Instituto Superior De Ciências De Educação da Huíla

ISCED-HUÍLA

Reestruturação da Rede de Computadores da Delegação Provincial do Ministério do Interior na Huíla

Autores

Dinilson Filipe Tiago Tchiwana

José Marcos Luciano

LUBANGO

2024

Instituto Superior de Ciências de Educação da Huíla

ISCED-HUÍLA

Reestruturação da Rede de Computadores da Delegação Provincial do Ministério do Interior na Huíla

Trabalho apresentado para a obtenção do Grau de Licenciado no curso de Informática Educativa

Autores:

Dinilson Filipe Tiago Tchiwana

José Marcos Luciano

Tutor: Msc. Tomás Francisco Lucas Selombo

LUBANGO

2024

Dedicatórias

A minha querida Mãe Judith Híngua Tiago, ao querido Padrasto Fernando António Gunza (em memória) e aos meus estimados irmãos.

Dinilson Filipe Tiago Tchiwana

A todos meus familiares, amigos, colegas e professores que contribuíram para a materialização dessa etapa da minha formação.

José Marcos Luciano

Agradecimentos

A Deus pai todo poderoso e nosso criador, pelos seus dons despertados em nós por meio de Jesus Cristo, em particular o dom da Vida, Saúde, Sabedoria e Ciência.

Ao professor **Tomás Lucas Selombo**, pelos conhecimentos transmitidos no decorrer do curso, mostrou ser um excelente profissional, paciente e dinâmico na transmição de conhecimentos, além de contribuir significativamente com a orientação do presente trabalho de fim de curso, presenteou-nos com seu apoio e voto de confiança, conselhos sábios e motivadores, investidos em nós, na certeza de que completaremos com sucesso a presente fase. Igualmente certificou ser um grande ser humano com virtudes que engrandecem uma convivência saudável dentro de uma comunidade científica e que inspira qualquer estudante a caminhar com segurança numa jornada de pesquisa e descobertas.

Agradecemos aos nossos familiares em geral por não terem poupado esforços para o sucesso desta caminhada académica, em particular aos nossos pais, irmãos, tios, primos, sobrinhos e amigos que na sua certeza contribuíram sem medir consequências, na esperança de verem esta fase académica concluída e que hoje está sendo efectivado.

As nossas amadas esposas, pelo amor, carinho e paciência que têm dedicado a nós e por estarem connosco nos bons e maus momentos.

Ao corpo docente, direcção e coordenação do curso de Informática Educativa do ISCED-Huíla, as nossos colegas e a todos que directa ou indirectamente contribuíram para que este sonho se tornasse realidade.

A Delegação Provincial do Ministério do Interior na Huíla, por anuir a progressão desta investigação, ao Director e ao pessoal da área TI pela disponibilidade e contribuição imensurável.

INSTITUTO SUPERIOR DE CIÊNCIAS DE EDUCAÇÃO

ISCED-HUÍLA

DECLARAÇÃO DE AUTORIA DO TRABALHO DE LICENCIATURA

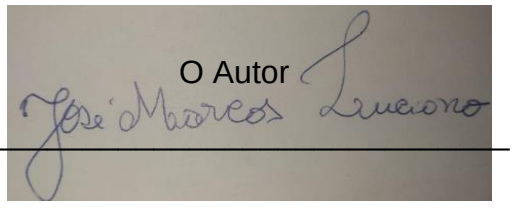
Temos consciência que a cópia ou o plágio, além de poderem gerar responsabilidade civil, criminal e disciplinar, bem como reprovação ou a retirada do grau, constituem uma grave violação da ética académica.

Nesta base, nós, DINILSON FILIPE TIAGO TCHIWANA E JOSÉ MARCOS LUCIANO, estudantes finalistas do Instituto Superior de Ciências de Educação da Huíla (ISCED-Huíla) do curso de Informática Educativa do Departamento de Ciências Exatas e Naturais, declaramos, por nossa honra, ter elaborado este trabalho, só e somente com o auxílio da bibliografia que tivemos acesso e dos conhecimentos adquiridos durante a nossa carreira estudantil e profissional.

Lubango, aos x de Março de 2024

O Autor

O Autor



Resumo

A investigação em causa foi realizada na Delegação Provincial do Ministério do Interior na Huíla, que é uma insituição vocacionada em congregar e normalizar as actividades ligadas aos órgãos de segurança pública, protecção civil e naõ só. A instituição em destaque, actualmente, conta com uma população de 127 funcionários. Nesta mesma instituição, durante a edificação de suas instalações, mapeou-se e implementou-se uma infra-estrutura de rede de computadores, porém sem dar resposta aos serviços que permitem dinamizar suas actividades, em caso particular a comunicação entre utilizadores, pelo que necessita de adequar-se as exigências de comunicação, implementando serviços que garantem com automação e segurança o tráfego de dados. Assim sendo, levantou-se a seguinte questão de investigação: Como melhorar os processos de comunicação e optimizar os recursos informáticos na rede de computadores do edifício da Delegação Provincial do MININT/HLA? Do qual o objectivo geral consubstancia-se em conceber um projecto de reestruturação da rede de computadores do edifício da Delegação Provincial do MININT/HLA. A amostra foi de 43 funcionários, dos quais 35 são utilizadores da rede de computadores e 8 são responsáveis pela manutenção da mesma. A presente investigação quanto aos objectivos é do tipo exploratória e quanto a metodologia de projecto optou-se pela top-down.

Palavras-chave: Restruturação, Rede de Computadores, Segurança da Informação.

Abstract

The investigation in question was carried out at the Provincial Delegation of the Ministry of the Interior in Huila, which is an institution dedicated to bringing together and normalizing activities linked to the bodies of the National Police and Civil Protection and Fire Services, both in the province of Huila. The highlighted institution currently has a population of 127 employees. This same institution, during the construction of its facilities, mapped and implemented a computer network structure, but without the configuration of services that allow it to streamline its activities, in particular communication between users, so it needs to adapt to the requirements communication, implementing services that guarantee automation and security of data traffic. However, the following research question was raised: How to improve communication processes and optimize IT resources in the computer network of the MININT/HLA Provincial Delegation building? The general objective of which is to design a project to restructure the computer network of the MININT/HLA Provincial Delegation building. The sample consisted of 43 employees, of which 35 are users of the computer network and 8 are responsible for maintaining it. The present investigation in terms of objectives is exploratory and in terms of project methodology, top-down was chosen.

Keywords: Restructuring, Computer Network, Information Security.

Índice

Índice de Figuras

Índice de gráficos

Índice de Tabelas

Lista de Abreviaturas

PNA	Polícia Nacional de Angola
SIC	Serviço de Investigação Criminal
SP	Serviços Penitenciários
SPCB	Serviços de Protecção Civil e Bombeiros
SISP	Sistema Integrado de Segurança Pública
CISP	Centro Integrado de Segurança Pública
MININT/HLA	Ministério do Interior na Huíla
ARPANET	Advanced Research Projects Agency Network
MILnet	Military Network
NSFnet	National Science Foundation Network
ISP	Internet Service Providers
LAN	Local Area Network
TCP	Transmission Control Protocol
UDP	User Datagrama Protocol
IP	Internet Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
RARP	Reverse Address Resolution Protocol
IGRP	Interior Gateway Routing Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
OSPF	Open Shortest Path First
Telnet	Teletype Network
FTP	File Transfer Protocol

SMTP	Simple Mail Transfer Protocol
HTTP	Hypertext Transfer Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
SNMP	Simple Network Management Protocol
P2P	Point to Point Protocol
IPC	Inter-Process Communication
FDDI	Fiber Distributed Data Interface
ATM	Asynchronous Transfer Mode
SCSI	Small Computer System Interface
PSI	Política de Segurança da Informação
VoIP	Voice over Internet Protocol
QoS	Quality of Service
IDS	Intrusion Detetion System
IPS	Intrusion Prevesion System

INTRODUÇÃO

INTRODUÇÃO

Durante a evolução das sociedades, o homem necessitou comunicar eficazmente, impulsionando métodos e técnicas para suprir essa necessidade. Esse processo persiste até hoje, com o surgimento e desenvolvimento de tecnologias dedicadas a facilitar a comunicação em tempo recorde. Atualmente, as tecnologias de informação e comunicação estão presentes em diversos dispositivos, sendo montadas em residências e empresas para permitir troca de informações com precisão através de um simples clique.

Os computadores utilizados pelo homem são aprimorados diariamente. Segundo Forouzan (2010), o desenvolvimento do computador pessoal trouxe significativas mudanças nas empresas, indústrias, ciências e educação, quando conectados, formam uma rede, geralmente chamada de rede de computadores, facilitando as trocas de dados essenciais para a comunicação entre entidades.

Podemos afirmar que computadores formam uma rede quando dois ou mais computaores estão conectados entre si, permitindo que os dados de um computador possam ser enviados para os demais (Vasconcelos & Vasconcelos, 2007).

As redes de computadores são ferramentas essenciais para o trabalho administrativo, permitindo a partilha de informações em tempo real. Isso torna os processos mais eficientes e ágeis, sendo a troca de dados um diferencial significativo para corporações, instituições e indivíduos, buscando obter informações com qualidade em tempo reduzido (Camolacande & Monteiro, 2020).

A Delegação Provincial do MININT/HLA mapeou e instalou no seu edifício uma estrutura de rede, mas sem configuração de serviços para dinamizar as atividades administrativas e operativas, incluindo a comunicação entre utilizadores. É crucial implementar serviços que garantam automação e segurança no tráfego de dados.

Baseando-nos nas ideias dos autores acima mencionados, verificou-se que o edifício da Delegação Provincial do MININT/HLA necessita de uma reestruturação na rede de computadores para usufruir dos benefícios de uma configuração eficiente, que priorize baixos custos e eficiência na troca de dados entre emissor e receptor. Focamo-nos, assim, em projetar a reestruturação da rede de

computadores para corrigir problemas de comunicação existentes e aprimorar os insatisfatórios.

Antecedentes do Tema

O contributo de outros pesquisadores em redes de computadores deve ser tido em conta, de modos a não repetir os seus erros e tirar proveito dos seus feitos, assim sendo, dos varíos trabalhos relaccionados ao nosso, entendemos destacar os seguintes:

Artur Epope Camolacande e Mila Castro Monteiro em 2020, no seu trabalho de investigação subordinado ao tema “Projecto de reestruturação da rede de computadores da Escola de Magistério Primário nº137 do Nambambi – Lubango”, concluiram que:

Depois de se ter realizado um diagnóstico, foi possível detectar a degradação e infuncionalidade da rede de computadores da Escola de Magistério Primário nº137 do Nambambi – Lubango, o que originava constrangimentos de comunicação interna, os funcionários de um gabinete para se comunicarem com os de outro gabinete fazem recurso à métodos arcaicos tais como deslocar estafetas para outros gabinetes para informar sobre um assunto ou mesmo fazer uso de um equipamento, tornando desta forma o trabalho administrativo mais letárgico.

Com isso, aprendemos que antes de se propor uma reestruturação é muito importante fazer um diagnóstico de modos a apurar melhor a situação problemática, assim sendo, efectuamos uma visita e aplicamos inquéritos de modos a diagnosticar os problemas da rede de computadores da Delegação Provincial do Ministério do Interior na Huíla.

Avelino Cangongo Vasco Caliata em 2020, no seu trabalho de licenciatura, com o tema “Proposta de reestruturação da infra-estrutura tecnológica dos laboratórios de informática do ISCED-Huila”, conclui o seguinte:

A reestruturação das salas com equipamentos informáticos está sugeita a um investimento dispendioso, porém indispensável para proporcionar melhores condições de trabalho.

Contextualizando a conclusão supra para o nosso trabalho, para que seja feita a reestruturação da rede de computadores do MININT/HLA será necessário que se faça um investimento, e antes disso um inventário dos equipamentos por adquirir, assim sendo, no decorrer do nosso trabalho, procuramos ilustrar os equipamentos necessários para suportar a infra-estrutura proposta.

Justificação da Investigação

O Ministério do Interior em Angola, no leque de suas competências constam a garantia da segurança pública a todos cidadãos angolanos e estrangeiros em toda sua extenção territorial, para tal, os mecanismos utilizados que realçam o modo de actuação, nos dias de hoje constituiem um dos interesses do governo angolano em evidar esforços em vários sectores, com vista a aquisição de meios de comunicação com tecnologia de ponta e que valorizam a segurança da informação.

Durante o processo de construção do edifício da Delegação Provincial do MININT/HLA, implementou-se uma estrutura de rede de computadores, mas não atende às normas físicas e lógicas, bem como tem a carência de técnicos. A comunicação interna enfrenta problemas, alguns computadores não estão conectados/configurados. Para a comunicação entre departamentos, métodos rudimentares são usados, resultando em baixa produtividade e risco de vazamento de informações confidenciais. A infraestrutura de rede do edifício apresenta problemas como: Estrutura lógica e física da rede inadequadas; Falta de comunicação entre alguns computadores através da rede corporativa; Necessidade de configuração de alguns serviços na rede e segurança na rede lógica e física débeis.

