



INSTITUTO
SUPERIOR
DE ANGOLA

DEPARTAMENTO DE ENGENHARIA
LICENCIATURA EM ENGENHARIA INFORMÁTICA

**PROPOSTA DE IMPLEMENTAÇÃO DE UMA REDE PRIVADA
VIRTUAL NO INSTITUTO SUPERIOR DE ANGOLA (ISA) NO I
SEMESTRE DO ANO LECTIVO 2024/2025**

Autor: António Mavacala Kulaz

Orientador: Gil da Conceição Manuel Campos, MsC.

Icolo e Bengo, 2025

DEPARTAMENTO DE ENGENHARIA
LICENCIATURA EM ENGENHARIA INFORMÁTICA

**PROPOSTA DE IMPLEMENTAÇÃO DE UMA REDE PRIVADA
VIRTUAL NO INSTITUTO SUPERIOR DE ANGOLA (ISA) NO I
SEMESTRE DO ANO LECTIVO 2024/2025**

Trabalho de Fim de Curso apresentado ao Instituto Superior de Angola (ISA), como requisito para obtenção do grau de Licenciatura em Engenharia Informática, sob orientação do Professor, Gil da Conceição Manuel Campos, MSc.

Autor: António Mavacala Kulazi

Orientador: Gil da Conceição Manuel Campos, MSc.

Icolo e Bengo, 2025

DEPARTAMENTO DE ENGENHARIA
LICENCIATURA EM ENGENHARIA INFORMÁTICA

FOLHA DE APROVAÇÃO

**PROPOSTA DE IMPLEMENTAÇÃO DE UMA REDE PRIVADA
VIRTUAL NO INSTITUTO SUPERIOR DE ANGOLA (ISA) NO I
SEMESTRE DO ANO LECTIVO 2024/2025**

O júri:

Presidente: _____

1º vogal: _____

2º vogal: _____

Secretário (a): _____

Classificação: _____

Data da defesa: _____ / _____ / _____

DEDICATÓRIA

A minha mãe, Nkiambi Regina, pela força, coragem que sempre me deu para não desistir dos estudos apesar da responsabilidade.

AGRADECIMENTOS

À Deus todo poderoso, pós ele me deu forças para poder terminar meus estudos.

À minha querida esposa, Alda Mateus Alberto Kulazi, pela força que me tem dado em prol desse trabalho.

Aos meus pais, Eduardo Kulazi Tussevo (em memória) e Nkiambi Regina, pelo amor, equilíbrio psico-emocional que me proporcionaram, permitiu terminar os estudos.

Aos meus irmãos, João Victor Kulazi, Garcia Victor Kulazi, Isabel Kulazi e Ana Nora Nkiambi Maria, pelos conselhos e carinho.

Ao meu orientador professor, Gil da Conceição Manuel Campos, pela disponibilidade prestada, sobretudo quando menos esperava.

Ao Instituto Superior de Angola (ISA), que tornou possível a minha formação no grau de licenciatura em engenharia informática.

Aos meus colegas, amigos, vizinhos e todos aqueles que me apoiaram directa ou indirectamente na minha formação. Muito obrigado.

EPÍGRAFE

A VPN é uma extensão da rede interna utilizando os meios físicos que não dispõe (meio público) para alcançar seu meio comum (sua rede privada).

(Silva, 2002).

RESUMO

O presente trabalho de pesquisa tem como tema Proposta de Implementação de uma Rede Privada Virtual no Instituto Superior de Angola (ISA), para a nossa pesquisa usamos a pesquisa descritiva, quanto a abordagem qualitativa, para a elaboração do presente trabalho levantamos a seguinte pergunta De que forma poderá ajudar a implementação de uma rede privada virtual no Instituto Superior de Angola (ISA), no I Semestre do ano lectivo 2024/2025? a configuração de uma VPN vai permitir melhor controle de acessos e privilégios dos usuários, diminuindo os riscos de ataques cibernéticos; Testando a disponibilidade do sistema de rede através do simulador Cisco Pack trace, precavendo as falhas subsequente. Para o presente Trabalho de pesquisa propusemos os seguintes objectivos, deral: Propor a implementação de uma Rede Privada Virtual no Instituto Superior de Angola. Específicos, indentificar os requisitos funconais e não funcionais do sistemas; desenhar a estrutura lógica do sistema a ser implementado; elaborar os diagramas lógicos do sistema; configurar o sistema através da ferramenta Pactrace; textar e implementar o sistema. A nossa pesquisa contou com 14 funcionários. A utilização da internet danos a possibilidade de usufruir dos serviços que alternativamente seria necessária a contratação de circuitos virtuais pelas operadoras, assim sendo dinamiza consideravelmente a rentabilidade da instituição, possibilitando a contratação de melhores serviços para o acesso à internet no Instituto Superior de Angola. Deve-se também fazer um investimento em aplicativos de segurança para o combate de malweres.

Palavras-Chaves: Implementação; Rede e Rede Privada Virtual.

ABSTRACT

The present research work has as its theme Proposal for Implementation of a Virtual Private Network at the Instituto Superior de Angola (ISA), for our research we used descriptive research, as well as the qualitative approach, for the elaboration of the present work we raised the following question: In what way can the implementation of a Virtual Private Network safeguard the problems of vulnerability and constant congestion in the information traffic of the Instituto Superior de Angola? configuring a VPN will allow better control of user access and privileges, reducing the risk of cyber attacks; Testing the availability of the network system through the Cisco Pack trace simulator, preventing subsequent failures. For this research work we proposed the following objectives, namely: Propose the implementation of a Virtual Private Network at the Higher Institute of Angola. Specific, identify the functional and non-functional requirements of the systems; design the logical structure of the system to be implemented; develop the system's logical diagrams; configure the system using the Pctrace tool; test and implement the system. Our survey included 14 employees. The use of the internet damages the possibility of enjoying services that would otherwise require the contracting of virtual circuits by operators, thus considerably boosting the profitability of the institution, enabling the contracting of better services for internet access at the Higher Institute of Angola. Investment should also be made in security applications to combat malware.

Keywords: Implementation; Network and Virtual Private Network.

LISTAS DE ABREVIATURAS E SIGLAS

ISA - Instituto Superior de Angola

LAN - Local Area Networks

MANs - Metropolitan Area Networks

WANs - Wide Area Networks

OSI - Open Systems Interconnection

PAN - Personal Area Network

PIX - Private Internet Exchange

TI - Tecnologia de Informação

VPN - Virtual Private Network

Wi-Fi - Wireless Fidelity.

LISTA DE FIGURA

Figura 1: Rede PAN.....	10
Figura 2: Funcionamento da rede MAN.....	12
Figura 3: Modelo OSI.....	17
Figura 4: Arquitetura Host – Host.....	20
Figura 5: Arquitetura Host – Rede.....	20
Figura 6: Arquitetura Rede – Rede.....	21
Figura 7: Transporte subjacente.....	22
Figura 8: Arquitetura Rede VPN.....	24
Figura 9: Processo de Tunelamento.....	26
Figura 10: Criptografia Assimétrica.....	27
Figura 11: Processo de Assinatura Digital.....	30
Figura 12: Exemplo de um Firewall.....	37
Figura 13: Diagrama lógico da Rede Isa.....	40
Figura 14: Topologia central.....	41
Figura 15: secretária rede central.....	42
Figura 16: Sub-rede do laboratório.....	43
Figura 17: Rede Isa.....	44
Figura 18: Sub-rede de finança da rede filiar.....	45
Figura 19: Sub-rede da secretária da rede filiar.....	46
Figura 20: Ilustração da interligação das redes.....	47
Figura 21: Ilustração do provedor do serviço de internet.....	48

ÍNDICE

Introdução.....	1
CAPITULO I. FUNDAMENTAÇÃO TEÓRICA.....	5
1.1. Definições de termos e conceitos.....	5
1.2. O surgimento das redes de computadores	6
1.3. Conceitos de redes de computadores.....	9
1.4. Classificação das redes quanto à extensão geográfica.....	9
1.4.1. PAN.....	10
1.4.2. LAN.....	10
1.4.3. MAN.....	11
1.4.3.1. Funcionamento da rede MAN.....	11
1.4.4. WAN.....	12
1.5. Formas de conexão de redes.....	12
1.5.1. Redes Cabeadas.....	13
1.5.2. Cabo de Par Trançado (Twisted Pair).....	13
1.5.3. Cabo Coaxial	13
1.5.4. Fibra Óptica.....	13
1.5.5. Redes Não Cabeadas.....	13
1.5.6. Wi-Fi (Wireless Fidelity)	14
1.5.7. Bluetooth.....	14
1.6. Tecnologia Celular (3G, 4G, 5G)	14
1.7. Infraestrutura de Rede Mesh.....	14
1.8. Vantagens e desvantagens das redes de computadores.....	14
1.8.1. Vantagens das Redes de Computadores	15
1.8.2. Desvantagens das Redes de Computadores.....	16
1.9. O modelo OSI.....	17
1.9.1. Camadas do modelo OSI.....	17
1.9.2. Função e Importância do Modelo OSI.....	18
1.10. Virtual Private Network (VPN)	19
1.10.1. Principais Tipos de VPN.....	19
1.10.2. Vantagens e Desvantagens da VPN.....	21
1.10.3. Principais Características e Requisitos.....	23
1.10.4. Tunelamento.....	23

1.11. Criptografia Assimétrica.....	25
1.12. Assinatura Digital.....	26
1.13. Certificado Digital.....	27
1.14. Tecnologia em redes VPN.....	28
1.14.1. Segurança.....	29
1.14.2. Firewall.....	30
1.14.3. Criptografia.....	31
1.14.4. Criptografia Simétrica.....	31
CAPÍTULO II. METODOLOGIA DE PESQUISA.....	33
2.1. Tipo de Pesquisa.....	33
2.2. Modelo de abordagem.....	33
2.3. Nível de estruturação de métodos.....	33
2.4. Técnicas de Recolha de dados.....	34
2.5. Instrumentos e procedimentos de recolha de dados.....	34
2.6. População e amostra.....	34
2.7. Dificuldades encontradas.....	35
CAPÍTULO III. DISCUSSÃO E RESULTADOS.....	36
3.1. Descrição e caracterização da instituição em estudo.....	36
3.2. Diagrama lógico da Rede Isa.....	37
3.3. Desenvolvimento de protótipo da Futura Rede do ISA.....	39
CONCLUSÃO.....	48
SUGESTÕES.....	49
REFERÊNCIAS BIBLOGRÁFICAS.....	50
APÊNDICES	
ANEXOS	

INTRODUÇÃO

O presente trabalho tem como tema “proposta de implementação de uma rede privada virtual no Instituto Superior de Angola (ISA), no I Semestre do ano lectivo 2024/2025”.

Actualmente, com o crescimento da Internet, o constante aumento de sua área de abrangência, e a expectativa de uma rápida melhoria na qualidade dos meios de comunicação associada ao aumento das velocidades de acesso com banda larga, a mesma passou a ser vista como um meio conveniente para as comunicações corporativas. No entanto, a transmissão de dados sensíveis pela rede somente se torna possível com o uso de tecnologias que tornem esse meio altamente inseguro em um meio confiável.

Com essa abordagem, o uso de VPN (Virtual Private Network) sobre o modelo de referência TCP/IP parece ser uma alternativa viável e adequada. Assim, uma VPN, ou Rede Privada Virtual, é uma rede privada construída sobre a infra-estrutura de uma rede pública, normalmente a Internet. Ou seja, ao invés de se utilizar links dedicados ou redes de pacotes (como Frame Relay e X.25) para conectar redes remotas, utilizase a infra-estrutura da Internet. Além de estabelecer comunicação entre duas redes privadas, as VPNs têm que garantir alguns aspectos em termos de comunicação segura, como: confidencialidade, autenticação, integridade e disponibilidade dos dados.

Uma VPN é baseada em conceitos de tunelamento, na qual existem vários protocolos que podem ser utilizados para a transferência de dados pela rede pública (Internet), sendo que o tunelamento pode ser definido como o processo de encapsular um protocolo dentro de outro. Analisando-se os principais conceitos de segurança e tunelamento, nota-se que o método de criptografia é de extrema importância durante a definição de uma VPN. Além da criptografia, pode-se ter outros métodos de segurança, como funções de hash, assinatura digital e certificado digital.

A segurança de qualquer sistema informático tem sido uma questão de discussão e que raramente chegasse a uma conclusão plausível todo pelo facto de nunca atingirmos a cem porcente quando se fala de proteção. Todavia O Instituto Superior de Angola vive o mesmo problema, Dai que a nossa preocupação é sem

dúvida ajudará a instituição com um projecto de VPN como forma de assegurar as informações do ISA:

- **De que forma poderá ajudar a implementação de uma rede privada virtual no Instituto Superior de Angola (ISA), no I Semestre do ano lectivo 2024/2025?**

Hipóteses

Segundo Baptista e Sousa (2011, p. 26), “as hipóteses são uma resposta prévia ao problema proposto e, habitualmente, são desenvolvidos com base em estudos anteriormente realizados de acordo com tema escolhido”, pelo que a “hipótese deve justificar o trabalho da parte empírica da investigação” (Hill e Hill, 2002, p. 22).

H1: A implementação de uma rede privada virtual (VPN) pode reduzir as vulnerabilidades na transmissão de dados do Instituto Superior de Angola.

H2: A configuração de uma VPN pode permitir melhor controle de acessos e privilégios dos usuários, diminuindo os riscos de ataques cibernéticos.

H3: A implementação de uma Rede Privada Virtual poderá acautelar os problemas de constantes congestionamento no tráfego da informação do Instituto Superior de Angola.

Objectivos do estudo

Para o presente trabalho de pesquisa propusemos os seguintes objectivos:

Geral:

Analisar a proposta da implementação de uma rede privada virtual no Instituto Superior de Angola.

Específicos:

- Indentificar os requisitos funcionais e não funcionais do sistemas da rede privada virtual no Instituto Superior de Angola;
- Desenhar a estrutura lógica do sistema a ser implementado da rede privada virtual no Instituto Superior de Angola;
- Elaborar os diagramas lógicos do sistema da rede privada virtual no Instituto Superior de Angola;

- Configurar o sistema da rede privada virtual através da ferramenta Pcaptrace;
- Testar a disponibilidade do sistema da rede privada virtual através do simulador Cisco Packet Tracer, prevenindo as falhas subsequentes.

Delimitação e Limitação de estudo

a) Delimitação

A nossa pesquisa realizou-se no Instituto Superior de Angola (ISA) no ano lectivo 2023/2024.

b) Limitação

O estudo limitou-se aos seguintes intervenientes: Presidente, Vice-Presidentes, Coordenadores, Professores e Estudantes.

Justificativa

A escolha do tema deve-se pelo interesse em ajudar no desenvolvimento do Instituto Superior de Angola ISA, mostrando as vantagens da implementação do mesmo e os ganhos da sua implementação, o que nos motivou a escolher o tema, aplicando os conhecimentos adquiridos.

No futuro a pesquisa poderá servir como base para outras pesquisas, impactando assim na sociedade, principalmente em pesquisas ligadas à área da tecnologia.

A implementação de uma VPN no Instituto Superior de Angola surge como uma solução capaz de minimizar problemas ligados à gestão de informações digitais, promovendo um ambiente seguro para a comunicação de dados e otimizando o fluxo de informações dentro da instituição.

Estrutura do trabalho

Este trabalho está estruturado em três capítulos:

No capítulo I. Fundamentação teórica, onde abordamos as definições de termos e conceitos de autores que sustentam a temática em estudo;

No capítulo II. Metodologia de pesquisa, onde aplicamos os métodos, técnicas que se usou para a elaboração da pesquisa;

No capítulo III. Discussão e resultados;

Conclusões;

Sugestões;

Referências bibliográficas.

CAPITULO I. FUNDAMENTAÇÃO TEÓRICA

1.1. Definições de termos e conceitos

1.1.1. Implementação

A implementação pode ser definida como o processo de colocar em prática uma estratégia, política ou programa, que envolve a execução de atividades específicas, a alocação de recursos necessários e o acompanhamento do progresso para alcançar os resultados desejados (Birkinshaw & Goddard, 2009, p. 305).

A implementação é a fase crítica de transformar uma ideia em ação tangível, abrangendo a tradução de conceitos em práticas concretas, a capacidade de recursos, a gestão de mudanças e a superação de desafios para alcançar os objetivos pretendidos, (Bresser-Pereira, 2004, p. 28).

Implementação: ação ou efeito de implementar; ato de colocar em execução ou em prática; realização, efetivação ou execução de um projeto, uma tarefa etc: a implementação do projeto deverá demorar alguns meses (Oliveira, 2004).

Implementação é um termo que pode ser utilizado em vários contextos, como no desenvolvimento de projetos em tecnologia, ou na aplicação de estratégias e metodologias.

1.1.2. Redes

Referem-se a dispositivos de computação interconectados que podem trocar dados e compartilhar recursos entre si. Esses dispositivos em rede usam um sistema de regras, chamados de protocolos de comunicação, para transmitir informações por meio de tecnologias físicas ou sem fio (Alencar, 2010).

Segundo Sousa (1999), “rede de computadores é um conjunto de equipamentos interligados de maneira a trocarem informações e compartilharem recursos, como arquivos de dados gravados, impressoras, modems, softwares e outros equipamentos”.

As redes de computadores constituem-se de um conjunto de dois ou mais computadores interligados com o objetivo de compartilhar recursos e trocar informações, (Franciscatto, 2014, p. 15).

Redes de computadores são formadas pela interligação de dois ou mais dispositivos computacionais por meio de um sistema de comunicação.

