantitativa quantifica, ou seja, transforma em números as opiniões e informações para depois classificá-las e analisá-las; requer o uso de recursos e técnicas estatísticas.

A pesquisa qualitativa não pode ser representada numericamente. É baseada na interpretação dos fenómenos observados e no significado que carregam, dada a realidade em que os fenómenos estão inseridos; considera a realidade e a particularidade de cada sujeito objecto da pesquisa. É descritiva e os pesquisadores tendem a analisar seus dados por intuição.

No presente trabalho procurou-se chegar a um entendimento profundo dos problemas mencionados, de modo que fossem seleccionadas soluções adequadas, pesquisando como outras Organizações têm respondido e gerenciado as solicitações e incidentes registados pelos seus usuários, como funcionam, na prática, os servidores *Web* e que aspectos são tomados em conta na documentação de uma rede de computadores numa Organização. Desta forma, a pesquisa do trabalho é qualitativa pois foi realizada sem recorrer à representações matemáticas, mas sim, ao aprofundamento da compreensão dos problemas.

- **Quanto aos objectivos**

A Pesquisa pode ser: Exploratória, Descritiva ou Explicativa.

A pesquisa exploratória visa facilitar a familiaridade do pesquisador com o problema objecto da pesquisa, para permitir a construção de hipóteses ou tornar a questão mais clara. Envolve levantamento bibliográfico e entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado. Em geral, assume as formas de pesquisa bibliográficas e caso de estudo.

A pesquisa descritiva busca a descrição de características de populações ou fenómenos e da correlação entre variáveis. Envolve o uso de técnicas padronizadas de coleta de dados (questionário e observação sistemática) e é apropriada a levantamentos.

As pesquisas explicativas têm uso mais restrito. Empregam o método experimental de pesquisa e são dotadas de complexidade, servindo para identificar atributos ou factores que determinem a ocorrência de fenómenos. Assumem, geralmente, as formas de pesquisa experimental e pesquisa *ex-post facto*.

No presente trabalho foi feita uma pesquisa exploratória na qual foram levantados problemas existentes na administração do sistema de computadores da OrdEM, determinando as limitações enfrentadas actualmente. Também foram feitas entrevistas à funcionários de outras instituições, que trabalham na área em questão, com a finalidade de resolver problemas específicos.

- **Quanto aos procedimentos**

a) **Pesquisa Bibliográfica** - Baseia-se em materiais já publicados como livros, artigos, material disponibilizado na internet, filmes, imagens, sons, reportagens, etc. Para Gil(1999) citado por Thesaurus(2016), a pesquisa bibliográfica é um trabalho de

natureza exploratória, que propicia bases teóricas ao pesquisador para auxiliar no exercício reflexivo e crítico sobre o tema em estudo. É a base teórica para o estudo, devendo constituir uma leitura selectiva, analítica e interpretativa para buscar ideias relevantes ao estudo, com registro fidedigno das fontes.

- b) **Pesquisa Documental** - A pesquisa documental consiste na procura, leitura, avaliação e sistematização de provas para clarificar fenómenos passados visando obter conclusões ou explicações para o presente. De acordo com Gil (2003, p.51) a pesquisa documental vale-se de materiais que não receberam ainda um tratamento analítico, ou que ainda podem ser reelaborados de acordo com os objectivos da pesquisa.
- c) **Estudo de Caso** - Para Lüdke e André (1999), o estudo de caso assemelha-se mais a uma abordagem metodológica de pesquisa que um tipo de procedimento. É composto por três fase: Fase exploratória, fase de sistematização de colecta de dados e delimitação do estudo e a fase de análise e interpretação das descobertas. Esse tipo de pesquisa envolve um estudo profundo e exaustivo de um ou poucos objectos de maneira que se permita o seu amplo e detalhado conhecimento.
- d) **Levantamento** – É a pesquisa realizada para o conhecimento e descrição de comportamentos e de características de indivíduos através de perguntas feitas aos próprios indivíduos. É caracterizada pelo questionamento directo aos indivíduos cujo comportamento se deseja conhecer. Geralmente, esse questionamento não é feito à todos os indivíduos, apenas a uma amostra significativa.
- e) **Pesquisa ex-post facto** – É realizada após a observação ou ocorrência do fenómeno ou do experimento. Ocorre quando o pesquisador não tem controle sobre as variáveis, mas trabalha como se estivesse a realizar um experimento. Ou seja, ocorre quando o “experimento” se realiza depois dos factos.
- f) **Pesquisa Participante** – Segundo Thesaurus(2016) é uma concepção de pesquisa em que a investigação social ocorre por meio de uma forte interação entre o pesquisador e o público pesquisado. Ou seja, desenvolve-se a partir da interação entre pesquisadores e membros das situações investigadas.
- g) **Pesquisa Acção** – “É caracterizada pela estreita cooperação entre os indivíduos pesquisados e o pesquisador, considerando-se que cada pessoa tem muito a dizer e a fazer” (Thiollent, 2005).

- h) **Pesquisa Experimental** - Determina um objecto de estudo, selecciona as variáveis que seriam capazes de influenciá-lo e define as formas de controle e de observação dos efeitos que a variável produz no objecto.

O presente trabalho recorreu à pesquisa bibliográfica, documental e ao estudo de caso como procedimentos da pesquisa.

1.5.2. Técnicas de Colecta de Dados e Tecnologias utilizadas

Para a realização do presente trabalho recorreu-se aos seguintes instrumentos de colecta de dados:

- Inicialmente foi realizada uma pesquisa bibliográfica profunda, recorrendo-se à *Web*, de forma a se ter acesso às publicações científicas para a justificação teórica e prática dos conceitos.
- Recorreu-se às sites de discussões, de forma a encontrar respostas para erros específicos na instalação e configuração do sistema de registo e gestão de incidentes de utilizadores.
- Sempre que havia alguma dificuldade recorria-se ao ex-funcionário da OrdEM, Sr. Rachid Verloppe, responsável pela montagem da rede LAN da OrdEM, ao Sr. Edon Tandana, responsável pela construção e actualização da página *Web* da OrdEM e ao supervisor Eng.º Elton Sixpence.
- Foram usadas a ferramenta Nmap e a aplicação *Android Fing* para *scanear* a rede da OrdEM bem como para identificar todos os dispositivos conectados a essa rede (vide nos anexos 1 e 2).
- Para o desenho do diagrama da rede da OrdEM, foi usada a ferramenta *draw.io* também conhecida por *diagrams.net* que é um software de desenho gráfico multiplataforma gratuito e de código aberto desenvolvido em HTML5 e *JavaScript*. Essa ferramenta pode ser usada para criar diagramas como fluxogramas, *wireframes*, diagramas UML, organogramas e diagramas de rede.

1.6. Estrutura do Trabalho

- **Capítulo I – Introdução**

Consiste na parte introdutória do trabalho, sendo constituída pela contextualização do tema, motivação, definição do problema, objectivos e pela metodologia usada.

- **Capítulo II – Revisão Bibliográfica**

Neste capítulo são apresentados tópicos importantes para a realização do presente trabalho.

- **Capítulo III – Caso de Estudo**

Neste capítulo faz-se a descrição da Ordem dos Engenheiros de Moçambique, visão, missão e dos constrangimentos na situação actual.

- **Capítulo IV – Desenvolvimento da solução proposta**

Neste capítulo apresenta-se a solução para o problema estudado no presente trabalho. Para tal, são mostrados os resultados de algumas actividades realizadas ao longo do estágio na OrdEM, em seguida, é proposto um sistema centralizado de modo a garantir a eficácia da rede.

- **Capítulo V – Discussão de resultados**

Neste capítulo procede-se a discussão dos resultados encontrados durante o processo de pesquisa.

- **Capítulo VI – Considerações finais**

Neste capítulo avalia-se o cumprimento dos objectivos do trabalho e propõe-se recomendações para trabalhos posteriores.

- **Secção das Bibliografias**

Consiste na apresentação das fontes usadas durante a realização do presente trabalho, quer tenham sido citadas ou não.

- **Secção dos Anexos**

Procede-se a apresentação de elementos adicionais que facilitem a compreensão do trabalho.

2. Capítulo II – Revisão da Literatura

2.1. Sistemas de Informação

Sordi e Meireles (2018) defendem que para o entendimento do conceito de Sistema de Informação é fundamental conhecer um pouco da Teoria Geral dos Sistemas (TGS), que surgiu em 1937, quando o biólogo húngaro Ludwig von Bertalanffy estudou a autorregulação dos sistemas orgânicos. A TGS surgiu como uma crítica à abordagem científica reducionista predominante na época, que reduzia as entidades para o estudo individual das suas propriedades e partes ou elementos. A TGS direciona a análise do pesquisador para o todo, ou seja, para as relações entre as partes que se interconectam e interagem orgânica e estaticamente.

Aplicada à ciência da administração, a TGS resultou em uma nova abordagem administrativa: a abordagem sistemática para gestão das organizações. As abordagens administrativas anteriores não consideravam o lado externo da organização, centravam-se na especialização de assuntos internos da organização de forma estanque, simplificando as organizações e, conseqüentemente, toda a gestão. Dessa forma não auxiliavam o gestor a entender e administrar toda a complexidade presente nas organizações. Com a aplicação dos conceitos da TGS na gestão das organizações, passou-se a considerar a complexidade crescente delas.

A abordagem sistêmica da administração está fundamentada em dois dos principais conceitos da TGS: a interdependência das partes e o tratamento adequado da realidade reconhecida como complexa. Para Sordi e Meireles (2018), o conceito de interdependência das partes refere-se à composição das entidades: o todo de uma entidade é composto por partes de outras entidades, que são interdependentes com relação ao todo. E o tratamento da realidade complexa é o reconhecimento de grande complexidade da sociedade moderna, que exige técnicas específicas para lidar com o pensamento complexo.

Para gestores empresariais, a organização auto gerenciada, no conceito de autorregulação regenerativa importada da TGS e incorporada à abordagem sistêmica de administração, é o estágio ideal, por implementar um sistema autorregulado cujo funcionamento é independente da substância concreta dos elementos que a formam, pois estes podem ser substituídos sem danos ao todo, quando o todo assume as tarefas da parte que falhou. Em outras palavras, a complexidade das partes que compõem um sistema deve ser conhecida, e esse conhecimento é fundamental para definição e divisão

das partes. Entre os principais aspectos a serem considerados quando da definição das partes de um sistema estão a continuidade da operação do sistema e a facilidade de substituição de partes defeituosas ou problemáticas do sistema.

2.1.1. Conceito de Sistema

Entende-se por sistema o conjunto de elementos interagentes e interdependentes, cada um com uma função específica, que trabalham em sintonia para atingir um determinado objectivo comum.

Segundo Mendes (2009, p.16), os sistemas podem ser classificados quanto à constituição e à natureza.

- Quanto à constituição os sistemas podem ser físicos ou abstratos. Os sistemas físicos ou concretos são compostos por equipamentos, máquinas e objectos reais, enquanto que abstratos são compostos por conceitos, hipótese e ideias.
- Quanto à natureza os sistemas podem ser abertos ou fechados. Sistemas abertos são aqueles que apresentam relações de intercâmbio com o meio ambiente, ou seja, sofrem influências do meio externo e funcionam num ambiente dinâmico gerando resultados de qualidade, como por exemplo os sistemas biológicos, sistemas sociais e empresariais. Sistemas fechados não apresentam intercâmbio com o meio onde estão inseridos, pois são isolados das influências ambientais e funcionam através de um ambiente estático gerando resultados de produtividade, como por exemplo o relógio.

2.1.1.1. Sistemas de Informação

Para Almeida (2011), Sistema de Informação (SI) é uma série de elementos ou componentes inter-relacionados que colectam, recuperam, processam, armazenam e distribuem a informação com a finalidade de facilitar o planejamento, o controle, a coordenação, a análise e o processo de tomada de decisão em empresas e organizações. A maioria dos SI começam como sistemas manuais e se transformam em computadorizados, configurados para colectar, manipular, armazenar e processar dados.

Os SI baseados em computadores são compostos por: *hardware*, *software*, base de dados, telecomunicações, pessoas e procedimentos (Farinha, 2015).

- **Hardware** - consiste no equipamento usado para executar as actividades de entrada, processamento e saída.
- **Software** - programas e instruções dadas ao computador para realizar as tarefas necessárias.
- **Base de dados** - colecção organizada de factos e informações que são armazenadas e podem ser manipuladas.
- **Telecomunicações** - permitem às empresas ligar os sistemas de computador em verdadeiras redes de trabalho.
- **Pessoas** - consiste no elemento mais importante na maior parte dos SI. Inclui todas as pessoas que gerenciam, executam, programam e mantêm o sistema de computador.
- **Procedimentos** - estratégias políticas, métodos e regras usadas pelo Homem para gerar os SI baseados em computadores.

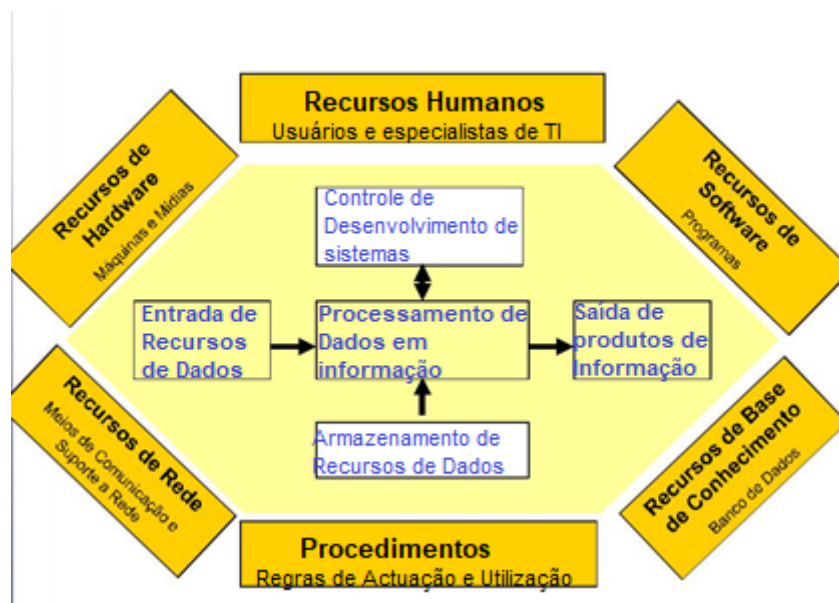


Figura 1: Sistema de Informação baseado em computadores

Fonte: Farinha (2015)

2.1.2. Classificação dos Sistemas de Informação

De acordo com Farinha (2015, p.27), os SI baseados em computadores podem ser classificados quanto à evolução, à amplitude de suporte e ao nível organizacional.

a) **Classificação quanto à evolução**

- **Sistemas de Processamento de Transacções** - utilizados para tarefas repetitivas, de alto volume e de computação de transacções. Têm o objectivo de reduzir custos através da automatização de rotinas dão suporte ao monitoramento, colecta, armazenamento, processamento e disseminação de dados das transacções empresariais. Ex: imprimir cheques.
- **Sistemas de Informações Gerenciais** - esses sistemas obtêm, organizam, resumem e exibem informações para dar suporte à tomada de decisão de rotina nas áreas funcionais. Têm o objectivo de produzir relatórios gerenciais para o planejamento e controle. Ex: relatório de custos totais da folha de pagamento.
- **Sistemas de Apoio à Decisão** - oferecem suporte baseado a computador para decisões complexas e não rotineiras. Têm o objectivo de dar apoio e assistência em todos os aspectos da tomada de decisões sobre um problema específico, sugerindo alternativas e dando assistência à decisão final. Ex: auxiliar a determinar a melhor localização para construir uma nova instalação industrial.
- **Sistemas Baseados na Web** - oferecem aplicações através da *Internet*. Por meio de navegadores as pessoas nessas organizações se comunicam, elaboram, obtêm grandes quantidades de informação e executam as tarefas e processos da organização.

b) **Classificação quanto à amplitude de suporte**

- **Sistemas Funcionais ou Departamentais** - são organizados em torno das funções tradicionais executadas nos departamentos. Ex: contabilidade, finanças, *marketing*, recursos humanos, etc.
- **Sistemas Corporativos** - atendem à diversos departamentos ou mesmo toda a corporação. Permitem que as pessoas se comuniquem entre si e tenham acesso à informações por toda a organização. Ex: ERP (*Enterprise Resource Planning* – Planejamento de Recursos Corporativos).
- **Sistemas Inter organizacionais** - conectam duas ou mais organizações dando suporte a muitas operações Inter organizacionais.

c) **Classificação quanto ao nível organizacional**

- **Nível Operacional** - composto por pessoas que lidam com as operações do dia-a-dia da organização, tomando decisões de rotina; e por sistemas de suporte aos gerentes organizacionais no desenvolvimento de actividades elementares e

transaccionais na organização. Ex: folhas de pagamento, compras, vendas e produção.

- **Nível de Gerência** - composto por gerentes de nível médio que tomam decisões táticas, que lidam em geral com actividades como planeamento, organização e controle a curto prazo; e por sistemas de suporte ao monitoramento, controle, tomada de decisões e actividades administrativas de gestores médios. Ex: resumos estatísticos, relatório de execução, relatórios periódicos, projecções e automação de rotinas.
- **Nível Organizacional** - composto por pessoas que actuam como consultores e assistentes para as gerências superiores e intermediárias, que normalmente sejam especialistas numa área específica; e por sistemas de suporte aos negócios para integrar novos conhecimentos e auxiliar a organização a controlar o fluxo de papéis.
- **Nível Estratégico** – composto por pessoas que tomam decisões que lidam com situações que podem mudar significativamente a maneira como os negócios são realizados; e por sistemas que auxiliam gerentes sêniores a manipular e situar questões estratégicas e tendências de longo-prazo, ambas na organização e no meio externo.

2.2. Redes de Computadores

Segundo Macebo et al. (2018), uma rede de computadores consiste num conjunto de dispositivos autônomos e interconectados com a finalidade de trocar dados por meio de uma única tecnologia.