Em sentido abrangente, para o funcionamento adequado de uma infraestrutura de rede, não precisa necessáriamente ser feita a partilha de recursos entre dispositivos. O objectivo é deixar todos os programas, equipamentos e especialmente, dados acessíveis para todos utilizadores da rede, independentemente da distância física entre o recurso e o utilizador (Tanenbaum & Wetherall, 2011).

No Ministério do Interior em Angola, o exemplo mais claro de uma infraestrura de rede com registo de bom funcionamento, é o sistema integrado de segurança

pública (SISP), que segundo o Grupo Técnico para Implementação do Sistema Integrado de Segurança Pública [GTISISP] (2022), é suportado por centros integrados de segurança pública (CISP), que auxilia os órgãos prestadores de serviços de emergência, na identificação e resolução rápida de situações de segurança e ordem pública, que impactam de forma directa ou indirecta na segurança interna e externa de Angola.

Outrossim os CISP, considerados como importantes estruturas de rede de computadores, impulsionam o Ministério do Interior de Angola a demonstrar um grande interesse em exercer suas competências com o auxílio das tecnologias, pois estas podem facilitar o exercício de várias actividades no âmbito da defesa e segurança pública, desta feita, outras estruturas funcionais do mesmo Ministério necessitam de ser globalizadas e adaptadas naquilo que são os padrões técnicos de modos a se tirar maior partido das vantagens dessas tecnologias.

DESENHO TEÓRICO

Questão de Investigação

Considerando a problemática apresentada, formulou-se a seguinte questão de investigação:

- Como melhorar os processos de comunicação e optimizar os recursos informáticos na rede de computadores do edifício da Delegação Provincial do MININT/HLA?

Objectivos de Investigação

Objectivo geral:

- Conceber um projecto de reestruturação da rede de computadores do edifício da Delegação Provincial do MININT/HLA.

Objectivos específicos:

- Fundamentar teoricamente a importância das redes de computadores e da segurança em redes;

- Diagnosticar a situação actual da Rede de Computadores do edifício da Delegação do MININT/HLA;
- Modelar o projecto da rede de computadores;
- Simular o projecto no Cisco Packet Tracer.

DESENHO METODOLÓGICO

Metodologia Empregue

A planificação de um estudo subordina-se não só ao contexto da investigação, mas também a natureza em que o mesmo está inserido, bem como ao nível de concepção do autor. Entretanto, podem existir muitos tipos de pesquisas (Köche, 2011).

Diante deste contexto, segundo Heerdt e Vilson (2022), a metodologia científica possui uma grande função: sugerir métodos, técnicas e instruções que possibilitem recolher, pesquisar, organizar, classificar, registrar, interpretar etc., informações, favorecendo a maior semelhança possível com a realidade.

A pesquisa exploratória é fundamental para obter uma compreensão mais específica sobre o problema em estudo no nosso trabalho e identificar as principais questões que precisam ser abordadas durante a reestruturação da rede de computadores, sustentando-se na metodologia de redes top-down, sendo esta uma forma de análise que desmitifica o funcionamento de uma organização e sua relação com os seus subsistemas (4infra, 2022).

A metodologia em causa estabelece que a arquitetura lógica e física apenas são concebidas após um processo detalhado de recolha de informações que enumera os requisitos comerciais e técnicos do cliente, bem como os objectivos que devem ser alcançados com sua implementação. O processo é dinámico, porque à medida que novas informações são identificadas, os diagramas lógico e físico são adaptados para atender às novas exigências (DEVMEDIA, 2019)

Conforme DEVMEDIA (2019), a metodologia de rede top-down, obedece as seguintes fases:

1) **Análise de Requisitos**: Análise dos objetivos comerciais e técnicos do projecto; Identificação de contradições e dificuldades; Caracterização do ambiente legado e dos principais fluxos de dados.
2) **Diagrama Lógico da Rede**: Definição de topologias de rede; Padronização de nomes e hierarquia de endereços IP; Detalhamento dos protocolos de camadas de enlace e rede; Estratégias adoptadas para segurança e gestão.
3) **Diagrama Físico da Rede**: Selecção efetiva de dispositivos e tecnologias para redes locais e distribuídas geograficamente.
4) **Testes, Optimização e Documentação do Projecto**: Planeamento de testes de validação e critérios de aceitação; Descrição de tecnologias para optimização, como redes IP multicast e qualidade de serviço; Abordagem dos principais itens da documentação formal do projecto.

População e Amostra

Segundo Silva (2022), toda pesquisa deve atender a um público-alvo, composto por um conjunto de pessoas com objectivos em comum, de acordo com o princípio da pesquisa. Esse conjunto é denominado população e representa indivíduos com características próprias. No estudo em questão, a população é constituída por 127 funcionários.

Silva (2022), diz ainda que amostra diz respeito a um subconjunto da população. Pois levaria mais tempo para concluir o trabalho ou até mesmo seria financeiramente dispendioso, dessa forma, o número de entrevistados corresponde a uma quantidade mais reduzida de elementos da população.

Técnica de Amostragem

Utilizou-se a técnica de amostragem não probabilística intencional. Para esta técnica o processo de seleção de amostra é feita intencionalmente de acordo com critérios e julgamentos estabelecidos pelos pesquisadores (Paula, 2019).

Para a selecção da amostragem selecionou-se 43 funcionários conforme tabela a baixo:

Tabela 1 - Seleção da amostragem

Selecção da amostragem

N/O	Amostragem	Critério de selecção	Nº. Selecionados
01	Utilizadores da rede	Funcionários que no desempenho de suas funções, com frequência fazem o uso do único serviço disponível na rede (internet), bem como aqueles que têm uma certa experiência em utilizar os meios de comunicação existentes.	35
02	Técnicos de manutenção da rede	Dado o número reduzido dos técnicos de mantunteção da rede, não baseou-se a nenhum critério, de modos a incluir todos na amostra.	8
Total			**43**

Métodos e Técnicas de Investigação

Métodos e técnicas diferenciam-se tanto no seu conceito como na sua utilização. Para Silva (2022), O método de pesquisa compreende os procedimentos para recolher, analisar e interpretar informação. Já as técnicas de pesquisa são os instrumentos específicos, como entrevistas, questionários, observação participante e análise de documentos. Portanto a forma de aplicação do método é a técnica (FastFormat, 2018).

Métodos e técnicas

Para se cumprir com os objectivos traçados na presente pesquisa houve a necessidade de utilizar os seguintes:

- **Pesquisa bibliográfica**: Viabilizou a identificação de informações reais existentes em fontes literárias consultadas de modos a responder a questão de investigação.
- **Inquérito por questionário**: É um documento contendo uma lista de perguntas fechadas, com alternativas pré-definidas, ou abertas. Suas vantagens incluem alcance de mais pessoas em pouco tempo. Para maior eficácia, frequentemente utiliza-se ferramentas on-line, com a possibilidade de gerar dados estatísticos apresentados em gráficos ou tabelas (Raymundo, 2020);
- **Estátistica descritiva** - Compreende a organização, o resumo e, em geral, a simplificação de informações que podem ser muito complexas. É uma das

técnicas utilizadas na análise exploratória de dados com o objetivo de ter um entendimento inicial dos dados. Essa técnica resume de forma quantitativa as principais características de um conjunto de dados (Oliveira, 2024).

Estrutura do Trabalho

O presente trabalho está estruturado da seguinte forma:

- Introdução – Foram apresentados aspectos relacionados ao desenho metodológico e teórico da investigação.
- Capítulo I - Neste ponto, foi revista a literatura sobre redes de computadores, segurança da informação e práticas recomendadas para gestão de infra-estrututra de redes;
- Capítulo II – Foi produzido neste capítulo, o projecto de Reestruturação da Rede de Computadores da Delegação Provincial do MININT-HLA;
- Conclusões/Sugestões – Foram apresentadas as principais conclusões a que os autores chegaram, bem como, sugestões para investigações futuras.

CAPÍTULO I - FUNDAMENTAÇÃO TEÓRICA

1. Capítulo I - Fundamentação Teórica

1.1. Introdução

Neste capítulo, abordou-se sobre a importância dos principais conceitos de redes de computadores, bem como a utilização destes para a governação eletrónica, destacando o funcionamento convergente de serviços em uma única infra-estrutura de rede. Igualmente constextualizou-se sobre a segurança em redes de computadores e a metodologia de projetos de rede. Fez-se um destaque desses aspectos para instituições de defesa e segurança, cujo papel é manter a ordem, segurança e soberania do estado.

No contexto de Angola, algumas instituições de defesa e segurança estão associadas ao ministério do interior, na qual a nível da Província da Huíla é representado pela Delegação Provincial do MININT/HLA, seu objectivo tange em coordenar actividades de diversas instituições relacionadas à defesa e segurança. A Delegação Provincial do MININT/HLA valoriza cada vez mais a qualidade e segurança na circulação da informação, reconhecendo sua importância diária nessas operações.

A busca pelas melhores condições de trabalho, constitui um grande desafios para as instituições, assim sendo, a comunicação com os seus utentes e não só, não fica de fora. Uma melhoria na rede de computadores de uma instituição certamente influenciará positivamente para a melhoria da comunicação, seja interna ou com o meio exterior (Amaral, 2012).

Amaral (2010) reforça a ideia afirmando que ao utilizar tecnologias, uma série de factores precisam ser levados em conta para garantir eficiência na comunicação. Podemos citar alguns deles: custo, taxas de transmissão, facilidade de acesso, padronização, segurança e portabilidade. As redes de computadores existem para atender às demandas das aplicações comerciais, das aplicações domésticas e dos utilizadores móveis.

A Delegação Provincial do MININT/HLA deu um outro rumo na aplicabilidade de suas competências, com a instalação de uma infra-estrutura de rede de computadores no seu edifício, com objectivo de melhorar a comunicação interna, mas no entanto, não dispõem de todos benefícios desta mesma rede.

A partir deste preceito, Conceição (2006) menciona que a flexibilidade de se comunicar com membros de outros departamentos ou secções da instituição sem ter de movimentar-se fisicamente é algo do qual não se pode abrir mão. A troca permanente de recursos e informações, constitui algo de imprescindível numa sociedade moderna.

A gestão da segurança da informação é uma actividade indispensável para proteger a informação de ameaças à sua integridade, bem como é responsável por assegurar o ambiente informacional em qualquer organização (Neto & Araújo, 2019).

Lyra (2008) citado por Neto e Araújo (2019) aborda que a segurança da informação é obtida com a implementação de um conjunto de políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles, além de implementados, precisam ser estabelecidos, monitorados, analisados criticamente e melhorados onde for necessário, para garantir que os objectivos do negócio e da segurança da organização sejam atendidos.

Associando as abordagens de Amaral, Conceição, Neto e Araújo tal como de Lyra, torna-se indispensável a utilização de um sistema de computação, em especial da rede de computadores em instituições ou organizações para dinamizar o fluxo de informação entre os funcionários, bem como a gestão da Segurança da informação.

1.2. Importância da utilização das redes de computadores

A grande necessidade de implementação das redes de computadores dentro das instituições se dá à partir da evolução que a tecnologia vem apresentando, podendo exigir um padrão tecnológico que possa dar estabilidade em todos os setores, os mesmos dependem dessa evolução para render mais e atingir os resultados pedidos para estar sempre um passo a frente da concorrência (Silva, 2022).

Sendo a Delegação Provincial do MININT/HLA a instituição em estudo, com o objectivo desta tirar proveito dos benefícios de uma rede de computadores bem estruturada, prevê-se que esta importante instituição contribua para o chamado da governação electrónica ou digital, visto que é parte integrante dos planos de governação do estado angolano.

A governação eletrónica subentende o uso de tecnológias para a gestão da comunicação e da informação governamental, bem como a participação do cidadão,

por meio de interações online, nos processos de tomada de decisão. A estratégia de governação eletrónica está organizada em três eixos: acesso à informação, prestação de serviços e participação social (TOTVS, 2023).

Ainda conforme TOTVS (2023) os objetivos da governação eletrónica consistem em: Ampliar e inovar a prestação de serviços digitais; Estimular a colaboração no ciclo de políticas públicas; Otimizar a interação direta entre sociedade e governos; Impulsionar o uso e a disponibilidade de dados abertos; Partilhar e integrar sistemas, processos, dados, serviços e infraestrutura; Melhorar a gestão e a governação por meio do uso de soluções tecnológicas; Ampliar e incentivar a participação social para criar e melhorar os serviços públicos; Garantir o sigílo dos dados do cidadão e a segurança da informação e comunicação do Estado; Facilitar o uso e o acesso aos serviços digitais, bem como garantir sua universalização; Ampliar o uso de tecnologias da informação e comunicação para promoção da transparência e publicitar a aplicação dos recursos públicos.

Por um lado, dadas as competências da Delegação Provincial do MININT/HLA conforme o ponto anterior, uma infra-estrutura de rede de computadores impactaria no seu modo de funcionamento, tornando-o mais preciso na execução de suas tarefas quotidianas, bem como consolida a sua integração na era digital, em especial na governação digital.

Para Coutinho (2023), as redes de computadores representam sistemas imprescindíveis para o compartilhamento de informações e recursos entre os utilizadores, porém importa mencionar algumas vantagens e desvantagens que se advêm:

Vantagens: Armazenamento de dados em um único servidor de arquivos; Conexão de diversas pessoas; Resolução de problemas de forma rápida e eficiente; Confiabilidade no funcionamento, acesso e da transmissão de dados; Flexibilidade; Segurança e a proteção das informações dos usuários; Aumento da capacidade de armazenamento.