1.1.3. Privada Virtual (VPN)

VPN significa “Virtual Private Network” (Rede Privada Virtual) e descreve a oportunidade de estabelecer uma conexão de rede protegida ao usar redes públicas. As VPNs criptografam seu tráfego de Internet e disfarçam sua identidade (Vasques, 2002).

A VPN é uma extensão da rede interna utilizando os meios físicos que não dispõe (meio público) para alcançar seu meio comum (sua rede privada) (Silva, 2002).

VPN ou rede privada virtual cria uma conexão de rede privada entre dispositivos através da Internet. As VPNs são usadas para transmitir dados de forma segura e anônima em redes públicas (Cabrini, 2012).

Uma Rede Privada Virtual (VPN) é uma rede de comunicação privada montada em cima de uma rede de comunicação pública através de protocolos padrão, não necessariamente seguros.

1.2. O surgimento das redes de computadores

Instituídas durante a década de 60, as primeiras redes de computadores 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 informações. No período entre 1970 e 1973, com a criação da Arpanet, foi possível a criação de uma rede para interligação entre universidades, instituições militares e empresas. Os hardwares utilizados nessa época eram os mainframes, caracterizados por um poder de processamento baixo e com preços elevados. Serviços como e-mail, FTP e DNS, foram criados, permitindo aos usuários realizar diferentes tipos de tarefas. Esses recursos serviram de base para o que se tem hoje, (Urbiêta, 2007).

O mesmo autor acrescenta, com a evolução crescente dos meios de comunicação e as tecnologias, a década de 90 ficou caracterizada com a expansão do acesso à internet. Neste caso, redes dos mais variados tipos ganharam seu espaço

no mercado. O padrão Ethernet popularizou-se e espalhou-se, sendo utilizado com frequência na construção de redes locais de computadores (LAN's). Neste período, o acesso à internet através de linha discada era uma realidade comum em empresas, haja vista que era necessário um modem e uma linha telefônica, o que muitas vezes tornava-se uma solução custosa. Como solução a esta alternativa discada, surgiram as linhas de frame relay (conexão dedicada com velocidades de 64 kbits). Esse tipo de conexão facilitava o acesso à internet em computadores de uma mesma rede, pois permitia compartilhar a conexão entre os computadores da rede, além de permitir que todos estivessem permanentemente conectados, (Urbiêta, 2007).

Hoje é possível construir redes através de inúmeras possibilidades: redes cabeadas (Ethernet, fibra óptica), sem-fio (rádio, Bluetooth, Wi-Fi), entre outros. O custo, velocidade entre outros fatores é influenciado pelas tecnologias e dispositivos empregados na construção desta rede. As redes de computadores apesar da evolução e crescente propagação, mantém seu objetivo primordial: compartilhar recursos (tanto de hardware como software) e propiciar a troca de informações. As redes de computadores e as tecnologias necessárias para a comunicação entre elas continuaram a comandar as indústrias de hardware, software e periféricos de computadores, impulsionadas pelo crescimento nos números e tipos de usuários. (Morimoto, 2008).

A fusão dos computadores e das comunicações teve uma profunda influência na forma como os sistemas computacionais eram organizados. Está totalmente ultrapassado o conceito de um “centro de computadores”, como uma sala para onde os usuários levam os programas a serem processados. O velho modelo de um computador atendendo às necessidades computacionais da organização foi substituído pelas redes de computadores, nas quais os trabalhos são realizados por uma série de computadores em rede. Dois computadores estão em rede quando podem trocar informações. (Scrimger, 2011)

Tanenbaum (2003), conceitua “rede” como um conjunto de computadores autônomos interconectados por uma única tecnologia. Em uma rede, os usuários devem logar-se explicitamente com uma máquina, submeter explicitamente as tarefas remotas e movimentar explicitamente os arquivos.

As redes de computadores são o núcleo da comunicação moderna: as

empresas têm um número significativo de computadores em operação, frequentemente instalados em locais distantes entre si. O escopo da comunicação cresceu significativamente na década de 90 e este aumento não teria sido possível sem o avanço das redes de computadores. (Pinheiro, 2003, apud Rigney, 2010).

O escopo da comunicação cresceu significativamente na década de 90 e este aumento não teria sido possível sem o avanço das redes de computadores. As redes permitem o compartilhamento de recursos, aumentam a confiabilidade dos sistemas, ajudam a otimizar investimentos e a economizar dinheiro, além de possibilitarem a escalabilidade (aumento gradual da capacidade de um sistema à medida que cresce o volume de carga). (Tanenbaum,1997).

Geralmente, uma rede de computadores é um conjunto de dois ou mais dispositivos (também chamados de nós) que usam um conjunto de regras (protocolos) em comum para compartilhar recursos entre si. Um protocolo é um conjunto de regras, especificações e procedimentos que deve governar entidades que se comunicam entre si. Num primeiro momento, os computadores eram interconectados nos departamentos da empresa, em que a distância entre os computadores era pequena e limitada a um mesmo local. Por este motivo as redes passaram a ser conhecidas como redes locais ou Local Area Networks (LAN). (Rigney, 2010)

Uma LAN é um conjunto de hardware e software que permite a computadores individuais estabelecerem comunicação entre si, trocando e compartilhando informações e recursos. Tais redes são denominadas locais por cobrirem apenas uma área limitada (10km no máximo); fisicamente, quanto maior a distância de um nó da rede ao outro, maior a taxa de erros que ocorrerão devido à degradação do sinal. Além disso, o pior tempo de transmissão das informações é limitado e conhecido, simplificando o gerenciamento da rede, (Rigney, 2010)

Uma das tecnologias mais utilizadas em LANs é a Ethernet. Baseada no envio de pacotes, o protocolo Ethernet tornou-se um padrão na década de 80 ao definir o cabeamento, os sinais elétricos para a camada física, o formato de pacotes e os protocolos para a camada de controlo de acesso ao meio. As necessidades continuaram a aumentar e a troca de informações somente entre computadores de um mesmo sector já não era suficiente. Surgiu a necessidade da troca de informações entre departamentos e filiais de uma empresa, prédios e edifícios espalhados por uma

área maior. Desta forma, os computadores passaram a ser interligados por distâncias maiores, caracterizando uma rede metropolitana ou Metropolitan Area Network (MAN). (Rigney, 2010).

Com o crescimento das empresas e maior volume de transações, as LANs e MANs não eram mais suficientes para atender à demanda, pois tornou-se necessário transmitir informações de uma empresa para outra de forma rápida e eficiente. Surgiram então as redes distribuídas geograficamente ou Wide Area Network (WAN) que conectaram redes dentro de uma vasta área geográfica, permitindo a comunicação de longa distância, o envio e recebimento de dados entre computadores, em qualquer lugar do planeta, facto que gerou o aparecimento do termo “rede de alcance mundial”, ou simplesmente Internet. (Tanenbaum, 1997).

1.3. Conceitos de redes de computadores

A fusão dos computadores e das comunicações e telecomunicações influenciaram diretamente na forma como os computadores são atualmente organizados. O modelo de um único computador realizando todas as tarefas requeridas não existe mais e está sendo substituído pelas redes de computadores, nas quais os trabalhos são realizados por vários computadores separados, interconectados por alguma via de comunicação. (Peterson, 2012).

Pinheiro (2003, citado por Peterson 2012), descreve o objetivo de uma rede como sendo garantir o compartilhamento rápido, seguro e confiável de recursos disponíveis, independentemente do tamanho e complexidade. Para isso, é necessário que uma rede de computadores tenha regras e mecanismos que assegurem o transporte seguro das informações entre os elementos constituintes.

1.4. Classificação das redes quanto à extensão geográfica

Neste quesito, as redes são classificadas quanto ao alcance das mesmas, sendo que diversas classificações são propostas como forma de caracterização destes tipos de redes, conforme os tópicos a seguir.

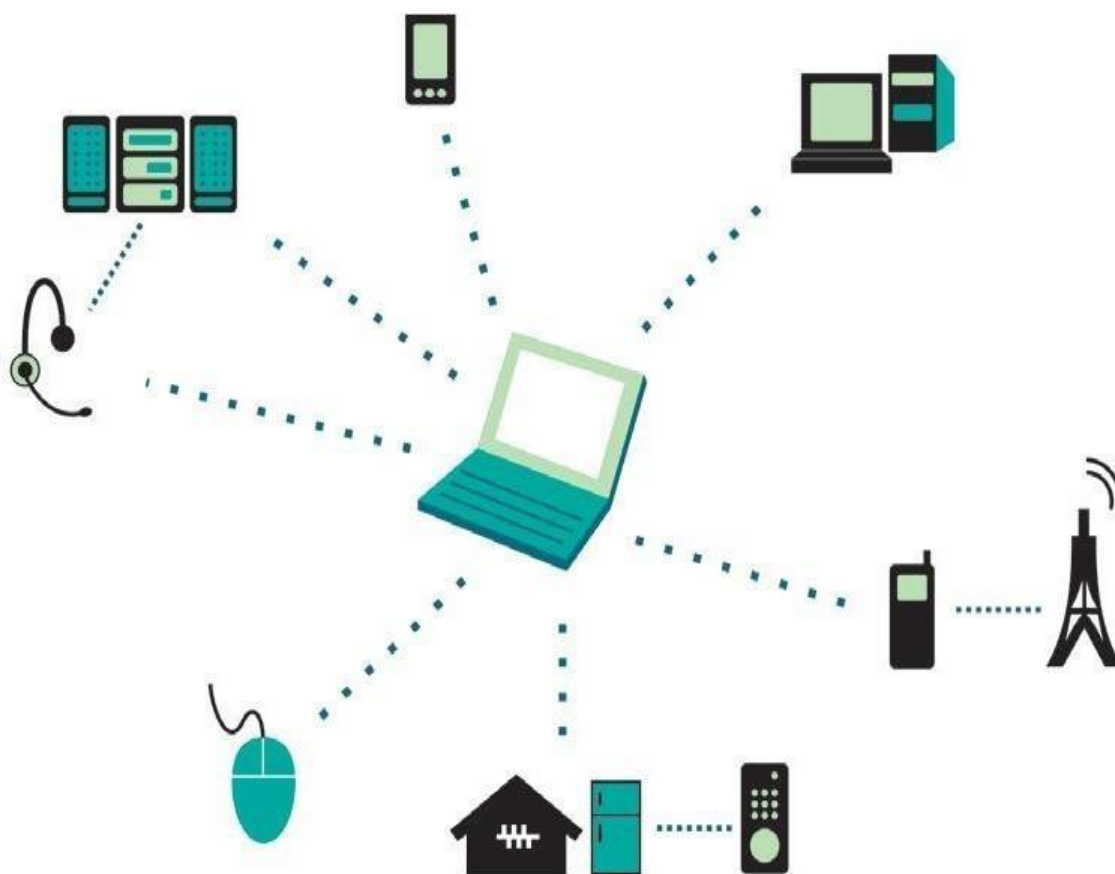
De acordo com Dantas (2002, apud Peterson, 2012), uma das características mais utilizadas para a classificação das redes é a sua abrangência geográfica. Assim, é convencionada a classificação das redes em locais – LANs

(Local Area Networks), metropolitanas – MANs (Metropolitan Area Networks) e geograficamente distribuídas – WANs (Wide Area Networks).

1.4.1. PAN

Uma PAN (Personal Area Network) ou Rede de Área Pessoal, constitui-se de uma rede de computadores formada por dispositivos muito próximos uns dos outros. Como exemplo deste tipo de rede, pode-se citar dois notebooks em uma sala trocando informações entre si e ligados a uma impressora. Redes formadas por dispositivos Bluetooth são exemplos de uma PAN.(Kurose, 2010).

Figura 1: Rede PAN



Fonte: Dantas (2002).

1.4.2. LAN

Segundo Dantas, (s.d, citado por Pinheiro, 2012), a rede local – LAN é uma facilidade de comunicação que fornece uma conexão de alta velocidade

entredispositivos em um único prédio ou campus. É uma tecnologia adequada para interligar dispositivos com distâncias curtas e largura de banda considerável.

1.4.3. MAN

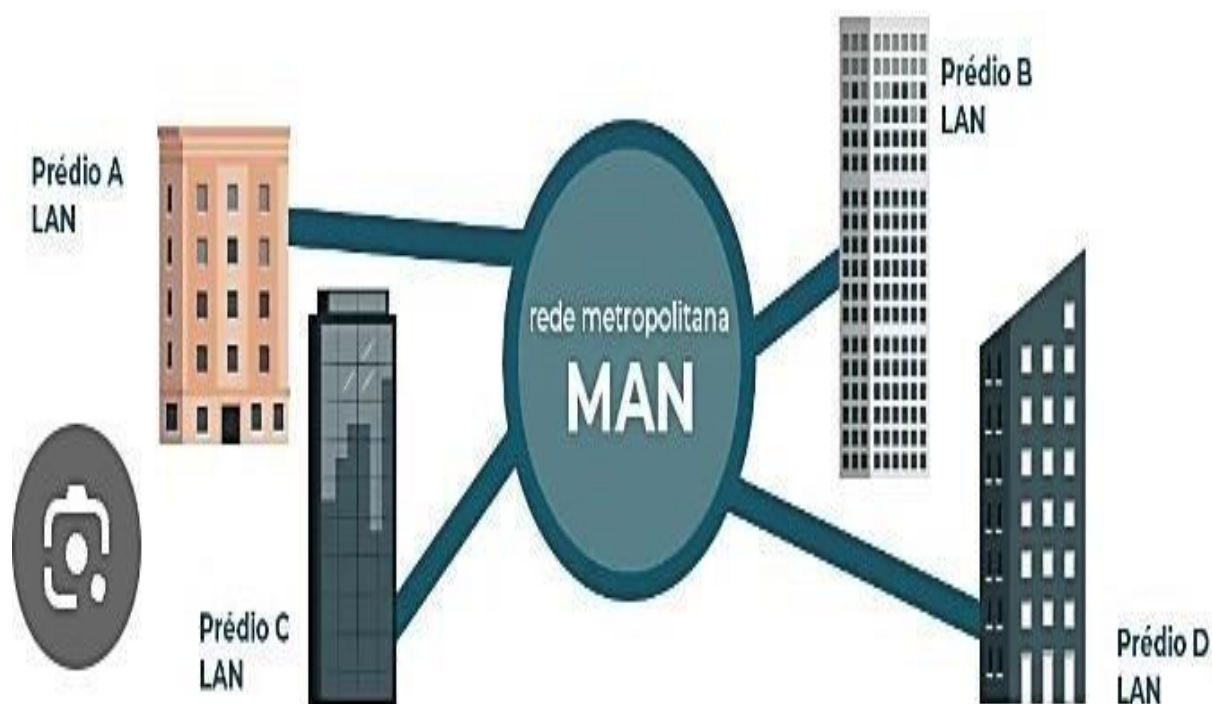
Redes metropolitanas interligam redes locais em uma área metropolitana, ou seja, elas podem ser entendidas como aquelas que proveem a interligação das redes locais em uma área metropolitana de uma determinada região. Uma rede metropolitana, ou MAN (Metropolitan Area Network), abrange uma cidade. O exemplo mais conhecido de MANs é a rede de televisão a cabo disponível em muitas cidades. Esses sistemas cresceram a partir de antigos sistemas de antenas comunitárias usadas em áreas com fraca recepção do sinal de televisão pelo ar. Nesses primeiros sistemas, uma grande antena era colocada no alto de colina próxima e o sinal era, então, conduzido até as casas dos assinantes (Pinheiro, 2012).

1.4.3.1. Funcionamento da rede MAN

Até alguns anos atrás, a expansão da conectividade em rede entre diferentes localidades de uma empresa, mesmo com endereços geograficamente próximos, era feita através das infraestruturas baseadas em soluções WAN. Essas conexões muitas vezes eram acompanhadas de custos proibitivos, especialmente quando se tratava de recursos terceirizados como linhas de comunicação alugadas. Por outro lado, as redes locais tradicionalmente cobriam apenas pequenas áreas, como um prédio ou um campus universitário. Assim, para conectar múltiplos endereços ou instalações em uma cidade ou região metropolitana era necessário o uso de cabeamento dedicado, geralmente montado com a ajuda de cabos de fibra óptica (Peterson, 2012).

Além disso, interligar LANs através de WANs quase sempre resultava em latências variáveis e tempos de resposta inconsistentes, de pendendo do tráfego e das capacidades do meio de transmissão de cada ambiente. As MANs foram projetadas para superar esses desafios, com recursos para oferecer uma solução para a transmissão de dados que poderia cobrir uma área metropolitana, além de conectividade de alta velocidade, confiabilidade e escalabilidade (Peterson, 2012).

Figura 2: Funcionamento da rede MAN



Fonte: Pera (2021).

1.4.4. WAN

Uma WAN é uma rede geograficamente distribuída que interliga computadores em distâncias maiores que uma região metropolitana. Quando as distâncias envolvidas na interligação dos computadores são superiores a uma região metropolitana, podendo ser a dispersão geográfica tão grande quanto a distância entre continentes, a abordagem correta é a rede geograficamente distribuída (WAN). (Pinheiro, 2012).

1.5. Formas de conexão de redes

As redes de computadores podem ser classificadas quanto ao tipo de conexão utilizada, sendo as principais formas as redes cabeadas e não cabeadas. Cada uma dessas formas possui características específicas que influenciam na escolha conforme as necessidades de uso e o ambiente onde serão implementadas.