Para Franciscatto et al. (2014), uma rede de computadores é um conjunto de dois ou mais computadores interligados com o objectivo de compartilhar recursos e trocar informações.

As primeiras redes de computadores surgiram na década de 60 e tinham o propósito de trocar dados entre dois computadores. O cartão perfurado era o meio utilizado para armazenar dados, sendo que o mesmo constituía-se como uma forma demorada e trabalhosa de transportar grandes quantidades de informação (Pera, 2021).

Durante o período da Segunda Guerra Mundial foi criado um projecto de defesa, chamado *Arpanet*. O objectivo da criação da *Arpanet* era que a informação sigilosa não

ficasse concentrada numa única localidade, pois se fosse atacada, os dados seriam destruídos para sempre. Com o fim da Segunda Guerra Mundial, os EUA perceberam que tinha uma tecnologia com extremo potencial em mãos e começaram os processos de disseminação da *Arpanet* para organizações militares, universidades e empresas.

2.2.1. Aplicações das Redes de Computadores

As redes de computadores são empregadas para potencializar diversas actividades do quotidiano das pessoas. A seguir são apresentadas aplicações das redes de computadores em diferentes áreas.

2.2.1.1. Aplicações Comerciais

Muitas empresas têm um número significativo de computadores. Por exemplo, uma empresa pode ter um computador para cada trabalhador e os usa para projectar produtos, criar documentos e elaborar a folha de pagamentos. Inicialmente, alguns desses computadores podem funcionar isoladamente dos outros, contudo, em determinado momento, podem decidir conectá-los para extrair e correlacionar informações sobre toda a empresa (Tanenbaum & Wetherall, 2011).

O compartilhamento de recursos, através da rede, representa um impacto positivo muito relevante, com o objectivo de deixar todos os programas, equipamentos e dados ao alcance de todas as pessoas na rede, independentemente da localização física do recurso ou do utilizador. Como por exemplo uma impressora conectada à rede. Geralmente uma impressora com grande capacidade conectada à rede é mais económica, rápida e de manutenção mais fácil que um conjunto de impressoras individuais.

Segundo Macebo et al. (2018), actualmente toda empresa tem uma dependência vital de informações digitalizadas. A maioria das empresas tem dados de clientes, informações de produtos, *stocks*, extratos bancários, informações sobre impostos e outras informações *online*. Essas empresas dependem intensamente das redes de computadores para permitir que seus funcionários acessem informações e documentos relevantes de forma instantânea.

As redes de computadores permitem que um utilizador tenha acesso à dados armazenados num computador localizado a milhares de quilómetros de distância como

se fossem dados locais, através de VPNs (*Virtual Private Networks*) que são usadas para unir as redes individuais em diferentes locais numa rede estendida. Funcionários podem aceder remotamente a base de dados com informações da empresa, armazenadas num servidor, normalmente instalado e mantido num local central. Uma rede de computadores pode oferecer um poderoso meio de comunicação entre os funcionários, através do recurso *e-mail* (correio electrónico), ligações telefónicas e mesmo vídeo-chamadas, de modo que os funcionários possam ver e ouvir uns aos outros enquanto realizam uma reunião, eliminando o custo e o tempo anteriormente dedicados à viagens.

Outra aplicação das redes de computadores em empresas é realizar negócios electronicamente, com clientes e fornecedores. Esse modelo é chamado *e-commerce* (comércio electrónico), adoptado por várias empresas que descobriram que muitos clientes gostam de fazer compras em casa. Consequentemente, as empresas oferecem catálogos dos seus produtos e serviços e recebem pedidos *online*. Com o uso das redes de computadores fabricantes podem emitir pedidos electrónicos de acordo com as necessidades, reduzindo a necessidade de grandes *stocks* e aumentando a eficiência.

2.2.1.2. Aplicações Domésticas

Muitas actividades domésticas também foram aprimoradas com o surgimento das redes de computadores. O acesso à *internet* oferece aos utilizadores domésticos, conectividade à computadores remotos, assim os utilizadores podem obter informações, comunicar-se com outras pessoas, comprar produtos e serviços com o comércio electrónico, etc.

Segundo Macebo et al. (2018), as principais aplicações domésticas das redes de computadores podem ser organizadas em cinco categorias: i) aplicações baseadas na interação entre pessoas e uma base de dados remota; ii) serviços que possibilitam a comunicação entre as pessoas; iii) comércio electrónico; iv) aplicações de entretenimento; e v) serviços para *Internet* das Coisas (IoT).

- A principal característica das aplicações baseadas na interação entre pessoas e uma base de dados remota consiste na concentração de grandes quantidades de dados disponibilizados em servidores numa rede de computadores. Como por exemplo: bibliotecas virtuais, jornais *online*, nos quais os usuários podem solicitar informações específicas. Outro exemplo de aplicação largamente utilizada consiste na *Netflix*,

onde utilizadores podem aceder um vasto acervo de vídeos como filmes, séries e documentários através de *smartphones*, *smart TVs*, computadores ou tablets.

- A segunda categoria de aplicações domésticas possibilitam a comunicação entre pessoas, com o objectivo de promover a interação entre elas, através das redes sociais, das mensagens instantâneas (que possibilitam não só o envio de mensagens de texto, como também o envio de conteúdos multimídia como áudio, vídeo, imagens ou chamadas de voz ou vídeo) e de serviços de edição de textos colaborativos como a *Wikipedia*.
- As aplicações do comércio electrónico possibilitam a democratização na compra de produtos. Antes do surgimento desta classe de aplicações, as pessoas dependiam fortemente da visita física nas lojas que vendiam os produtos do seu interesse. Com o *e-commerce*, essa dependência foi eliminada, facilitando a aquisição e o pagamento de produtos. Assim tornou-se fácil comparar os preços dos produtos empregados no mercado local com os oferecidos por lojas de diferentes regiões geográficas.
- A forma como as pessoas desempenham actividades de lazer foi aprimorada com o surgimento de aplicações voltadas ao entretenimento. As actividades de lazer mais praticadas através da internet consistem em assistir, escutar música e jogos online, jogos com suporte à múltiplos jogadores conectados em diferentes regiões geográficas.
- A última categoria de serviços e aplicações das redes de computadores para utilizadores domésticos é projectada através do conceito de *Internet das Coisas*, que surgiu como resultado de pesquisas no campo de redes sem fio. Esta aplicação pode prestar serviços relacionados com cuidados de saúde, colectando sinais vitais de um indivíduo através de sensores localizados na sua camisa, enquanto o mesmo assiste.

2.2.1.3. Mobilidade

De acordo com Macebo et al. (2018), empresas de telefonia móvel actuam como provedores de uma infra-estrutura capaz de servir usuários móveis, explorando infra-estruturas de antenas usadas para a comunicação de tráfego de áudio de ligações. A prestação de serviços móveis desperta o interesse de vários segmentos, como por exemplo, o sector de telefonia móvel e indústria militar. Estima-se que nos próximos anos venham a se consolidar outras tecnologias construídas com base na mobilidade, como por exemplo o *Google Glass*, que é um dispositivo como um óculos tradicional, que agrega uma pequena tela acima do campo de visão para possibilitar a interação com

rotas de mapas, opções de música, realizar vídeo-chamadas ou tirar fotos e compartilhar e aceder conteúdos disponíveis na internet.

2.2.2. Classificação das Redes de Computadores

Pera (2021), afirma que as redes de computadores podem ser classificadas de acordo com a sua disposição geográfica e hierarquia.

2.2.2.1. Classificação das redes de computadores quanto à extensão geográfica

- a. **Redes Pessoais (PAN - *Personal Area Network*)** - é uma rede de computadores formada por dispositivos muito próximos uns dos outros. As redes pessoais permitem que dispositivos se comuniquem pelo alcance de uma pessoa. Como por exemplo, uma rede sem fio que conecta um computador com os seus periféricos (teclado, *mouse*, impressoras, etc.) ou uma rede composta por dispositivos que trocam informações por *Bluetooth*.



Figura 2: Exemplo de uma rede PAN

Fonte: (Pera, 2021)

- b. **Redes Locais (LAN - *Local Area Network*)** - corresponde a uma rede que possui uma “cobertura limitada” quanto à extensão geográfica que pode actuar, ou seja, é uma rede particular que opera dentro e próximo de um único prédio, como residência, um escritório ou uma fábrica. As LANs são muito usadas para conectar computadores pessoais e aparelhos electrónicos, para permitir que compartilhem recursos e troquem informações. Quando as LANs são usadas pelas empresas, são chamadas de redes empresariais.

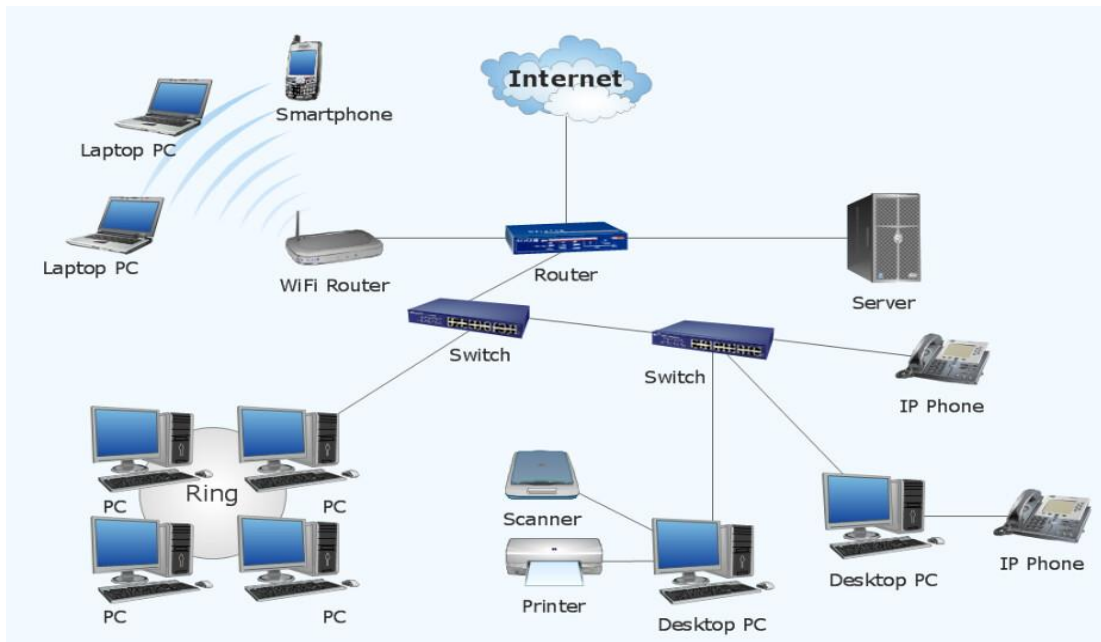


Figura 3: Exemplo de uma rede LAN

Fonte: Pera (2021)

- c. **Redes Metropolitanas (MAN - Metropolitan Area Network)** - são redes de computadores que correspondem um espaço de média dimensão como uma cidade, região, campus, entre outros. Geralmente uma MAN é associada a interligação de várias LANs e é considerada uma parte menor de uma WAN (que será descrita a seguir). Exemplos: a rede de televisão a cabo disponível em muitas cidades e as redes ISP (*Internet Service Provider* - Provedor de Serviços de Internet).

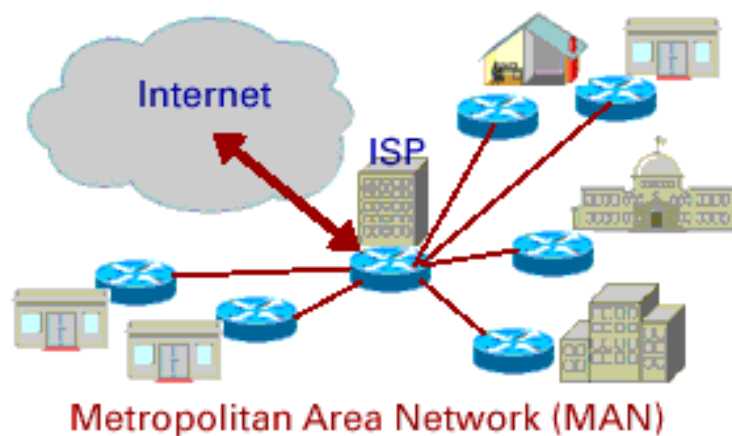


Figura 4: Exemplo de uma MAN

Fonte: Andrade (2015)

- d. **Redes de longas distâncias (WAN - *Wide Area Network*)** - abrangem uma grande área geográfica, como um país ou continente. As WANs permitem a comunicação a longa distância, interligando redes dentro de uma grande região geográfica.



Figura 5: Exemplo de uma WAN

Fonte: Andrade (2015)

De acordo com (Franciscatto et al., 2014), são utilizadas outras nomenclaturas para descrever outros tipos de redes, quanto à extensão geográfica que as mesmas actuam, como por exemplo:

- **WMAN** - rede metropolitana sem fio, destinada principalmente a operadores de telecomunicações.
- **WWAN** - rede de longa distância sem fio, comumente utilizada para a criação de redes de transmissão celular.
- **RAN (*Regional Area Network*)** - considerada uma subcategoria de uma MAN, corresponde a uma rede de computadores de uma região geográfica específica.
- **CAN (*Campus Area Network*)** - corresponde a uma rede de computadores formada por computadores dispostos em edifícios, prédios, campus, entre outros (Franciscatto et al., 2014).

2.2.2.2. Classificação das redes de computadores quanto à hierarquia

- a) **Redes Ponto-a-ponto (*Peer-to-peer*)** - são utilizadas em pequenas redes. Neste tipo de redes os computadores trocam informações entre si, compartilhando arquivos e recursos como música, vídeos, fotos, entre outros. A grande vantagem

desse tipo de rede é a fácil implementação e baixo custo e o ponto negativo é o baixo nível de segurança. As redes ponto-a-ponto não possuem base de dados centralizados, cada usuário mantém a sua própria base de dados local e oferece uma lista de outros dispositivos vizinhos que são da mesma rede (Tanenbaum & Wetherall, 2011).



Figura 6: Rede ponto-a-ponto

Fonte: Franciscatto (2014)

b) Redes Cliente-Servidor - possuem um ou mais servidores, responsáveis por prover serviços da rede aos clientes, computadores conectados ao servidor para aceder dados remotos. Quando um cliente deseja aceder um determinado serviço ou recurso faz uma solicitação ao servidor da rede. Segundo (Franciscatto et al., 2014), esse tipo de rede surgiu da necessidade de criar uma infra-estrutura que centralizasse o processamento num computador central (o servidor). Os computadores clientes (também chamados de nós) são as estações de trabalho (notebooks, desktops, smartphones ou tablets) utilizados pelos usuários para aceder informações armazenadas no servidor e executar aplicações locais. Uma das vantagens desse tipo de rede é o elevado nível de segurança, pois as informações encontram-se centralizadas no servidor, o que facilita o controle e gerenciamento das mesmas. Um ponto negativo é a complexidade e maior custo na implementação.

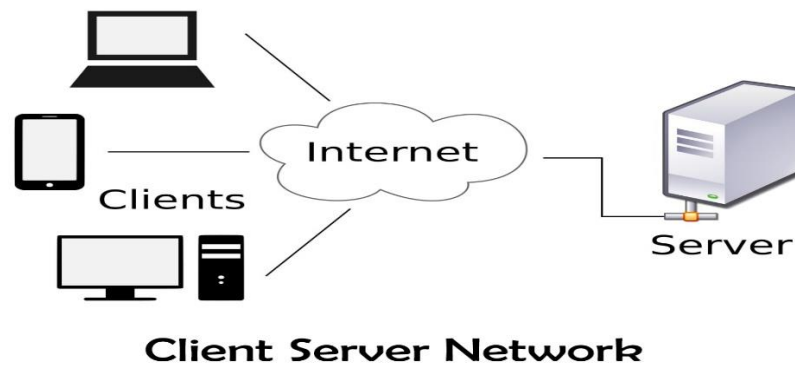


Figura 7: Rede Cliente-Servidor

Fonte: Pera (2021)

2.2.3. Principais Componentes de uma Rede de Computadores

De acordo com Pera (2021), uma rede de computadores é formada por diversos dispositivos, equipamentos, entre outros, para que funcione correctamente e cumpra o objectivo geral de uma rede: a troca de informações e o compartilhamento de recursos, sejam eles de hardware ou software. Para o mesmo autor, os principais componentes de uma rede de computadores podem ser descritos conforme apresentado nos pontos abaixo.

2.2.3.1. Servidores

Um servidor, numa rede de computadores, provê diferentes serviços aos computadores, ou seja, disponibiliza e armazena recursos para os seus clientes. São diversas as vantagens de utilizar um servidor numa rede de computadores. A seguir são citadas algumas delas:

- **Centralização de serviços** - os serviços da rede ficam centralizados num mesmo local, o que facilita a tarefa do administrador do servidor.
- **Backup** - ao centralizar serviços de rede, tem-se a facilidade de administrar as cópias de segurança (backup), pois todos os serviços, directórios e arquivos estão centralizados numa única máquina e não espalhados por diferentes computadores.
- **Acesso Remoto** – um servidor implementa o serviço de acesso remoto. Dessa forma, os usuários podem aceder servidores de uma empresa como se estivessem na mesma rede local.