Desvantagens: **Falta de robustez**: caso houver uma falha em algum dispositivo de ponte ou em um servidor de link, toda a rede pode ficar estagnada; **Carência de independência**: os utilizadores dependem de diversas aplicações para a execução

de suas necessidades; **Vírus e malware**: os dispositivos conectados em rede estão sujeitos a vírus e a malware; **Custo da rede**: a instalação e execução das redes demandam de investimentos, dependendo das necessidades dos utilizadores.

1.3. Arquitectura de redes e Protocolos

Em redes de computadores, protocolos são essenciais como a linguagem universal de comunicação. Protocolos contribuem para a organização, segurança e escalabilidade durante o fluxo de informações numa arquitectura de redes. Lima (2018) nos diz que: “uma arquitectura de redes é um modelo abstracto que permite descrever a organização e o comportamento dos sistemas que constituem a rede”.

Existem as seguintes arquitecturas que definem como os diferentes sistemas se comunicam através de redes de computadores: Modelo OSI e o TCP/IP.

De acordo com os ideiais de White (2012), “o conjunto de protocolos **TCP/IP** é um modelo de trabalho (actualmente utilizado na internet), enquanto o modelo **OSI** (originalmente desenvolvido para ser um modelo de trabalho) é tido apenas como modelo teórico”.

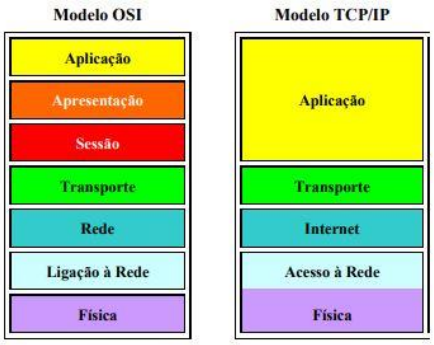


Figura 1 - Comparação entre o modelo TCP/IP e o modelo OSI

Fonte: Lima (2018)

É notória a importância dos modelos de rede em camadas para a partilha de dados, com destaque para o modelo TCP/IP escolhido na pesquisa devido à sua simplicidade. A figura 1 mostra o TCP/IP com 5 camadas, enfatizando a dependência entre as duas primeiras. Em análise ascendente, são consideradas quatro camadas com protocolos específicos no modelo TCP/IP:

1) **Acesso à rede**: Ethernet, FastEthernet, GigabitEthernet e Token Ring
2) **Internet:** IP, ICMP ARP, RARP, IGRPP, EIGRPP e OSPF

3) **Transporte:** TCP e UDP
4) **Aplicação:** Telnet, FTP, SMTP, HTTP, DHCP, DNS e SNMP

Uma rede devidamente projetada não apenas prevê a comunicação entre sistemas, mas também define o mapeamento da rede e a função de cada equipamento. Esses requisitos são garantidos pelo modelo hierárquico da Cisco. No entanto, destacaremos a importância tanto do modelo TCP/IP quanto do modelo Cisco hierárquico na rede de computadores da instituição em estudo.

1.3.1. Modelo TCP/IP

Neto, Vargas, Chapetta e Ferreira (2019), apresentam que o conjunto de protocolos TCP/IP foi projetado especialmente para ser o protocolo utilizado na Internet. Sua característica principal é o suporte directo à comunicação entre redes de diversos tipos. Neste caso, a arquitectura TCP/IP é independente da infra-estrutura de rede física ou lógica empregue.

O protocolo TCP, também destacado por Neto et al. (2019), desempenha funções como controle de fluxo, controle de erro, sequenciação e multiplexação para garantir comunicações mais confiáveis entre origem e destino, funções estas, bastante úteis para o presente estudo.

Antes da troca de dados, o protocolo TCP estabelece uma conexão por meio do "three-way handshake" (aperto de mão em três vias), envolvendo a troca de pacotes. (França, 2010).

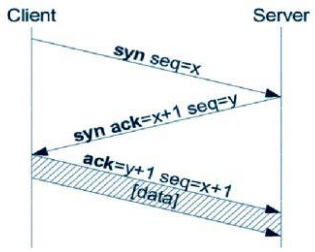


Figura 2 - Three-way Handshake

Fonte: França (2010)

Os protocolos TCP/IP são versáteis, podendo ser empregues em diversas estruturas de rede, desde ligações ponto-a-ponto até redes complexas como Ethernet, Token-Ring, entre outras (Neto et al., 2019).

Ao reestruturar a rede de computadores, é essencial considerar políticas de segurança, definir funções de comunicação e estabelecer normas de comportamento. A relação entre softwares e seus componentes deve ser cuidadosamente organizada, funcionalidades devem ser ordenadas em elementos para otimizar a eficácia da rede.

1.2.1. Modelo Cisco hierárquico

Conforme Diógenes (2002) citado por Camolacande e Moteiro (2020), numa rede de computadores os equipamentos são organizados de forma hierárquica, baseados no modelo CISCO, o qual divide uma rede em três camadas: Core (núcleo), Distribuição e Acesso.

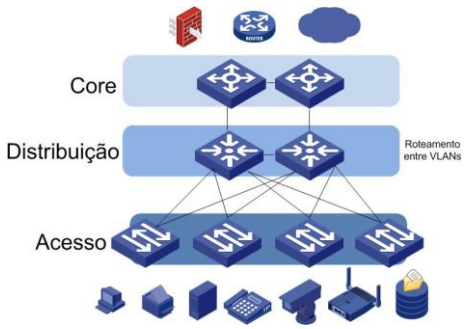


Figura 3 - Exemplo de rede hierárquica em três camadas

Fonte: Dias (2012)

De um modo geral, as redes de computadores com a disposição de equipamentos baseadas no modelo cisco hierárquico oferecem muitos benefícios, tais como melhor desempenho, fiabilidade e escalabilidade, melhor segurança, gestão e concepção mais fáceis e melhor relação custo-benefício (Transparency, 2022).

Com base nos princípios do modelo Cisco hierárquico, organizaram-se os diagramas lógico e físico da rede para uma melhor disposição dos equipamentos, desde os armários até aos utilizadores. Isso permite mapear redes convergentes semelhantes a que propomos com este estudo e disponibilizar vários serviços. O objetivo foi projetar uma rede na Delegação Provincial do MININT/HLA dividida em camadas, proporcionando alto desempenho e facilitando a gestão.

1.4. Serviços de Rede

Tecnologia (2012) citado por António (2016) retrata serviços de rede como sendo os serviços disponíveis em uma rede de computadores para os seus utilizadores. Tais serviços podem ser oferecidos por protocolos.

Segundo Camolacande e Monteiro (2020), existem vários serviços de rede, inclusive, alguns deles estão a cair em desuso, sendo em seguida substituídos por outros, principalmente por aqueles que funcionam na web. Os autores ainda descrevem como principais serviços de rede os seguintes: DHCP, Correio electrónico, Serviços de arquivos, Serviços de Impressão e de internet.

Em concordância com os autores citados, enquadramos como sendo indispensável no rol de serviços da infra-estrutura de rede de computadores o VoIP. Luciano e Nascimento (2021), definem VoIP como sendo a tecnologia usada para fazer chamadas dentro de uma rede de computadores. A voz humana, como qualquer outro arquivo, pode ser transmitida pela rede convertendo-se em um pacote de dados e enviando-o ao destinatário.

1.4.1. A importância das redes convergentes na integração de serviços

Conforme Júnior (2009) citado por Barral, Cardoso e De Souza (2018), as redes convergentes surgem como forma de substituição dos transportes tradicionais dos serviços, desenvolvida pela tecnologia IP. Possibilitando a configuração de diversos tipos de serviços em uma única estrutura de rede. Barral et al. (2018). Foi desta forma que o termo rede convergente se originou da flexibilidade da rede em si, em aceitar novas tarefas em uma infra-estrutura.

Segundo Alctel (2020), nas redes convergentes trafegam imagens, voz e dados em uma única infra-estrutura. Isso facilita a gestão da rede, garantindo melhor acompanhamento dos serviços, minimizando gastos de manutenção. Além disso, possibilita criar estratégias de gestão de recursos, conseguindo dessa forma melhoria nos serviços.

Da Costa, De Almeida, De Almeida e Perreira (2022), descrevem que a fim de se adaptar às grandes tendências de evolução da rede, flexibilidade, distribuição inteligente e abertura para serviços de terceiros, as redes convergentes são fundamentadas na visão de tráfego de informação totalmente IP.

Alctel (2020), enuncia que as principais vantagens das redes convergentes são: Maior agilidade na comunicação, redução de custos na manutenção de estrutura de TI, centralização das informações, maior segurança para a rede, escalabilidade de acordo com a demanda, conectividade multiplataformas, automação de rede e arquiteturas simples e repetíveis.

Para atender às necessidades de uma infraestrutura de rede da, o estudo propôs o mapeamento de uma infraestrutura de rede convergente com foco em serviços de qualidade (QoS - Quality of Service), visando a gestão eficiente e distribuição da largura de banda no segmento de cabeamento estruturado.

1.4.1.1. Qualidade de Serviços

QoS são ferramentas que monitoram e estabelecem as prioridades para o fluxo de dados dentro de uma infra-estrutura de rede. Elas fazem a alocação optimizada da banda de transmissão, garantem melhor desempenho de aplicações problemáticas e evitam a interferência de serviços na rede.Trata-se de uma tecnologia que controla o fluxo de dados na rede, monitora os dispositivos envolvidos na transmissão de dados e os caminhos utilizados, alterando caso necessário a largura de banda e a rota dos pacotes para evitar latência (Net, 2022).

Figura 4 - Comparação entre a utilização e a não utilização do DoS em um segmento com suporte de vários serviços

Fonte: Net (2022)

Ferramentas de QoS normalmente são exigidos em redes que transportam dados para sistemas com uso intensivo de recursos, como serviço de televisão por IP (IPTV), jogos online, streaming de mídia, videoconferência, vídeo sob demanda (VOD) e voz sobre IP (VoIP). Seus principais benefícios compõem a priorização ilimitada de aplicativos, melhor gestão de recursos, experiência aprimorada dos utilizadores, gestão de tráfego, prevenção contra perda de pacotes e redução de latência (Net, 2022).

Para a infra-estrutura de rede da Delegação Provincial do MININT/HLA, o QoS pode ser assegurada com Firewall, visto que dispõem de recursos de controle de largura

de banda e possibilidade de priorizar comunicações a partir da modelagem do fluxo de dados.

1.4.1.2. Ferramentas de gestão de rede

Uma ferramenta de monitoramento de redes é fundamental para que uma rede fique estável. A partir de uma rede devidamente monitorada, pode-se fazer recolha de informações e assim gerar relatórios que podem ser visualizados posteriormente e identificar possíveis instabilidades na sua operação (Da Silva, 2022).

Existem várias ferramentas que podem ser utilizadas para realizar o monitoramento de gestão da rede de computadores, algumas delas podemos encontrar predefinidas no equipamento Cisco ASA (Adaptative Security Appliance), na qual foi utilizado no simulador cisco packet tracer para demostrar a implementação do presente estudo.

1.5. Sistema de cabeamento estruturado

A definição da rede estruturada baseia-se na disposição de uma série de cabos, integrando os serviços de voz, dados e imagens que, facilmente podem ser redireccionados no sentido de prover um caminho de transmissão entre quaisquer pontos desta rede. Numa rede projectada seguindo este conceito, as necessidades de todos os utilizadores podem ser atendidas com facilidade e flexibilidade (Costa, 2010). Existem muitas soluções de cabeamento defendidas e implementadas por diversos autores, sendo que conforme Roffé (2022), as principais soluções de cabeamento compõem-se em:

1) **Cabeamento primário:** normalmente feitos pelos ISPs na via pública, são cabeamentos onde qualquer usuário se conecta para acesso aos serviços de rede;
2) **Cabeamento Secundário:** é todo aquele feito dentro de um edifício onde se configura a infra-estrutura de rede. Esta solução pode ser feita com cabos metálicos e ópticos, permite estender os cabos de forma horizontal.

De acordo com Roffé (2022), o cabeamento estruturado, possui alguns subsistemas, sendo os mais relevantes:

- **Entrada do edifício**: Interface entre uma IPS e a rede interna, pode ser subterrânea, enterrada e aérea;

- **Sala de Equipamentos**: onde são instalados principais equipamentos como roteadores, switches, pach panel, etc, servindo como ponto de partida para o primeiro nível de backbone;
- **Sala de telecomunicações**: tem a função de abrigar as conexões cruzadas horizontais bem como os equipamentos activos;
- **Área de Trabalho**: local onde funcionam as estações de trabalho, impressoras, etc;
- **Cabeamento backbone**: providencia a interligação de salas de telecomunicações, equipamentos, prédios em ambientes externos e entrada de edifício;

1.6. Importância da segurança de redes

A Segurança de redes, que também pode assumir outras designações como segurança da informação, é nada mais do que a protecção oferecida para um sistema de comunicação a fim de garantir a integridade e disponibilidade dos serviços e recursos (Stallings, 2015).