1.5.1. Redes Cabeadas

Segundo Peterson (2012), redes cabeadas utilizam cabos físicos para conectar dispositivos entre si e à rede principal. Esses cabos podem ser de diferentes tipos, cada um com suas próprias vantagens e desvantagens:

1.5.2. Cabo de Par Trançado (Twisted Pair)

O cabo de par trançado é um dos mais comuns em redes LAN. Ele é composto por pares de fios de cobre trançados para reduzir interferências eletromagnéticas. Segundo Tanenbaum e Wetherall, esse tipo de cabo é amplamente utilizado devido ao seu baixo custo e facilidade de instalação. Existem variações, como os cabos Categoria 5 (Cat5), Categoria 5e (Cat5e) e Categoria 6 (Cat6), que oferecem diferentes níveis de desempenho (Silva, 2002).

1.5.3. Cabo Coaxial

O cabo coaxial, embora menos comum hoje em dia, ainda é utilizado em algumas redes específicas. Ele consiste em um fio de cobre central rodeado por um isolamento, uma malha metálica e uma capa externa. Forouzan observa que os cabos coaxiais são mais resistentes a interferências e podem transportar sinais a distâncias maiores que os cabos de par trançado, porém são mais caros e difíceis de manusear (Silva, 2002).

1.5.4. Fibra Óptica

Os cabos de fibra óptica utilizam filamentos de vidro ou plástico para transmitir dados na forma de luz, o que permite altas velocidades e longas distâncias sem perda significativa de sinal. Kurose e Ross destacam que a fibra óptica é ideal para backbone de redes e conexões de longa distância, embora seu custo de instalação e manutenção seja maior comparado aos cabos de cobre (Silva, 2002).

1.5.5. Redes Não Cabeadas

Redes não cabeadas, ou redes sem fio, utilizam ondas de rádio ou outros meios de transmissão sem fio para conectar dispositivos. Essas redes são essenciais em ambientes onde a mobilidade e a flexibilidade são importantes:

1.5.6. Wi-Fi (Wireless Fidelity)

Wi-Fi é a tecnologia sem fio mais comum usada em redes locais. Ela permite que dispositivos como computadores, smartphones e tablets se conectem à rede sem a necessidade de cabos. Segundo Comer, a popularidade do Wi-Fi deve-se à sua conveniência e à capacidade de suportar múltiplos dispositivos simultaneamente. A cobertura e a velocidade do Wi-Fi podem variar dependendo do padrão utilizado (por exemplo, 802.11n, 802.11ac, 802.11ax), (Comer, 2007).

1.5.7. Bluetooth

Bluetooth é utilizado para conexões de curto alcance entre dispositivos, como fones de ouvido, teclados e mouses. Forouzan menciona que o Bluetooth é ideal para PANs (Redes Pessoais), pois oferece uma solução de baixo consumo de energia para conectar dispositivos em uma área limitada (Comer, 2007).

1.6. Tecnologia Celular (3G, 4G, 5G)

As redes celulares utilizam torres de rádio para fornecer conectividade sem fio a dispositivos móveis em grandes áreas geográficas. Tanenbaum e Wetherall explicam que as tecnologias 4G e 5G oferecem velocidades de dados comparáveis às redes cabeadas, com a vantagem adicional da mobilidade. O 5G, em particular, promete menores latências e maior capacidade de conexão simultânea de dispositivos (Comer, 2007).

1.7. Infraestrutura de Rede Mesh

Redes mesh consistem em uma topologia de rede onde cada nó se conecta a vários outros nós, criando uma malha de conexões redundantes. Kurose e Ross destacam que esse tipo de rede é altamente resiliente, pois permite a rerotação do tráfego em caso de falha de um dos nós. As redes mesh são utilizadas em ambientes onde a cobertura uniforme e a confiabilidade são cruciais, como em grandes instalações e cidades inteligentes. (McClean, 2004).

1.8. Vantagens e desvantagens das redes de computadores

As redes de computadores oferecem diversos benefícios, mas também apresentam algumas desvantagens que devem ser consideradas na hora de planejar

e implementar uma rede (Mclean, 2004).

1.8.1. Vantagens das Redes de Computadores

❖ Compartilhamento de Recursos

Uma das maiores vantagens das redes de computadores é a capacidade de compartilhar recursos, como arquivos, impressoras e conexões à Internet. Tanenbaum e Wetherall observam que isso não apenas reduz custos, mas também aumenta a eficiência, pois os recursos podem ser centralizados e gerenciados de forma mais eficaz, (Mclean, 2004).

❖ Comunicação e Colaboração

Redes permitem uma comunicação rápida e eficiente entre usuários, seja através de e-mails, mensagens instantâneas ou videoconferências. Forouzan menciona que essa conectividade facilita a colaboração entre equipes, independentemente da localização geográfica dos membros, promovendo um ambiente de trabalho mais integrado e produtivo, (Mclean, 2004).

❖ Acesso Remoto

Com as redes, especialmente aquelas com suporte para VPNs e outras tecnologias de acesso remoto, os usuários podem acessar seus recursos e dados de qualquer lugar do mundo. Kurose e Ross destacam que essa flexibilidade é crucial para a mobilidade da força de trabalho moderna, permitindo que os funcionários trabalhem de casa ou durante viagens (Comer, 2007).

❖ Escalabilidade

Redes bem projetadas são altamente escaláveis, permitindo a adição de novos dispositivos e usuários sem grandes reestruturações. Comer enfatiza que essa característica é essencial para empresas em crescimento, pois permite que a infraestrutura de TI se adapte às necessidades crescentes sem interrupções significativas, (Comer, 2007).

❖ Segurança Centralizada

Em uma rede, as políticas de segurança podem ser centralizadas, facilitando

a implementação de medidas de segurança uniformes em todos os dispositivos conectados. Stallings aponta que essa centralização simplifica o gerenciamento de segurança e pode incluir medidas como controle de acesso, autenticação e criptografia, (McClean, 2004).

1.8.2. Desvantagens das Redes de Computadores

❖ Complexidade de Configuração e Manutenção

A configuração e manutenção de uma rede podem ser complexas, exigindo conhecimentos técnicos especializados. Tanenbaum e Wetherall observam que a implementação de redes, especialmente as maiores e mais complexas, pode demandar tempo e recursos significativos, além de pessoal treinado para sua manutenção (Sardinha, 2015).

❖ Custo Inicial

Embora as redes possam reduzir custos operacionais a longo prazo, o custo inicial de instalação pode ser alto. Isso inclui a compra de hardware (como roteadores, switches e cabos) e software, bem como os custos de instalação. Forouzan destaca que esses investimentos iniciais podem ser uma barreira para pequenas empresas ou organizações com orçamento limitado, (Sardinha, 2015).

❖ Segurança

Apesar das vantagens de segurança centralizada, as redes também introduzem riscos de segurança. Kurose e Ross mencionam que uma vez que um invasor consegue acesso à rede, ele pode potencialmente acessar uma vasta gama de recursos e dados. Portanto, a segurança de rede deve ser constantemente monitorada e atualizada para mitigar essas ameaças (Sardinha, 2015).

❖ Dependência da Rede

A operação contínua dos dispositivos e dos sistemas de uma organização pode se tornar altamente dependente da rede. Comer aponta que falhas na rede podem resultar em interrupções significativas das operações, afetando a produtividade e a eficiência até que o problema seja resolvido (Sardinha, 2015).

❖ Problemas de Latência e Confiabilidade

Em redes maiores ou mais complexas, problemas de latência e

confiabilidade podem surgir. Stallings observa que atrasos na transmissão de dados ou falhas intermitentes podem afetar negativamente a experiência do usuário e a eficiência operacional, especialmente em aplicações que exigem alta disponibilidade e desempenho operacional, especialmente em aplicações que exigem alta disponibilidade e desempenho (Peterson, 2012).

1.9. O modelo OSI

Conforme Torres (2004), para facilitar a interconexão de sistemas de computadores, a ISO (International Standards Organization) desenvolveu um modelo de referência chamado OSI (Open Systems Interconnection), para que fabricantes pudessem criar protocolos a partir desse modelo.

1.9.1. Camadas do modelo OSI

Segundo Spurgeon (2000), o modelo de referência OSI é o método para descrever como os conjuntos interconectados de hardware e software de rede podem ser organizados para que trabalhem concomitantemente no mundo das redes. Com efeito, o modelo OSI oferece um modo de dividir arbitrariamente a tarefa da rede em pedaços separados, que estão sujeitos ao processo formal de padronização.

Figura 3: Modelo OSI



Fonte: <http://static.hsw.com.br/gif/nat-osi.jpg>.

Quadro 1. Camadas do modelo OSI

Camada	Descrição
Físico	Esta camada pega os quadros enviados pela camada de enlace e os transforma em sinais compatíveis com o meio por onde os dados deverão ser transmitidos.
Enlace de Dados	A camada de enlace pega os pacotes de dados recebidos da camada de rede e os transforma em quadros que trafegarão pela rede, adicionando informações como o endereço da placa de rede de origem, o endereço da placa de rede de destino, os dados de controle, os dados em si e a checagem de redundância cíclica (CRC).
Rede	É responsável pelo endereçamento dos pacotes, convertendo endereços lógicos em endereços físicos, de forma que os pacotes consigam chegar corretamente ao destino.
Transporte	Esta camada é responsável por pegar os dados enviados pela camada de sessão e dividi-los em pacotes que serão transmitidos à camada de rede.
Sessão	A camada de sessão permite que duas aplicações em computadores diferentes estabeleçam uma sessão de comunicação.
Apresentação	A camada de apresentação converte o formato do dado recebido pela camada de aplicação em um formato comum a ser usado na transmissão desse dado.
Aplicação	A camada de aplicação faz a interface entre o protocolo de comunicação e o aplicativo que pediu ou receberá a informação através da rede.

Fonte: (Spurgeon, 2000).

1.9.2. Função e Importância do Modelo OSI

O Modelo OSI é fundamental para entender como diferentes protocolos e tecnologias de rede interagem e se integram. Ele permite que desenvolvedores e engenheiros de redes projetem sistemas de comunicação modulares e interoperáveis. Forouzan enfatiza que o modelo facilita a padronização dos protocolos de rede e a compatibilidade entre diferentes fabricantes e tecnologias (Davie, 2009).

Além disso, o Modelo OSI ajuda a identificar e resolver problemas de rede de forma estruturada. Cada camada pode ser analisada separadamente para diagnosticar falhas e implementar soluções, o que simplifica o processo de manutenção e troubleshooting. Kurose e Ross destacam que o uso de um modelo de camadas permite a implementação de novas tecnologias em uma camada específica sem afetar as outras, promovendo a inovação e a flexibilidade no desenvolvimento de redes (Sousa, 2010).

1.10. Virtual Private Network (VPN)

A sigla VPN significa Virtual Private Network, ou seja, Redes Privadas Virtuais,

onde:

- Rede corresponde às redes de computadores;
- Privada corresponde à forma como os dados trafegam neste caso os dados podem ser criptografados o que garante a privacidade das informações;
- Virtual por não fazerem, necessariamente, parte do mesmo meio físico.

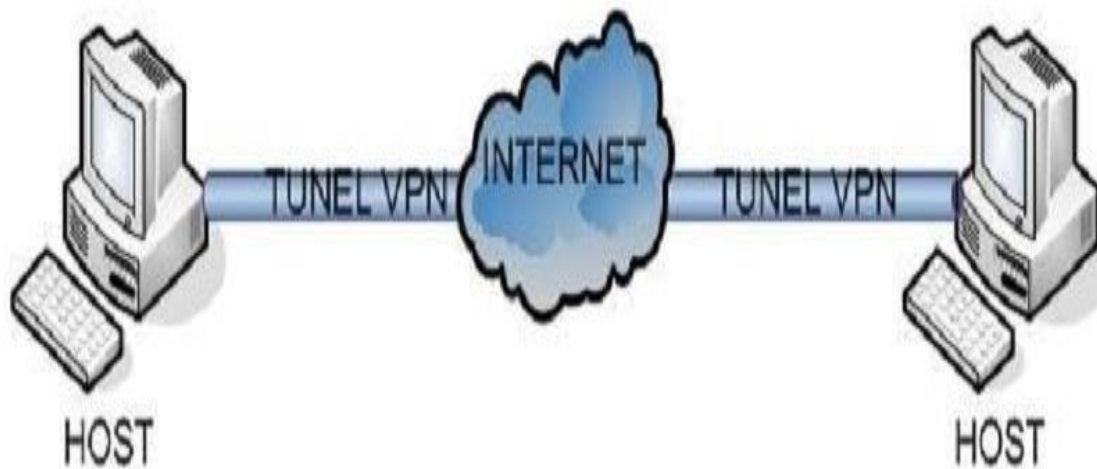
Então, uma VPN é uma rede privada construída sobre a infra-estrutura de uma rede pública já existente, normalmente a Internet, onde o acesso e a troca de dados só são permitidos a pessoas que estejam autorizadas. Desta forma, tem-se a construção de um túnel entre duas ou mais redes, pelo qual pode ser configurado para garantir autenticidade de dados, sigilo de informação, controle de acesso através de criptografia do tráfego de informação entre uma rede e outra. (Fagundes, 2007).

1.10.1. Principais Tipos de VPN

Existem basicamente, três tipos de configuração para o uso de uma VPN:

Host- Host: Neste tipo de configuração de VPN, há o estabelecimento de um túnel seguro entre duas máquinas (hosts), para que ambas possam se comunicar através do meio público (Internet). As máquinas podem estar em redes separadas ou na mesma rede, tal como ilustra a figura . (Fagundes, 2007).

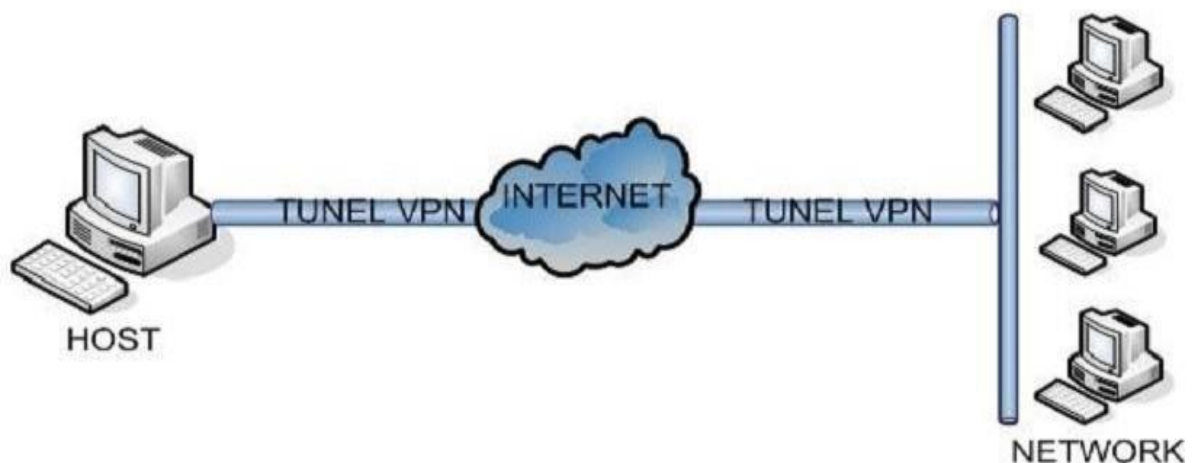
Figura 4: Arquitetura Host – Host



Fonte: (Fagundes, 2007).

Host – Rede: Neste tipo de configuração de VPN, a principal finalidade é estabelecer uma comunicação de um host externo com uma rede privada (Alencar, 2010). Por exemplo, esta estrutura pode ser utilizada quando se deseja estabelecer comunicação entre um computador de casa com a rede privada corporativa de uma empresa, tal como ilustra a figura.

Figura 5: Arquitetura Host – Rede



Fonte: (3way, 2010) Elementos de uma conexão VPN

Os principais elementos de uma conexão VPN são: tunelamento, autenticação das extremidades e o transporte subjacente (Gomes, 2001).

Tunelamento – O tunelamento se dá pela forma como os dados trafegam pela conexão VPN. A idéia do túnel surge quando para enviar os dados uma das extremidades da conexão, primeiro criptografa e depois encapsula o pacote original dentro de um novo pacote.

Autenticação das Extremidades – Ao utilizar a autenticação das extremidades em uma conexão VPN garantimos que somente usuários válidos estão participando da transmissão, através de protocolos de autenticação, que em sua maioria implementam algoritmos de hash. O que garante a integridade das mensagens (Gomes, 2001).

Transporte Subjacente – Devido ao protocolo TCP/IP ser a base da Internet, ele é amplamente utilizado para a comunicação entre redes. Entretanto, ele é muito inseguro. Por isso, uma VPN utiliza a infra-estrutura da rede já existente do TCP/IP para transmitir os seus pacotes pela Internet adicionando alguns cabeçalhos, o que possibilita a instalação destes em qualquer parte da rede (Gomes, 2001).

Figura 6: Transporte subjacente



Fonte: (Gomes, 2001).

1.10.2. Vantagens e Desvantagens da VPN

Segundo Chin (2010), uma das grandes vantagens decorrentes do uso das VPNs é a redução de custos com comunicações corporativas, pois elimina a necessidade de links dedicados de longa distância que podem ser substituídos pela Internet. As LANs podem, por exemplo, através de links dedicados ou discados, conectarem-se a algum provedor de acesso local e interligar-se a outras LANs, possibilitando o fluxo de dados através da Internet.

No entanto, uma VPN depende da rede pública (Internet) para realização de suas conexões. Logo, esta rede pública deve estar quase que sempre disponível,

porém isto é praticamente impossível, pois podem ocorrer falhas nas mesmas, falhas de seguranças, ataques externos (Chin, 2010). Por exemplo, uma VPN é capaz de:

- Ampliar a área de conectividade;
- Aumentar a segurança;
- Reduzir custos operacionais (em relação a uma rede WAN);
- Reduzir tempo de locomoção e custo de transporte dos usuários remotos;
- Aumentar a produtividade;
- Simplificar a topologia da rede;
- Proporcionar melhores oportunidades de relacionamentos globais;
- Prover suporte ao usuário remoto externo;
- Prover compatibilidade de rede de dados de banda larga;
- Prover retorno de investimento mais rápido do que a tradicional WAN.