Tipos de Servidores

Actualmente existem diferentes tipos de servidores, classificados conforme a tarefa que realizam. Abaixo são listados os principais:

- **Servidor de arquivos** - tem a função de armazenar os dados compartilhados por diferentes usuários conectados a uma determinada rede de computadores. Esses dados ou arquivos podem ser documentos, planilhas, gráficos, imagens, músicas, entre outros. Os programas que manipulam os arquivos são instalados e executados individualmente em cada uma das máquinas.
- **Servidor de impressão** - processa pedidos de impressão solicitados pelos usuários da rede e controla a ordem de impressão em caso de pedidos simultâneos, em empresas em que o uso da impressora é compartilhado. Esse servidor proporciona o controle do que vai ser imprimido, do quanto e por quem será impresso.
- **Servidor de aplicações** - é responsável por executar aplicações cliente-servidor, como por exemplo, uma base de dados. Os clientes enviam pedidos ao servidor, este processa e devolve-os para serem exibidos em aplicação cliente. A vantagem deste tipo de serviço é que vários usuários podem utilizar uma aplicação ao mesmo tempo.
- **Servidor de e-mail** - responsável pelo armazenamento, processamento de envio e recepção de mensagens eletrônicas (*e-mail*).
- **Servidor Web** - também conhecido como servidor de hospedagem, armazena os *web sites* que ficarão disponíveis na *internet*, para que sejam acessados pelos clientes através de navegadores.
- **Servidor de Backup** - responsável por executar, armazenar e atualizar as cópias de segurança dos dados armazenados no servidor.
- **Servidor DNS (*Domain Name System* ou Sistema de Nomes de Domínios)** trata-se de um sistema de direcção de nomes distribuídos para computadores, é essencial para tudo que envolve pesquisa, localização e acesso a *sites*. Isto é, é um servidor encarregado pela localização, tradução e conversão para o endereço IP dos *sites* digitados nos navegadores. Toda informação referente aos nomes dos domínios é associada pelo servidor DNS. Por exemplo, ao

digitar no navegador *www.ordeng.co.mz*, o servidor DNS traduz esse endereço para um endereço IP, que é o real endereço do *site*.

- **Servidor DHCP (*Dynamic Host Configuration Protocol* ou **Configuração Dinâmica de Endereços de Rede**)** – é um protocolo utilizado em redes de computadores que permite às máquinas obterem um endereço IP automaticamente.
- **Servidor de Virtualização** – comumente utilizado como uma forma de reduzir o número de servidores físicos, um servidor de virtualização permite a criação de várias máquinas virtuais no mesmo computador servidor. Desta forma, pode se ter, na mesma rede, diferentes servidores separados, no mesmo equipamento, fazendo com que dessa forma tenha-se maior eficiência em termos de energia, sem prejudicar as funcionalidades de vários sistemas operacionais.

2.2.3.2. Sistemas Operacionais de Servidores

Quanto aos softwares utilizados como sistemas operacionais para um servidor numa rede de computadores, tem-se diversas opções sendo que algumas delas são pagas (comerciais) e outras livres (quanto à utilização, modificação e alteração). Os sistemas operacionais para servidores são basicamente os sistemas operacionais *Windows*, *Linux* e *Mac OS X*.

| Windows | Linux | Mac OS X |
|---------------------|-----------|------------------------------|
| Windows 2000 Server | Suse | Mac OS X v10.0 Cheetah |
| Windows 2003 Server | Debian | Mac OS X v10.1 Puma |
| Windows 2008 Server | Ubuntu | Mac OS X v10.2 Jaguar |
| Windows 2012 Server | Mandriva | Mac OS X v10.3 Panther |
| Windows 2016 Server | Red Hat | Mac OS X v10.4 Tiger |
| Windows 2019 Server | Fedora | Mac OS X v10.5 Leopard |
| | Slackware | Mac OS X v10.6 Snow Leopard |
| | | Mac OS X v10.7 Lion |
| | | Mac OS X v10.8 Mountain Lion |

Tabela 1: Sistemas Operacionais em Servidores

Fonte: Macebo et al. (2018)

2.2.3.3. Principais dispositivos da rede de computadores

- **Host** - dispositivo utilizado pelos usuários finais para processamento das aplicações e conexão à rede. Exemplo: notebook, computadores pessoais, smartphones, etc.
- **Interface de rede** - cada computador, *notebook* ou outros dispositivos se conectam à determinada rede de computadores através de uma placa de rede, chamada *interface* de rede. Uma placa de rede pode ser do tipo *Ethernet* cabeada ou sem fios.
- **Hub** - é um dispositivo cuja função é interligar os computadores de uma rede local. O funcionamento do hub se difere de um switch, pois o hub simplesmente repassa o sinal vindo de um computador para todos os computadores ligados a ele.
- **Switch** - semelhante ao *hub*, com a diferença de que ao receber um sinal vindo de um computador origem e entrega este sinal somente ao computador destino. Isto é possível devido a capacidade deste equipamento em criar um canal de comunicação exclusivo (origem/destino). Esta prática diminui consideravelmente o número de colisões e perda de pacotes na rede.



Figura 8: Switch

Fonte: Andrade (2015)

- **Bridge** - ponte de ligação entre duas ou mais redes.
- **Gateway** - na arquitetura TCP/IP, é o equipamento que conecta os *hosts* à rede. Em outras arquiteturas de redes, um *gateway* é um dispositivo (*hardware* ou *software*) que converte mensagens de um protocolo em mensagens de outro protocolo.
- **Roteador** - dispositivo de rede que interconecta duas ou mais redes físicas e encaminha pacotes entre elas.



Figura 9: Router

Fonte: Franciscatto et al (2014)

- **Ponto de acesso wireless (access point)** - equipamento responsável de fazer a interconexão entre todos os dispositivos móveis numa rede sem fio. Uma prática comum é a interligação de um *access point* a uma rede cabeada, para, por exemplo, prover acesso à internet numa rede local de computadores.



Figure 10: Access Point

Fonte: Amaral (2012)

2.2.3.4. Principais conceitos relacionados às redes de computadores

- **Protocolo** - conjunto de regras e convenções que definem a comunicação dos dispositivos numa rede. Um dos protocolos mais conhecidos é o protocolo de *internet*, TCP/IP.
- **TCP/IP** - o protocolo TCP/IP é a junção de dois protocolos diferentes o TCP e o IP. O protocolo TCP (*Transmission Control Protocol*) é o protocolo padrão que define o serviço de circuito virtual da camada de transporte da arquitectura TCP/IP. O protocolo IP (*Internet Protocol*) é protocolo padrão que define o serviço de entrega não confiável e não orientado à conexão da camada de rede do TCP/IP.
- **Endereço IP** - um endereço IP é um identificador de dispositivo pertencente a uma rede de computadores. Também conhecido como endereço lógico, pode conter endereços reservados, que são utilizados dentro de uma rede local,

também conhecidos como não-roteáveis e endereços IPs válidos, utilizados publicamente, inclusive no acesso à internet.

- **Endereço MAC** - um endereço MAC (*Media Access Control*) também conhecido como endereço físico, é atribuído na fabricação de uma *interface* de rede, por exemplo. Este endereço é único para cada dispositivo (Pera, 2021).
- **Porta** - uma porta de rede de computadores corresponde a representação interna do sistema operacional de um ponto de comunicação para envio e recepção de dados. Uma porta é representado por um número, na qual é realizado determinado acesso.

2.2.4. Topologias de Redes de Computadores

De acordo com (Pera, 2021), uma topologia de rede tem o objectivo de descrever como é estruturada uma rede de computadores, tanto fisicamente como logicamente. A topologia física demonstra como os computadores estão dispostos na rede (aparência física da rede), enquanto que a topologia lógica demonstra como os dados trafegam na rede (fluxo de dados entre os computadores que compõem a rede). As principais classificações de topologias de rede são: Barramento, Anel, Estrela, Malha, Árvore e Híbrida.

2.2.4.1. Barramento

Na topologia em barramento todos os computadores trocam informações entre si através do mesmo cabo, utilizado para transmitir dados entre os computadores.

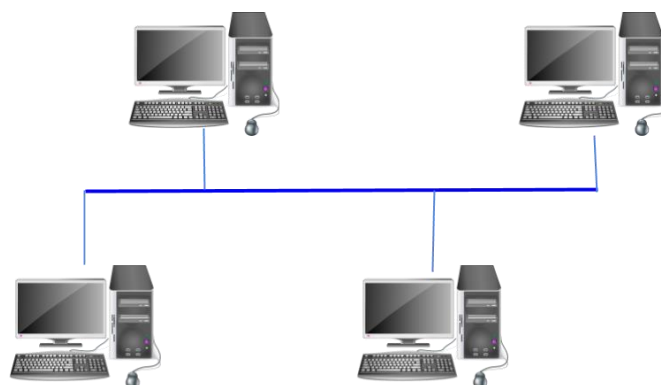


Figura 11: Exemplo de uma topologia em barramento

Fonte: Franciscatto et al. (2014)

Vantagens

Para Silva (2010) citado por (Pera, 2021), as vantagens da topologia em barramento são:

- Compartilhamento do mesmo cabo por estações de trabalho.
- Fácil instalação.
- Pouca quantidade de cabo.
- Baixo custo e fácil implementação em lugares pequenos.

Desvantagens

- Somente um computador pode transmitir informações por vez. Caso mais de uma estação tente transmitir informações ao mesmo tempo, haverá colisão de pacotes. A cada colisão que ocorre na rede é necessário que o computador reenvie o pacote, essa tentativa de reenvio de pacote acontece várias vezes até que o barramento esteja disponível para a transmissão e os dados cheguem ao computador receptor.
- Problemas no cabo afectam directamente todos os computadores da rede.
- Velocidade de rede variável, de acordo com a quantidade de computadores ligados ao barramento.
- Gerenciamento complexo (erros e manutenção da rede).

2.2.4.2. Anel

Possuem o formato de um anel, pois os dispositivos conectados à rede formam um circuito fechado em forma de círculo. Neste tipo de topologia os dados são transmitidos de forma unidirecional, isto é, numa única direcção até chegar ao computador destino. Assim, o sinal emitido pelo computador origem passa por diversos computadores, que retransmitem esse sinal até que chegue ao computador destino.

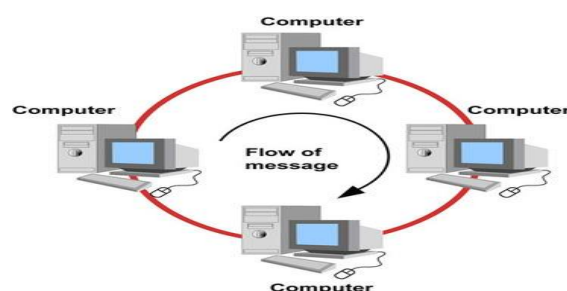


Figura 12: Topologia anel

Fonte: Macebo et al. (2018)

Vantagens

- Inexistência de perda do sinal, uma vez que este é retransmitido ao passar por um computador da rede.
- A identificação de falhas no cabo é realizada de forma mais rápida que na topologia em barramento.

Desvantagens

- Atraso no processamento de dados, já que estes dados passam por estações diferentes do computador destino.
- A confiabilidade diminui conforme aumenta o número de computadores na rede.

2.2.4.3. Estrela

Conforme Amaral (2012, p.24), o nome Estrela se deve ao facto de existir um concentrador na rede, onde se conectam todas as estações da rede. Um concentrador é um dispositivo (*hub*, *switch* ou *router*) que faz a comunicação entre os computadores da rede. Dessa forma, qualquer computador que queira trocar dados com outro computador da mesma rede, deve enviar esta informação ao concentrador para que o mesmo faça a entrega dos dados.

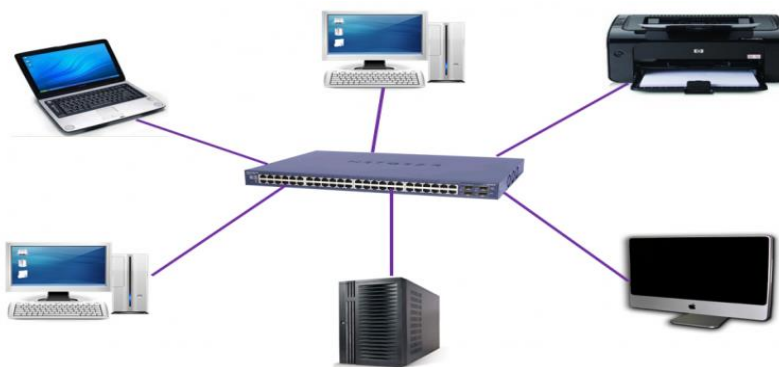


Figura 13: Topologia Estrela

Fonte: Amaral (2012)

Vantagens

- Fácil identificação de falhas em cabos.
- A instalação de novos computadores ligados à rede, ocorre de forma mais simples em relação às outras topologias.

- Facilidade na identificação e correcção de origens de falhas.
- A ocorrência de falhas num computador não afecta as demais estações ligadas ao concentrador.

Desvantagens

- O custo de instalação aumenta proporcionalmente à distância do computador ao concentrador da rede.
- A ocorrência de falha no concentrador afecta toda a rede conectada a ele.

2.2.4.4. Malha

A topologia em malha refere-se a uma rede de computadores onde cada estação de trabalho está ligada a todas as demais directamente. Dessa forma, é possível que todos os computadores da rede, possam trocar informações directamente com todos os demais, sendo que a informação pode ser transmitida da origem ao destino por diversos caminhos. As vantagens desta topologia são: tempo de espera reduzido (devido a quantidade de canais de comunicação) e problemas na rede não interferem no funcionamento dos demais computadores. A desvantagem é o alto custo financeiro.

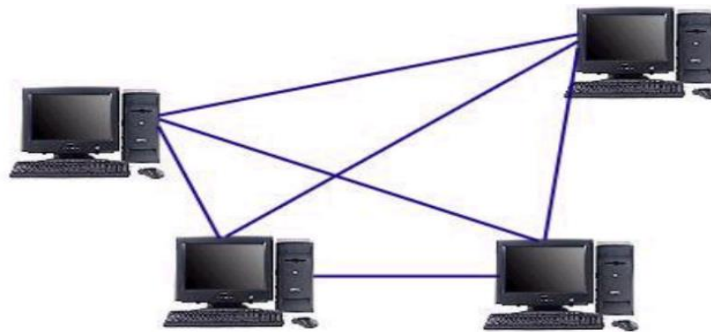


Figura 14: Topologia em malha

Fonte: Andrade (2015)

2.2.4.5. Árvore

Neste tipo de topologia um concentrador interliga todos os computadores de uma rede local, enquanto outro concentrador interliga as demais redes, fazendo com que um conjunto de redes locais sejam interligadas e dispostas no formato de árvore.

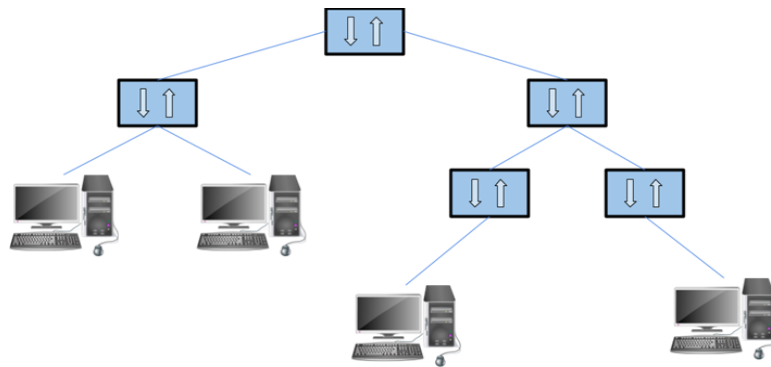


Figura 15: Topologia em árvore

Fonte: Macebo et al. (2018)

2.2.4.6. Híbrida

Essa topologia é aplicada em redes maiores que uma LAN. É chamada de topologia híbrida pois pode ser formada por diferentes tipos de topologia, ou seja, é formada pela união de topologias.

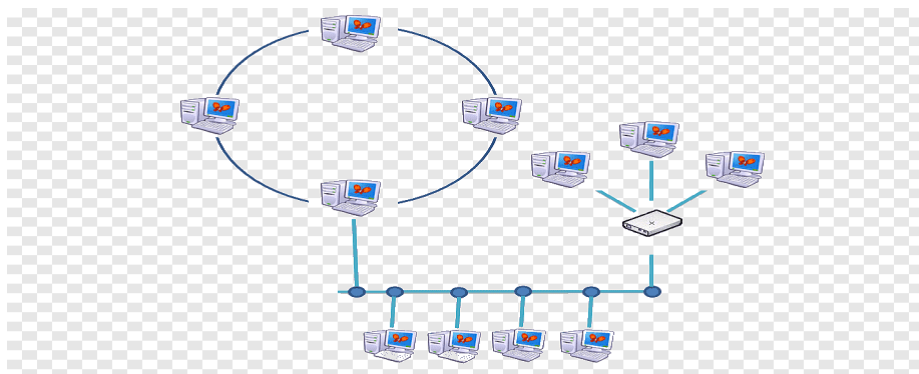


Figura 16: Topologia híbrida

Fonte: Macebo et al. (2018)

2.3. Firewall

Segundo Silva (2013), *Firewall* é uma solução de segurança baseada em *hardware* ou *software* que, a partir de um conjunto de regras ou instruções, analisa o tráfego da rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

Ferreira (2018, p.20), define *Firewall* como o ponto entre duas ou mais redes, que pode ser um componente ou um conjunto de componentes, no qual passa todo o tráfego,

permitindo que o controle, a autenticação e os registos de todo o tráfego sejam realizados.

O *firewall* actua como um filtro de pacotes, inspecciona todo e qualquer pacote que entra e sai. Os pacotes que atenderem aos critérios descritos nas regras formuladas pelo administrador da rede serão remetidos normalmente, mas os que falharem no teste serão descartados sem cerimônia (Tanenbaum & Wetherall, 2011). O *firewall* é uma combinação ou conjunto de *hardware* e *software* que isola a rede local de uma organização da rede pública, a Internet. Ele controla e regula o tráfego de dados dentro de uma rede ou entre redes distintas, impedindo a comunicação e acessos não permitidos de uma rede para outra.