A segurança em redes de computadores é extremamente importante por várias razões. Em primeiro lugar, a maioria das informações importantes e confidenciais das empresas e organizações é armazenada em seus sistemas de rede. Isso inclui informações financeiras, estratégias de negócios, propriedade intelectual e dados pessoais de clientes e funcionários (Júnior, 2023).

ISO/IEC 17799:2005, citado por Aramuni e Maia (2020), define segurança da informação como sendo a protecção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar seus riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

As redes de computadores são alvos frequentes de ataques cibernéticos, como malware, phishing e invasões de hackers. Esses ataques podem causar danos significativos, como roubo de informações, interrupção de serviços e danos à reputação da empresa (Júnior, 2023).

Firewalls como o ASA, Mikrotik e o Pfsense, são tecnologias concebidas para implementar políticas de segurança em redes de computadores, de modos a garantir a protecção das mesmas contra ameaças, principalmente vindas da Internet, essas

tecnologias igualmente ajudam a estruturar melhor a rede, de modos que seja fácil a identificação de vulnerabilidades, detecção e correcção de avarias.

Stallings (2019) citado por Cassanga e Guelepete (2023), menciona que, a definição de segurança de redes está voltada para “três objectivos principais que são o coração da segurança de computadores”. Estes objectivos são normalmente chamados de tríade CIA (do acrónimo em inglês para confidentiality, integrity e availability). O mesmo autor entende que a autenticidade e responsabilização/legalidade devem ser igualmente considerados e enquadrados na tríade, completando assim os principais objectivos de segurança da informação.

Para garantir a segurança em redes de computadores, é necessário implementar medidas de segurança, como firewalls, antivírus, criptografia e autenticação de usuários. É importante também manter atualizados todos os softwares e sistemas operacionais utilizados na rede, além de realizar backups regularmente e treinar os funcionários em segurança cibernética para evitar ataques de engenharia social (Júnior, 2023).

1.6.1. Camadas da segurança da informação

Manhice (2022), entende que muitas organizações se preocupam com aspectos tecnológicos e se esquecem dos aspectos físicos e humanos, que são tão relevantes para uma boa segurança do negócio quanto os aspectos tecnológicos. O mesmo autor estabelece as seguintes camadas de segurança da informação:

- **Camada física**: é o ambiente onde está instalado fisicamente o hardware, podendo ser o escritório da empresa, a fábrica ou até a residência do usuário no caso de acesso remoto ou uso de computadores portáteis;
- **Camada lógica**: constituída pelos softwares, responsáveis pela funcionalidade do hardware e dos modelos de infra-estrutura de rede;
- **Camada humana**: é formada por todos os recursos humanos presentes na organização, sendo principalmente os que possuem acesso directo à camada física, seja para a manutenção ou uso.

Conforme Schneier (2001) citado por Aramuni e Maia (2020), das três camadas de segurança existentes: física, lógica e humana, a camada humana é a mais difícil de se avaliar os riscos e gerir a segurança, pois envolve o fator humano, com

características psicológicas, socioculturais e emocionais, que variam de forma individual. Aramuni e Maia (2020) enfatizam que para reduzir os riscos relacionados à erros humanos ou actos criminosos por parte dos utilizadores internos, é aconselhável que a organização estabeleça políticas de segurança da informação, controles e procedimentos enfocando a área de pessoal.

1.6.2. Tipos de segurança de redes

Com a identificação dos objectivos da segurança da informação e dos perigos apresentados em diferentes camadas, é importante implementar mecanismos que visam assegurar o bom funcionamento da infra-estrutura da rede, de modos que o usufruto de seus benefícios seja contínuo. Promover a segurança dentro de uma infra-estrutura de rede subentende a utilização de métodos que protejam a rede no âmbito físico, lógico e humano.

Dependente da camada e dos objectivos de segurança da informação, existem vários dispositivos, aplicativos, protocolos e métodos que constituem os tipos de segurança de redes. Para o presente estudo, abordaremos apenas aqueles que serão utilizados durante a simulação da rede no cisco packet tracer, reservando os demais para as sugestões, desta feita para a restruturação da rede da Delegação Provincial do MININT/HLA, inicialmente necessitará dos seguintes tipos de segurança de rede:

Firewall: é uma ferramenta que limita o acesso às portas e janelas do computador e assim impede a entrada de invasores. Dessa forma, somente utilizadores autorizados terão permissão para algumas funcionalidades da máquina (Fernandes, 2019).

Port Security: possibilita que um administrador de rede associe endereços MAC específicos à uma interface, o que pode impedir que um invasor conecte seu dispositivo. Dessa forma, pode-se restringir o acesso a uma interface para que apenas os dispositivos autorizados possam usá-la. Se um dispositivo não autorizado estiver conectado, pode-se decidir qual acção o switch tomará, por exemplo, descartando o tráfego e desligando a porta na qual o dispositivo desconhecido esteja conectado (CCNA, 2013).

NAT: O NAT (Network Address Translation) conserva endereços IP, permitindo que redes privadas se conectem à Internet usando endereços não registrados. Operando em um roteador, converte endereços privados antes de encaminhar pacotes para outra rede. Pode ser configurado para anunciar apenas um endereço, proporcionando segurança ao ocultar a presença da rede interna (Cisco, 2020).

Hotspot: tendo em conta o controlo de acesso a rede wi-fi, com a finalidade de aplicar um melhor controle de autenticação, assim como, um controle de banda larga, segundo Sabóia (2021) é uma ferramenta que oferece o serviço de internet, sejam eles pagos ou gratuítos e controle de autenticação, essa ferramenta geralmente é mais utilizada em locais públicos onde se tem muitos acessos.

Proxy: é um intermediário entre um computador e um servidor remoto, geralmente localizado na internet. Quando o utilizador solicita, por exemplo, uma página da web ou um arquivo, ele não se conectará directamente ao servidor. A solicitação será enviada ao proxy que, por sua vez, envia o pedido ao servidor onde a informação desejada está armazenada (Alleasy, 2018).

VPN: é uma solução de rede para proteger os acessos em uma comunicação da empresa. Funciona como um mecanismo que encapsula o caminho da comunicação para evitar interferências e acções de mal-intencionados (Algar Telecom, 2022).

Sistemas de detenção e prevenção de intrusão (IDS/IPS): servem para prevenir ciberataques, monitorizar o tráfego na rede, emitir alertas de actividades potencialmente suspeitas; estes “sinais” são geralmente enviados para ferramenta de gestão de rede (Paula, 2022).

1.6.3. Políticas de segurança da informação

Para Dantas (2011) citado por Manhice (2022) pode-se definir a política de segurança como um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades sobre o que deve ser feito para alcançar um padrão desejável de protecção para as informações. Ela é basicamente um manual de procedimentos que descreve como os recursos de TI da empresa devem ser protegidos e utilizados e é o pilar da eficácia da segurança da informação.

Para Dechechi et al. (2020), política de Segurança da Informação, também conhecida como PSI, é o documento que orienta e estabelece as directrizes

corporativas, ou seja, regras de boas práticas para protecção dos activos de uma empresa.

Conforme Manhice (2022), uma PSI deve representar os objectivos da organização, e é importante que todos os colaboradores participem no desenvolvimento da PSI a ser adoptada. Existem várias directrizes para a implementação de uma política de segurança da informação, e para tal, a norma ISO/IEC 27002:2005 fornece um conjunto de referência de controles genéricos de segurança da informação, incluindo directrizes de implementação, projectado para ser usado por organizações, afirma que este documento deve conter o seguinte:

a) Uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação;

b) Uma declaração do comprometimento da direcção, apoiando as metas e princípios da segurança da informação, alinhada com os objectivos e estratégias do negócio;

c) Uma estrutura para estabelecer os objectivos de controle, incluindo a estrutura de análise/avaliação e gestão de risco;

d) Breve explanação das políticas, princípios normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo:

1) Conformidade com a legislação e com requisitos regulamentares contratuais;
2) Requisitos de conscientização, treinamento e educação em segurança da informação;
3) Gestão da conformidade do negócio;
4) Consequências das violações na política de segurança da informação;

e) Definição das responsabilidades gerais na gestão da segurança da informação, incluindo o registo dos incidentes de segurança da informação;

f) Referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que os utilizadores devem seguir.

ISO (2022) determina que é essencial que uma organização determine seus requisitos de segurança da informação. Acrescenta que existem três fontes principais de requisitos de segurança da informação:

a) A avaliação de riscos para a organização, levando em consideração a estratégia e os objectivos globais do negócio da organização;
b) Os requisitos legais, estatutários, regulamentares e contratuais que uma organização e suas partes interessadas (parceiros comerciais, prestadores de serviços, etc.) têm que cumprir e seu ambiente sociocultural;
c) O conjunto de princípios, objectivos e requisitos de negócio para todas as etapas do ciclo de vida da informação que uma organização desenvolveu para suportar suas operações.

Para elaborar uma Política de Segurança da Informação (PSI), é crucial realizar uma análise de riscos e compreender os fundamentos da segurança. Isso requer um conhecimento profundo da organização, seus processos e objetivos centrais. É essencial entender cada passo dos processos e como cada setor funciona para identificar melhorias na segurança dos ativos (Manhice, 2022).

Posteriormente é preciso que se faça a listagem de todos os activos da empresa, os internos bem como os externos, para cada processo entender os pontos chave, e desenvolver regras que serão cumpridas, com vista a estabelecer dentre os processos realizados um padrão, garantindo assim nível de segurança alto e zelar pelos recursos de TI e por todas as informações que estão dentro da empresa (Manhice, 2022).

Para a Delegação Provincial do MININT/HLA, é essencial incorporar uma PSI na sua infraestrutura de rede, sendo imperativo devido às leis que directa e indirectamente exigem na sua elaboração e implementação, conforme documentos específicos:

Lei nº 7/17 de 16 de Fevereiro - Proteção das Redes e Sistemas Informáticos: Tem como objetivo de responder eficazmente aos desafios da sociedade da informação; Proteção do espaço cibernético angolano contra riscos associados; Promoção da inclusão digital e melhoria da oferta de serviços digitais; Acesso dos cidadãos à informação e ao conhecimento.

Lei nº 22/11 de 17 de Julho - Proteção de Dados Pessoais: Estabelece regras para o tratamento de dados pessoais; Garante o respeito pelas liberdades públicas e os direitos fundamentais das pessoas singulares; Aplica-se ao tratamento automatizado e não automatizado de dados pessoais.

Lei nº 2/20 de 22 de Janeiro - Videovigilância: Regula a autorização e uso de sistemas de videovigilância; Captação, gravação e tratamento de imagem e som para proteção de pessoas e bens; Aplica-se a locais públicos ou privados de uso comum, locais com especial proteção e locais condicionados ou vedados ao público por razões de segurança pública**.**

Os objetivos de segurança da informação envolvem os dados gerados pelos utilizadores e pelos serviços de rede, quer em redes corporativas quer na internet. A segurança dessas redes podem ser comprometidas se a política de segurança da informação não for implementada, uma vez que qualquer pessoa poderá explorar, de forma intencional ou acidental, as suas vulnerabilidades, constituindo uma ameaça aos principais objetivos da segurança da informação ou facilitando o livre trânsito para ataques realizados por invasores com diferentes designações.

1.7. Metodologia de Projectos de Rede de Computadores

Para Pinheiro (2007) citado por António (2016), uma metodologia deve ser estruturada no sentido de incluir um projecto lógico antes de constituir um projecto físico e abordar os requisitos dos utilizadores do sistema antes de considerar outras variáveis. Deve ser interactiva, ou seja, novas informações devem entrar progressivamente no projecto, à medida que se conhece melhor os requerimentos dos utilizadores, a fim de corrigir desvios e eventuais falhas.

Segundo Oppenheimer (2010) citado por Camolacante e Monteiro (2020), dentre os diferentes tipos de metodologias de projectos de rede existentes temos a citar: **top-down, bottom-up e middle Out**.

No presente trabalho, utilizou-se a metodologia top-down, uma vez que focou-se no funcionamento da rede em relação a sua estrutura física.

Oppenheimer (2010) citado por Cassanga e Guelepete (2023), estipula que a Metodologia top-down é um método utilizado no projecto de redes de computadores que inicia o seu desenvolvimento por meio da camada mais alta do modelo de

referência OSI (Open Systems Interconnection), enfocando o levantamento das aplicações, os fluxos de dados e os tipos de serviços necessários para o transporte de dados, em detrimento da selecção dos equipamentos (switches, roteadores, firewall, balanceadores de carga, entre outros) e das tecnologias de cabeamento e interconexão que serão utilizadas.

Com a metodologia top-down, será feito o seguinte:

1) Análise de Requisitos;
2) Projecto Lógico;
3) Projecto Físico;
4) Teste da rede no cisco packet tracer.

CAPÍTULO II - REESTRUTURAÇÃO DA REDE DE COMPUTADORES DA DELEGAÇÃO PROVINCIAL DO MINISTÉRIO DO INTERIOR NA HUÍLA

2. Capítulo II - Reestruturação da Rede de Computadores da Delegação Provincial do Ministério do Interior na Huíla

Neste ponto retrataremos do actual estado da rede de Computadores existente na Delegação Provincial do MININT/HLA, tanto em aspectos funcionais que vem a ser a maneira como a informação tráfega pela rede, isso com a ajuda de um diagrama lógico, bem como em termos estruturais que será a disposição física dos equipamentos pelo edifício, por intermédio de um diagrama físico baseado na planta original do edifício.