Um bom projeto de rede VPN deve considerar e incorporar os seguintes aspectos:

- Segurança;
- Confiabilidade;
- Escalabilidade;
- Gerência da rede;
- Gerência de diretrizes.

Figura 7: Arquitetura Rede VPN

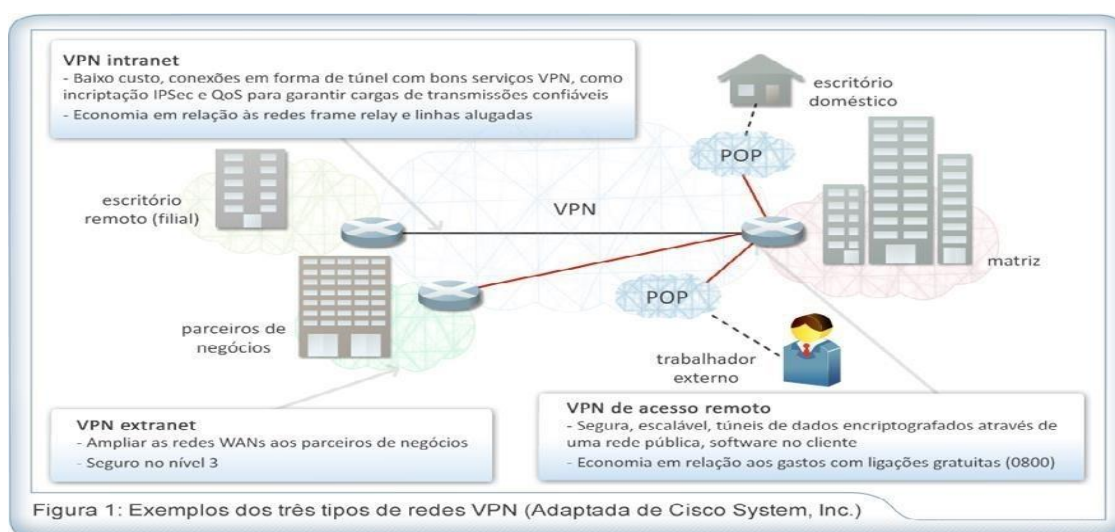


Figura 1: Exemplos dos três tipos de redes VPN (Adaptada de Cisco System, Inc.)

Fonte: Chin (2010).

1.10.3. Principais Características e Requisitos

De acordo com Chin (2010, p. 88), quando se desenvolve um VPN, deve-se ter em mente algumas características e requisitos que podem fazer parte do projeto a ser implementado. Dentre as principais características, destacam-se:

- **Autenticação de usuário:** Verificação da identidade do usuário, restringindo o acesso às pessoas autorizadas. Na maioria de vezes, temos recursos de usuário e senha para garantir a autenticação;
- **Gerenciamento de endereços:** O endereço do cliente na sua rede privada não deve ser divulgado, devendo-se adotar endereços fictícios para o tráfego externo, ou seja, são criados endereços virtuais quando se estabelece um túnel entre duas pontas da rede;
- **Compressão e Criptografia dos dados:** Os dados devem trafegar na rede pública ou privada num formato cifrado e, caso sejam interceptados por usuários não autorizados, não deverão ser decodificados, garantindo a privacidade da informação. Além disso, tais dados devem ser comprimidos e compactados, quando forem transferidos para o canal de comunicação da VPN;
- **Gerenciamento de chaves:** O uso de chaves que garantem a segurança das mensagens criptografadas deve funcionar como um segredo compartilhado exclusivamente entre as partes envolvidas. O gerenciamento de chaves pode garantir a troca periódica das mesmas, visando manter a comunicação de forma segura;
- **Suporte a múltiplos protocolos:** Uma VPN pode dar suporte aos mais variados tipos de protocolos existentes usados em redes públicas, como: IP, IPX, Appletalk, etc.

1.10.4. Tunelamento

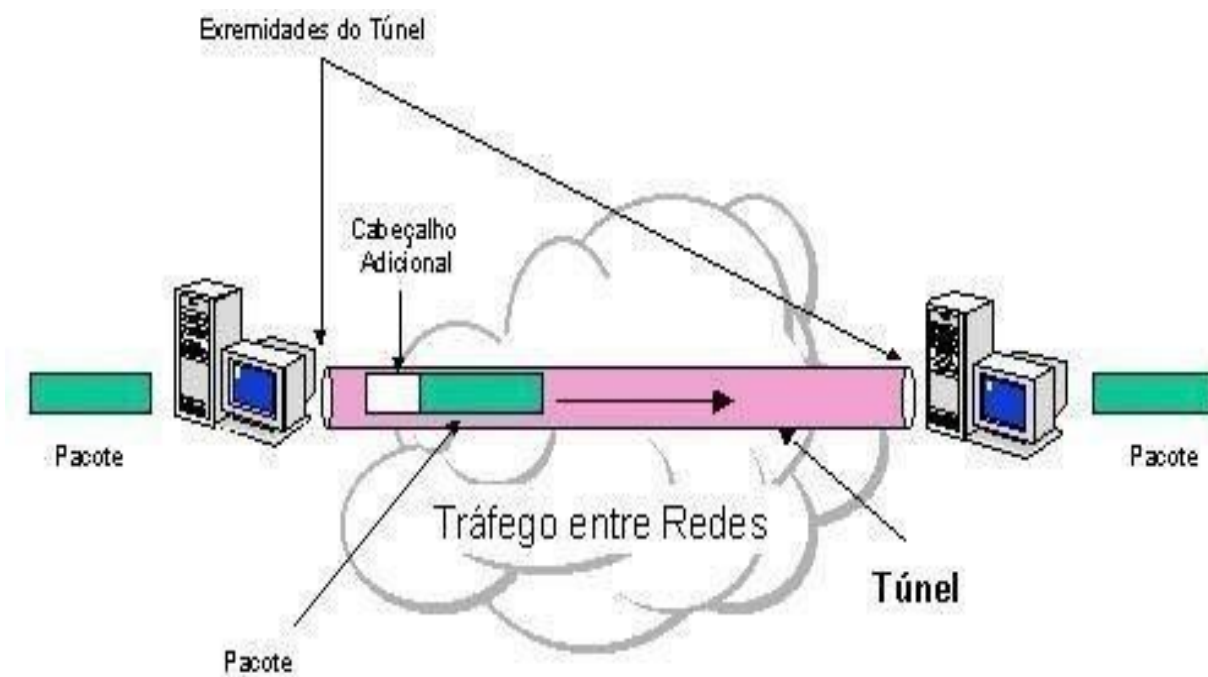
De acordo com Marleta (2007), o tunelamento é uma técnica utilizada pela VPN para encapsular um protocolo dentro de outro. Assim, pode-se utilizar esta técnica para que seja possível que um pacote dentro de uma rede que não usa o protocolo IP, possa trafegar pela Internet.

No entanto, quando se utiliza o tunelamento por meio de VPN, existem estratégias de criptografia a serem adicionadas ao processo, antes de encapsular

um pacote que irá ser transportado pela rede. Logo, o processo de tunelamento em uma VPN é composto pelas seguintes fases (Assis, 2003):

- Criptografia dos dados: Criptografar o pacote a ser transportado, de forma que o torne ilegível em caso de interceptação da transmissão;
- Encapsulamento: Um dado protocolo de tunelamento encapsula os pacotes com um cabeçalho que contém informações de roteamento, com identificação do destino do pacote;
- Transmissão ao longo da rede: Os pacotes são roteados entre as extremidades do túnel na rede intermediária (rede pública), até chegarem ao seu destino;
- Desencapsulamento: No destino, o pacote é desencapsulado, deixando apenas informações do protocolo da rede local;
- Decriptografia dos dados: Realiza a descryptografia dos pacotes finais, de forma que o torne legível para a outra extremidade do túnel.

Figura 8: Processo de Tunelamento



Fonte: (Chin, 2010).

Segundo Whitman e Mattord (2011, p. 57), pode-se ter dois tipos de tunelamento:

- **Tunelamento Voluntário:** Quando uma estação de trabalho ou um servidor utiliza um software para o cliente de tunelamento para criar uma conexão até o servidor VPN. Este método é utilizado por clientes dial-up que primeiro conectam-se a Internet, para depois criar o túnel utilizando o software, com isso o cliente passa a ser o fim do túnel;
- **Tunelamento Compulsório:** Neste tipo de tunelamento, o computador do usuário não funciona como extremidade do túnel. Existe um servidor de acesso remoto, que está localizado entre o computador do usuário e o servidor do túnel, pelo qual funciona como uma das extremidades do túnel. Desta forma, não é necessário que os clientes de rede tenham software cliente para tunelamento.

1.11. Criptografia Assimétrica

Na criptografia assimétrica, a criptografia e a decriptografia são realizadas usando chaves diferentes, na qual existe uma chave privada e uma chave pública. Desta forma, tal método transforma o texto claro em texto cifrado usando uma das duas chaves e um algoritmo de criptografia, e usando a outra chave associada e um algoritmo de decriptografia, o texto claro é recuperado a partir do texto cifrado (Stallings, 2008).

Segundo Stallings (2008, p. 65), um esquema de criptografia assimétrica possui seis componentes:

- **Texto claro:** Essa é a mensagem ou dados legíveis, como entrada para o algoritmo;
- **Algoritmo de criptografia:** O algoritmo de criptografia realiza várias transformações no texto claro;
- **Chaves públicas e privadas:** Esse é um par de chaves que foi selecionado de modo que, se uma for usada para criptografia, a outra será usada para decriptografia. As transformações exatas realizadas pelo algoritmo dependem da chave pública ou privada que é fornecida como entrada;
- **Texto cifrado:** Essa é a mensagem codificada produzida como saída. Ela depende do texto claro e da chave. Para uma determinada mensagem, duas chaves diferentes produzirão dois textos cifrados diferentes;

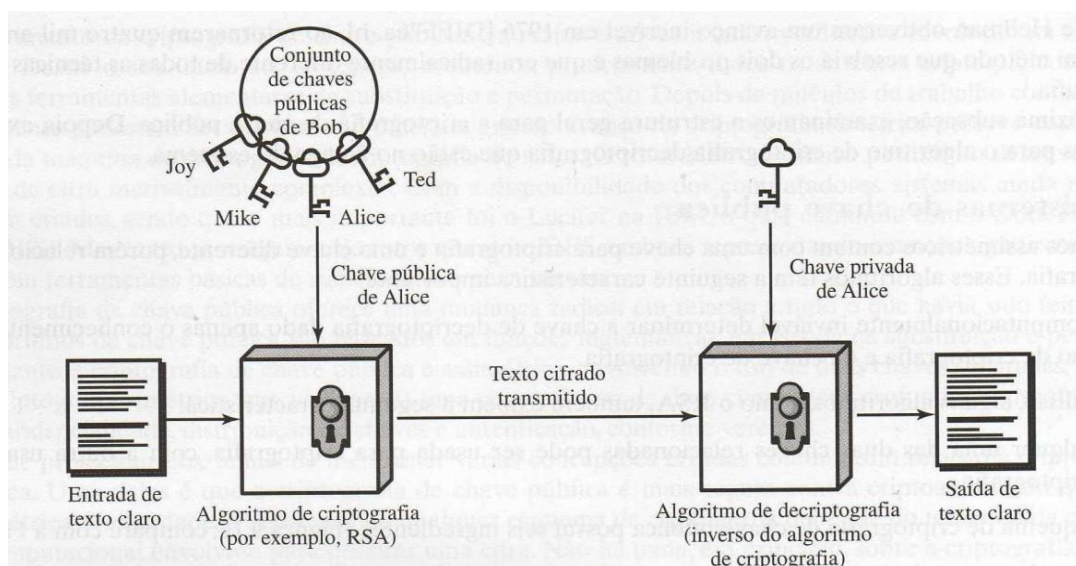
- **Algoritmo de decryptografia:** Esse algoritmo aceita o texto cifrado e a chave correspondente e produz o texto claro original.

As etapas essenciais são as seguintes:

- Cada usuário gera um par de chaves a ser usado para a criptografia e a decryptografia das mensagens.
- Cada usuário coloca uma das duas chaves em um registro público ou outro arquivo acessível. Essa é a chave pública. A outra chave permanece privada.
- Se um emissor deseja enviar uma mensagem confidencial para receptor, o emissor criptografa a mensagem usando a chave pública do receptor.

Quando o receptor recebe a mensagem, ele a decryptografa usando sua chave privada. Nenhum outro destinatário pode decryptografar a mensagem, pois somente o receptor conhece a sua chave (Figura 7).

Figura 9: Criptografia Assimétrica



Fonte: (Stallings, 2008).

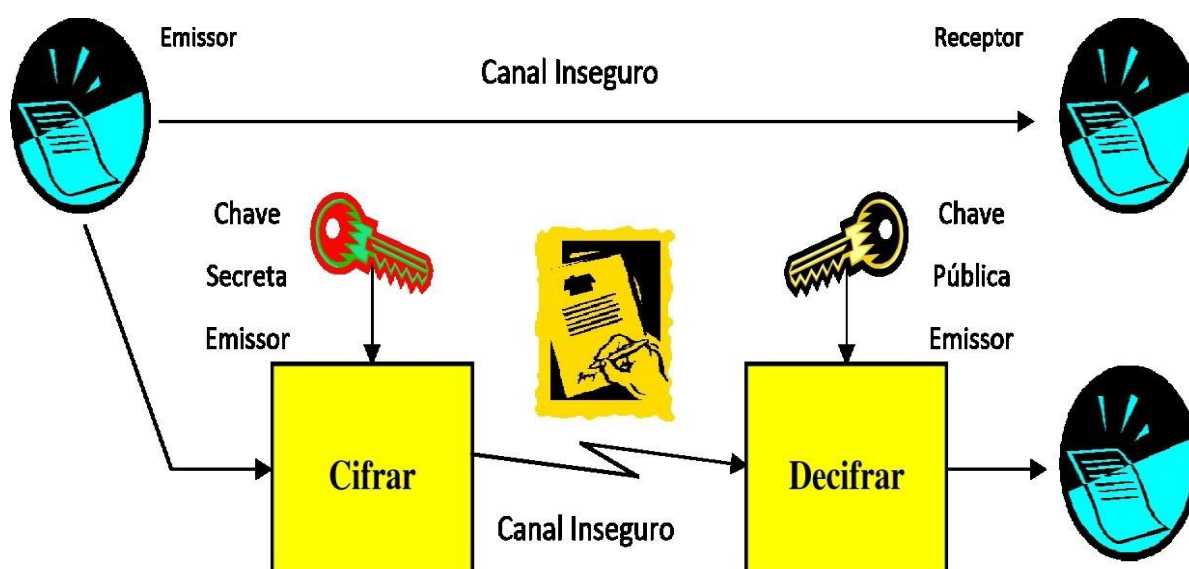
1.12. Assinatura Digital

A assinatura Digital é uma função de assinatura eletrônica que consiste em um selo eletrônico que é acrescentado a um documento e que é criado através de

um sistema de criptografia assimétrica, ou seja, a chave privada serve para assinar o documento e a chave pública serve para verificar a assinatura (Maguione, 2010)

Então, um sistema de assinatura digital simples possui o seguinte processo: quando um emissor quer assinar sua mensagem para ser entregue a um receptor, ele irá fazer uso de sua chave privada para assinar a mensagem. No momento que o receptor receber esta mensagem, ele irá utilizar a chave pública do emissor para produzir uma cópia da mensagem e fazer uma comparação com a recebida. Desta forma, pode-se claramente comprovar que foi realmente o emissor original da mensagem que a enviou, não sendo alterada durante a transmissão, (Marleta, 2007).

Figura 10: Processo de Assinatura Digital



Fonte: (Guilherme, 2010).

Adicionalmente, o processo de assinatura digital pode também usar o conceito de função de hash. Como o uso de algoritmos de chaves públicas nas assinaturas digitais pode causar muita demora em um processo de decifragem, a função de hash se mostra como uma solução ideal (Guilherme, 2010).

1.13. Certificado Digital

O certificado digital é um tipo de documento que armazena a chave pública de um usuário e seus dados de identificação. Este documento deve ser assinado e reconhecido por uma entidade confiável, conhecida como Autoridade Certificadora.

Logo, os certificados digitais são utilizados para garantir a integridade e origem de chaves públicas depositadas em bases de dados de acesso público. O padrão mais utilizado para certificados digitais é o denominado X.509. (James e Keith, 2009).

Um Certificado Digital normalmente possui as seguintes informações:

- Nome da pessoa ou entidade a ser associada à chave pública;
- Período de validade do certificado;
- Chave pública;
- Nome e assinatura da entidade que assinou o certificado;
- Número de série.

Portanto, conseguindo uma chave pública de um usuário associada a um certificado, confiando-se na autoridade certificadora, podemos ter certeza de que a chave realmente pertence ao usuário solicitado, (James e Keith, 2009).

1.14. Tecnologia em redes VPN

Dependendo do tipo de rede VPN (acesso remoto ou ponto a ponto), precisamos incluir certos componentes para construir nossa rede VPN (Morimoto, 2015). Dentre eles estão:

- Programa cliente para o computador de cada um dos usuários remotos;
- Equipamentos dedicados como um concentrador para redes VPN ou firewall PIX seguro;
- Servidor VPN dedicado, para serviços de discagem;
- NAS (Network Access Server) usado pelo provedor de serviços de um usuário remoto com acesso à rede VPN;
- Central de gerenciamento de políticas e de redes VPN.