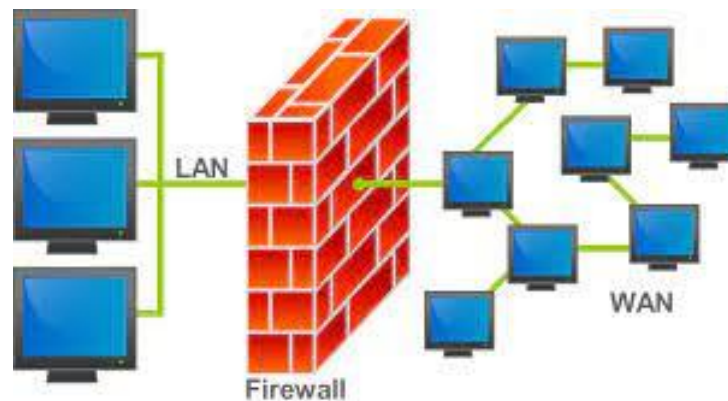


Figura 17: Exemplo de Firewall

Fonte: Silva (2013)

O *firewall* protege a rede interna contra tráfego indesejado proveniente do exterior da rede e contra a violação da privacidade da interna. Entretanto a implementação do *firewall* traz algumas desvantagens como:

- Constituindo o único ponto de entrada na rede controlada, se lhe for comprometido por um atacante, toda a rede interna pode ser comprometida também.
- Impacto do desempenho, visto que aumenta a latência ao tráfego entre a rede controlada e a internet, na medida em que o mesmo tem de ser analisado.

2.3.1. Tipos de Firewall

Segundo (Soeira et al., 2013), os tipos de *firewall* são: *firewall proxy*, *firewall* de inspeccção com estado, *firewall* de filtros de pacotes, *firewall* de gerenciamento unificado de ameaças (UTM), *firewall* de última geração e *firewall* virtual.

2.3.1.1. Firewall Proxy

O *firewall* de aplicação, também conhecido como *proxy* de serviços ou apenas *proxy* é uma solução de segurança que actua como intermédio entre um computador e uma rede interna e outra rede, normalmente a internet. Geralmente instalados em servidores potentes por precisarem lidar com um grande número de solicitações, *firewalls* desse tipo são opções interessantes de segurança porque não permitem a comunicação directa entre a origem e o destino (Soeira et al., 2013). No entanto, isso também pode afectar os recursos de rendimento e os aplicativos que ele pode suportar.

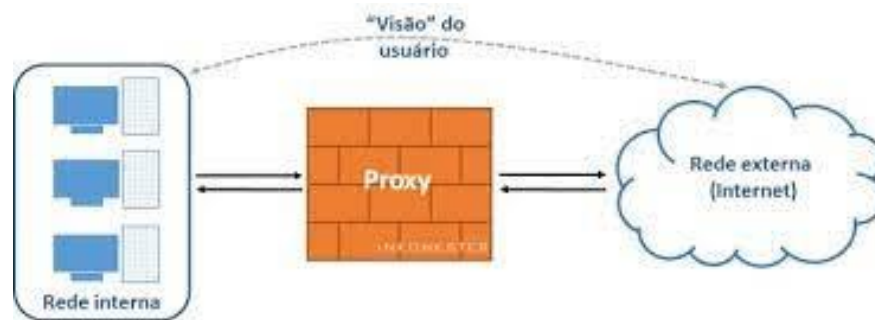


Figura 18: Firewall Proxy

Fonte: Soeira et al. (2013)

2.3.1.2. Firewall de Inspeção com estado

Considerado um *firewall* tradicional, um *firewall* de inspeção com estado permite ou bloqueia o tráfego com base no estado, porta e protocolo. Ele monitora todas as actividades, desde a abertura de uma conexão até o seu fechamento. As decisões de filtragem são feitas com base nas regras definidas pelo administrador e no contexto, que se refere ao uso de informações de conexões anteriores e pacotes pertencentes a mesma conexão.

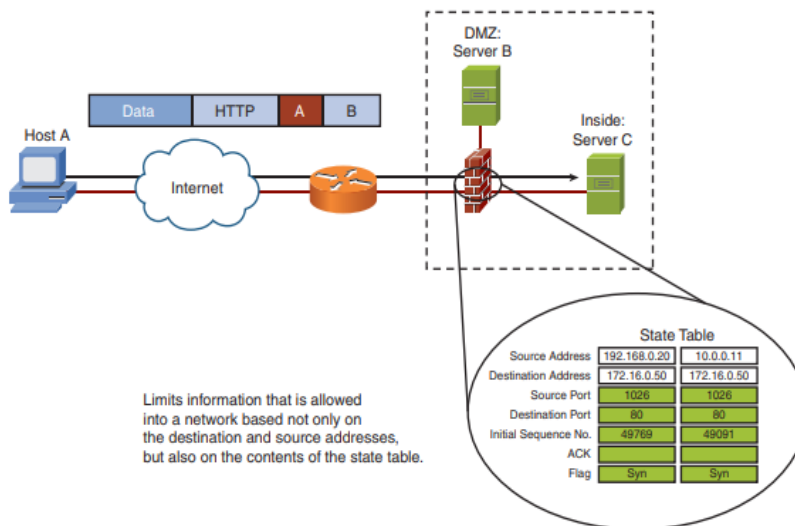


Figura 19: Firewall de inspeção com estado.

Fonte: Amaral (2012)

2.3.1.3. Firewall de filtro de pacotes

A filtragem de pacotes é o tipo de tecnologia *firewall* mais antigo e é muito utilizada actualmente. Como o nome sugere, um filtro de pacotes, com base numa lista de controlo de acesso, é aplicada a uma interface para filtrar pacotes que atravessam a interface. A lista de controle de acesso dita a política de segurança ou base de regras de *firewall* e especifica que o tráfego pode ou não atravessar o *firewall*.

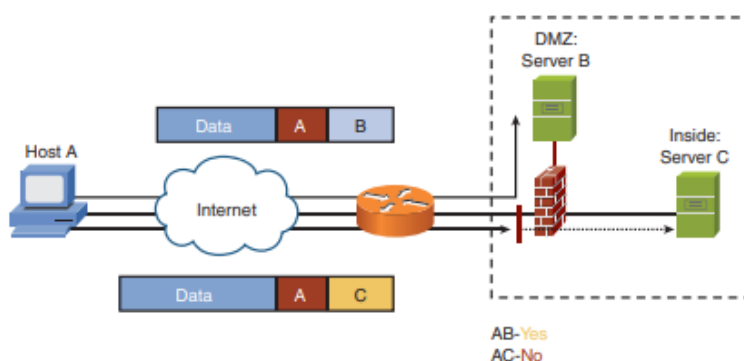


Figura 20: Firewall de filtro de pacotes.

Fonte: Macebo et al. (2018)

2.3.1.4. Firewall de Gerenciamento Unificado de Ameaças (UTM)

Um dispositivo UTM geralmente combina, de forma fracamente acoplada, as funções de um *firewall* de inspecção com estado com prevenção de intrusão de antivírus. Pode incluir serviços adicionais e, geralmente gerenciamento em nuvem. Os UTMs concentram-se na simplicidade e facilidade de uso.

2.3.1.5. Firewall de Última Geração (NGFW)

De acordo com Ferreira (2018), a maioria das empresas têm implantado *firewalls* de última geração para bloquear ameaças modernas, com o *malware* avançado e ataques de camada de aplicação. Um *firewall* de última geração inclui:

- Recursos de *firewall* padrão, como inspecção com estado;
- Prevenção de intrusos integrada;
- Conscientização e controle de aplicativos para ver e bloquear aplicativos perigosos;
- Atualização dos caminhos para incluir futuros feeds de informação;
- Técnicas para lidar com as ameaças de segurança em evolução.

2.3.1.6. NGFW focado em ameaças

Esse *firewall* inclui todos os recursos de um NGFW tradicional e também fornece detecção e correção avançada de ameaças. Com um NGFW focado em ameaças, pode-se:

- Saber quais activos estão em maior risco;
- Reagir rapidamente a ataques com automação de segurança inteligente que define políticas e fortalece suas defesas dinamicamente;
- Detectar melhor actividades evasivas ou suspeitos com a correlação de eventos de rede e *endpoint*;
- Diminuir significativamente o tempo desde a detecção até a limpeza com segurança retrospectiva que monitora continuamente actividades e comportamentos suspeitos, mesmo após a inspecção inicial.

2.3.1.7. Firewall virtual

Um *firewall* virtual normalmente implantado como um dispositivo virtual numa nuvem privada (*Vmware ESXi*, *Microsoft Hyper-V*, *KVM*) ou nuvem pública (*AWS*, *Azure*, *Google*, *Oracle*) para monitorar e proteger o tráfego em redes físicas e virtuais. Um *firewall* virtual costuma ser um componente-chave em redes definidas por *software*.

2.3.2. Arquitecturas de implementação de *firewall*

O principal objectivo do *firewall* é garantir que todos os dados que trafegam de uma rede para outra passem obrigatoriamente por ele. Para isso é aconselhável realizar uma avaliação da arquitectura na qual o sistema será implantado, assim como o grau de segurança exigido, podendo ser utilizado quantos níveis de acesso forem necessários para adequar esse sistema (Soeira et al., 2013).

Para Ferreira (2018), as principais arquitecturas são: *Dual-homed host*, *screened host* e *screened subnet*.

2.3.2.1. Arquitectura *Dual-Homed Host*

A arquitectura *dual-homed host* pode ser implementada por um *host* que apresenta duas interfaces de rede, uma para LAN e outra para a rede externa, tornando-se a única porta de entrada. Segundo Ferreira (2018), nessa arquitectura o roteamento é desabilitado, fazendo com que os pacotes não possam ser roteados entre as redes, garantindo o isolamento do tráfego, conforme mostra a figura 21.

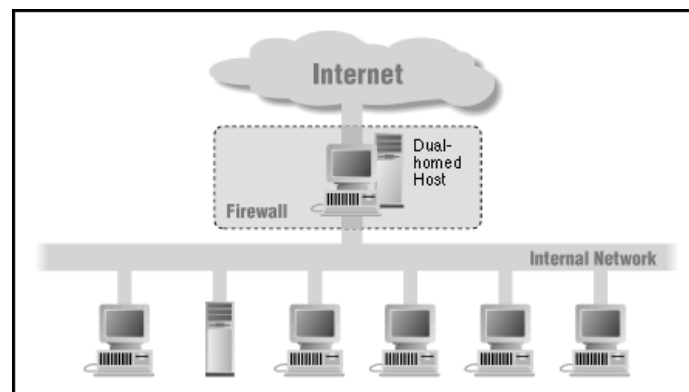


Figura 21: Arquitectura *Dual-Homed Host*.

Fonte: Ferreira (2018)

Assim, os pacotes IP de uma rede (por exemplo, a internet) não são directamente encaminhados para a outra rede (por exemplo, a rede interna protegida). Os sistemas internos e externos do *firewall* podem comunicar-se com *dual-homed host*, mas não podem se comunicar directamente uns com os outros. O tráfego IP entre eles é completamente bloqueado.

É um sistema de arquitectura simples, mas pode se tornar um problema, pois o acesso externo para o utilizador não é transparente, podendo tornar a rede indisponível (Ferreira, 2018). Essa arquitectura é indicada para uma rede que possua um tráfego pequeno para

internet, onde o tráfego à internet não seja vital para o negócio da empresa e que a mesma não provenha nenhum serviço para a internet.

2.3.2.2. **Arquitectura Screened Host**

Essa arquitectura é um pouco mais elaborada que a anterior, é formada por um filtro de pacotes e um *bastion host*. As regras de filtro devem permitir o tráfego para a rede interna através do *bastion host*, de modo que os usuários externos, que queiram aceder um sistema interno, devam primeiro se conectar ao *bastion host*. O *bastion host* funciona como um *proxy*, exigindo que os utilizadores internos acedam à internet através dele. Outra possibilidade é que os utilizadores internos tenham acesso aos serviços externos por meio de regras de pacotes do *bastion host*.

Um dos problemas dessa arquitectura é que caso o *bastion host* seja comprometido, o invasor já terá entrado na rede interna da organização. Outro problema é o filtro de pacotes e o *bastion host* que formam o único ponto de falha, de forma que, se ele for atacado, a comunicação da organização com a internet será comprometida.

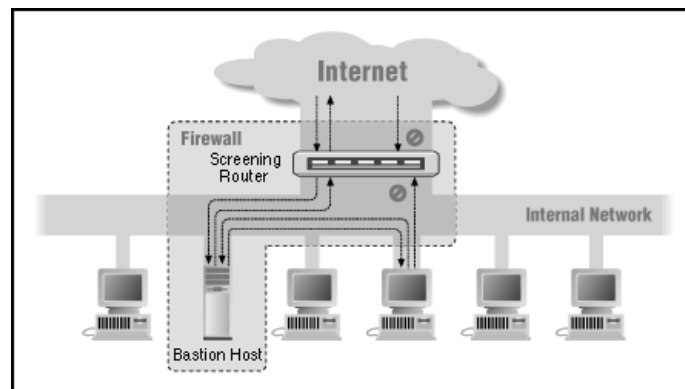


Figura 22: *Arquitectura Screened Host*

Fonte: Ferreira (2018)

2.3.2.3. **Arquitectura Screened Subnet**

Essa arquitectura também possui um *bastion host* na sua composição, a diferença entre essa arquitectura e a *screened host* é a adição de uma rede DMZ, o que aumenta ao nível de segurança. Nesse caso, o problema de ataque ao *bastion host*, que deixava a rede interna disponível para um invasor, não acontece. O *bastion host* fica na rede DMZ, que é considerada uma zona de confinamento entre a rede externa e a interna, existente entre dois filtros.

O filtro interno permite somente a passagem de requisições e respostas dos serviços permitidos aos utilizadores internos. Permitir o tráfego do *bastion host* para a rede interna comprometeria a segurança da mesma, caso ele seja atacado, além de ser desnecessário. O filtro externo permite o tráfego dos serviços disponíveis na DMZ, bem como o tráfego das requisições dos utilizadores internos. Nessa arquitectura existe uma variação comum que é a utilização de um equipamento com três interfaces de rede, uma para a rede externa, uma para a rede interna e outra para a DMZ.

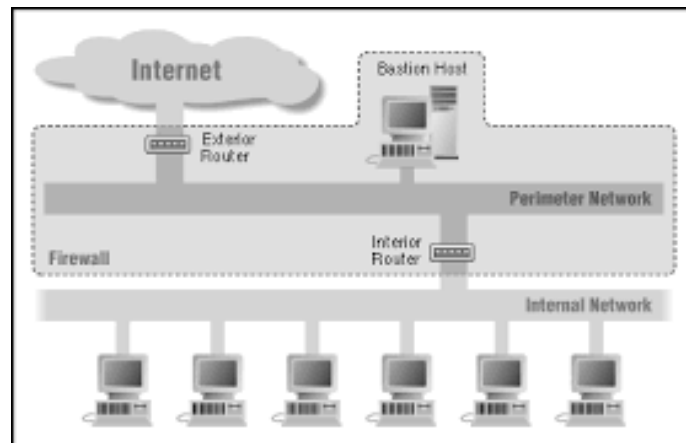


Figura 23: Arquitectura Screened Subnet.

Fonte: Ferreira (2018)

2.3.3. Políticas de *Firewall*

Segundo Franciscatto et al. (2014), uma política de *firewall* define como esses devem lidar com o tráfego da rede de entrada e saída, para endereços IP específicos e intervalos de endereços, protocolos, aplicativos e tipos de conteúdo. A maioria dos *firewalls* usa informações de cabeçalho de pacote para determinar se um pacote específico deve ter permissão para passar ou deve ser proibido.

Existem duas políticas de *firewall*: a política proibitiva e a política permissiva.

- **Política Proibitiva**

“Tudo o que não é expressamente permitido é proibido.” Com essa estratégia, os protocolos que poderão passar pelo *firewall* e os hosts específicos que podem passar dados são específicos. O que pode ser especificado pela política tem o acesso negado à rede.

- **Política Permissiva**

“Tudo o que não é expressamente proibido é permitido.” Nesse caso, é definido um conjunto de condições que irão resultar no bloqueio de dados. Qualquer host ou protocolo não coberto pela sua política será permitido por *default*.

O modelo de política proibitiva é mais seguro e comumente adotado pelas empresas.

2.3.4. Zonas em Firewall

De acordo com Amaral (2012), uma zona é uma ou mais interfaces virtuais ou físicas que foram combinadas em grupos. Essa coleção de interfaces geralmente representa um segmento da rede que possui mesmos requisitos de política de segurança. Isso permite que um administrador aplique facilmente as regras de política a todas as interfaces numa zona, numa só vez. As principais zonas são: DMZ, LAN e WAN.

a) Zona Desmilitarizada (DMZ - DeMilitarized Zone)

Tanenbaum & Wetherall (2011, p.529), afirma que a DMZ é a parte da rede da empresa que se encontra fora do perímetro de segurança e tudo passa por ali. A DMZ é uma zona para servidores acessados publicamente e é configurada com um nível de segurança que varia de 1 a 99% e pode conectar até cinco portas.

b) LAN - até seis portas podem pertencer a esta zona. O tráfego nesta zona é bloqueado por padrão e uma regra *firewall* deve ser criada para permitir qualquer conexão com ela. O tráfego entre portas na mesma zona, mas em redes diferentes, deve ter uma regra firewall LAN para a LAN criada. Esta zona considera-se, por padrão, com 100% de segurança.

c) WAN - a rede externa ou simplesmente a internet onde podemos encontrar todo tipo de tráfego proveniente de qualquer lugar do mundo, possui uma fraca segurança, sendo assim, essa zona é considerada de nível 0% de segurança, por padrão.