2.1. Diagnostico da Situação actual

Com base nas observações feitas à estrutura de rede da Delegação Provincial do MININT/HLA, aquando da realização da visita guiada e aplicação dos inquéritos, com o objetivo de obter informações sobre o estado actual da estrutura de rede e compreender detalhadamente as reais dificuldades de comunicação entre os utilizadores, com vista a reunir os requisitos para melhor elaboração do projecto de reestruturação da rede de computadores.

Identificou-se que por intermédio do cabeamento primário por via aérea pertencente a ISP TVCabo, a Delegação Provincial do MININT/HLA efectuou uma conexão multiponto disponibilizada pela provedora, permitindo deste modo a existência da actual rede de computadores. Para transmissão de dados, a rede de computadores da Delegação Provincial do MININT/HLA, no seu cabeamento, utiliza cabos UTP e STP Cat-6 e conectores RJ-45, que como ponto de partida estão instalados numa sala de equipamentos, dentro de um bastidor, no seu interior possui um pach panel para 30 conexões e um Switch de 8 portas, que levam o tráfego de dados para os demais equipamentos, já o serviço de CCTV, funciona de maneira isolada em um sistema análogico.

Figura 5 - Armário da rede existente

Possui também serviços de voz, assegurados por uma estação de telefonia, instalada no edifício exterior a Delegação Provincial do MININT/HLA, pelo que no seu cabeamento foram usados os cabos cat-5e com conectores RJ-11.

Quanto a configuração geral do cabeamento da rede de computadores da Delegação Provincial do MININT/HLA é quase todo ele secundário metálico horizontal embutido, em pouquíssimos casos é secundário metálico horizontal aparente.

2.1.1. Resultado da recolha de dados

Colheu-se informações aos funcionários da Delegação Provincial do MININT/HLA sobre a utilização da rede de computadores daquela instituição. Para o efeito, utilizou-se a técnica de recolha de dados, que segundo Martins (2019) é um processo que visa reunir os dados para uso secundário por meio de técnicas específicas de pesquisa.

Aplicou-se o questionário fechado, para determinar o seguinte: Identificar as dificuldades de comunicação dos funcionários da Delegação Provincial do MININT-HLA; Apurar o posicionamento dos técnicos de T.I. relativamente aos desafios da rede de computadores instalada na Delegação Provincial do MININT/HLA.

Desta feita, seleccionou-se quarenta e três (43) funcionários para aplicação do questionário, dos quais trinta e cinco (35) são funcionários administrativos utilizadores da rede de computadores e oito (8) são técnicos de manutenção da rede.

2.1.1.1. Questionário aplicado aos administradores da rede de computadores da Delegação Provincial do MININT/HLA

O questionário aplicou-se a oito (8) funcionários responsáveis em administrar a rede, na qual apresentamos-lhes cinco (5) questões fechadas.

Gráfico 1: Resposta a questão 1 aplicada aos administradores de rede

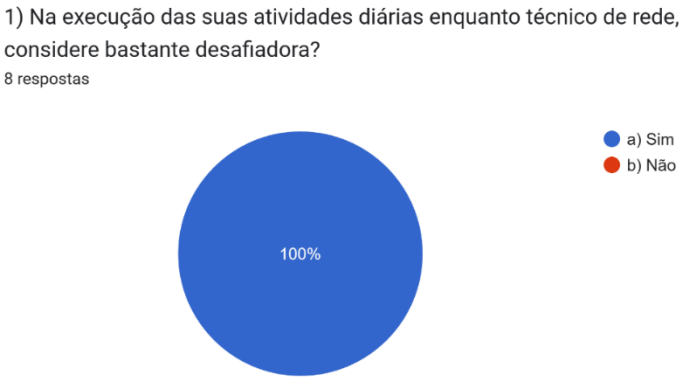


Gráfico 1 - Resposta a questão 1 aplicada aos administradores da rede

Fonte: Autores

Esta questão foi colocada com o objectivo de saber se os mesmos têm dificuldades de executar algumas tarefas ligadas a gestão e manutenção da rede. No gráfico acima, os oito (8) administradores da rede, o que corresponde a 100%, afirmam positivamente de que na execução de suas actividades diárias, tem tarefas que consideram bastante desafiadoras.

Gráfico 2: Resposta complementar a questão 1 aplicada aos administradores de rede

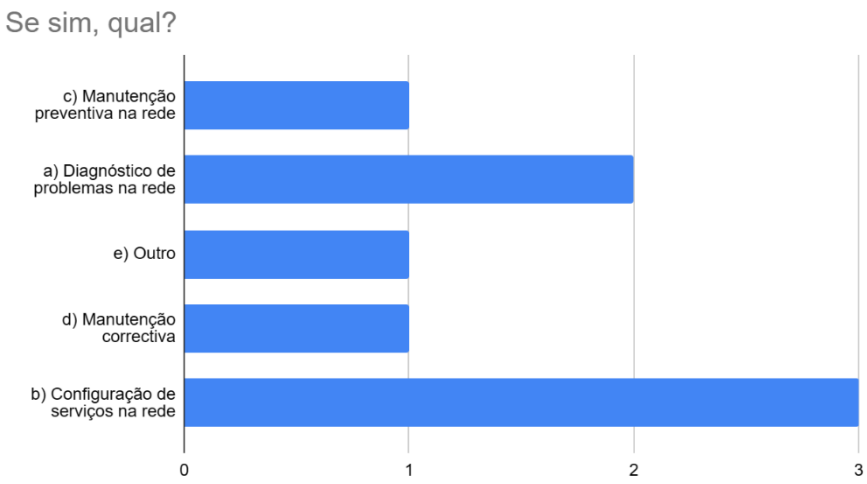


Gráfico 2 - Resposta completar a questão 1 aplicada aos administradores da rede

Fonte: Autores

O gráfico 2, completa a questão colocada no gráfico 1, teve-se como objectivo, saber quais as tarefas que os administradores da rede consideram desafiadoras durante as suas actividades diárias. Como se pode observar, somando as percentagens das respostas “configuração preventiva na rede” com 37,5%, “diagnóstico de problemas na rede” com 25%, “manutenção preventiva na rede” com 12,5%, “manutenção corretiva” com 12,5% e “outras tarefas” com 12,5%. Conclui-se que várias são as tarefas consideradas como desafidoras pelos administradores da rede, com maior frequência a tarefa de configuração de serviços na rede, por falta habilidades por parte dos técnicos.

Gráfico 3: Resposta a questão 2 aplicada aos administradores da rede

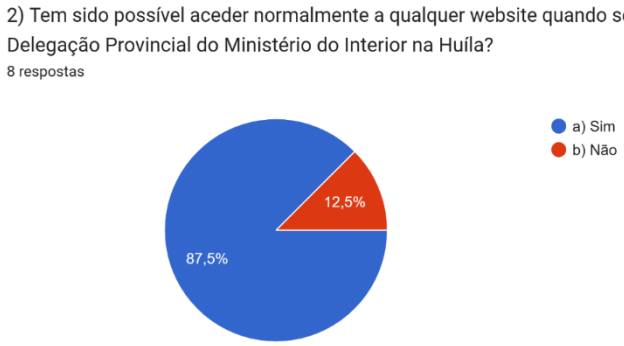


Gráfico 3 - Resposta questão 2 aplicada aos administradores da rede

Fonte: Autores

Com esta questão, teve-se como objectivo, saber sobre os aspectos ligados a segurança da informação, caso particular a bloqueio de sites inseguros e os não autorizados. Observando o gráfico 3, somando as percentagens, 87,5% responderam “sim” e 12,5% responderam “não”. Conclui-se que a rede não tem uma política de segurança aplicada, e se tiver não é eficaz.

Gráfico 4: Resposta a questão 3 aplicada aos administradores da rede

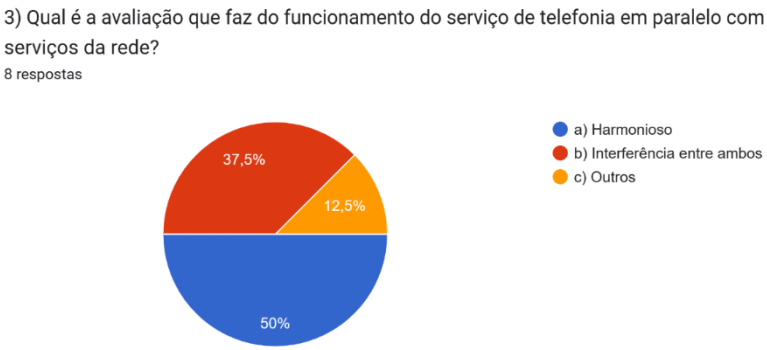


Gráfico 4 - Resposta a questão 3 aplicada aos administradores da rede

Fonte: Autores

Esta questão foi colocada com objectivo de saber se os administradores de rede têm noção da existência de interferências entre os serviços de voz e dados. Com o gráfico 4, somando as percentagens das respostas “harmonioso” com 50%, “interferência entre ambos” com 37,5% e “outros” com 12,5%. Dadas respostas recolhidas, pode-se perceber que uma parte dos administradores da rede, apontam a existência de uma possível interfência entre os serviços de voz e dados.

Gráfico 5: Resposta a questão 4 aplicada aos administradores da rede

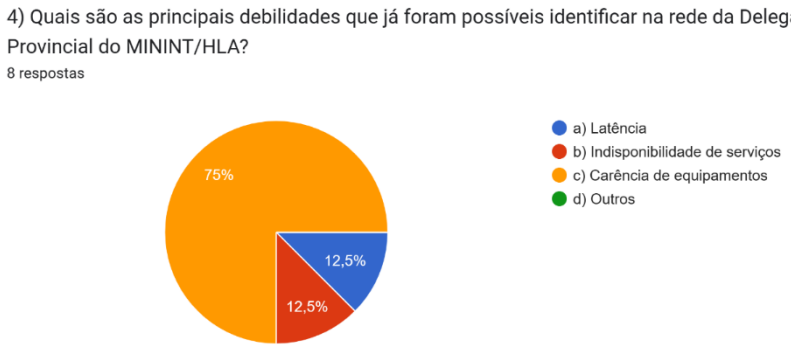


Gráfico 5 - Resposta a questão 4 aplicada aos administradores da rede

Fonte: Autores

Como esta questão, teve-se como objectivo de saber se os administradores da rede já tiveram a oportunidade de identificar algumas debilidades na rede de computadores da Delegação Provincial do MININT/HLA. Observando o gráfico 5, a soma das percentagens das respostas “carência de equipamento” com 75%, “latência” com 12,5% e “indisponibilidade de serviços” com 12,5%. Conclui-se que a rede de computadores da Delegação Provincial do MININT/HLA tem debilidades.

Gráfico 6: Resposta a questão 5 aplicada aos administradores da rede

Gráfico 6 - Resposta a questão 5 aplicada aos administradores da rede

Fonte: Autores

Esta questão foi colocada com o objectivo de saber se as respostas dos administradores da rede, apontam para necessidade de melhorias na rede de computadores em estudo. Com o gráfico 6, os 8 administradores da rede, o que corresponde a 100%, apontam que a rede de computadores da Delegação Provincial do MININT/HLA necessita de melhorias.

Gráfico 7: Resposta complementar a questão 6 aplicada aos administradores da rede

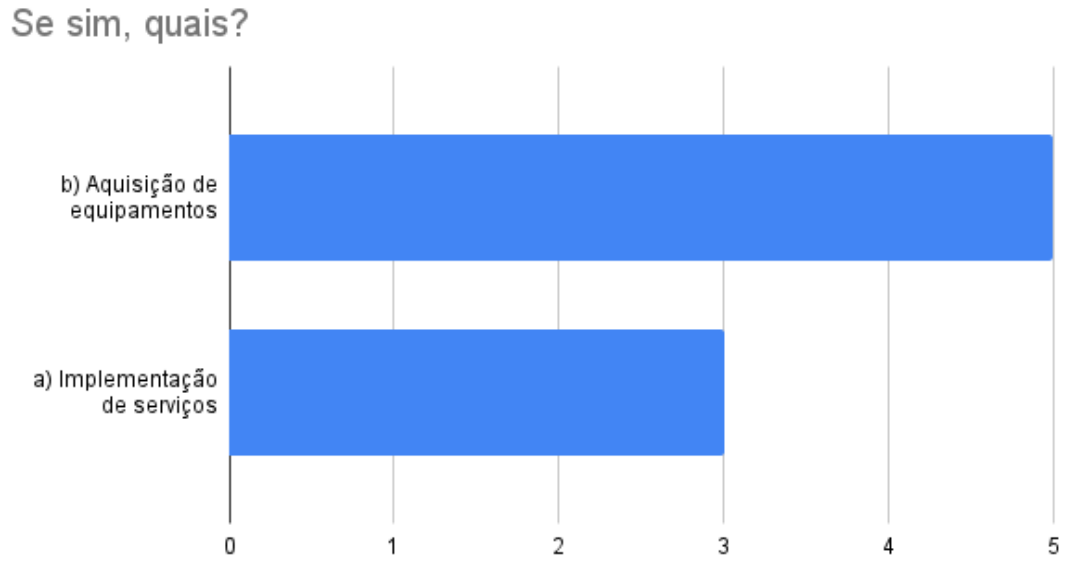


Gráfico 7 - Resposta complementar a questão 6 aplicada aos administradores da rede

Fonte: Autores

Dada as respostas no gráfico 6, com esta questão teve-se como objectivo apontar quais as melhorias que devem ser feitas na rede de computadores da Delegação Provincial do MININT/HLA. Com o gráfico 7 acima, a soma das percentagens das respostas “aquisição de equipamentos” com 62,5% e “implementação de serviços” com 37,5%. Conclui-se que se torna indispensável implementar as melhorias acima apontadas.