Por não existir um padrão amplamente aceito para se implementar uma rede VPN, muitas empresas acabam desenvolvendo soluções próprias. A Cisco System, por exemplo, é conhecida por oferecer soluções completas e é considerada uma das mais importantes empresas fabricantes de dispositivos e equipamentos para redes de computadores. Incorporando as mais avançadas técnicas de criptografia e autenticação disponíveis, os concentradores VPN da Cisco são construídos

especificamente para a criação de VPN de acesso remoto. Eles oferecem alta disponibilidade, alto desempenho e escalabilidade e incluem componentes, chamados de módulos de processamento escalável de criptografia (SEP), que permitem aos usuários aumentar facilmente a capacidade de processamento. Os concentradores são oferecidos em modelos apropriados para cada tipo de necessidade, desde pequenos escritórios com até 100 usuários de acesso remoto até grandes organizações com até 10 mil usuários remotos simultâneos. (Morimoto, 2015).

Existem, também, roteadores otimizados VPN, os quais são capazes de prover escalabilidade, roteamento, segurança e QoS (qualidade de serviço). O firewall PIX (Private Internet Exchange), é um outro equipamento interessante, pois combina tradução de endereços da rede dinâmica, servidor proxy, filtragem de pacote, firewall e capacidades das redes VPN em um só equipamento. Independentemente do equipamento ou do fabricante, o mais importante é você saber que diversas soluções estão disponíveis nos dias de hoje. Soluções específicas em hardware são capazes de oferecer maior confiabilidade, segurança e rapidez. Claro que estas soluções possuem um custo inicial considerável, mas são muito mais eficientes do que soluções simples, onde, por exemplo, apenas software é utilizado para o gerenciamento da rede. (Marleta, 2007).

1.14.1. Segurança

Segundo Tanenbaum (2003), a segurança é um assunto abrangente e inclui diversos tipos de problemas. De maneira geral, a segurança foca-se em garantir que pessoas malintencionadas não leiam ou modifiquem secretamente mensagens enviadas a outros destinatários.

Com a introdução do computador, tornou-se evidente a necessidade de ferramentas automatizadas para proteger arquivos e outras informações armazenadas no computador. Esse é especialmente o caso de um sistema compartilhado, como um sistema de time-sharing. A necessidade é ainda mais evidente para sistemas que podem ser acessados por meio de uma rede telefônica pública, rede de dados ou a Internet. O nome genérico para o conjunto de ferramentas projetadas para proteger dados e impedir hackers é a segurança do computador, (Stallings, 2008).

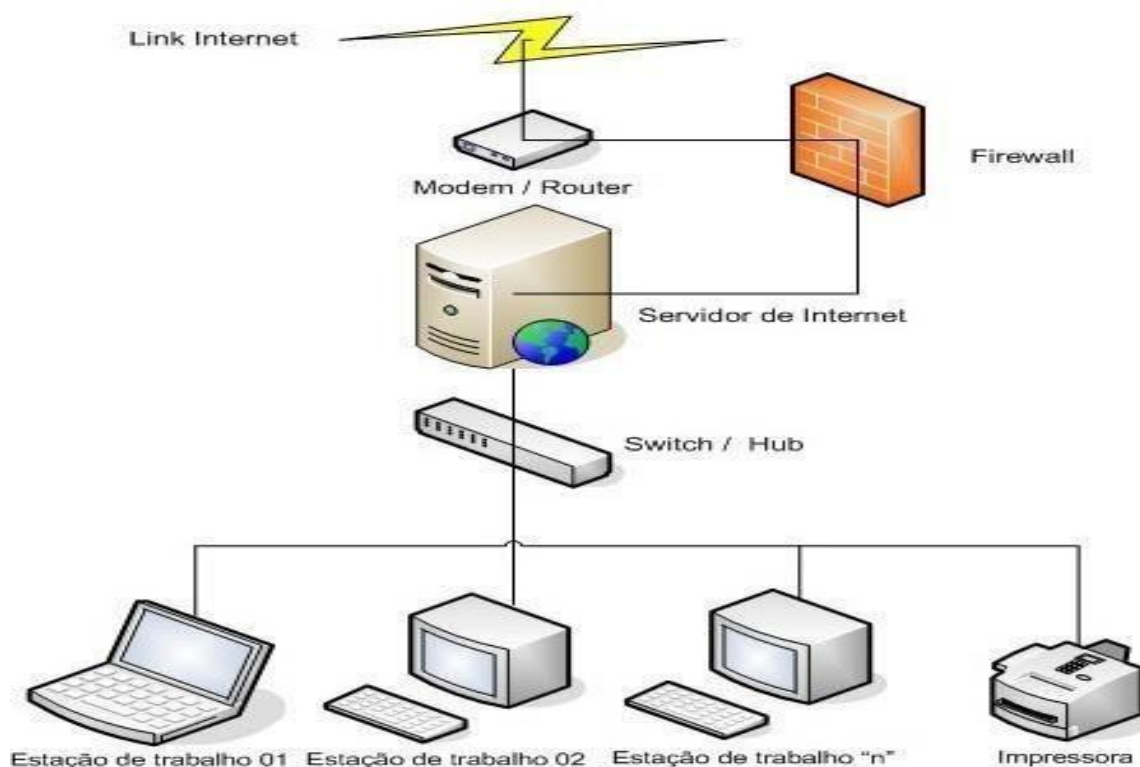
Deste modo, conforme Kurose e Ross (2004), pode-se identificar as seguintes propriedades desejáveis para uma comunicação segura:

- **Confidencialidade:** Somente o remetente e o destinatário pretendido devem poder entender a mensagem transmitida;
- **Autenticação:** O remetente e o destinatário precisam confirmar a identidade da outra parte envolvida na comunicação;
- **Integridade:** Mesmo que o remetente e o destinatário consigam se autenticar reciprocamente, eles também querem assegurar que o conteúdo da comunicação não seja alterado, por acidente ou por má intenção, durante a transmissão;
- **Disponibilidade:** Manter os recursos disponíveis, mesmo em caso de ataques.

1.14.2. Firewall

Um firewall é uma combinação de hardware e software que tem a função de isolar a rede interna de uma organização da Internet, permitindo que alguns pacotes passem e bloqueando outros (Casnova, 2010).

Figura 11: Exemplo de um Firewall



Fonte: (Casnova, 2010).

Há mais de uma forma de funcionamento de um firewall, que varia de acordo com o sistema, aplicação ou do desenvolvedor do programa. No entanto, existem dois tipos básicos de conceitos de firewalls: o que é baseado em filtragem de pacotes IP e o que é baseado em controle de aplicações, que é geralmente instalado em servidores.

1.14.3. Criptografia

De acordo com Tanenbaum (2010), a palavra criptografia vem das palavras gregas (Kryptos = escondido, oculto e Grafia = escrita) que significam “escrita secreta”. As mensagens a serem criptografadas, conhecidas como texto simples (plain text) são transformadas por uma função que é parametrizada por uma chave. Em seguida, a saída do processo de criptografia, conhecida como texto cifrado (cipher text), é transmitida, normalmente através de um mensageiro. Presume-se que o inimigo, ou intruso, “ouça” e copie cuidadosamente o texto cifrado completo. No entanto, ao contrário do destinatário pretendido, ele não conhece a chave para descriptografar o texto e, portanto, não pode fazê-lo com muita facilidade.

Em sistemas de criptografia, deve-se observar que a chave é o elemento mais importante. A chave é formada por uma combinação de bits, e quanto maior for esta combinação, maior será a segurança adquirida, entretanto ocorrendo uma maior sobrecarga de processamento. Então, dependendo do tipo de chave utilizada, tem-se criptografia simétrica ou criptografia assimétrica (Tanenbaum, 2010).

1.14.4. Criptografia Simétrica

Na técnica de criptografia simétrica, tem-se a mesma chave para criptografar e descriptografar os dados. Logo, esta chave será previamente trocada entre o emissor e receptor, por meio de uma comunicação segura (Stallings, 2008).

Segundo Stallings (2008), um esquema de criptografia simétrica possui cinco componentes:

- **Texto claro:** Esta é a mensagem ou dados originais, como entrada para o algoritmo.
- **Algoritmo de criptografia:** O algoritmo de criptografia realiza diversas substituições e transformações no texto claro.

- **Chave secreta:** A chave secreta também é a entrada para o algoritmo de criptografia. A chave é um valor independente do texto claro e do algoritmo. O algoritmo produzirá uma saída diferente, dependendo da chave específica sendo usada no momento. As substituições e transformações exatas realizadas pelo algoritmo dependem da chave;
- **Texto cifrado:** Essa é a mensagem embaralhada, produzida como saída. Ela depende do texto claro e da chave secreta.
- **Algoritmo de decriptografia:** Esse é basicamente o algoritmo de criptografia executado de modo inverso. Ele toma o texto cifrado e a chave secreta e produz o texto claro original.

A sigla VPN significa Virtual Private Network, ou seja, Redes Privadas Virtuais, onde: Rede corresponde às redes de computadores;

- Privada corresponde à forma como os dados trafegam neste caso os dados podem ser criptografados o que garante a privacidade das informações;

Virtual por não fazerem, necessariamente, parte do mesmo meio físico. Então, uma VPN é uma rede privada construída sobre a infra-estrutura de uma rede pública já existente, normalmente a Internet, onde o acesso e a troca de dados só são permitidos a pessoas que estejam autorizadas. Desta forma, tem-se a construção de um túnel entre duas ou mais redes, pelo qual pode ser configurado para garantir autenticidade de dados, sigilo de informação, controle de acesso através de criptografia do tráfego de informação entre uma rede e outra (Fagundes, 2007).

CAPÍTULO II. METODOLOGIA DE PESQUISA

2.1. Tipo de Pesquisa

Para a elaboração do presente trabalho, definimos a pesquisa Descritiva.

Para Kocher (2013, p. 35), pesquisa descritiva que busca-se descrever uma dada realidade, sem interferir nela. Essa pesquisa nos permitiu descrever factos sem a manipulação, buscando com precisão distribuir a frequência em que um fenómeno ocorre e a sua relação com outros factores.

2.2. Modelo de abordagem

Segundo Severino (2013, p. 115), diz que abordagem qualitativa possibilita a recolha de informação mais profunda, rica e precisa e, faz a descrição dos fenómenos que ocorrem durante o processo de recolha de informações.

Para a presente pesquisa utilizamos abordagem qualitativa, na medida que utilizamos a observação e consulta em postelados que por sua vez serviu de meio de execução do aplicativo de rede para a Instituição.

2.3. Nível de estruturação de métodos

De acordo com Lakatos & Marconi (2010, p. 88), método é o conjunto das actividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objectivo-conhecimentos válidos e verdadeiros, traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista.

a) Nível teórico

❖ Hipotético-dedutivo

O método hipotético/dedutivo inicia pela percepção de uma lacuna nos conhecimentos acerca da qual formula hipótese e pelo processo de inferência dedutiva, testa a predição da ocorrência de fenómeno abrangendo pela hipótese (Severino, 2023).

b) Nível emprírico/experimental

Os métodos de nível emprírico / experimental para pesquisa foi, a entrevista dirigida aos membros da Direcção e alguns funcionários do Instituto Superior de Angola, assim como a observação participante. Com este método foi possível alcançar os objectivos proposto, bem como a confirmação das hipóteses.

2.4. Técnicas de Recolha de dados

Documentos: Vamos consultar os diferentes tipos de documentos de trabalho que a direcção colocar a nossa disposição.

Bibliografias: Onde podemos consultar os diferentes livros e monografias, fascículos e arquivos.

Observação: Está técnica permitiu nos ter uma visão clínica de como funciona o sistema actual, e que de certo modo permitiu nos a ter uma prespectiva de como deve ser o novo sistema.

2.5. Instrumentos e procedimentos de recolha de dados

Entrevista: tivemos a oportunitade de entrevistar alguns funcionários e os membros da direcção do complexo de tal modo que com as informações dadas, servisse-nos de base para execução das ideis para implementação da infraestrutura de rede.

Observação: Usamos a observação como instrumento de pesquisa pelo facto dela constituir uma técnica pela qual podemos ter uma visão olística do sistema actual, e através da mesma ajudarnos a prespectivar um sistema mais moderno face os aspectos a ter em conta na observação ora feita antes.

2.6. População e amostra

2.6.1. População

Segundo Gil (2002, p.89) população é “o conjunto definido de elementos que possuem determinadas características”.

Sendo assim, definiu-se como população de pesquisa 26 efectivos distribuídos entre as áreas.

2.6.2. Amostra

De acordo com Severino, (2007), “amostra é a parte da população ou do universo, seleccionada de acordo com uma regra ou plano”.

Por sua vez a nossa população de pesquisa é de 100%: sendo assim entrevistamos 14 funcionários, 70% do sexo masculino e 30% do sexo feminino, possuindo idades no intervalo de 27 à 52 anos, funcionários residentes no Município de Cacuaco na Provincia de Luanda.

2.7. Dificuldades encontradas

No que diz respeito a esse quisito, algumas das dificuldades encontradas foi o acesso as informações uma vez que este elemento constitui o cerne da pesquisa:

- ✓ Tivemos problemas com o materiais para executar de forma prática a infraestrutura de rede;
- ✓ Infraestruturas já encontrados na instituição é um tanto quanto débil, pois em nada contribui para uma dinâmica functional e estrtural da rede estalada;
- ✓ Dificuldades manter um contacto permanente de modo a ter mais informações sobre a implementação da rede privada virtual;
- ✓ A falta de energia eléctrica tem dificultado o funcionamento da escola;
- ✓ Dificuldades financeiras.

CAPÍTULO III. DISCUSSÃO E RESULTADOS

3.1. Descrição e caracterização da instituição em estudo

Nome do Escola: Instituto Superior de Angola, endereço: Cacuaco, Nova urbanização. Cidade: Luanda. Ramo de actividade: Ensino Superior Ciência e Tecnologia (Ensino e Aprendizado)

❖ Missão da Empresa

Formar profissionais qualificados e comprometidos com desenvolvimento sustentável de Angola.

❖ Visão da Empresa

Consolidar o estatuto de Escola de referência do Ensino Superior, a nível nacional e internacional, particularmente nos países da CPLP e da África Austral.

❖ Valores:

- ✓ Rigor científico e profissional;
- ✓ Inovação e criatividade;
- ✓ Responsabilidade social e ambiental;
- ✓ Compromisso com o desenvolvimento humano e sustentável;
- ✓ Unidade curricular.

❖ Secção de Ciências Sociais e Humanas

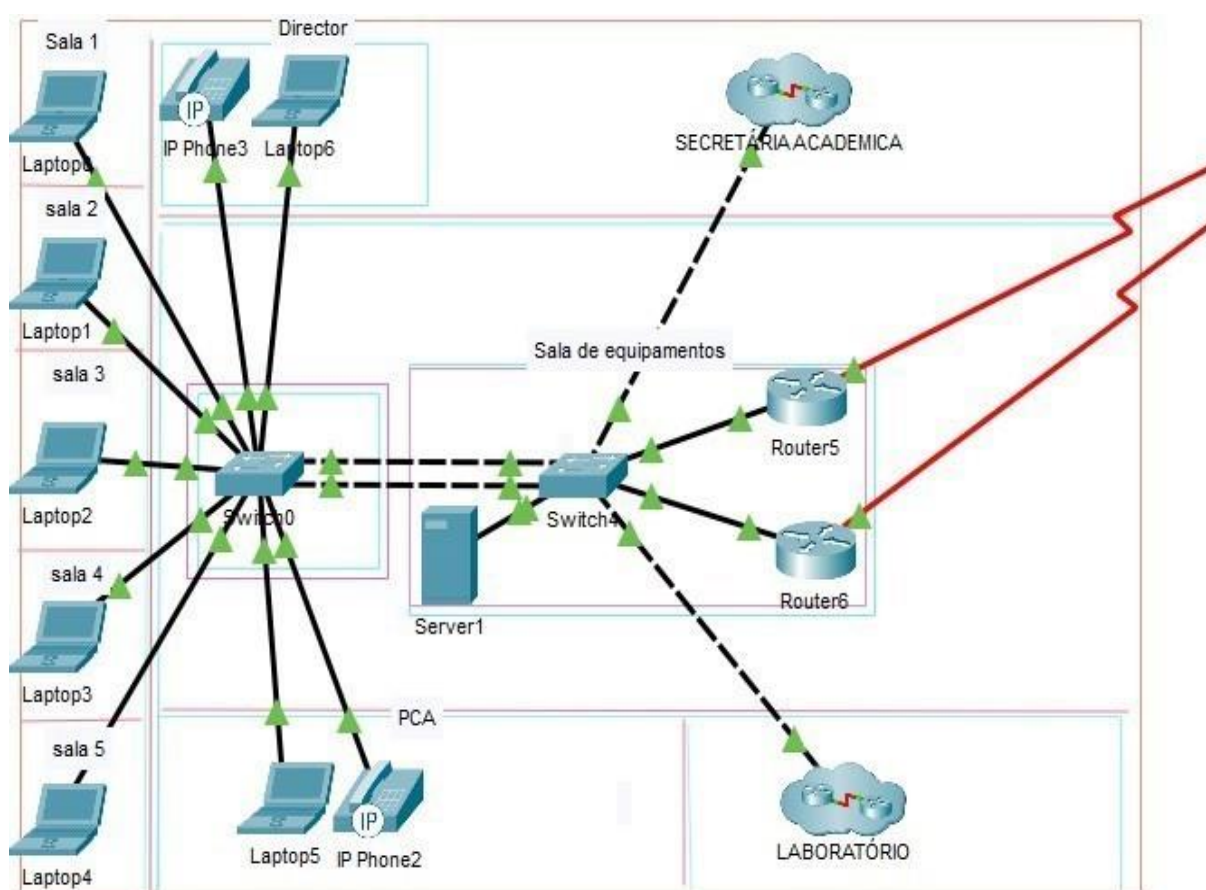
- ✓ Ciências Políticas e Administrativas;
- ✓ Comunicação Social;
- ✓ Direito;
- ✓ Educação Física;
- ✓ Geração de Recursos Humanos;
- ✓ Pedagogia;
- ✓ Psicologia;
- ✓ Sociologia;
- ✓ Secção de Ciências;
- ✓ Gestão de Empresas:
- ✓ Economia;
- ✓ Marketing.