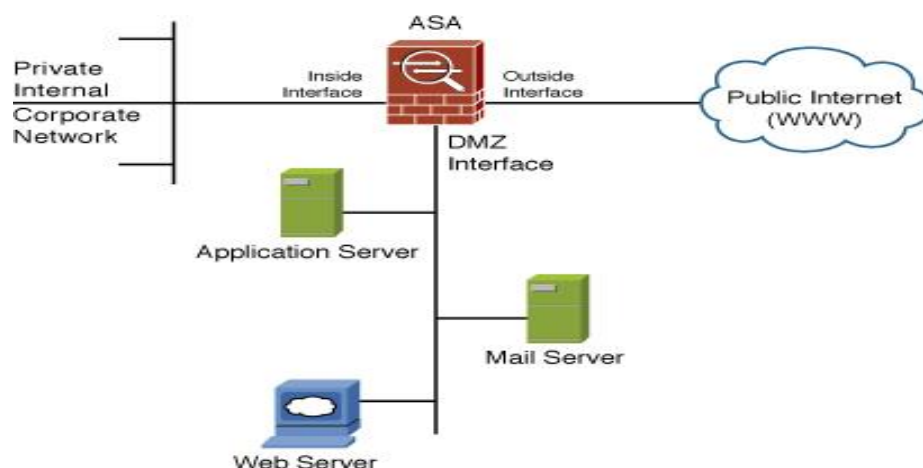


Figura 24: Zonas em firewall

Fonte: Amaral (2012)

2.4. Rotinas de *Backups*

Segundo Chemane et al. (sem data), backup são cópias de segurança dos arquivos de um computador. O objectivo do *backup* é armazenar a informação de uma organização (com processo de negócio baseados em TI), gerando uma cópia fiel dos dados essenciais, devendo ser criada e retida visando a recuperação em casos de perda ou desastres. Fazer *backup* de dados evita que os arquivos sejam permanentemente perdidos ou danificados em caso de algum incidente como, por exemplo, uma falha humana.

Para J. Silva et al. (2015), existem várias formas de realizar a cópia desses arquivos. Pode ser através de uma simples cópia de um local de armazenamento para outro, como também de forma programada e específica através de ferramentas de *backup*.

2.4.1. Tipos de *Backup*

De acordo com Cavalcanti (2021), os tipos de *backup* são completo, incremental e diferencial.

2.4.1.1. *Backup* Normal ou Completo

Um *backup* completo copia todos os arquivos seleccionados e marca-os como arquivos que já passaram pelo *backup*. Segundo Cavalcanti (2021), esse tipo de *backup* possui algumas vantagens como a disponibilidade da cópia de todos os dados num único

conjunto de mídia, maior possibilidade de recuperar os dados íntegros, menor complexidade e tempo na operação de recuperação dos dados. No *backup* completo a leitura e escrita de todo o sistema de arquivos é lenta e requer mais espaço de armazenamento. Geralmente o *backup* completo é feito no primeiro dia.

2.4.1.2. Backup Incremental

De acordo com Chemane et al. (sem data), um *backup* incremental copia somente os arquivos criados ou alterados desde o último backup normal ou incremental e marca-os como arquivos que já passaram pelo *backup*. Uma das suas vantagens é a redução do tamanho dos *backups*, uma vez que apenas uma pequena percentagem de arquivos muda num determinado tempo, tornando assim o *backup* mais rápido. A desvantagem desse tipo de *backup*, segundo Cavalcanti (2021), é na recuperação de dados, envolvendo um procedimento mais complexo e potencialmente mais lento, pois depende da recuperação do último *backup* completo para, em seguida, recuperar os dados incrementais. O *backup* incremental deve ser feito do segundo dia em diante, para copiar apenas os novos arquivos criados.

2.4.1.3. Backup Diferencial ou Acumulativo

No *backup* diferencial apenas os dados modificados desde o último *backup* completo são copiados (Cavalcanti, 2021). O processo de recuperação de dados inicia restaurando o último *backup* diferencial apropriado. A recuperação é mais simples, pois exige apenas o último *backup* completo e o último *backup* diferencial. Porém, a restauração completa pode levar mais tempo do que se for usado o *backup* completo.

O *backup* pode ser classificado com relação ao estado de aplicação; *hot* (quente) e *cold* (frio). No processo de *cold backup* (*offline backup*) a aplicação encontra-se inativa, enquanto que no *hot backup* (*online backup*) a aplicação está em execução com os utilizadores acedendo os dados. A disponibilidade do serviço não é comprometida no *hot backup*, no entanto existe uma degradação do desempenho.

2.4.2. Armazenamento de dados

Segundo Costa & Delcastanher (2004), todos os sistemas de armazenamento de dados são classificados em três grandes grupos: *storages* DAS, NAS e SAN. A variação da nomenclatura está associada na forma como os computadores se conectam entre eles.

2.4.2.1. Armazenamento Directamente Conectado (DAS - *Direct Attached Storage*)

É um armazenamento digital conectado directamente ao sistema (ao computador ou servidor) através de um cabo interno, para a leitura ou gravação de informações. Essa conexão é física, directa e os dados não podem ser acessados sem um host. Esse tipo de armazenamento pode ser útil na preservação de informações em redes instáveis e é uma forma fácil de transferir pequenos arquivos no dia-a-dia. No entanto, o DAS não é a melhor opção nos critérios escalabilidade e compartilhamento, pois só podem ser acessados por um dispositivo, dificultando a distribuição da informação.

2.4.2.2. Armazenamento Conectado à Rede (NAS - *Network Attached Storage*)

NAS é um tipo de armazenamento em que os dados podem ser acessados facilmente em redes internas, por diferentes dispositivos. As informações ficam registadas num *hardware* servidor. É uma boa possibilidade para centralizar dados, controlando o seu acesso por utilizadores que pertencem à rede. Além disso, é possível demandar por mais espaço e transferir arquivos com mais facilidade do que com dispositivos DAS.

2.4.2.3. Área de Armazenamento em Rede (SAN - *Storage Area Network*)

As SANs são infra-estruturas de rede que interligam servidores e unidade de armazenamento para proporcionar maior segurança e performance no tráfego de dados. Uma SAN unifica os recursos de armazenamento numa infra-estrutura de dados através de uma rede exclusiva, independente e de alto desempenho. Uma infra-estrutura SAN exige cabeamento próprio, controladores de barramento e switches. Trata-se de uma rede voltada a eliminar os gargalos entre sistemas de armazenamento, servidores e estações de trabalho.

Cada servidor e sistema de armazenamento numa rede SAN devem estar interligados e essas conexões físicas devem suportar altos níveis de transmissão de dados, visando proporcionar uma largura de banda para todas as aplicações. Desta forma, se um servidor precisar acessar qualquer storage numa rede SAN, uma solicitação de acesso é enviada para esse dispositivo, utilizando essa rede exclusiva para a comunicação e tendo todo o acesso controlado e gerenciado conforme regras previamente estabelecidas.

2.4.2.4. Sistema de agregação e protecção de disco

A necessidade de armazenar cada vez mais informação cresceu mais rapidamente que a capacidade dos discos magnéticos podiam oferecer isoladamente. Uma solução foi desenvolvida para atender a essa necessidade, baseada num processo de agregação e virtualização de vários discos, criando-se um disco virtual de maior capacidade.

Almeida (2006, p.39) afirma que o conceito de agregação de discos magnéticos surgiu para aumentar a capacidade e melhorar o desempenho e a disponibilidade dos dispositivos de armazenamento. As funções básicas de agregação de discos são: concatenação, distribuição, espelhamento de combinação.

a) RAID

O RAID (*Redundant Array of Independent Disk*) é uma tecnologia na qual os dados são armazenados de forma distribuída entre grupos de discos para conseguir, simultaneamente, redundância e taxas mais altas de transferência de dados. Ao invés de armazenar os dados num único disco rígido que pode falhar, o RAID mantém uma forma de redundância de informação baseada nos dados gravados entre diversos discos. Almeida (2006, p.40) descreveu seis configurações combinando múltiplos discos.

- **RAID 0** - distribuição de dados em vários discos (*Striping*). Neste caso, as informações são espalhadas em vários discos para se ter um desempenho maior fazendo a gravação em paralelo entre eles. As taxas de transferência são muito altas, porém não há protecção contra falha nos discos. Isto é, se um dos discos falha, todo o volume lógico será comprometido. O RAID 0 é ideal para armazenamento não crítico de dados que precisam ser lidos e gravados em alta velocidade.
- **RAID 1 (Espelhamento)** – todos os dados são sempre gravados em dois ou mais discos, o que fornece a mais alta confiabilidade de dados. Para leitura, a taxa de transferência de dados é mais alta do que para um único disco, pois pode ler de qualquer um dos discos simultaneamente.
- **RAID 2** – distribuição de dados em vários discos, com informação de redundância (paridade) sendo gravada em múltiplos discos. A paridade que se usa é o código de detecção de erros, Hamming Code. Na prática, não é um método usado porque as próprias controladoras de discos actuais já possuem mecanismos de detecção e correcção de erros.

- **RAID 3** – distribuição de dados em vários discos com um disco adicional com redundância (paridade). Todos os discos trabalham de forma sincronizada e a gravação é feita de forma simultânea, em tiras (*stripes*) por todos os discos de dados. No disco de paridade, a informação é a operação lógica XOR de todos os dados da “tira”. No caso de falha de qualquer disco, é possível continuar a entregar dados a partir dos discos restantes.
- **RAID 4** – similar ao RAID 3, porém não trabalha de maneira sincronizada e a informação básica da “tira”, usada para calcular a redundância, é um bloco de dados.
- **RAID 5** – similar ao RAID 3, entretanto ao invés de usar a paridade num único disco, todos os discos contêm tiras para dados e tiras para armazenar a paridade dos outros discos do grupo RAID.

3. Capítulo III – Caso de Estudo

3.1. Ordem dos Engenheiros de Moçambique

Segundo o Estatuto da Ordem dos Engenheiros de Moçambique (OrdEM), presente no Boletim da República, Lei nº 16/2002, a OrdEM é uma pessoa colectiva, de direito público, representativa dos engenheiros em exercício em Moçambique, que em conformidade com os preceitos do Estatuto e demais disposições legais aplicáveis, exercem a engenharia. A OrdEM é independente dos órgãos do estado, regendo-se por regras próprias. A OrdEM tem personalidade jurídica e goza de autonomia administrativa, financeira, patrimonial, científica e regulamentar.

3.1.1. Missão

A OrdEM tem como missão:

- Liderar o processo da engenharia pondo-a ao serviço do desenvolvimento nacional;
- Registrar e acreditar os engenheiros que querem exercitar a engenharia em Moçambique;
- Zelar pelo cumprimento das regras de ética profissional e o nível de qualificação profissional dos engenheiros;
- Defender os interesses, direitos e prerrogativas dos seus membros;
- Zelar pela função social, dignidade e prestígio da profissão de engenheiro;
- Fomentar o desenvolvimento do ensino e investigação da engenharia;
- Promover, organizar e apoiar a formação contínua dos seus membros e outros técnicos de engenharia;
- Contribuir para a estruturação das carreiras dos engenheiros;
- Atribuir e proteger o título profissional de engenheiro, promovendo o procedimento judicial contra quem o use ou exerça ilegalmente;
- Promover a cooperação e solidariedade entre os seus membros;
- Prestar a colaboração técnica e científica solicitada por quaisquer entidades, públicas ou privadas, quando exista interesse público;
- Desenvolver relações com outras Ordens e associações afins, nacionais e estrangeiras, podendo aderir uniões e federações internacionais;
- Exercer jurisdição disciplinar sobre os engenheiros;
- Zelar pela qualidade e segurança dos estudos, projectos e obras de engenharia;

- Apoiar o governo, tecendo pareceres sobre projectos de desenvolvimento de infra-estruturas públicas, licenciamento de empreiteiros para obras públicas, contratação de engenheiros estrangeiros e sobre outros assuntos relacionados com a engenharia, desde que haja interesse público.

3.1.2. Visão

Regular a actividade de engenharia em Moçambique, através do registo e certificação e do exercício da acção disciplinar e de controlo sobre os profissionais desse ramo ao abrigo na Lei nº 16/2002 de 26 de Junho, que determina que a inscrição e reconhecimento pela OrdEM são condições obrigatórias para o exercício da actividade de Engenharia em Moçambique.

3.1.3. Colégios de especialidade

De acordo com o Estatuto da OrdEM, designa-se por engenheiro o titular de licenciatura, ou equivalente legal em curso de engenharia, inscrito na OrdEM como membro efectivo, e que se ocupa da aplicação das ciências técnicas respeitantes aos diferentes ramos de engenharia nas actividades de investigação, concepção, estudo, projecto, fabrico, construção, reparação, operação, manutenção, produção, fiscalização e controlo de qualidade, incluindo a coordenação e gestão dessas actividades e outras com elas relacionadas.

Entende-se por colégio de especialidade um vasto domínio de actividade da engenharia, com características técnicas e científicas próprias, que assuma no país, grande relevância económica e social. Para além das que vierem a ser reconhecidas pelos órgãos competentes da OrdEM, estão desde já estruturadas na OrdEM, os colégios de especialidades:

- Engenharia Civil;
- Engenharia Electrotécnica;
- Engenharia Mecânica;
- Engenharia de Minas e Geotécnica;
- Engenharia Química;
- Engenharia Agronómica e Florestal;
- Engenharia Informática e de Computadores;
- Engenharia Geográfica.

Tendo em conta o número de membros existentes nas especialidades acima indicadas, estão presentemente em vigor cinco especialidades, nomeadamente:

- Engenharia Civil;
- Engenharia Electrotécnica;
- Engenharia Mecânica;
- Engenharia Química;
- Engenharia Agronómica e Florestal.

Os membros cujas especialidades não fazem parte da lista acima indicada em função dos respectivos currículos dos candidatos, o comité de avaliação e qualificação integra-os nos colégios de especialidades com alguma similaridade.

Os titulares de licenciatura, ou equivalente legal, em curso de engenharia com uma especialidade ainda não estruturada na OrdEM, são inscritos naquela que o conselho de admissão e qualificação considere como a mais adequada de entre as especialidades reconhecidas.

A estruturação organizativa de novas especialidades e a constituição de novos colégios competem ao conselho directivo, sob parecer do conselho de admissão e qualificação, ouvido os presidentes dos conselhos de colégio de especialidade.

3.1.4. Membro da Ordem dos Engenheiros de Moçambique

Ser membro da OrdEM é cumprir com os requisitos da Lei nº 16/2002 de 26 de Junho criada com o objectivo de regular a actividade de engenharia em Moçambique, através do registo e certificação e do exercício da acção disciplinar e de controlo sobre os profissionais desse ramo. Ao abrigo da Lei em referência, a inscrição e reconhecimento pela OrdEM são condições obrigatórias para o exercício da actividade de engenharia em Moçambique.

Os membros da OrdEM distribuem-se pelas seguintes categorias: membro efectivo, estagiário, honorário, colectivo e correspondente.

- **Membro Efectivo:** membro cuja a admissão está sujeita a titularidade de licenciatura ou equivalente legal, em curso de engenharia, e prestação, com sucesso, de provas ou estágios, para o efeito, realizados pela OrdEM.
- **Membro Estagiário:** tem a categoria de membro estagiário o titular de licenciatura ou equivalente legal, em curso de engenharia, conferido por instituições de ensino

superior, nacionais ou estrangeiras que esteja a efectuar estágio ou provas de admissão a membro efectivo da OrdEM nos termos do nº 2 do Artigo 8 do Estatuto da OrdEM,

- **Membro Honorário:** indivíduo ou colectividade que, exercendo ou tendo exercido actividade de reconhecido interesse público e contribuído para a dignificação e prestígio da engenharia, seja considerado como merecedor de tal distinção. Actualmente, na OrdEM não há algum membro honorário.
- **Membro Colectivo:** pessoa colectiva que com ela estabeleça acordo escrito e que desenvolva actividades de formação, investigação, aplicação ou difusão do conhecimento em área directamente relacionada com a engenharia, ou ainda tenha a engenharia como uma das suas áreas profissionais. Exemplo: Organizações como a Mozal.
- **Membro Correspondente:** o profissional com grau académico de licenciado que, não exercendo a profissão de engenheiro nem tendo a respectiva formação escolar, exerça actividades afins e apresente um currículo valioso, como tal reconhecido pelo órgão competente da OrdEM ou membro de associações congéneres estrangeiras que confirmam igual tratamento aos membros da OrdEM. Isto é, um indivíduo que pratica actividades de engenharia, mas não é licenciado em engenharia.

3.2. Situação actual

A Ordem dos Engenheiros de Moçambique tem a sua sede na cidade de Maputo, podendo abrir delegações ou outras formas de representação em todo o território moçambicano. A OrdEM possui uma página *Web* cujas actualizações são feitas por demanda.

A rede de computadores da OrdEM é composta por um *router*, um *switch*, um *FileServer*, um *access point*, três impressoras (duas *wireless* e uma a cabo) e seis computadores clientes (quatro do tipo *desktop* e dois *notebooks*), como mostra a figura abaixo.