2.1.1.2. Questionário aplicado aos funcionários administrativos utilizadores da rede de computadores da Delegação Provincial do MININT/HLA

O questionário aplicou-se a trinta e cinco (35) funcionários administrativos utilizadores da rede de computadores da Delegação provincial do MININT/HLA, na qual apresentamos-lhes sete (7) questões fechadas.

Gráfico 8: Resposta a questão 1 aplicada aos funcionários administrativos

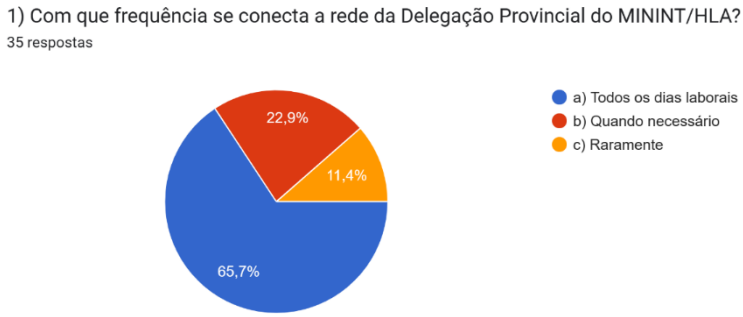


Gráfico 8 - Resposta a questão 1 aplicada aos funcionários administrativos

Fonte: Autores

Com esta questão, teve-se como objectivo saber a regularidade com que os funcionários administrativos se conectam a rede. Com o gráfico 8, a soma das percentagens das respostas "todos os dias laborais" com 65,7%, "quando necessário" com 22,9% e "raramente" com 11,4%. Portanto, percebe-se que maior parte dos funcionários administrativos têm uma frequente necessidade de se conectar a rede.

Gráfico 9: Resposta a questão 2 aplicada aos funcionários administrativos

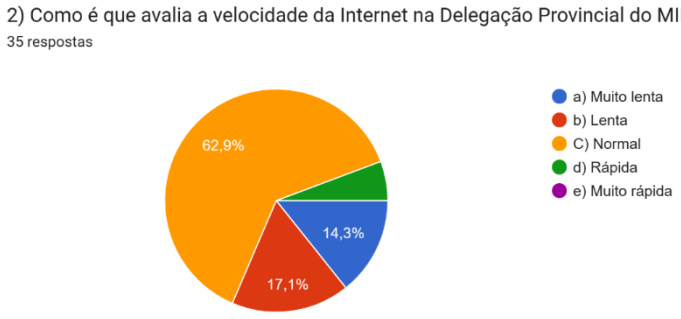


Gráfico 9 - Resposta a questão 2 aplicada aos funcionários administrativos

Fonte: Autores

Com a questão do gráfico 9, o objectivo é de saber da qualidade dos serviços de internet. Com a soma das percentagens das respostas, apontam que é "muito lenta" com 14,3%, "lenta" com 17,1%, "normal" com 62,9% e "rápida" com 5,7%. Conclui-se que a velocidade dos serviços de internet na rede de computador da Delegação Provincial do MININT/HLA não é suficientemente boa, abrindo a possibilidade de apontar e solucionar alguns factores que influenciam na velocidade deste serviço.

Gráfico 10: Resposta a questão 3 aplicada aos funcionários administrativos

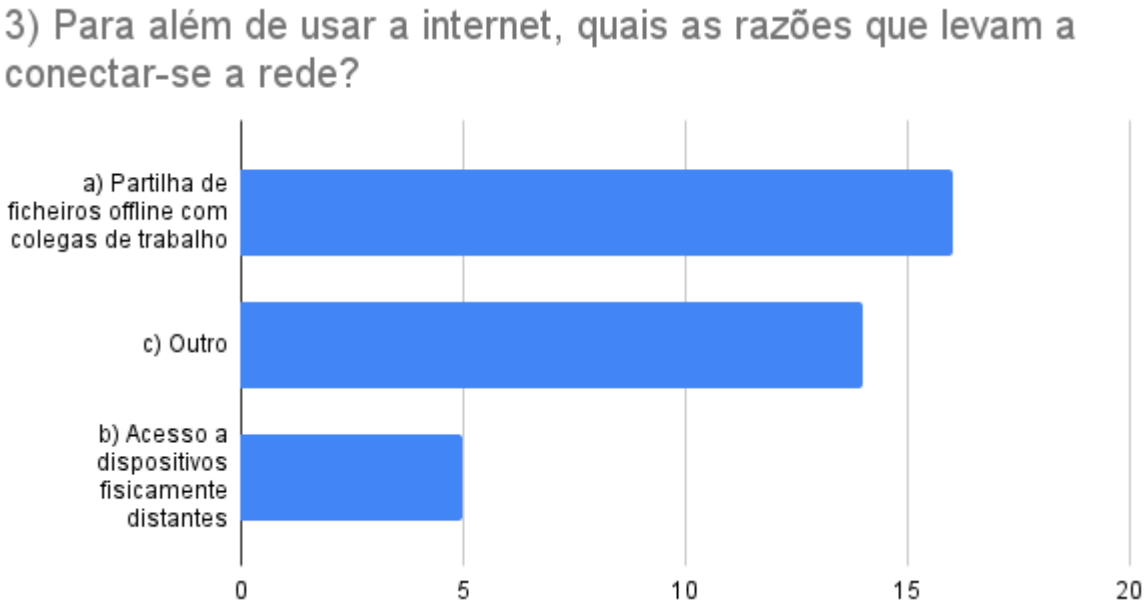


Gráfico 10 - Resposta a questão 3 aplicada aos funcionários administrativos

Fonte: Autores

Com a questão do gráfico 10, o objectivo é de saber se além da utilização dos serviços de internet, têm outras razões que os levam a conectar-se a rede. Com o gráfico 10, a soma das percentagens das respostas apontam a “partilha de ficheiros offline com colegas de trabalho” com 45,7%, “acesso a dispositivos fisicamente distantes” com 14,3% e “outras razões” com 40%. Como conclusão, para os funcionários administrativos, além da utilização dos serviços de internet, existem outras razões que os levam a conectar-se a rede.

Gráfico 11: Resposta a questão 4 aplicada aos funcionários administrativos

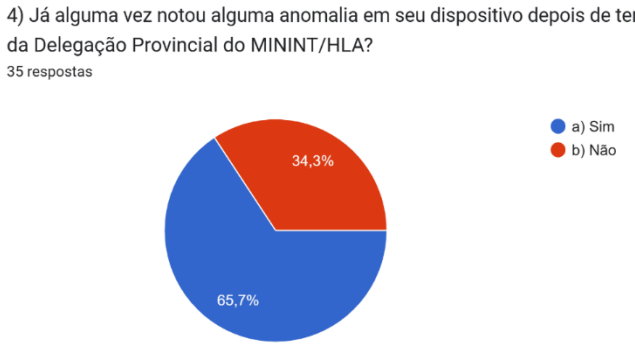


Gráfico 11 - Resposta a questão 4 aplicada aos funcionários administrativos

Fonte: Autores

Com esta questão, o objectivo é de saber se os dispositivos já foram afectados por algum malware depois de se conectar a rede. Com o gráfico 11, as somas das

percentagens apontam “sim” com 65,5% o que corresponde a 23 funcionários e “não” com 34,3% correspondendo a 12 funcionários. Portanto, maior parte confirma que depois de conectar o dispositivo a rede, este apresentou algumas anomalias, o que faz considerar a possibilidade de ter algum software malicioso.

Gráfico 12: Resposta complementar a questão 4 aplicada aos funcionários administrativos

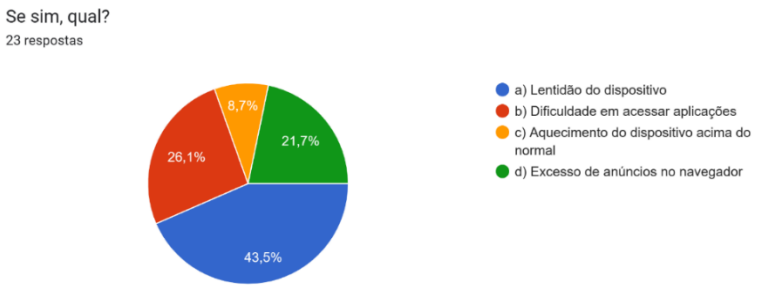


Gráfico 12 - Resposta complementar a questão 4 aplicada aos funcionários administrativos

Fonte: Autores

Com a questão acima, o objectivo é de perceber quais são as anomalias apresentadas nos dispositivos depois de conectar a rede, isto é, em função dos 23 funcionários administrativos que responderam “sim” à questão colocada no gráfico 11. Com as somas das percentagens das respostas no gráfico 12, apontam a “lentidão do dispositivo” com 43,5%, “dificuldade de aceder aplicações” com 26,1%, “aquecimento do dispositivo acima do normal” com 8,7% e “excesso de anúncios no navegador” com 21,7%. Desta feita e com suporte aos estudos de Buscape (2022), conclui-se que os dispositivos têm sido infectados por malwares depois de conectar a rede.

Gráfico 13: Resposta a questão 5 aplicada aos funcionários administrativos

Gráfico 13 - Resposta a questão 5 aplicada aos funcionários administrativos

Fonte: Autores

O objectivo da pergunta colocada no gráfico 13, é de saber se existe uma política de restrição de acesso a sites com conteúdos inapropriados. Com as somas das percentagens das respostas, “sim” com 71,4% e “não” com 28,6%. Conclui-se que maior parte consegue navegar a qualquer site. Deste modo presume-se que a rede de computadores da Delegação Provincial do MININT/HLA não possui nenhum mecanismo que faça restrições de acesso a sites inapropriados, se tiver não é eficaz.

Gráfico 14: Resposta a questão 6 aplicada aos funcionários administrativos

Gráfico 14 - Resposta a questão 6 aplicada aos funcionários administrativos

Fonte: Autores

O objectivo da questão colocada no gráfico 14, é de saber sobre a existência de timeouts na rede. Com a soma das percentagens das respostas, “sim” com 85,7% o que equivale a 30 funcionários, e “não” com 14,3%, equivalente a 5 funcionários. Conclui-se que maior parte dos inqueridos confirma que já notou uma inexplicável perda de sinal.

Gráfico 15: Resposta complementar a questão 6 aplicada aos funcionários administrativos

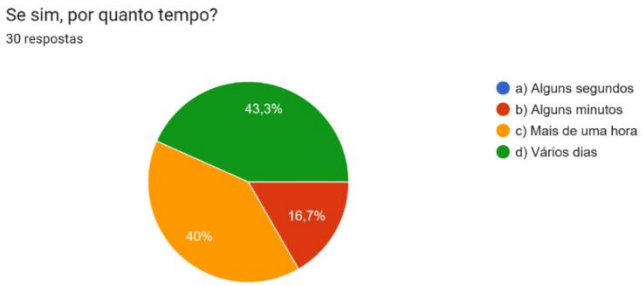


Gráfico 15 - Resposta complementar a questão 6 aplicada aos funcionários administrativos

Fonte: Autores

Em função dos 30 funcionários administrativos que já notaram uma inexplicável perda de sinal, conforme no gráfico 14, esta questão tem como objectivo saber em quanto tempo permanece a perda de sinal. Com o gráfico 15, a soma das percentagens das respostas “alguns minutos” com 16,7%, “mais de uma hora” com 40% e “vários dias com 43,3%. Conforme o depoimento dos 30 funcionários administrativos, conclui-se que existe timeouts na rede e que maior parte deles dura um tempo considerável.

Gráfico 16: Resposta a questão 7 aplicada aos funcionários administrativos

Gráfico 16 - Resposta a questão 7 aplicada aos funcionários administrativos

Fonte: Autores

Com a questão colocada no gráfico 16, teve-se como objectivo saber se os inqueridos já tiveram a oportunidade de verificar a qualidade dos serviços quando estes são usados em paralelo. Com as percentagens das respostas, 68,6% diz que “sim” o que equivale a 24 inqueridos e 31,4% diz que “não”, na qual equivale a 11 inqueridos. Conclui-se que maior parte já presenciou o uso dos serviços de dados e voz em paralelo.