❖ **Secção de Ciências e Tecnologias**

- ✓ Análises Clínicas (Técnicas de Laboratório);
- ✓ Enfermagem;
- ✓ Fisioterapia;
- ✓ Ciências Aeronáuticas;
- ✓ Ciências Alimentares;
- ✓ Electrónica e Telecomunicações;
- ✓ Engenharia Informática;
- ✓ Agronomia.

3.2. Diagrama lógico da Rede ISA

Figura 12: Diagrama lógico da Rede ISA



Fonte: Própria (2025)

Tabela 1: Orçamento dos materias

Qtda	Descrição	Preço unit. (com IVA)	Valores
1	Cabo rede 350M UTP Cat6 intell	44.782,00	44.782,00
1	Reuter 2800 Cisco	470,000.00	470,000.00
1	Switch TP-LINK 24 Portas	55.783,00	55.783,00
1	Conector cat6 rj45/ 120 unidades	8.266,00	8.266,00
1	Patch panel-48 portas Cat6 48 Portas	47.996,00	47.996,00
1	Armário 06U 600X450 INT 19 AÇO (Rack)	68.000,00	68.000,00
1	Router DLINK Wife VPN 4 X LAN/2 X	258.078,00	258.078,00
1	UPS WINTECH 2000 VA TOUCH	129.168,00	72.340,00
1	Servidor	390,000.00	390,000.00
22	Portatil Lenovo	377.630,50	377.630,50
		Sub-total	1.849.703,5

Fonte: Própria (2025).

Tabela 2: Orçamento de mão de obra

Orçamento de mão de Obra	
Cabeamento	150.000,00
Instalação e configuração	60.000,00
Configuração de estação de trabalho	70.000,00
Treinamento	60.000,00
Manutenção	70.000,00
Total: 410.000,00	

Fonte: Própria (2025).

Tabela 3: Orçamento geral do projecto

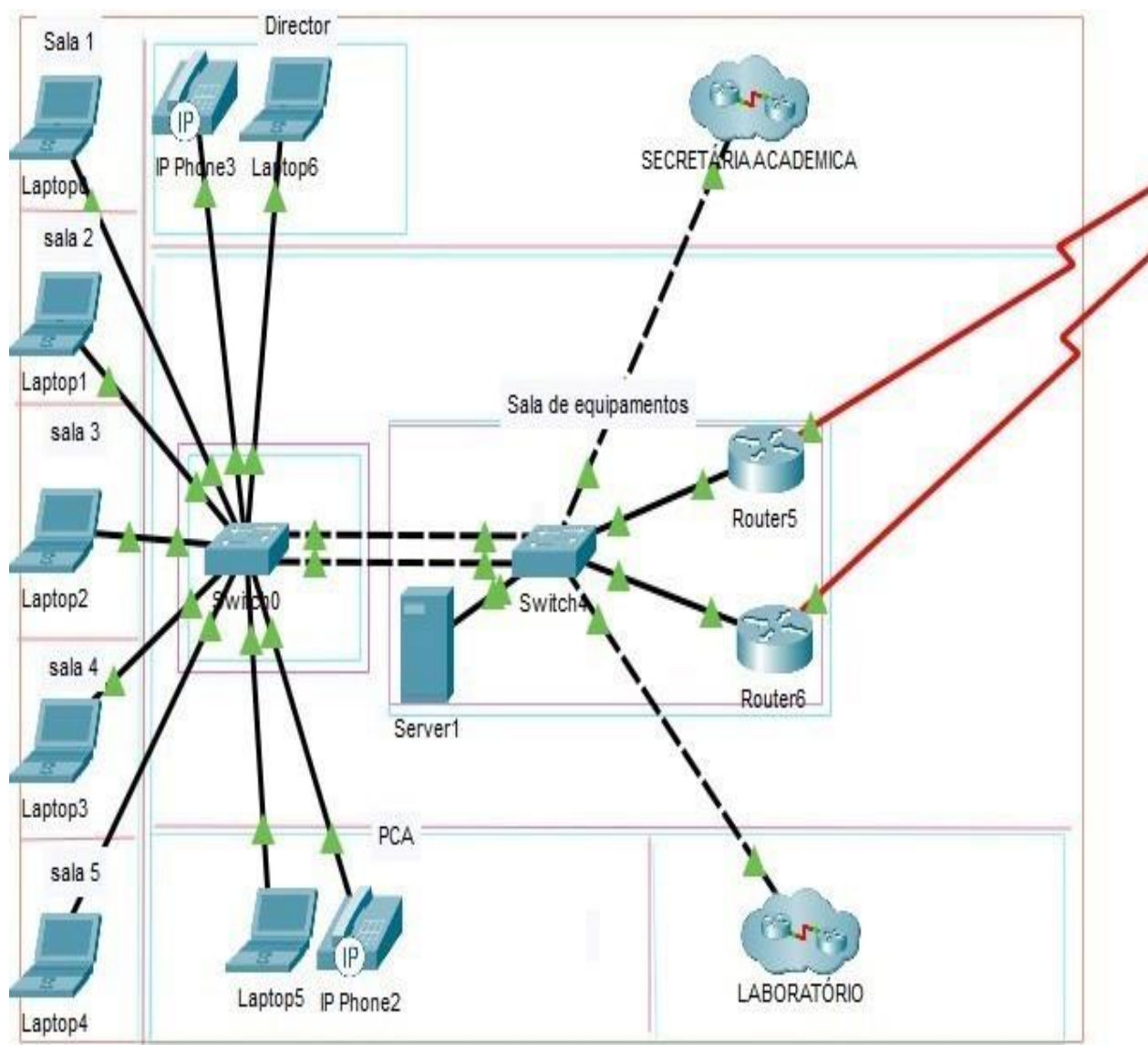
Matérias	4.514.950,00
Serviços	410.000,00
Imprevistos	150.000,00
Total geral: 5.074.950,00	

Fonte: Própria (2025).

3.3. Desenvolvimento de protótipo da Futura Rede do ISA

Para ilustrar a rede foi montada a topologia representada pela figura abaixo e implementada em laboratório.

Figura 13: Topologia central

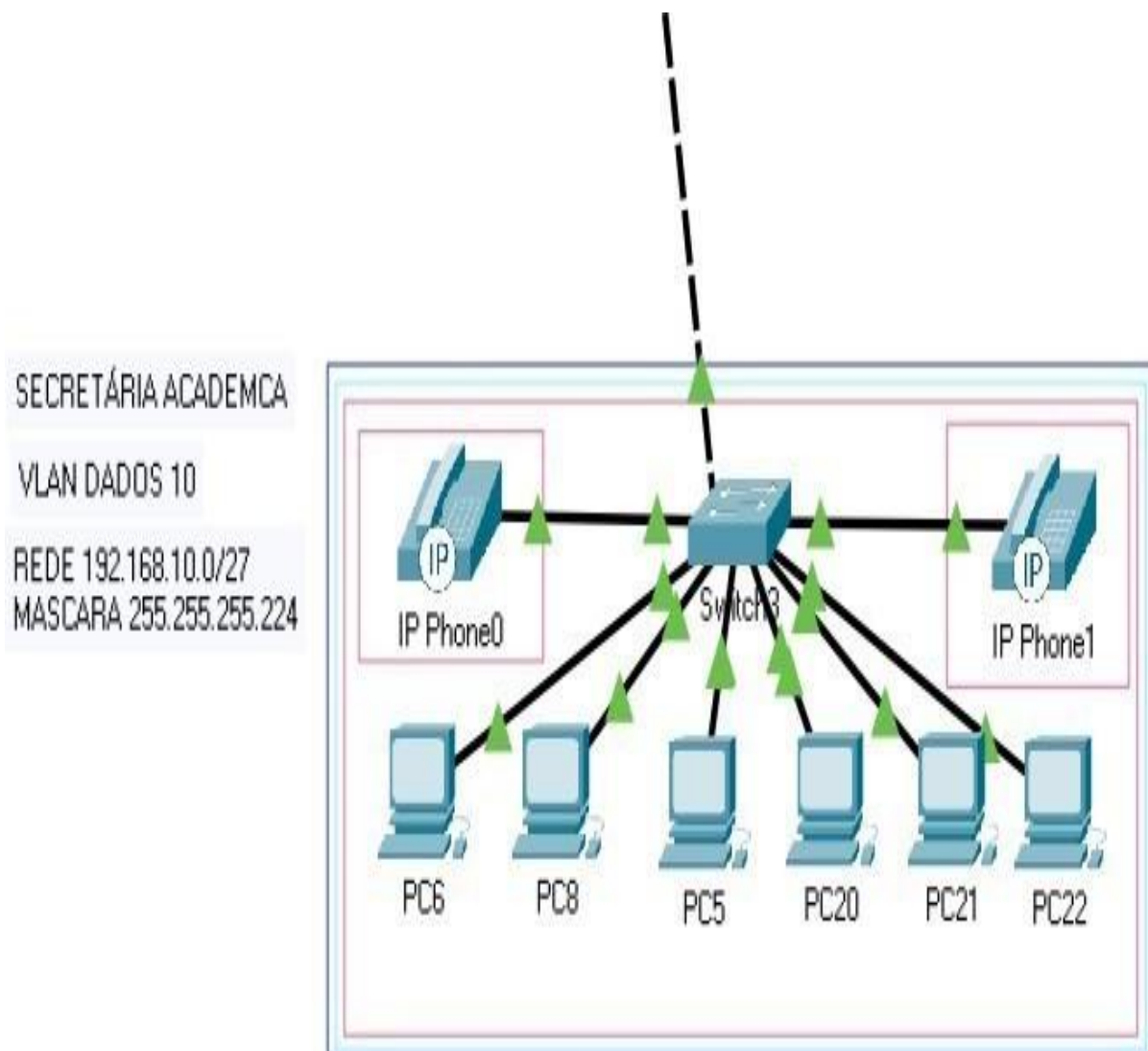


Fonte: Própria (2025).

3.3.1. Secretaria geral

Para ilustrar a rede da secretária foi montada a topologia representada pelas figuras abaixo e implementada em laboratório.

Figura 14: Secretária rede central

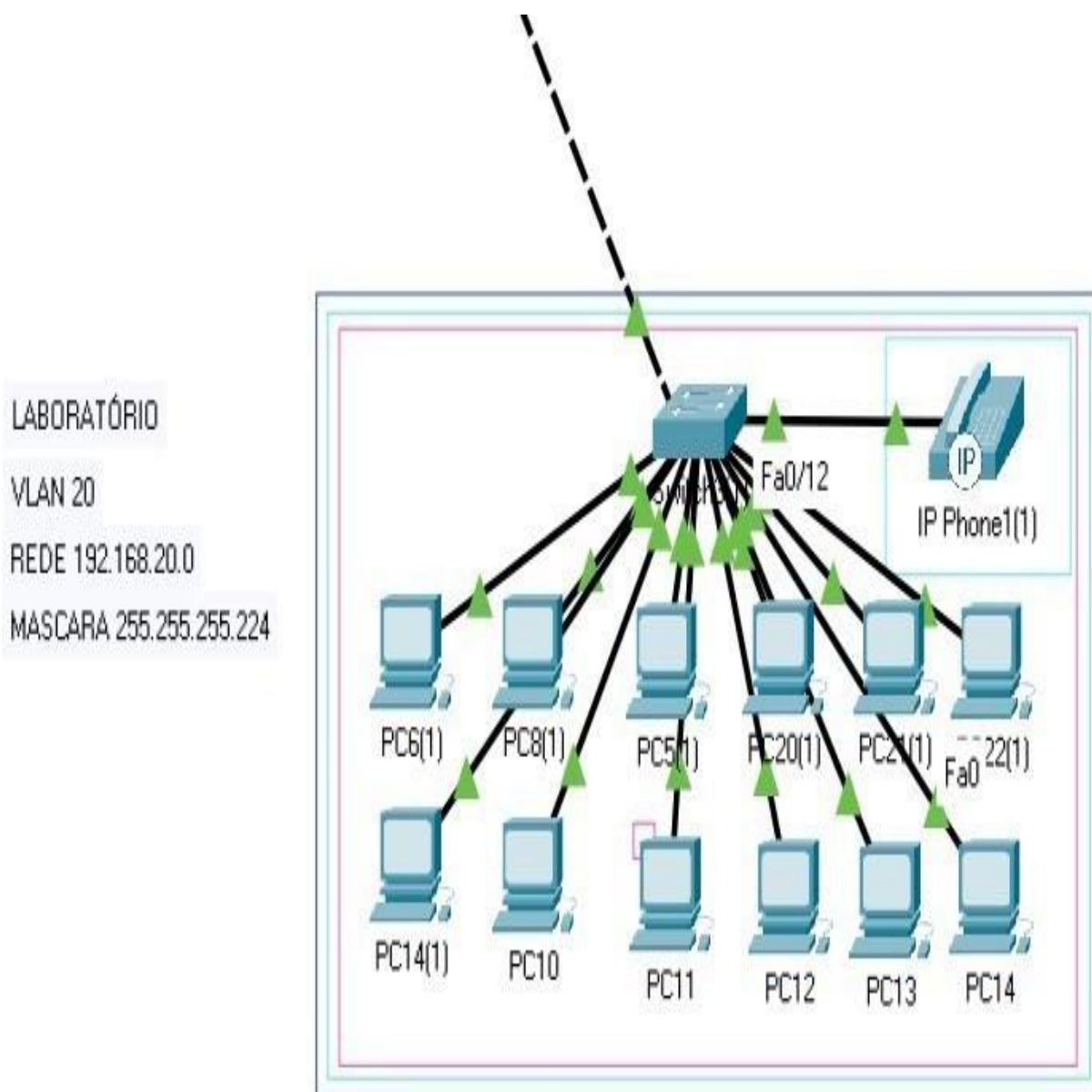


Fonte: Própria (2025).

3.3.2. Laboratório

Para ilustrar a sub-rede do laboratório foi montada a topologia representada pela figura abaixo e implementada em laboratório.

Figura 15: Sub-rede do laboratório

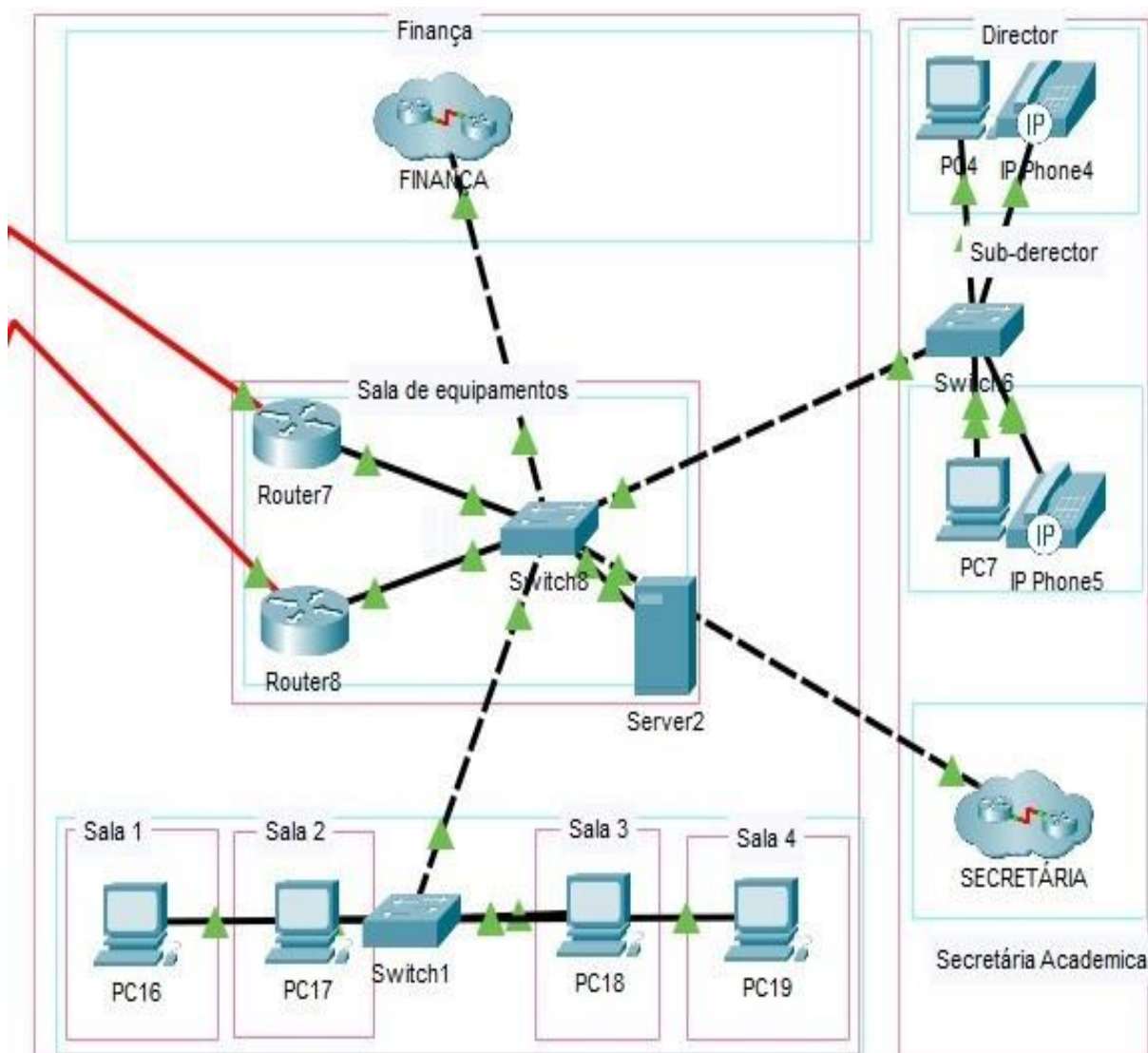


Fonte: Própria (2025).