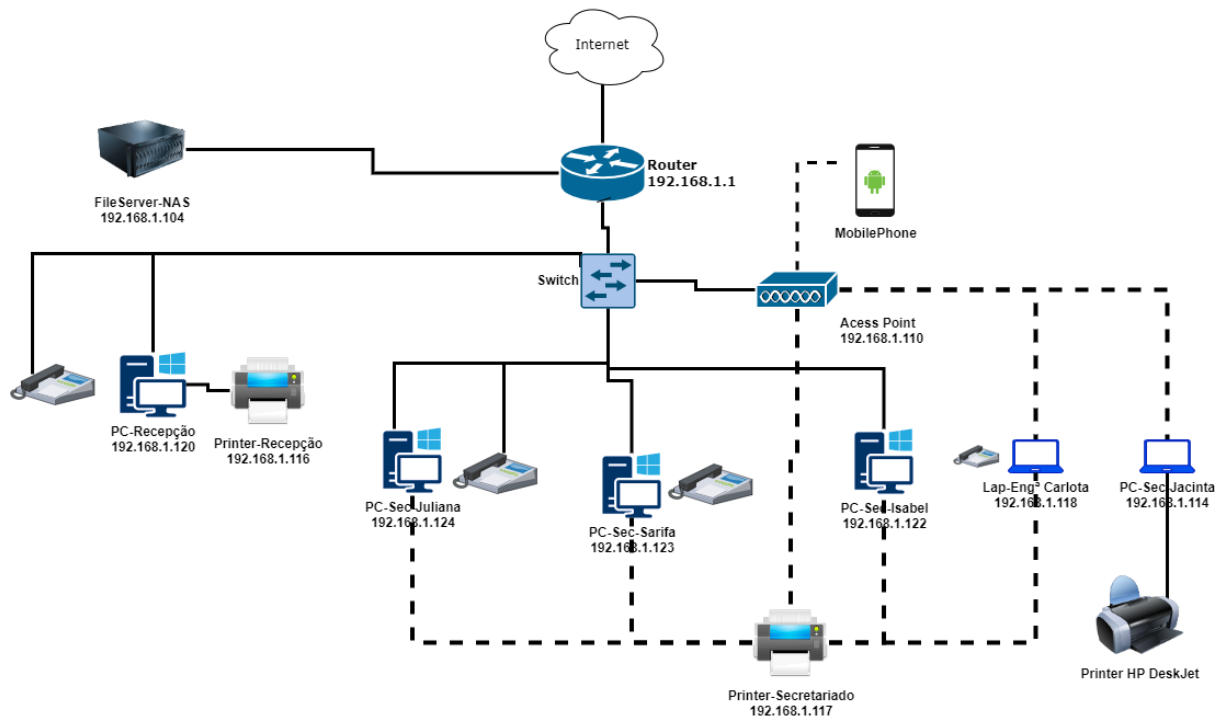


Figura 25: Diagrama da rede LAN da OrdEM.

Fonte: Elaborada pela autora

- O Router tem um firewall integrado, porém desabilitado, um serviço DHCP activo, um protocolo de segurança WPS activo e a DMZ desabilitada.
- O *FileServer* usa um sistema de armazenamento do tipo NAS, portanto todos os usuários permitidos podem ter acesso à informação lá armazenada através da rede. O NAS da OrdEM tem uma configuração RAID 1, com dois discos rígidos de 1TB cada, formando o Volume 1. No NAS foram criados dois usuários, *secgeral* e *secretariado*. Actualmente o RAID 1 é o único sistema de backup implementado.
- Os computadores da OrdEM usam o Sistema Operativo *Windows 10 Pro*, com licença vitalícia, o pacote *Office 2016* e o antivírus *Kaspersky Internet Security*.

3.2.1. Constrangimentos Identificados

- Não existe um esquema de actualização da página *Web* da OrdEM, assim sendo, não se sabe com que período deve ser feita alguma actualização e nem o responsável (a pessoa que fornece a informação) pela mesma. Actualmente são demandadas actualizações de informações urgentes ou críticas e as outras páginas ficam “esquecidas”;

- Até então a rede LAN da OrdEM não foi documentada, o que dificulta o processo de comunicação e diagnóstico de problemas;
- Embora tenha sido configurado o RAID 1 no servidor NAS, no caso de ocorrência de um desastre, que destrua o dispositivo físico do *FileServer* incluindo os dois discos que formam o volume lógico, toda a informação contida lá será perdida;
- Na rede LAN da OrdEM não foi implementado nenhum tipo de *firewall* (que é a linha de defesa contra todo o tipo de ameaça da rede externa), portanto a rede está susceptível à invasão de vírus, *malwares* ou agentes que façam uso dos recursos da rede para fins maléficos, correndo o risco de perder os dados ou mesmo o controle da rede;
- Ainda que uma parte dos dados essenciais para o funcionamento da OrdEM esteja armazenada num servidor centralizado (NAS), existem arquivos armazenados em computadores individuais, com informação crítica, que não possuem nenhuma rotina de *backups* implementada. Sendo o sistema parcialmente centralizado, quando for implementada uma rotina de backup para os arquivos armazenados nos computadores, será necessário trabalhar em cada um dos computadores.

4. Capítulo IV – Desenvolvimento da solução proposta

Nesse capítulo, inicialmente serão apresentados os resultados de algumas actividades executadas durante o estágio profissional na OrdEM e posteriormente será apresentada uma proposta de infra-estrutura da rede LAN da OrdEM, tendo em conta os constrangimentos verificados na situação actual.

4.1. Rotina de Actualização da Página Web da OrdEM

Foi elaborado um plano geral do *website* da OrdEM (vide no anexo 3), onde estão listadas todas as páginas do *website*, a periodicidade das actualizações e o responsável por fornecer as informações para efeitos de actualização. Dessa forma, será simples saber quando determinada página deve ser actualizada e quem será o responsável pela disponibilização da informação.

4.2. Documentação da rede LAN da OrdEM

A documentação apresentada a seguir pertence a rede do diagrama mostrada no capítulo III (caso de estudo), figura 25. O Diagrama da rede da OrdEM foi desenhado utilizando a ferramenta *Draw.io*, também conhecida por *Diagrams.net*, que é um software de desenho gráfico multiplataforma gratuita e de código aberto desenvolvido em HTML5 e JavaScript. É usada também para criar diagramas como fluxogramas, wireframes, diagramas UML e organogramas.

| Dispositivo | Marca | Interface | Endereço IP | Máscara | Gateway |
|--------------|----------|-----------|----------------|---------------|----------------|
| Router | TP-Link | WAN | 197.249.18.196 | 255.255.248.0 | 197.249.23.254 |
| | | LAN | 192.168.1.1 | 255.255.255.0 | ---- |
| Switch | TP-Link | LAN | ---- | 255.255.255.0 | 192.168.1.1 |
| Access Point | Ubiquiti | LAN | 192.168.1.110 | 255.255.255.0 | 192.168.1.1 |
| FileServer | D-Link | LAN | 192.168.1.104 | 255.255.255.0 | 192.168.1.1 |
| Printer | HP | NIC | 192.168.1.116 | 255.255.255.0 | 192.168.1.1 |
| Printer | HP | NIC | 192.168.1.117 | 255.255.255.0 | 192.168.1.1 |
| Computador | HP | NIC | 192.168.1.120 | 255.255.255.0 | 192.168.1.1 |
| Computador | HP | NIC | 192.168.1.124 | 255.255.255.0 | 192.168.1.1 |
| Computador | HP | NIC | 192.168.1.123 | 255.255.255.0 | 192.168.1.1 |
| Computador | HP | NIC | 192.168.1.122 | 255.255.255.0 | 192.168.1.1 |
| Computador | HP | NIC | 192.168.1.118 | 255.255.255.0 | 192.168.1.1 |
| Computador | HP | NIC | 192.168.1.114 | 255.255.255.0 | 192.168.1.1 |

| IPs disponíveis | DHCP | Local | Usuário | Senha | Descrição |
|-----------------|---------|--------------|------------|-------|---------------------------------|
| ---- | ---- | ---- | ---- | ---- | ---- |
| 254 | 110-199 | Secretariado | Admin | ***** | <i>Firewall</i> desabilitado |
| 24 | YES | Secretariado | ---- | ---- | <i>Switch</i> não gerenciável |
| 80 | YES | Secretariado | OrdEM | ***** | ---- |
| ---- | NO | Secretariado | Admin | ***** | RAID 1 |
| ---- | YES | Recepção | ---- | ---- | --- |
| ---- | YES | Secretariado | ---- | ---- | ---- |
| ---- | YES | Recepção | Serafina | ***** | <i>Desktop</i> |
| ---- | YES | Recepção | Juliana | ***** | <i>Desktop</i> |
| ---- | YES | Secretariado | Sarifa | ***** | <i>Desktop</i> |
| ---- | YES | Secretariado | Isabel | ***** | <i>Desktop</i> |
| ---- | YES | Secretariado | Sec. Geral | ***** | <i>Notebook</i> |
| ---- | YES | Secretariado | Jacinta | ***** | <i>Notebook</i> |

Tabela 2: Documentação da rede LAN da OrdEM

Fonte: Elaborado pela autora

Para descobrir todos os dispositivos pertencentes à rede da OrdEM, com os respectivos endereços IP, máscara e marca foram usados dois programas, o Nmap (vide no anexo 1) e o *Fing* (vide no anexo 2). O Nmap faz o scan completo da rede, apenas com o endereço IP da rede, desde que o computador do usuário que pretende *scanear* esteja conectado à essa rede. O *scan* é feito através do código *nmap -sP ip da rede/slash*, na linha de comandos. O *Fing* é uma aplicação *android* que *scaneia* a rede, apenas conectando o *smartphone* à rede, através do *wi-fi*. Para ter acesso as configurações do *Router* e do *File Server*, foi usado um *browser*, o IP, o *username* e a *password* de acesso ao painel de configuração de cada dispositivo.

4.3. Implementação de uma rotina de *Backups*

De modo que haja recuperação dos arquivos críticos para o funcionamento da OrdEM, armazenados nos computadores dos funcionários da OrdEM, caso ocorra um incidente ou desastre, foi usado o *Google Drive*, que é um serviço de armazenamento e sincronização de arquivos em nuvem da empresa *Google*. *Google Drive* foi instalado em

cada computador, utilizando uma única conta de *login* para todos. Em seguida foi criada uma pasta na conta do *Google Drive*, “OrdEM”, que contém quatro pastas referentes aos usuários dos computadores com informação crítica, nomeadamente, “Serafina”, “Sarifa”, “Isabel” e “Juliana”. Foram copiadas todas as pastas dos arquivos relevantes de cada um dos usuários para o *Google Drive*, estabelecendo a sincronização entre o *Google Drive* e os computadores. Desta forma, sempre que se precisar trabalhar sobre os arquivos sincronizados, o utilizador deverá dirigir-se à pasta do *Google Drive* no *File Explorer* do seu computador, seguindo o caminho, da figura abaixo e entrar na pasta que contenha o seu nome.

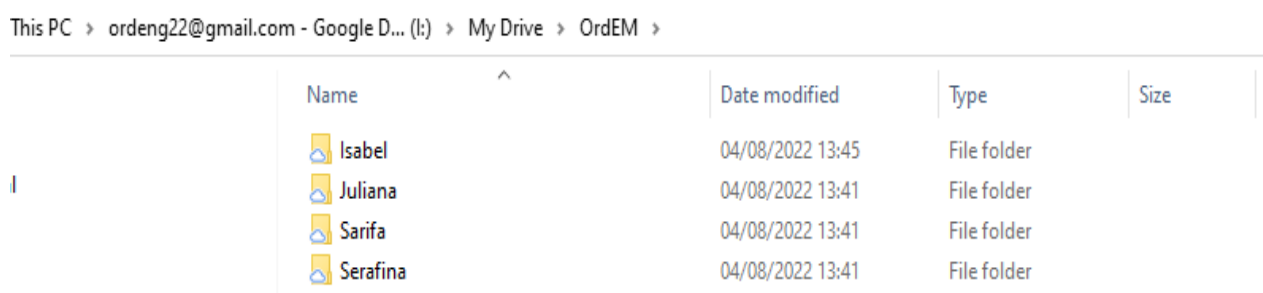


Figura 26: Directório das pastas do *Google Drive* no *file explorer*

Fonte: Capturado pela autora

No *Google Drive* as pastas estão organizadas desta forma:

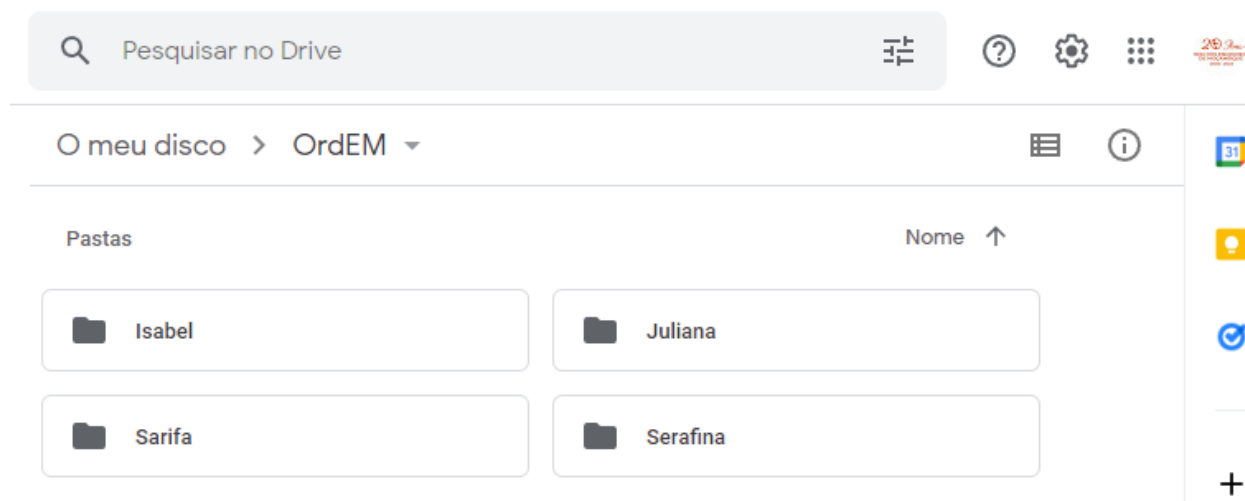


Figura 27: Pastas no *Google Drive*

Fonte: Capturado pela autora

Assim, por mais que os arquivos sejam apagados no *File Explorer*, por falhas humanas ou outro tipo de incidente, estes podem ser recuperados e restaurados na caixa de “lixo”

da *google drive*, que conserva os arquivos excluídos por cerca de 30 dias e após esse período os arquivos serão apagados definitivamente.

Para a informação armazenada no NAS foi implementado um tipo de *backup*, o RAID 1. Sendo assim, no caso de uma unidade falhar, os dados não precisarão ser reconstruídos, apenas precisará serem copiados para a unidade de substituição. Porém esse tipo de *backup* é ariscado, pois se ocorrer um roubo, incidente ou desastre que destrua o servidor, toda a informação lá contida será comprometida ou perdida totalmente, pensando nisso, foi proposto que se fizesse uma imagem do NAS ou se implemente um software de backup do NAS, como por exemplo o Hyper Backup.

4.4. Proposta de solução

Para a resolução dos constrangimentos identificados no capítulo III (caso de estudo), propôs-se uma arquitectura centralizada para administração da rede local da OrdEM, descrita na figura abaixo.

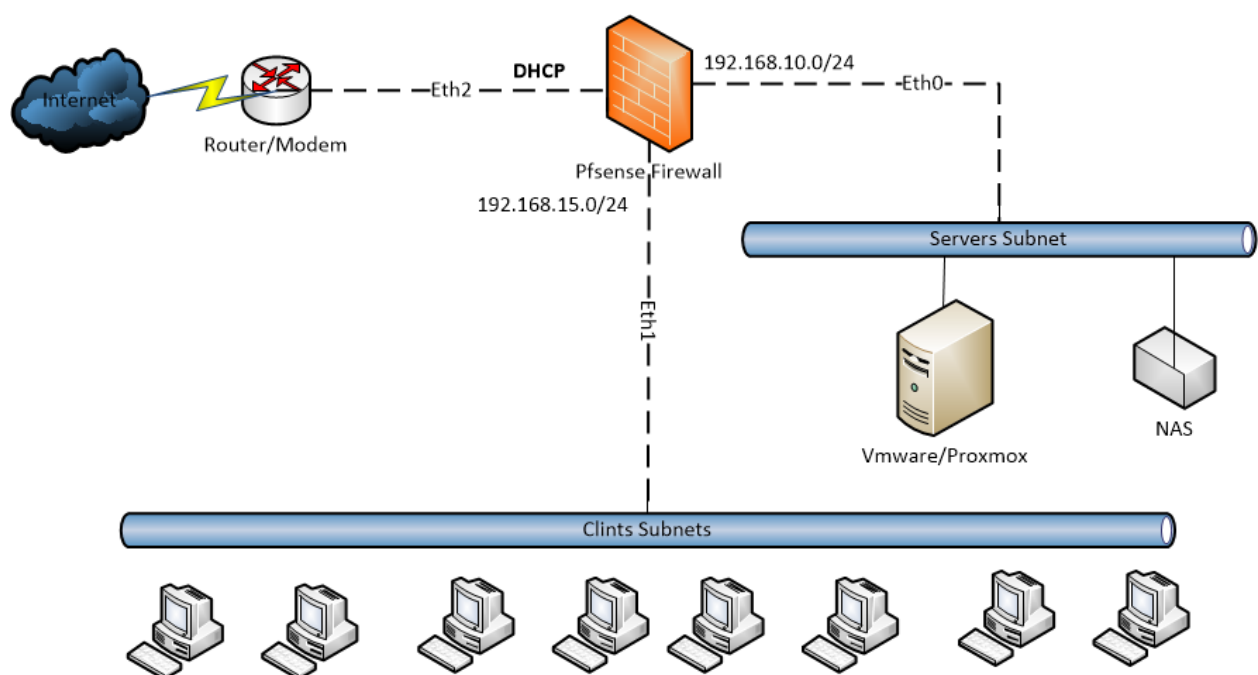


Figure 28: Arquitectura da solução proposta

Fonte: Elaborada pela autora

4.4.1. Princípio de funcionamento

A solução proposta tem o seguinte princípio de funcionamento: #

1. O acesso à *Internet* é fornecido por um ISP, o router presente na infra-estrutura da ordem é que realiza a conexão através da porta WAN.
2. Através da porta LAN do *router* a infra-estrutura da OrdEM tem o acesso à *Internet*
3. O *firewall* escolhido pelo autor é o *pfsense*, que é uma ferramenta, *open-source* muito útil para infra-estruturas de gestão de redes e activos de informação de uma organização. Será instalado num computador da OrdEM que possui pelo menos três placas de rede e será ligado ao *router*, dessa forma, agirá como filtro que recebe os pedidos dos clientes e envia respostas de acordo com as regras de segurança especificadas.
4. A solução é composta por duas sub-redes, uma sendo para os clientes, que são as estacoes de trabalho da OrdEM e a outra será para os servidores.
5. Na sub-rede dos servidores terá um servidor de gestão da infra-estrutura da OrdEM e um servidor de armazenamento de arquivos (NAS). O servidor de gestão será virtualizado pois pretende-se a alta disponibilidade, performance e escalabilidade. O NAS funcionará como armazenamento de *backups* para toda a infra-estrutura, nomeadamente: (i) máquinas virtuais, (ii) pastas partilhadas e outros.
6. Uma das máquinas virtuais será o Windows Server, onde serão activados serviços como DNS, AD-DS, *file transfer*, *printers* e outros para garantir que a centralizado.