Gráfico 17: Resposta complementar a questão 7 aplicada aos funcionários administrativos

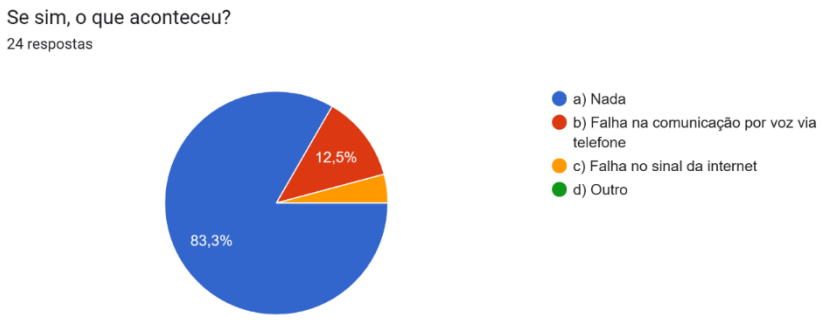


Gráfico 17 - Resposta complementar a questão 7 aplicada aos funcionários administrativos

Fonte: Autores

Conforme o gráfico 16, em que 24 inqueridos confirmam que já usaram os serviços de internet enquanto alguém usava o telefone fixo, o objectivo da questão colocada no gráfico 17 é de saber se alguém notou uma possível interferência entre os serviços de dados e voz. Com a soma das percentagens das respostas, “nada” com 83,3%, “falha na comunicação por voz via telefone” com 12,5% e “falha do sinal de internet” com 4,2%. Conclui-se que alguns notaram interferências entre os serviços de voz e dados.

2.1.2. Diagrama lógico da rede existente

O presente diagrama demonstra como os dados são hierarquicamente distribuídos pelos equipamentos activos na rede de computadores instalada na Delegação Provincial do MININT/HLA. Os equipamentos de CCTV e telefonia não serão aqui ilustrados por serem subsistemas até o momento independentes e analógicos, desta feita, não se tem muito a dizer sobre o seu funcionamento ou configuração.

A topologia utilizada é a estrela, possui um nó central, onde se encontra actualmente um roteador da provedora, a ele está ligado o switch de distribuição, por sua vez interliga outros equipamentos de acesso aos utilizadores.

Com ajuda do Microsoft Visio, foi traçado o seguinte diagrama lógico da rede existente:

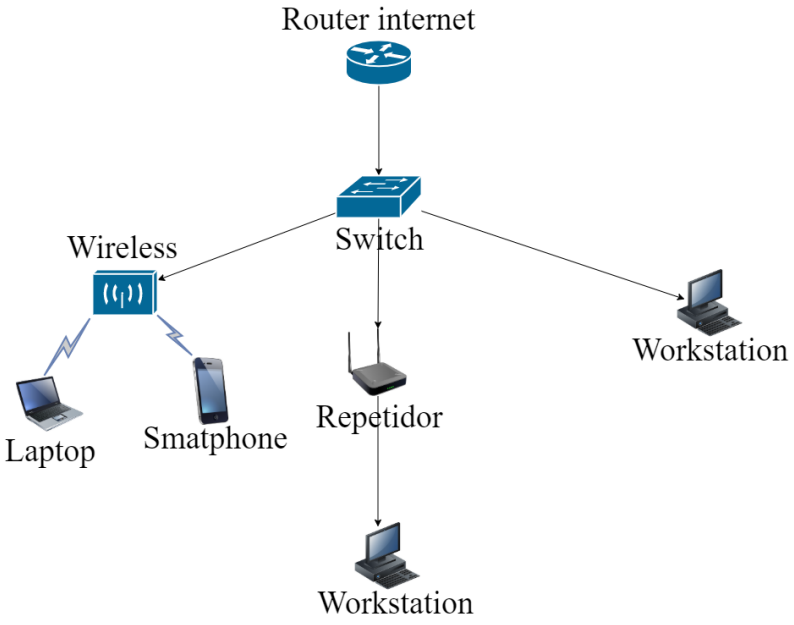


Figura 6 - Diagrama lógico da rede existente

A infra-estrutura de rede da Delegação Provincial do MININT/HLA, é maioritariamente constituída por equipamentos que solicitam a disposição de páginas web, assegurada pelo link multiponto da provedora TV Cabo (router internet), conforme a figura 6, conectado na porta WAN do router, que por sua vez leva o tráfego aos equipamentos localizados no edifício principal e no edifício anexo, intermediado através das portas LAN de um switch. Quanto a este último, considerado como principal distribuidor, em suas portas LAN através de um painel de conexão, interliga um ponto de acesso wireless localizado no edifício anexo, bem como distribui o sinal de dados até ao edifício principal através de alguns repetidores, conectando somente algumas estações de trabalho.

Conforme descrito nos pontos anteriores, a infra-estrutura de rede da Delegação Provincial do MININT/HLA, somente dispõem do serviço de acesso a internet via cabo e wireless e dos serviços configurados em cabeamentos independentes para suporte analógico para voz e para CCTV. Entre estes serviços citados, não dispõem de nenhuma outra configuração, tanto para o âmbito de serviços, segurança e outros requisitos a nível do modelo TCP/IP como do modelo cisco hierárquico.

2.1.3. Diagrama físico da rede existente

A Delegação Provincial do MININT/HLA é constituída por dois edifícios, sendo um principal de dois pisos e um anexo de um piso, na qual partilham a mesma infra-estrutura de rede de computadores, por meio de um sistema de cabeamento estruturado, com os serviços de acesso à internet, sem outros serviços configurados que permitem a interacção de recursos entre os utilizadores.

Com o Microsoft Visio, projectou-se os seguintes diagramas físicos existentes:

Diagrama físico da rede de computadores do edifício anexo

Piso 0: Composto por quatro (4) gabinetes, um (1) quarto de banho particular, uma (1) arrecadação, um (1) corredor de acesso a escadas e um (1) corredor de acesso aos compartimentos.

Piso 1: Composto por cinco (5) gabinetes, dois (2) quartos de banho colectivos, um (1) corredor de acesso a escadas e um (1) corredor de acesso aos compartimentos.

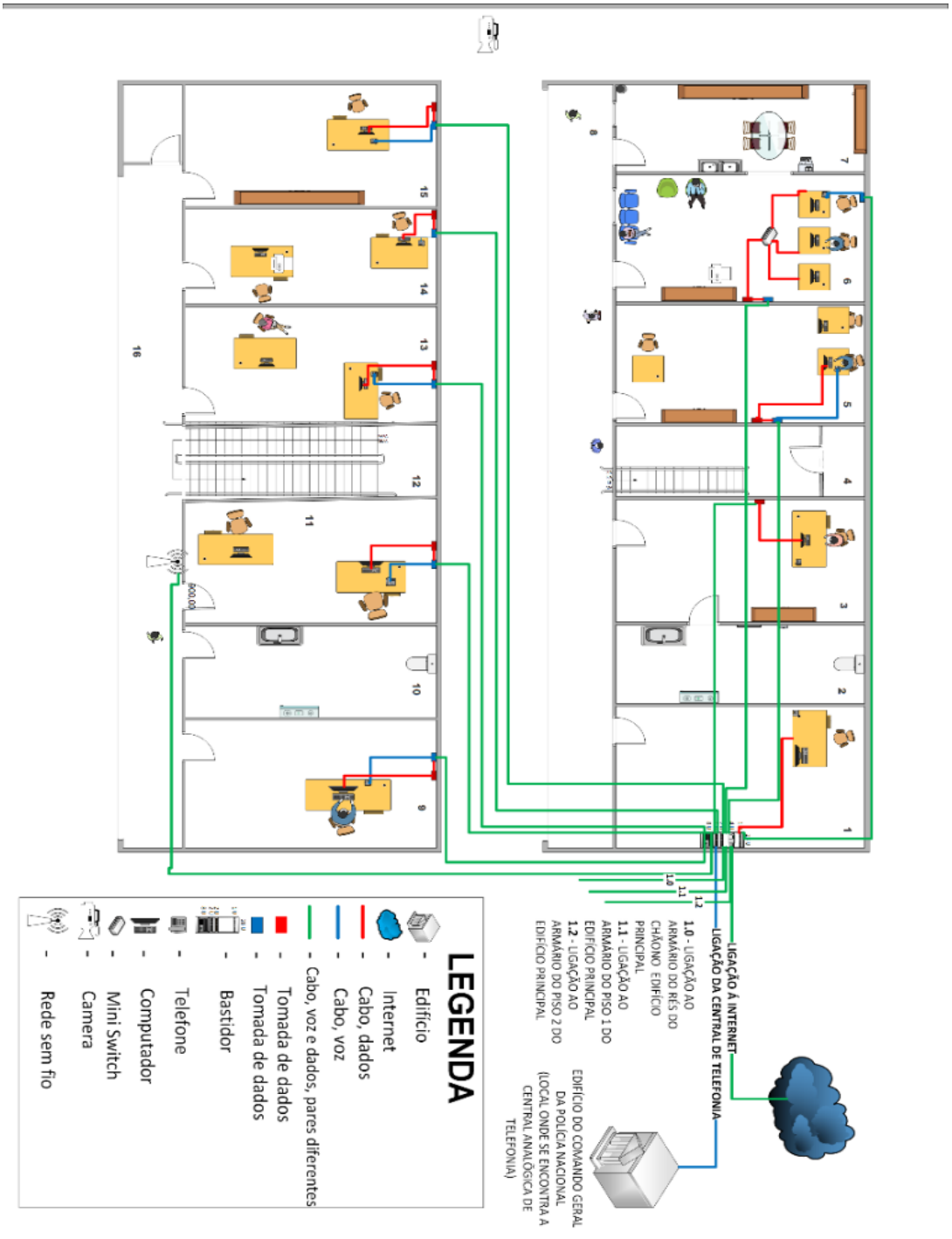


Figura 7 - Diagrama físico da rede no edifício anexo

A legenda da figura acima, demonstra que as linhas em vermelho ilustram a ligação de dados, enquanto as azuis ilustram a ligação de voz. A ligação de voz é proveniente de uma central instalada no edifício adjacente à Delegação Provincial do MININT/HLA (Comando Municipal da PNA/HLA), já a ligação de dados é proveniente da provedora TVCabo.

No edifício anexo, está localizada a sala de equipamentos (piso 0, sala nº1), onde tem instalado um armário e outros equipamentos activos e passivos, para distribuição dos serviços de voz e dados, nos dois pisos e para o edifício principal.

Diagrama físico da rede de computadores do edifício principal

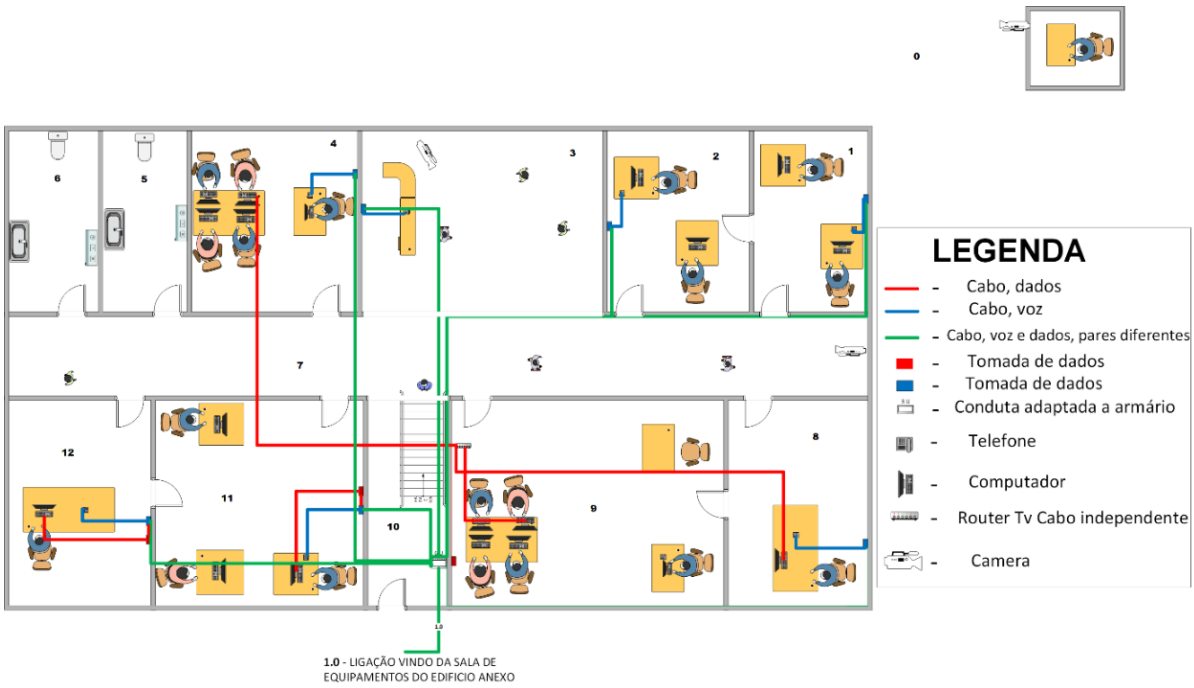


Figura 8 - Diagrama físico da rede no piso 0 do edifício principal

Piso 0: Composto por sete (7) gabinetes, dois (2) quartos de banho colectivos, uma (1) área para recepção, um (1) corredor de acesso a escadas e um (1) corredor de acesso aos compartimentos, acordo a figura 9.