3.3.3. Rede ISA

Para ilustrar a proposta da rede do ISA foi montada a topologia representada pela figura abaixo e implementada em laboratório.

Figura 16: Rede ISA

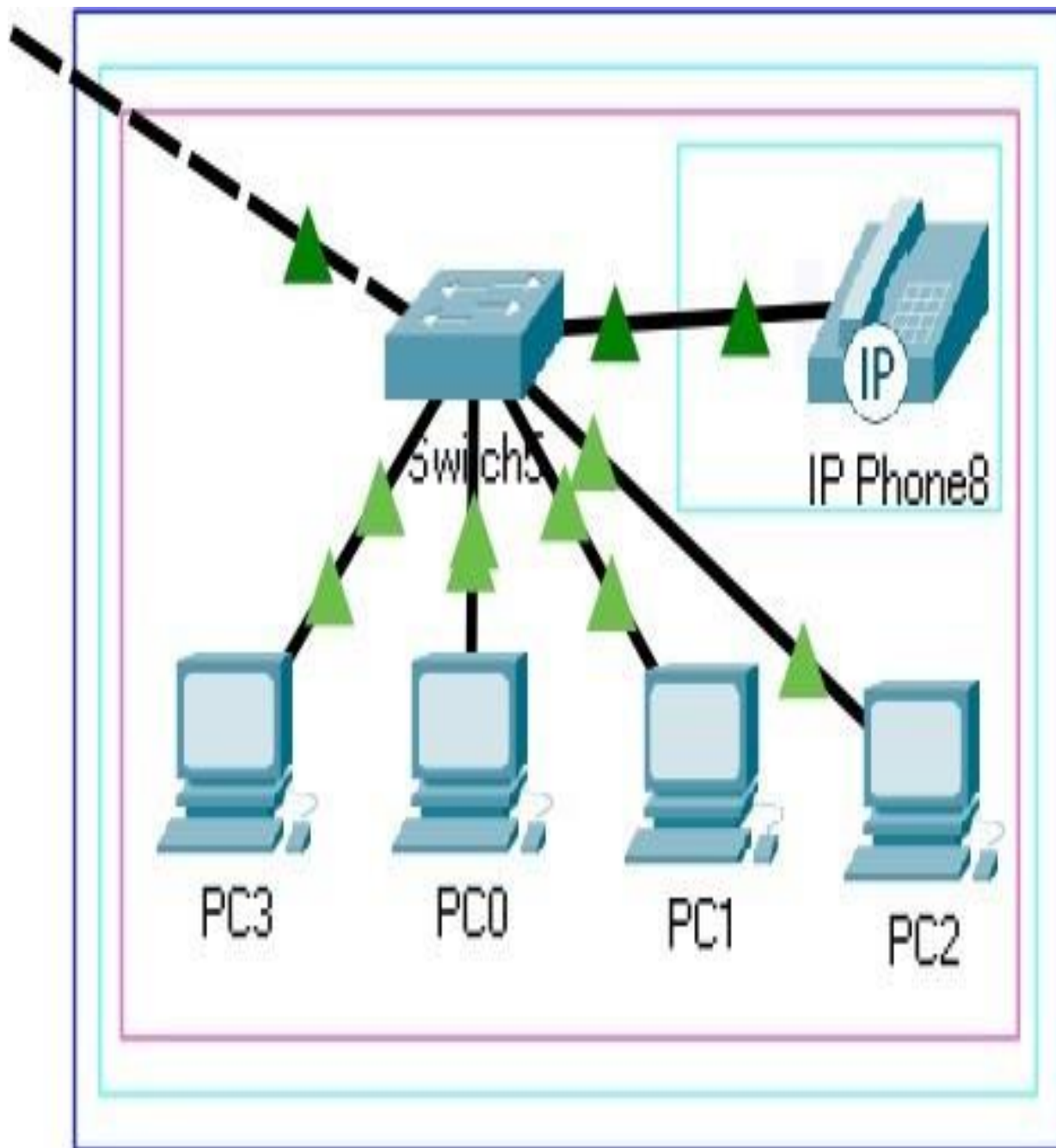


Fonte: Própria (2025)

3.3.4. Finança

Para ilustrar a proposta da sub-rede de finança foi montada a topologia representada pela figura abaixo e implementada em laboratório.

Figura 17: Sub-rede de finança da rede filiar

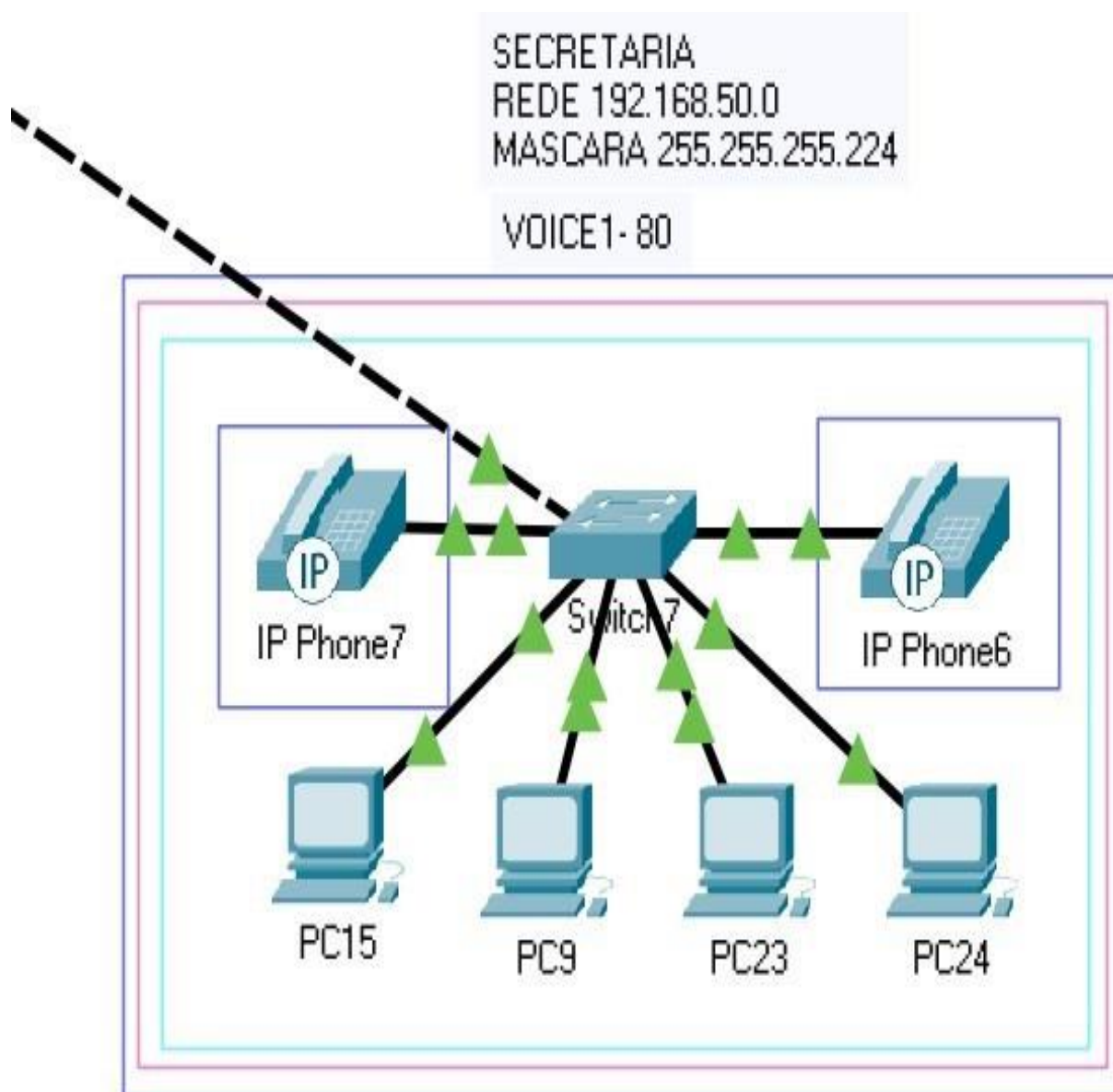


Fonte: Própria (2025).

3.3.5. Secretária

Para ilustrar a proposta da rede do ISA foi montada a topologia representada pela figura abaixo e implementada em laboratório.

Figura 18: Sub-rede da secretária da rede filiar

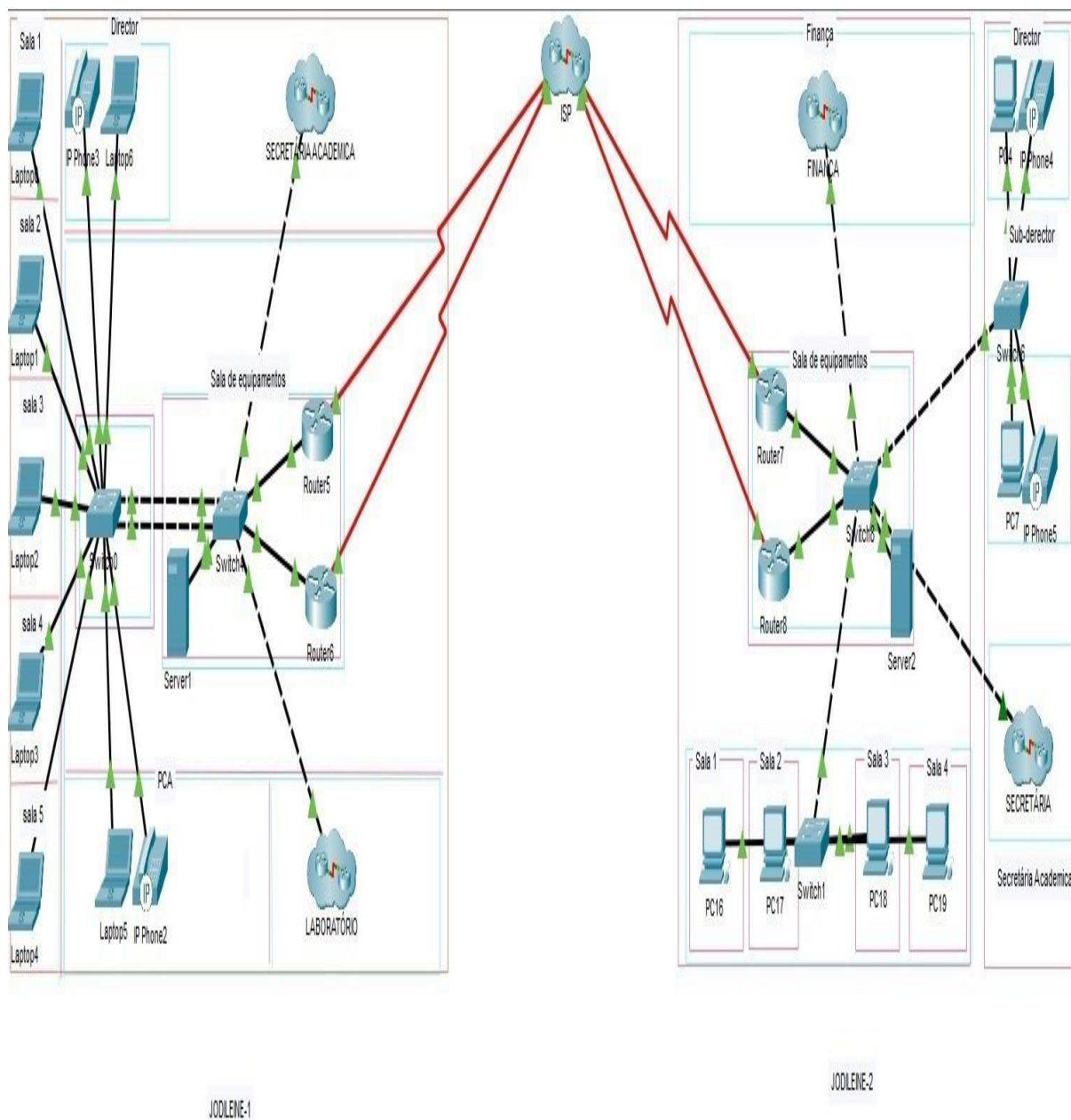


Fonte: Própria (2025).

3.3.6. Representação da Interligação das redes

Para ilustrar as redes foi montada a topologia representada pela as figuras abaixo e implementada em laboratório.

Figura 19: Ilustração da interligação das rede

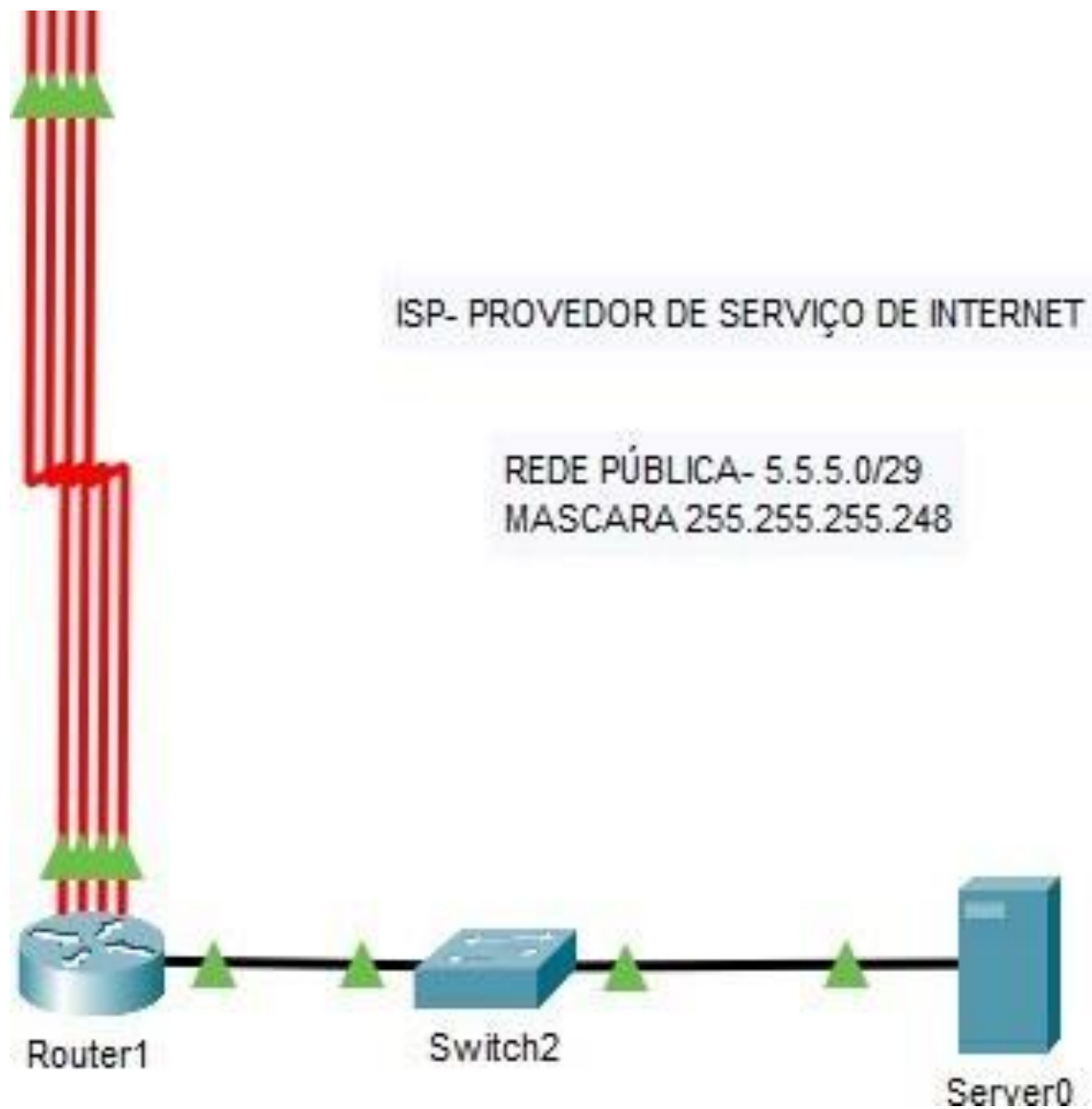


Fonte: Própria (2025).

3.3.7. Provedor de Serviço de Internet

Para ilustrar as redes foi montada a topologia representada pela as figuras abaixo e implementada em laboratório.

Figura 20: Ilustração do provedor do serviço de internet



Fonte: Própria (2025).

CONCLUSÃO

Portanto, depois de um longo período de investigação podemos afirmar que as VPN são de suma importância nos dias de hoje, visto quase todas as empresas trafegam pacotes a partir da internet, a VPN é um modo seguro de trafegar pacotes (informação) através da internet.