Serviços:

Alguns dos serviços que serão configurados no Windows Server são:

- **DHCP:** será activado para a distribuição dinâmica de IPs para todos os dispositivos da rede da OrdEM, definindo um intervalo (*range*) de IPs.
- **DNS:** será activado para converter nomes de domínio legíveis por humanos em endereços IP legíveis por máquinas.
- **AD-DS:** será activado para o controle da rede e fornecerá os serviços de diretório necessários para estabelecer um domínio, incluindo o repositório de dados que armazena informações sobre objectos na rede e as disponibiliza para os usuários da OrdEM.

- **Configuração de impressoras:** para o compartilhamento de recursos a grupos específicos da OrdEM.

4.4.2. Testes da solução

Como forma de compreender o funcionamento da solução foi instalada a ferramenta VMware, onde foi instalado o Windows Server 2012 R2 com o propósito de simular a solução proposta. Os resultados da simulação são apresentados no Anexo 4.

O computador utilizado para efectuar os testes possui as seguintes especificações de *hardware*:

- Processador: Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz
- Memória RAM: 4GB
- Disco Rígido: 1 TB
- Sistema operacional: Windows 10 Pro 64bits

5. Capítulo V – Discussão de resultados

5.1. Definição do problema

A elaboração do presente trabalho surgiu de vários propósitos apresentados na definição do problema, tais como: (i) a ausência de rotinas de *backup* de informação, o que pode originar a perda da mesma e, conseqüentemente, uma pausa do trabalho; (ii) a ausência da documentação da rede local da OrdEM, o que dificulta o processo de comunicação e diagnóstico de problemas; (iii) elevado nível de exposição ao vírus informático nos computadores da OrdEM. Ao longo da realização do estágio profissional, os três propósitos provaram-se verdadeiros.

A definição do problema constituiu a primeira e o mais importante marco para a realização do presente trabalho.

5.2. Revisão da literatura

A revisão da literatura visou, primeiro, abordar de forma geral os sistemas de informação, apresentando os seus conceitos e classificações. Em seguida, abordou-se os principais conceitos sobre redes de computadores, tais como conceitos, aplicações, classificação das redes de computadores, principais componentes e as topologias. Depois debruçou-se do *firewall*, concretamente os tipos, as arquitecturas de implantação, políticas e zonas de *firewall*. E por fim foram abordados conceitos relacionados com rotinas de *backups*, onde foram apresentados os tipos de *backups* e sistemas de armazenamento de dados.

Na revisão da literatura pôde-se verificar que o tema administração de sistemas de computadores é muito amplo, dessa forma, a autora pegou apenas os aspectos mais relacionados com os problemas definidos.

5.3. Caso de estudo

No caso de estudo abordou-se, primeiro, a descrição da OrdEM, especificamente a visão, missão, colégios de especialidades e o ser membro da OrdEM. Com isso a autora pretendia dar a entender ao leitor, de uma forma geral, o funcionamento e os serviços que a OrdEM se pressupõe.

Em seguida foi descrita a situação actual da OrdEM, identificando os constrangimentos enfrentados. Toda a informação desse capítulo foi adquirida com base em observações, conversas com os funcionários da OrdEM, reuniões com o supervisor da OrdEM e através do estatuto da OrdEM.

5.4. Desenvolvimento da proposta de solução

No desenvolvimento da proposta de solução foram apresentados os resultados de algumas actividades praticadas ao longo do estágio profissional na OrdEM, nomeadamente, o esquema geral da página *web*, a documentação da rede local e a implementação de rotinas de *backups*. Em seguida, foi proposta uma arquitectura centralizada, focando-se na resolução dos problemas identificados. Depois descreveu-se o funcionamento da solução proposta, a qual é baseada em três pilares descritos no capítulo IV, nomeadamente (i) implementação de um *firewall*; (ii) servidores e (iii) estações de trabalho. E por fim, foram feitos alguns testes e simulações de modo a compreender melhor a implementação da solução proposta.

6. Capítulo VI – Considerações finais

6.1. Constrangimentos

Durante a realização do trabalho foram enfrentados alguns constrangimentos, destacando-se a falta de uma orientação prática na execução das actividades de administração da rede de computadores, o que provocava receio por parte da autora, por se tratar de uma instituição muito séria. O tempo limitado previsto para a realização do trabalho. Outro constrangimento foi verificado na actividade atribuída pelo supervisor da instituição, a instalação e gestão de um sistema de registo de incidentes de utilizadores, que seria um marco muito grande para o trabalho, visto que seria um tema novo abordado num trabalho de final de curso. Porém, por muito tempo, houve uma confusão referente ao objetivo da instalação do dito sistema, o que obrigou a autora a retirá-lo do trabalho.

6.2. Conclusões

O presente trabalho teve como ponto de partida, para a sua realização, diversas actividades de administração de sistemas de computadores atribuídas pelo supervisor da instituição, onde foram identificados os problemas da rede local da OrdEM, desde a ausência de backups da informação crítica para o funcionamento da OrdEM até ao elevado nível de exposição ao vírus. Desta forma, o trabalho tem como objetivo geral – conceber e implementar um conjunto de boas práticas no âmbito da gestão da LAN da OrdEM. Os pontos apresentados no capítulo IV constituem um conjunto de boas práticas.

Os objectivos específicos foram igualmente alcançados, pois foi possível, na revisão da literatura, abordar os principais conceitos relacionados à administração de sistemas de computadores, desde o conceito de sistemas de computadores até às rotinas de *backups*.

No capítulo IV foram apresentados os seguintes pontos: a concepção da implementação de rotinas de actualização da página *web* da OrdEM, a documentação da rede local, a implementação de rotinas de *backups* e por fim, a proposta de uma arquitectura centralizada de redes de computadores.

6.3. Recomendações

A ambição da autora era também implementar um sistema de registo de incidentes de utilizadores, que funcionaria como *service desk*, que ofereceria suporte e respostas à solicitações, reclamações, problemas e incidentes que podem ser registados por clientes ou outros utilizadores do sistema de computadores ou serviços de uma organização, de modo a garantir qualidade dos serviços. Recomenda-se que pesquisas posteriores sejam dedicadas a esses tipos de sistemas.

Bibliografias

- [1]. Almeida, Arivaldo. 'Arquitecturas de rede de armazenamento de dados'. Instituto de Computação-Universidade Estadual de Campinas, 2006.
- [2]. Andrade, Jorge. 'Gestão de Redes e Sistemas'. Porto, 2015.
- [3]. Atlassian. 'Integração Do Jira Service Management e Jira Software'. Accessed 23 July 2022. <https://www.atlassian.com/br/software/jira/service-management/jira-integration>.
- [4]. Cavalcanti, Tiago. 'Rotinas De Backup e Prevenção de Vírus'. *Estrategia Concursos*, 2021, 15.
- [5]. Chemane, Lourino, Ivone Cipriano, and Délcio Chadreca. 'Cópia de Segurança e Raid'. Maputo, n.d.
- [6]. Costa, João Pedro, and Ricardo Delcastanher. 'Internet small computer system interface: Um estudo de caso para storage area network'. Universidade Federal de Santa Catarina, 2004.
- [7]. Demo, Pedro. *Metodologia Científica em Ciências Sociais*. São Paulo: Atlas, 1996.
- [8]. Farinha, Carlos. 'Administração de Sistemas de Informação I'. 2015, n.d., 17.
- [9]. Ferreira, Adriano. 'Análise Comparativa de Tecnologias de Firewall para Empresas'. Instituto Federal de Educação, Ciência e Tecnologia, 2018.
- [10]. Fontanetti, Leonardo. 'Segurança Da Informação Em Redes Empresariais Com Firewalls Netfilter'. Faculdade de Tecnologia de Americana, 2018.
- [11]. Franciscatto, Roberto, Fernanda Cristo, and Tiago Perlin. *Redes De Computadores*. Santa Maria: UFSM, 2014.
- [12]. Gil, António Carlos. *Métodos e Técnicas de Pesquisa Social*. 5th ed. São Paulo: Atlas, 1999.
- [13]. Gouveia, Luís, and João Ranito. *Sistemas de Informação de Apoio à Gestão*. © SPI – Sociedade Portuguesa de Inovação., 2011.
- [14]. Lakatos, Eva, and Marina Marconi. *Metodologia Científica*. 3ª. Brasil: Atlas, 1999.
- [15]. Lampert, Edna, and Greisse Badalotti. *Sistemas de Informação*. 5ª. Brasil: Indaial : UNIASSELVI, 2015.

- [16]. Leeuwen, H. J. van. '[Back complaints; a continuing problem]'. *Tijdschrift Voor Ziekenverpleging* 28, no. 15 (22 July 1975): 689–95.
- [17]. Macebo, Ricardo, Roberto Franciscatto, Guilherme Cunha, and Cristiano Bertolini. *Redes de Computadores*. 1ª. Brasil: Santa Maria RS: UFSM, 2018.
- [18]. Mendes, Francisco. *Administração de Sistemas Informáticos*. Vol. 1. Rio de Janeiro: Fundação CECIERJ, 2009.
- [19]. WEKA. 'NAS vs. SAN vs. DAS | Data Storage Comparison | Pros & Cons | Weka IO'. Accessed 7 August 2022. <https://www.weka.io/learn/nas-vs-san-vs-das-storage-comparison/>.
- [20]. Neves, Filipe, Leonardo Machado, and Rodrigo Centenário. 'Implantação de Firewall Pfsense'. Universidade Tecnológica Federal do Paraná, 2014.
- [21]. 'Ordem Dos Engenheiros de Moçambique'. Accessed 14 August 2022. <https://ordeng.org.mz/>.
- [22]. Pera, Bruno. *Apostila de Redes*. Brasil: UNIVAP, 2021. <https://www.univap.br/COLEGIOS>.
- [23]. Soeira, Bárbara, Fernando Silva, and Letícia Taborda. 'Implementação do Firewall Cisco ASA 5500'. Universidade Tecnológica Federal do Paraná, 2013.
- [24]. Tanenbaum, Andrew S, and David J Wetherall. *Redes de Computadores*. 5ª. São Paulo: Pearson Prentice Hall, 2011.
- [25]. Tulloch, Mitch. *Introducing Windows Server 2012 R2*. Redmond, Washington: Microsoft, 2013.
- [26]. Turato, Egberto Ribeiro. *Tratado da metodologia da pesquisa clínico-qualitativa*. 2nd ed. Brasil: Editora Vozes, 2004.
- [27]. Verma, Dinesh Chandra. *Principles of Computer Systems and Network Management*. Heidelberg [u.a.]: Springer, 2009.

Outras Bibliografias

- [1]. Pereira, Rafaela. 'Desenvolvimento e Implementação de Sistemas e Tecnologias de Informação'. Universidade de Coimbra, 2010.

- [2]. Rodrigues, Wilson. 'Análise dos procedimentos de backup dos institutos federais'. UFPE, 2017. <http://www.cin.ufpe.br/~posgraduacao>.
- [3]. Silva, João, Sylvio Neto, and Eugênio Almeida. 'Análise de um sistema de Backup/Recovery para grandes volumes de dados', 2015, 11.
- [4]. Silva, Lucas Rodrigues. 'Estudo comparativo de soluções de Firewalls: Netfilter/Iptables'. Faculdade Campo Limpo Paulista, 2013.
- [5]. Sistemas para armazenamento de dados: Tudo sobre DAS, NAS e SAN. 'Sistemas para armazenamento de dados: Tudo sobre DAS, NAS e SAN'. Accessed 7 August 2022. <https://www.controle.net/faq/sistemas-para-armazenamento-de-dados-das-nas-san>.

Anexos

Anexo 1: Scan da rede local da OrdEM através do Nmap

```
Administrator: Command Prompt
Nmap done: 1 IP address (0 hosts up) scanned in 3.85 seconds

C:\>nmap route -n
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-29 10:05 GMT Summer Time
Failed to resolve "route".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.51 seconds

C:\>nmap -sP 192.168.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-29 10:09 GMT Summer Time
Nmap scan report for 192.168.1.1
Host is up (0.0048s latency).
MAC Address: C4:E9:84:66:A9:3E (Tp-link Technologies)
Nmap scan report for 192.168.1.104
Host is up (0.0040s latency).
MAC Address: CC:B2:55:8A:FF:0B (D-Link International)
Nmap scan report for 192.168.1.110
Host is up (0.0040s latency).
MAC Address: 78:8A:20:53:68:A9 (Ubiquiti Networks)
Nmap scan report for 192.168.1.116
Host is up (0.13s latency).
MAC Address: 7C:76:35:41:05:D2 (Intel Corporate)
Nmap scan report for 192.168.1.117
Host is up (0.010s latency).
MAC Address: 48:9E:BD:55:7C:BE (HP)
Nmap scan report for 192.168.1.120
Host is up (0.0060s latency).
MAC Address: 10:62:E5:01:83:F1 (Hewlett Packard)
Nmap scan report for 192.168.1.122
Host is up (0.0030s latency).
MAC Address: 10:62:E5:01:84:6F (Hewlett Packard)
Nmap scan report for 192.168.1.123
Host is up (0.0020s latency).
MAC Address: 10:62:E5:01:84:64 (Hewlett Packard)
Nmap scan report for 192.168.1.124
Host is up (0.0010s latency).
MAC Address: 10:62:E5:01:84:06 (Hewlett Packard)
Nmap scan report for 192.168.1.112
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 4.46 seconds
```

Figura 29: Scan da rede através do Nmap

Fonte: Capturado pela autora

Anexo 2: Scan da rede local da OrdEM através do Fing

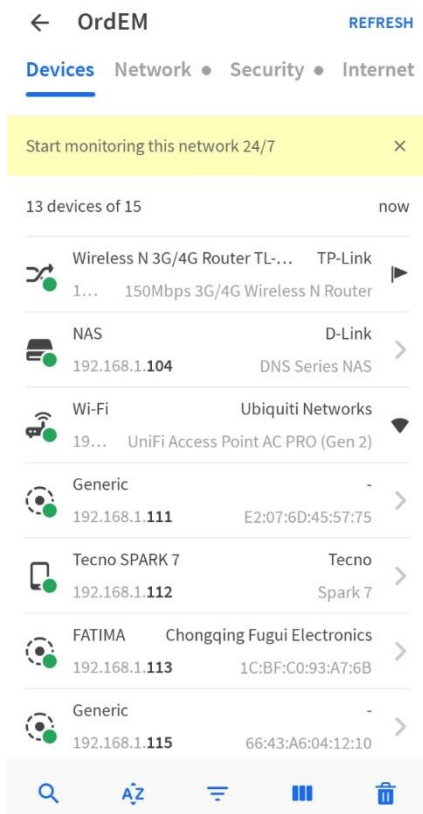


Figura 30: Scan da rede a partir do Fing

Fonte: Capturado pela autora

Anexo 3: Plano Geral da Página Web da OrdEM

Plano Geral da Página Web da OrdEM

Nas Réguas de Tabuladores
 ↓
 No Painel de Navegação
 ↓

Doc.
 Nº 1
 Vers. Inicial
 15-Abril-2022

| Ficha Nº | Nº | | Nível 1 Nív2 | | |
|------------|----------|--|---|--------------------------------------|--------------------------------------|
| | | | | | |
| | 1 | | Homepage Ordem dos Engenheiros de Moçambique | Periodicidade da Actualização | Responsável Pela Actualização |
| 1.1 | 1.1 | | A ORDEM | | |
| | 1.1.1 | | Mensagem do Bastonário | Trimestralmente | Bastonário |
| | 1.1.2 | | Missão | De 5 em 5 anos | |
| | 1.1.3 | | Visão | D De 5 em 5 anos | |
| | 1.1.4 | | Atribuições | D De 5 em 5 anos | |
| | 1.1.5 | | Estatutos | D De 5 em 5 anos | |
| | 1.1.6 | | Plano Estratégico | D De 5 em 5 anos | |
| | 1.1.7 | | Contactos | Por demanda | Secretariado |
| 1.2 | 1.2 | | ÓRGÃOS | | |
| | 1.2.1 | | Assembleia Geral | De 5 em 5 anos | |
| | 1.2.2 | | Bastonário | De 5 em 5 anos | |
| | 1.2.3 | | Conselho Directivo | De 5 em 5 anos | |
| | 1.2.4 | | Conselho Consultivo | De 5 em 5 anos | |
| | 1.2.5 | | Conselho Fiscal | De 5 em 5 anos | |
| | 1.2.6 | | Conselho Jurisdicional | De 5 em 5 anos | |
| | 1.2.7 | | Conselho de Admissão e Qualificação | De 5 em 5 anos | |
| | 1.2.8 | | Órgãos Sociais Eleitos | De 5 em 5 anos | |
| 1.3 | 1.3 | | O ENGENHEIRO | | |
| | 1.3.1 | | Lista de Inscritos | Mensalmente | Secretariado |
| | 1.3.2 | | Título de Engenheiro | De 5 em 5 anos | |
| | 1.3.3 | | Colégios de Especialidade | De 5 em 5 anos | |
| | 1.3.4 | | Código Deontológico | De 5 em 5 anos | |
| | 1.3.5 | | Requisitos para inscrição | Por demanda | |
| | 1.3.6 | | Ficha de Incrição | Por demanda | |
| | 1.3.7 | | Sistema de Gestão de Membro | Sistema em Construção | |

| | | | | | |
|-------|------------------------|----------------|---|-----------------------------------|-----------------|
| 1.4 | 1.4 | O MEMBRO | Servidor indisponível | Secretariado | |
| | | 1.4.1 | Actualização de Dados | | Trimestralmente |
| | | 1.4.2 | Lista de Membros com Dados Actualizados | | De 5 em 5 anos |
| | | 1.4.3 | Porquê ser Membro | | Trimestralmente |
| | | 1.4.4 | Membro Honorári | | Trimestralmente |
| | | 1.4.5 | Membro Colectivo | | Trimestralmente |
| | | 1.4.6 | Membro Correspondente | | Trimestralmente |
| | | 1.4.7 | Quota de Membro | | De 5 em 5 anos |
| | | 1.4.8 | Forma de Pagamento de Quotas | | De 5 em 5 anos |
| 1.4.9 | Regulamento de Estágio | De 5 em 5 anos | | | |
| 1.5 | 1.5 | PUBLICAÇÕES | Anualmente | Eng. ^a Carlota Salomão | |
| | | 1.5.1 | Relatório da OrdEM 2019 | | Anualmente |
| | | 1.5.2 | Boletim N°1 2020 | | Anualmente |
| | | 1.5.3 | Demonstração de Resultados Orç ### | | Anualmente |
| | | 1.5.4 | Mapa de Reintegração e Amortização da OrdEM e (Autosaved) | | Anualmente |
| | | 1.5.5 | Protocolo OrdEM e OEP | | Anualmente |
| | | 1.5.6 | Discurso do Bastonário | | Por demanda |
| 1.5.7 | Comunicações Técnicas | Por demanda | | | |
| 1.6 | 1.6 | AGENDA | Por demanda | Secretariado | |
| | | 1.6.1 | Anúncios | | Por demanda |
| | | 1.6.2 | Eventos Internacionais | | Por demanda |
| | | 1.6.3 | Palestras | | Por demanda |
| | | 1.6.4 | Seminários | | Por demanda |
| | | 1.6.5 | Congressos | | Por demanda |
| | | 1.6.6 | Desporto | | Por demanda |
| 1.7 | 1.7 | GALERIA | Por demanda | Secretariado | |