A utilização da internet danos a possibilidade de usufruir dos serviços que alternativamente seria necessária a contratação de circuitos virtuais pelas operadoras, assim sendo dinamiza consideravelmente a rentabilidade da instituição, possibilitando a contratação de melhores serviços para o acesso à internet no Instituto Superior de Angola

No entanto, com a implementação de uma VPN irá permitir interligar dois pontos geograficamente distantes, e poderá garantir a segurança de pacotes através do método de criptografias das VPN.

Desta forma podemos também concluir que a pesquisa foi um facto na medida em que as hipóteses levantadas foram todas confirmadas, e de frisar que a instituição por sua vez poderá usufruir de forma eficaz e eficiente a aplicação. Outro sim também da se no facto dos objectivos preconizados na pesquisa foram de certo modo materializados aí que pensamos que a presente instituição no caso o instituto superior de Angola, caso pore m prática a presente proposta de implementação obviamente vai conseguir ter um tráfego de suas informações mais eficiente e com uma eficacia mais adequado.

SUGESTÕES

Como forma de sugestão temos de sugerir o seguinte:

Há que se fazer um investimento arduo de maneira que haja uma segurança mais eficiente através da utilização do mecanismo de restrições a rede usando o serviço VPN;

Deve-se também fazer um investimento em aplicativos de segurança para o combate de malwares;

Para o manuseamento da rede eficiente é sem dúvida importante um treinamento constante por parte dos peaplwares da instituição;

É necessário investir em softwares e hardwares para garantir o beckuaps.

REFERÊNCIAS BIBLIOGRÁFICAS

- Alencar, M. A. S. (2010). *Fundamentos de redes de computadores*. Universidade Federal do Amazonas, CET lecrim, E. (2004, novembro 08). *Diferenças entre hub, switch e roteador*. Info Wester. Disponível em: <http://www.infowester.com/hubswitchrouter.php> (Acesso em: 14 fev. 2013).
- Assis, J. M. (2003). *Implementando VPN em Linux (Monografia de Pós-Graduação)*. Universidade Federal de Lavras, Lavras.
- Bresser-Pereira, L. C. (2004). *Políticas de gestão do Estado e políticas econômicas: Novos desafios*. Revista de Economia Política, 24(4), 26-41.
- Birkinshaw, J., & Goddard, J. (2009). *O que é implementação?* *Organization Science*, 20(1), 311- 320.
- Bilien, J., & Daound, A. (2010). *Documentation: Streaming HowTo*. Disponível em: [http://wiki.videolan.org/Documentation:Streaming HowTo](http://wiki.videolan.org/Documentation:Streaming_HowTo) (Acesso em: 3 out. 2010).
- Brown, J. C. (2021). *Network security essentials*. 6ª edição. Pearson.
- Catalin. (2010). *Unicast and multicast streaming*. Disponível em: <http://www.thehdstandard.com/hd-streaming/unicast-and-multicast-streaming/> (Acesso em: 8 set. 2010).
- Catramby, G. F. (2010). *VPN – Virtual Private Network*. Disponível em: http://www.gta.ufrj.br/grad/99_1/gabriela/vpn.html#5 (Acesso em: 10 abr. 2010).
- Casnova, T. I., Consulting. (2010). *Firewall, qos, vpn linux: Segurança da sua rede local*. Disponível em: <http://www.casnova.com.br/casnova> (Acesso em: 11 out. 2010).
- Comer, D. E. (2007). *Redes de computadores e internet*. Porto Alegre: Bookman.
- Davie, L. L., & Peterson, B. S. (2004). *Redes de computadores: Uma abordagem de sistemas*. Rio de Janeiro: Campus.

- Fagundes, B. A. (2007). *Uma implementação de VPN*.
- Franciscatto, R. (2014). *Redes de computadores*. Universidade Federal de Santa Maria, Colégio Agrícola de Frederico Westphalen.
- GTA – Grupo de Teleinformática e Automação. (2010). *SSL: Secure Socket Layer*. Disponível em: http://www.gta.ufrj.br/grad/00_2/ssl/ssl.htm (Acesso em: 10 mai. 2010).
- Guimarães, F. R. (2004). *Como fazer? Diretrizes para a elaboração de trabalhos monográficos*. Edijur.
- Guilherme, J. (2013). *Criptografia, chaves públicas e assinatura digital para leigos*.
- Johnson, R. E. (2010). *Introduction to security: Operations and management* (4th ed.). Prentice Hall.
- Kurose, J. F., & Ross, K. W. (2009). *Computer networking: A top-down approach* (5th ed.). Pearson.
- Kurose, J. F., & Ross, K. W. (2004). *Redes de computadores e a Internet: uma nova abordagem*. Pearson Education do Brasil.
- Kurose, J. F., & Ross, K. W. (2010). *Redes de computadores e a Internet: uma abordagem top-down*. Addison-Wesley.
- Kurose, J. F., & Ross, K. W. (2017). *Redes de computadores e a Internet*.
- Kocher, P. (2013). *Métodos e técnicas de pesquisa social* (2ª ed.). Silva, L. S. (2002). *Virtual private network – VPN*. Novatec.
- Malhotra, N. K. (2011). *Pesquisa de marketing: Foco na decisão* (3ª ed.). Bookman.
- Marconi, M. A., & Lakatos, E. M. (2016). *Técnicas de pesquisa: Planejamento e execução de pesquisas, amostragens e técnicas de pesquisas, elaboração, análise e interpretação de dados* (6ª ed.). Atlas.
- McLean, J. C. (2004). *Windows Server 2003 network infrastructure: Implementing, managing, and maintaining a Microsoft*.
- Maguione, M. (2010, maio 5). *Configuração de um servidor VPN com OpenVPN e chave estática*. Viva o Linux. Disponível em <http://www.vivaolinux.com.br/artigo/Configuracao-de-um-servidor-VPN->

comOpenVPN-e-chave-estatica.

Marleta, M. H. (2007). *Projeto de uma VPN (Rede Virtual Privada) baseada em computação reconfigurável e aplicada a robôs móveis*.

Morimoto, C. E. (2010). *Criando VPNs usando chaves estáticas*. Guia do Hardware. Disponível em <http://www.guiadohardware.net/tutoriais/openvpn/pagina3.html> Mendes, D. R. (2007). *Redes de computadores – Teoria e prática*. Novatec.

Moraes, A. F., & Cirone, A. C. (2003). *Redes de computadores – Da Ethernet à internet*.

Morimoto, C. E. (2007). *Faixas de endereços IP, CIDR e máscaras de tamanho variável*. Guia do Hardware. Disponível em <http://www.hardware.com.br/tutoriais/endereco-ip-cidr/pagina2.html>

Pearson. Tanenbaum, A. S. (2003). *Redes de computadores* (V. D. de Souza, Trad.). Elsevier. Torres, G. (2009). *Redes de computadores*. Nova Terra.

Pearson Prentice Hall. Scrimger, R. (2011). *TCP/IP: A bíblia*. Campus.

Peterson, L. L., & Davie, B. S. (2012). *Computer networks: A systems approach* (5th ed.). Morgan Kaufmann.

Ramos, S., & Naranjo, E. (2014). *Metodologia de investigação científica* (2ª ed.). Editora Escolar.

Rigney, C., Willens, S., Rubens, A., & Simpson, W. (2000). *Remote Authentication Dial In User Service (RADIUS)*.

Rossi, M. A. G., & Franzin, O. (2010). *VPN – Virtual Private Network (Rede Virtual Privada)*. GPR. Disponível em <http://www.gpr.com.br/download/vpn.pdf>

Stallings, W. (2008). *Criptografia e segurança de redes: Princípios e práticas*. (4ª ed.).

Sardinha, G. (2009). *Virtualização de servidores*. Voo Livre Linux. Disponível em <http://voolivrelinux.blogspot.com/2009/09/virtualizacao-deservidores.html>

Sauvé, J. (2010). *Estrutura de dados – Arquivos*. Disponível em <http://www.dsc.ufcg.edu.br/~jacques/cursos/p2/html/ed/arquivos.html>

- Severino, A. J. (2007). *Metodologia do trabalho científico* (23ª ed.). Cortez. Smith, M. K. (2015). *Managing information technology* (7th ed.). Pearson. Stallings, W., & Case, T. (2013). *Business data communications: Networking* (12th ed.). Pearson.
- Silva, L. S. (2002). *Virtual Private Network*. São Paulo: Novatec. Sousa, R. (1999). *Redes de computadores*. Rio de Janeiro: Campus.
- Silva, C. C. (2010). *Redes de computadores – Conceito e prática*. Viena.
- Sousa, R., & Puttini, P. S. (2010). *O protocolo SSL 3.0*. Disponível em <http://www.redes.unb.br/security/ssl3/protocolo.html>
- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Redes de computadores*.
- Urbiêta, J. L. (2007). *Estudo das soluções de transmissão de vídeo utilizando software livre* (Monografia de Pós-Graduação). Universidade Federal de Lavras, Lavras.
- Vasques, T. A., & Schuber, R. P. (2002). *Implementação de uma VPN em Linux utilizando o protocolo IPSec* (Trabalho de Conclusão de Curso). Centro Universitário do Estado do Pará – CESUPA, Belém.
- Whitman, M. E., & Mattord, H. J. (2011). *Princípios de segurança da informação: Teoria e prática* (2ª ed.). Cengage Learning.
- Wrightson, T. (2014). *Segurança de redes sem fio: Guia do iniciante*. Bookman.
- WAY Networks. (2010, 5 de outubro). *Virtual Private Networks – VPN*. Disponível em <http://fgsl.aslgo.org.br/fgsl3/images/atividades/vpn.pdf>.

APÊNDICES

ENTREVISTA DIRIGIDA AO PRESIDENTE E FUNCIONÁRIOS DO INSTITUTO SUPERIOR DE ANGOLA

Estimado Presidente, a realização desta entrevista inseri-se no âmbito de uma investigação conducente em ciências das engenharias, nomeadamente a licenciatura em engenharia informática, tem como objectivo Propor a implementação de uma Rede Privada Virtual no Instituto Superior de Angola.

Ocupação:_____ Tempo de serviço:___ Idade:___ Nivel academico:_____

1 - De que forma poderá ajudar a implementação de uma rede privada virtual no Instituto Superior de Angola (ISA)?

R:_____

2 - A implementação de uma rede privada virtual (VPN) pode reduzir as vulnerabilidades na transmissão de dados do Instituto Superior de Angola?

R:_____

3 - A configuração de uma VPN pode permitir melhor controle de acessos e privilégios dos usuários, diminuindo os riscos de ataques cibernéticos?

R:_____

4 - A implementação de uma Rede Privada Virtual poderá acautelar os problemas de constantes congestionamento no tráfego da informação do Instituto Superior de Angola?

R:_____

5 - Em que consiste a implementação de uma rede privada virtul no ISA?

R:_____

6 - Quais seriam as vantagens ao implementar um sistema de comunicação por computadores de maneira privada?

R:_____

Muito obrigado

QUESTIONÁRIO DIRIGIDA AO PRESIDENTE E FUNCIONÁRIOS DO INSTITUTO SUPERIOR DE ANGOLA

Estimado Presidente, a realização desta entrevista inseri-se no âmbito de uma investigação conducente em ciências das engenharias, nomeadamente a licenciatura em engenharia informática, tem como objectivo Propor a implementação de uma Rede Privada Virtual no Instituto Superior de Angola.

Ocupação:_____ Tempo de serviço:___ Idade:___ Nivel academico:_____

Em cada questão responde com clareza sem omitir a verdade, marcando (X) nas respostas que mais lhe convêm.

1 - A infraestrutura de rede de computadores da instituição é segura?

Sim (), b) Não (), C) Nem tanto ().

2 - O instituto tem políticas de rígidas para os backups de segurança?

Sim (), b) Não (), C) Nem tanto ().

3 - As infraestruturas de redes tem ramificações ao ponto da informação fluir sem constrangimentos)

Sim (), b) Não (), C) Nem tanto ().

4 – Os gestores de redes sabem sobre o tunenamento?

a)- Sim (), b) Não (), C) Nem tanto ().

Muito obrigado

ANEXOS

ZICAI GRUPO, LDA
NIF: 5417012670
Vila de Cacauco
Cacauco - Luanda
Telef. 929050530
E-mail: info@zicaigrupo.com

Pro-Forma

FACTURA PROFORMA

Data

2025-03-29

Número

PP 20012025/647

ANTÓNIO KULAZI

LUANDA

LUANDA

Angola

ORIGINAL

Página 01

Entidade	V/Contribuinte	Vendedor	V/Encomenda	Mod.Pag.	Armazém	Validade
999999999	-----	---		PRONTO P	1	2025-03-29

ESTA PROFORMA TEM VALIDADE DE 2 DIAS

Cód. Produto	Designação	Un	Quant.	Unitário	Desc.	Total
CCA-23UTP-CAT6	CCA UTP CAT6 23AWG 305M	UN	1,00	46 228.00		46 228.00
TL-SF1024D	SWITCH TP-LINK 24 PORT 10/100MBPS	UN	1,00	55 783.00		55 783.00
502399	CONNECTOR INTELL CAT5	UN	1,00	9 703.20		9 703.20
PATCH-PANEL/48P	PATCH PANEL CAT6 48 PORTS	UN	1,00	47 996.00		47 996.00
WIN-2000T	UPS WINTECH 2000 VA TOUCH	UN	1,00	129 168.00		129 168.00
82C2	PORTATIL LENOVO 14POL CELERON /4GB/1TB	UN	1,00	377 630.50		377 630.50



Sub-Total	Incidência IVA	Taxa	Total IVA	Total Desc.	Total
666 508.70	666 508.70	14%	93 311.22	0.00	666 508.70
		%		IVA CATIVO:	0.00
			TOTAL DO IVA:		93 311.22
			TOTAL DO DOCUMENTO + IVA:		759 819.92

Este documento não serve de factura

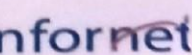
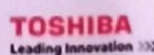
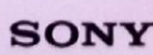
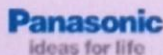
Extensão: Setecentos e Cinquenta e Nove Mil Oitocentos e Dezanove KWANZAS e Noventa Dois CENTIMOS

BIR - Akz: 001463817-10-001 - IBAN: AO06 0067 0000 0146 3817 1018 9
BAI - Akz: 217555412-10-001 - IBAN: AO06 0040 0000 1755 5412 1016 0
BFA - Akz: 38934302-30-001 - IBAN: AO06 0006 0000 3893 4302 3012 4
BIC - Akz: 042789478-10-001 - IBAN: AO06 0051 0000 4278 9478 1013 7
SOL - Akz: 83711323-10-001 - IBAN: AO06 0044 0000 8371 1323 1019 3
ATL - Akz: 29295864-10-001 - IBAN: AO06 0055 0000 2929 5864 1018 3

Hora: 09:49

TLTw-Processado por programa validado n.29/AGT/2019 - Pmr-Software
Licenciado a ZICAI GRUPO, LDA

Operador: MADALENA ANTÓNIO







INSTITUTO
SUPERIOR
DE ANGOLA

A
DIRECÇÃO DO INSTITUTO SUPERIOR DE ANGOLA

LUANDA

CREDENCIAL

Ref.: 121/DAC/ISA/024

Melhores Cumprimento,

Excelência,

O Instituto Superior de Angola – ISA foi aprovado pelo Decreto Presidencial nº 168/12 de 24 de Julho, com sede em Luanda, bairro da Pedreira, município de Cacuaco, apostado na formação de quadros qualificados na investigação científica para dar resposta as necessidades locais e nacionais de acordo com as orientações emanadas pelo Executivo Central.

Havendo necessidade de credenciar e enviar aos diferentes locais para a pesquisa da temática do Trabalho de fim de Curso para obtenção do grau de licenciatura em **Informática** o (a) estudante:

NOME: António Mavacala Kulazi

TEMA: PROPOSTA DE IMPLEMENTAÇÃO DE UMA REDE PRIVADA VIRTUAL NO INSTITUTO SUPERIOR DE ANGOLA (ISA), NO I SEMESTRE DO ANO 2024.

Vimos por intermédio desta, solicitar os vossos ofícios, no sentido de autorizar o estudante a realizar a pesquisa/recolha de dados na instituição que vossa excelência mui dignamente dirige.

O INSTITUTO SUPERIOR DE ANGOLA, em Luanda aos 7 de Outubro de 2024.

O vice - Presidente Para os Assuntos Científicos

Prof. Dr. Moisés Kafala Neto

À
Presidente do Instituto Superior de Angola
Luanda

Assunto: Solicitação de pesquisa/recolha de dados

António Maracala Kulazi, filho de Eduardo Kulazi Tsumo e de Miambi Regina, nascido aos 06/01/1991, portador de BI nº 00366572LA025, residente no Bairro Ndale Nkulula Casa nº Município de Ingombata, Província de Luanda.

Contacto telefónico 924 2415 65.

Estudante do 4º ano do curso de Licenciatura em Engenharia Informática, Salº nº 200289, Período Manhã, do ano académico 2023/2024.

Venho muito respeitosamente solicitar a Sua Excelência que se digne mandar passar uma pesquisa de recolha de dados de tema: Proposta de implementação de uma rede privada virtual no Instituto Superior de Angola (ISA), no 1º Semestre do ano 2024.

Pelo que,

Espera deferimento

Luanda aos 01 de 11 de 2024

O Requerente

António Maracala Kulazi

ENTRADA
15/11/2024

Felícia Mario

Recebido
em 15/11/2024
pelo
Serviço de
Informática
Nº 11/2024