Figura 31: Plano geral da página web da OrdEM

Fonte: Capturado pela autora

Anexo 4: Testes do Windows Server 2012 R2

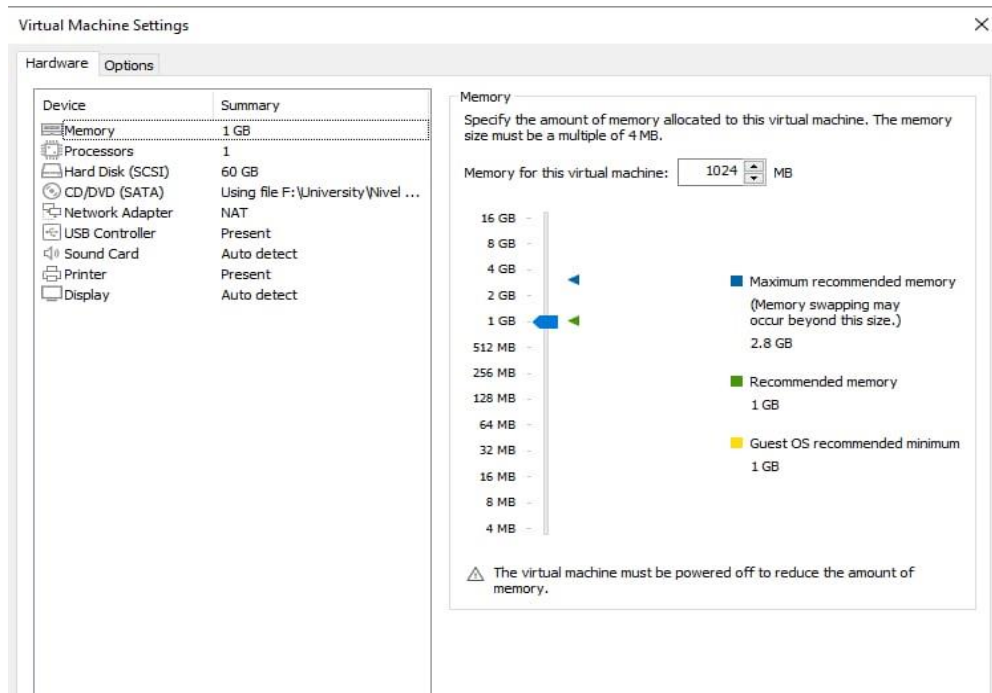


Figura 32: Configuração dos requisitos do Windows Server 2012

Fonte: Capturado pela autora

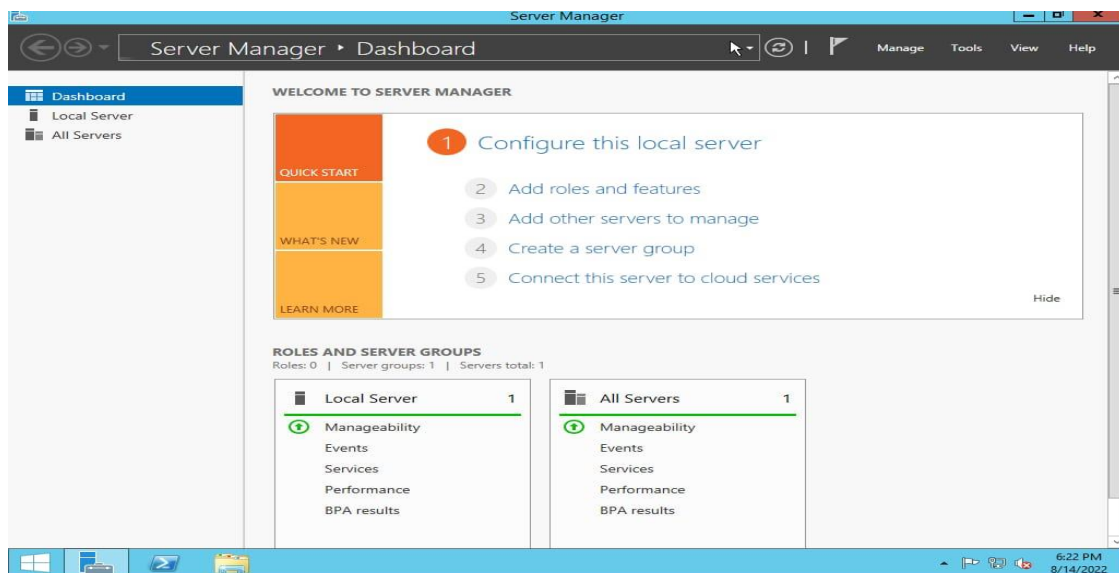


Figura 33: Server Manager Dashboard

Fonte: Capturado pela autora

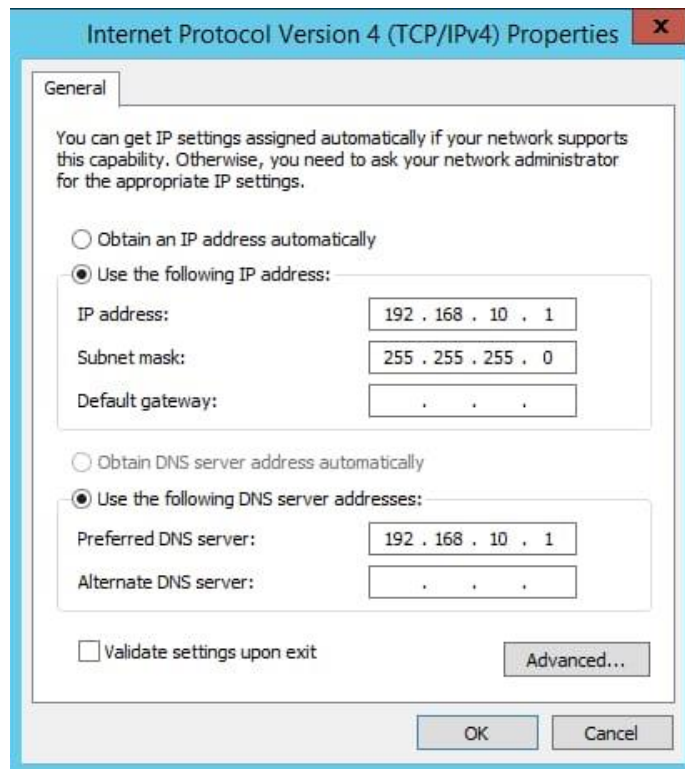


Figura 34: Atribuição de um IP fixo ao servidor

Fonte: Capturado pela autora

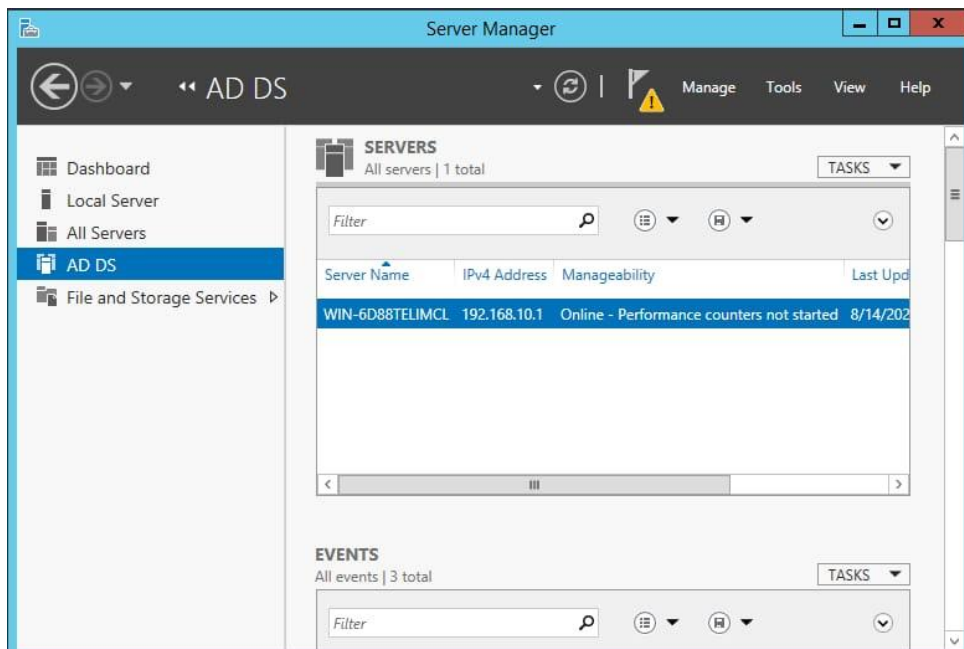


Figura 35: AD-DS

Fonte: Capturado pela autora

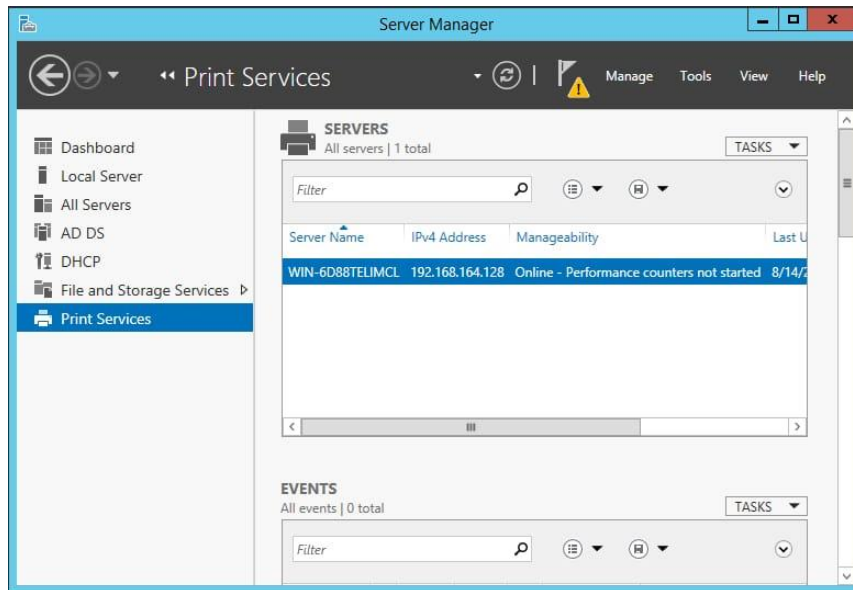


Figura 36: Serviços de impressão

Fonte: Capturado pela autora

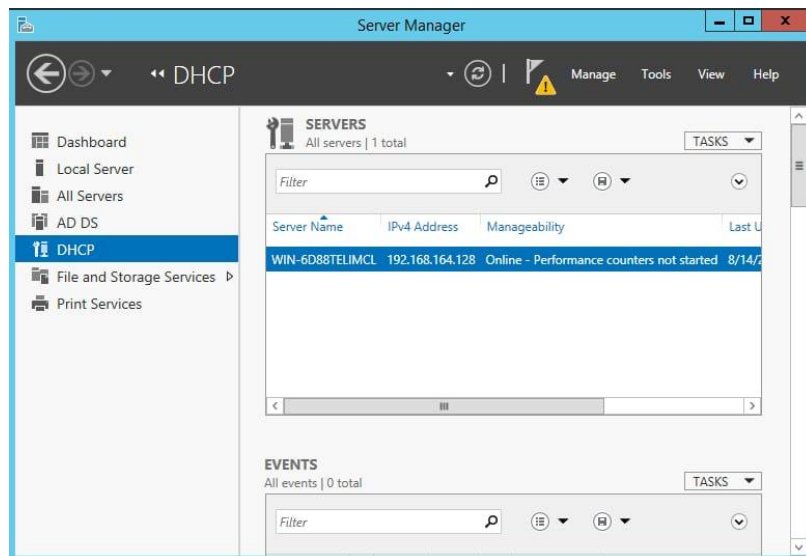


Figura 37: Serviço DHCP

Fonte: Capturado pela autora

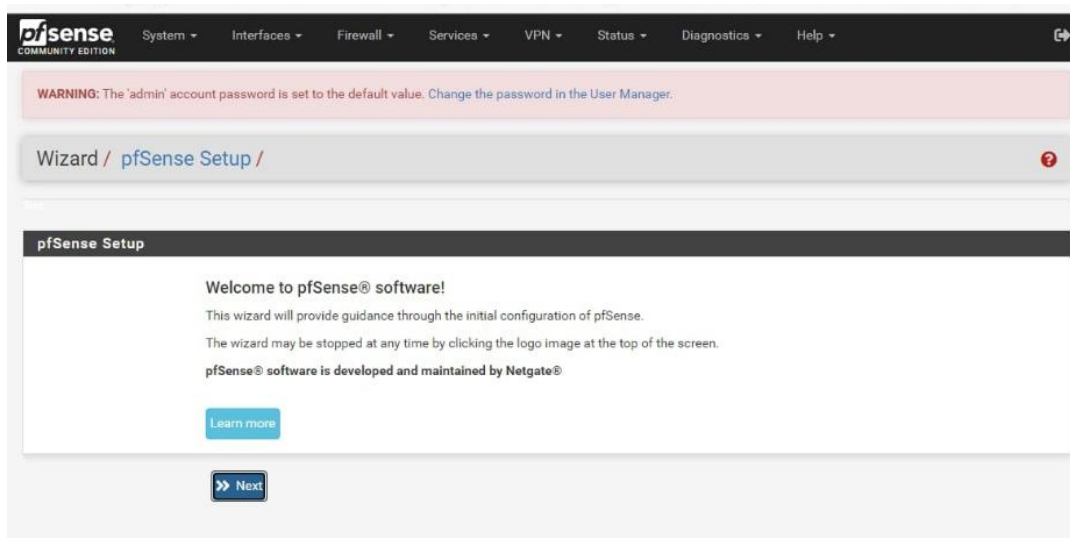


Figura 38: Tela inicial do Pfsense

Fonte: Capturado pela autora

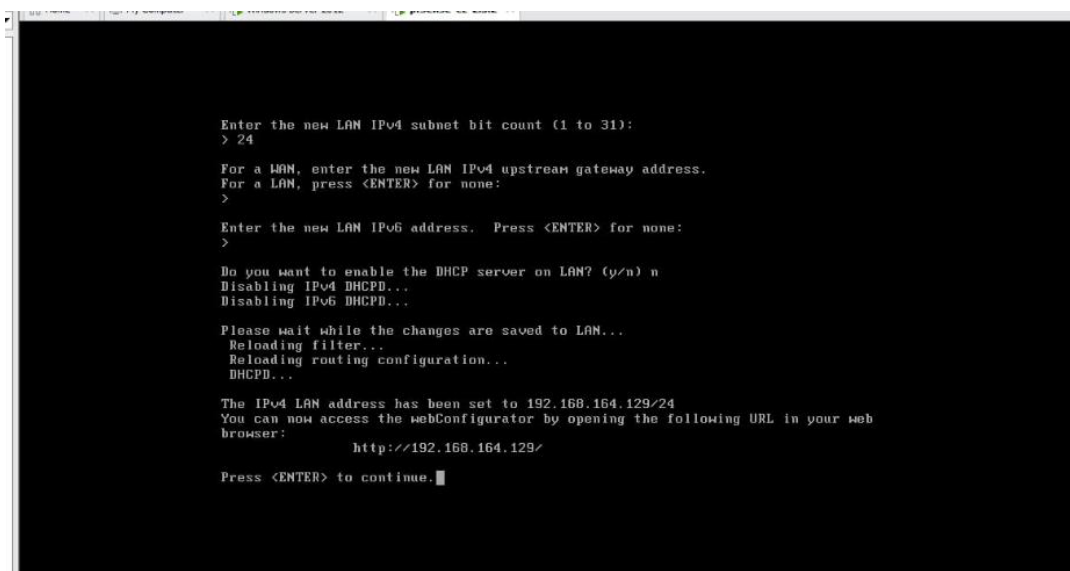


Figura 39: Atribuição de um IP para o WebConnector do pfsense

Fonte: Capturado pela autora