Por intermédio do cabeamento secundário metálico horizontal embutido, que tem o ponto de partida a sala de equipamentos localizada no edifício anexo conforme a figura 8, com o ponto de chegada e distribuição dos cabos numa pequena conduta no corredor de acesso a escadas do edifício principal. A partir desde ponto os cabos levam o sinal de dados e de voz a todas as tomadas do edifício principal.

A sala 09 da figura 8, dispõem de um router da provedora TV Cabo, sendo um router a parte, tem um link de acesso a internet directamente disponibilizado pela provedora, através do qual, distribui o sinal de dados via cabo e wireless.

Piso 1: Constituído por quatro (4) gabinetes, uma (1) sala de reuniões, um (1) quarto de banho particular, dois (2) quartos de banho colectivos, uma (1) arrecadação, dois (2) corredores de acesso aos compartimentos e um corredor de acesso a escadas.

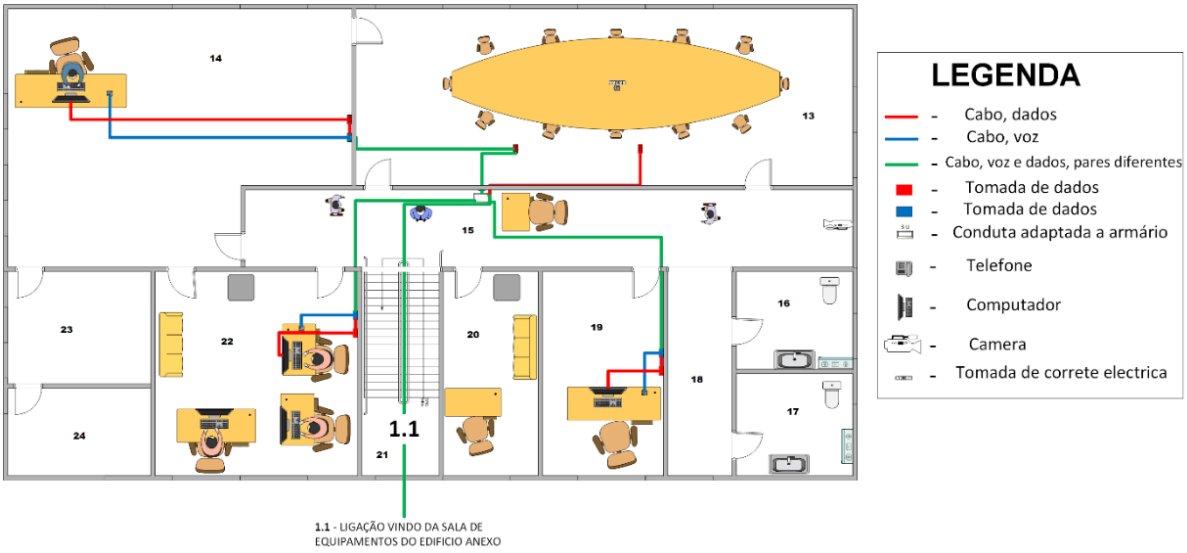


Figura 9 - Diagrama físico da rede no piso 1 do edifício principal

Através da figura 9, os segmentos que partem do piso 0 são recebidos em um ponto do corredor de acesso aos compartimentos do piso 1, na qual por meio de calhas embutidas, são distribuídos para interligar as tomadas. Ainda no piso 1, com excepção da sala nº 25 que não tem acesso aos serviços de voz e internet, por conta da organização administrativa e sala de reunião tendo apenas uma tomada para acesso a dados, os demais compartimentos têm tomadas para os serviços de voz e dados.

Piso 2: Possui oito (8) gabinetes, dois (2) quartos de banho e dois (2) corredores de acesso aos compartimentos.

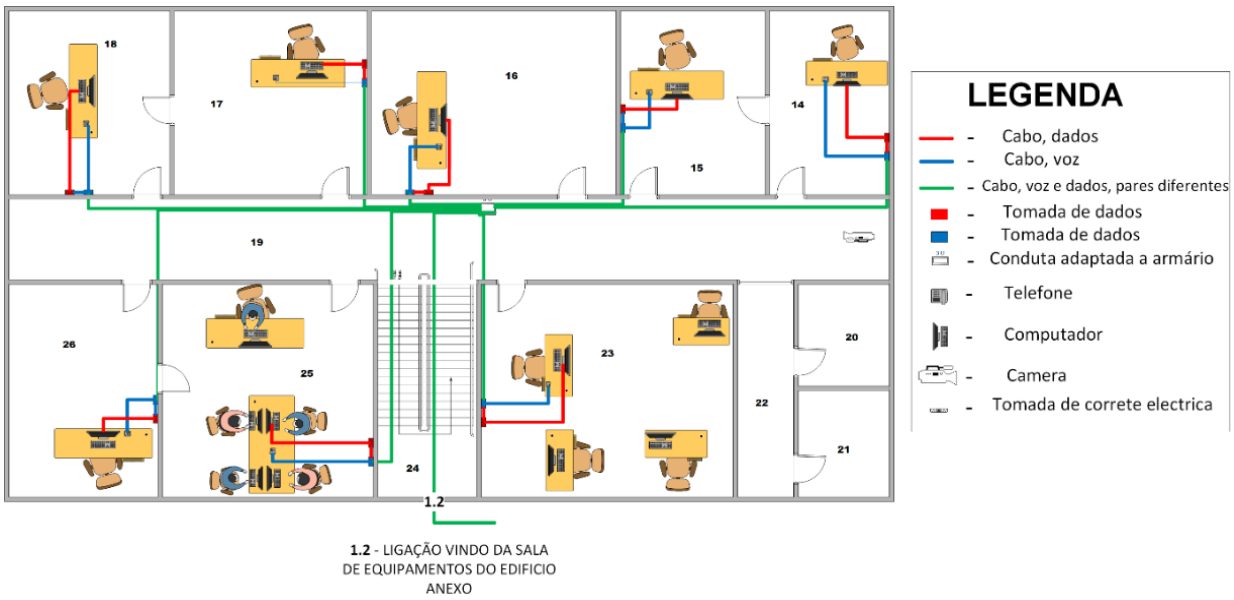


Figura 10 - Diagrama físico da rede no piso 2 do edifício principal

A figura 10, demostra a disposição física da rede de computadores no piso 2, mas importa realçar que numa das salas deste mesmo piso, tem instalado um sistema analógico de monitoramento por vídeo vigilância.

Portanto, em cada um dos compartimentos ilustrados, tanto do edifício anexo como do principal, podemos encontrar pelo menos duas tomadas, sendo neste momento distribuídas uma para voz e outra para dados.

Pontos fortes

1) Infra-estrutura de rede com sistema de cabeamento estruturado instalado, configurado e aproveitável;
2) Existência de dois links fornecidos por uma IPS;
3) Existência de equipamentos como computadores, switchs, routers, painel de conexão, wireless, impressoras e armário;
4) Existência de espaços no edifício para sugerir novas salas de equipamentos e de telecomunicação;
5) Possibilidade de instalação e configuração de outro ISPs como plano de contingência.

Pontos fracos

1) A estrutura de rede é tradicional, visto que foi projectada para suportar telefones analógicos utilizando cabos de rede UTP e tomadas com interface RJ-11;
2) Nas tomadas RJ-11 inicialmente projectadas, foram subtraídos 3 pares de cabo para instalação de uma nova tomada com interface RJ-45 para a transmissão de dados, fazendo com que numa das suas extremidades do cabo UTP, um par é crimpado a uma tomada para telefone e os outros 3 na tomada para as estações de trabalho;
3) Dependência da central telefónica instalada no edifício adjacente para comunicação interna de voz;
4) Configurados telefones analógicos que funcionam com uma corrente abaixo dos 48 Volts, sendo que na utilização dos serviços de voz, interfere no tráfego de pacotes de dados de internet, consubstanciando com timeouts, ou seja, há

correntes paralelas em um mesmo cabo de rede, porque têm nas suas extremidades configuradas duas tomadas para serviços diferentes;

5) Não há contingência quanto aos serviços de dados, ou seja, em caso de falha da TVCabo não há uma outra provedora onde se possa recorrer para atender as necessidades dos utilizadores;

6) Infra-estrutura de rede sem um plano de segurança de dados, tornando vulnerável o sistema a qualquer ataque;

7) Sistema de cabeamento sem um quadro de conexões;

8) As tomadas para as estações de trabalho estão directamente ligadas aos armários de edifício, o que não é uma boa prática;

9) Sala de equipamento sem um sistema de segurança física;

10) Ausência de uma régua de tomadas monofásicas, de montagem rack para a correcta alimentação eléctrica dos equipamentos de comunicação, sendo que a actual alimentação eléctrica é feita de forma adaptada;

11) Inexistência de uma fonte de alimentação ininterrupta e estabilizada (UPS - Uninterrupted Power Supply) de montagem rack;

12) Congestionamentos de cabos no cabeamento do armário de equipamentos;

13) Ausência de um servidor para processamento, gestão e disponibilidade de importantes serviços de rede;

14) Muitas estações de trabalho sem acesso a internet;

15) Todas impressoras com placas de rede não se encontram conectadas e configuradas na rede;

2.2. Proposta de reestruturação

Um dos pontos fortes da rede da Delegação Provincial do MININT/HLA, é a existência de uma estrutura de rede cabeada, através do qual, optou-se pela metodologia top-down, como espelhado anteriormente, sendo assim esta metodologia descreve o projecto de rede nos seguintes passos:

- ✓ Identificação das necessidades;
- ✓ Projecto lógico de rede;
- ✓ Projecto físico de rede;
- ✓ Implementação da rede no simulador cisco packet tracer.

Este projecto tem como objectivo fornecer as premissas para a reestruturação da rede de computadores da Delegação Provincial do MININT/HLA, a qual abrange conceitos e ferramentas que atendem a uma nova metodologia de rede, na qual dispõe de:

1) Servidores de serviços e aplicações (DHCP, Firewall, Proxy, VPN e Port security);
2) Disponibilidade de serviços (partilha de arquivos, impressoras e backup realizado periodicamente);
3) Gestão de contas de todos utilizadores da rede, na qual cada um terá um perfil criado pela gestão da TI, configurada de acordo com as necessidades de cada utilizador;
4) Controle de acesso de utilizadores a recursos na rede de acordo com o perfil criado;
5) Centralização da gestão da área de TI. Esta nova infra-estrutura tem como objectivo, de garantir disponibilidade e partilha de recursos, gestão da rede e segurança de acesso.

2.3. Análise de requisitos

Das constatações e inquéritos realizados durante os primeiros dias da nossa pesquisa, conseguimos apurar que o pessoal da Delegação Provincial do MININT/HLA tenciona melhorar os seguintes aspectos em sua rede:

Tabela 2 – Requisitos do negócio e técnicos

N/0	Requisitos de negócio	Requisitos técnicos
01	Possibilitar que a conexão à rede esteja disponível para todo utilizador autorizado.	Expansão e redistribuição do sinal por intermédio de switchs e routers.
02	Possibilitar a troca de informação numa rede de internet.	Gestão da largura de banda.
03	Garantir a segurança das informações trafegadas na rede	Firewall contra intrusos, VPN para criptografia dos dados e Port security para segurança das portas do switch.
04	Gestão de impressoras disponíveis.	Partilhar as impressoras existentes na rede com as devidas restrições.
05	Convergir serviços de dados, voz e vídeo na rede.	Implementar QoS, para não congestionar a largura de banda em função dos vários serviços.
06	Controle de acesso de utilizadores e de acesso a sites com conteúdos não autorizados.	Configuração de sistema de obtenção de dados sobre as actividades dos utilizadores e ferramentas para filtrar conteúdos indesejáveis de acordo à política da instituição e controle de acesso de utilizadores na rede de acordo com o perfil criado.

07	Limitação de downloads	Serviços proxy.
08	Cabeamento protegido dentro do edifício.	Implementação de soluções de cabeamento secundário.
09	Cópia de Segurança	Backups permanentes, de modos a manter a informação segura e disponível em caso de uma falha nos equipamentos.
10	Segurança física dos equipamentos e da instituição	Câmaras de vigilância e sistemas de alarme.

2.4. Políticas e mecanismos de segurança da rede

De acordo com as competências exercidas pela Delegação Provincial do MININT/HLA, a segurança e a manipulação da informação compõem um dos importantes critérios para o seu normal funcionamento, bem como é parte integrante das políticas de segurança da instituição em causa. Com a utilização de uma rede de computadores, estabelecer um plano de segurança da rede de computadores, implica protegê-la de qualquer evento malicioso.

Conforme as leis nº 7/17 de 16 de Fevereiro, lei de protecção das redes e sistemas informáticos, nº 22/11 de 17 de Julho, lei da protecção de dados pessoais e a nº 2/20 de 22 de Janeiro, lei da videovigilância, bem como as políticas de segurança vigentes na Delegação Provincial do MININT/HLA, propomos que seja implementado no projecto de rede, funcionalidades de um firewall, podendo ser dispositivo ou software, controles no router e nos switchs dispostos na rede, seguindo os requisitos de negócio. Estes controles minimizam os riscos de indisponibilidade de serviços, vazamento de informação e acesso a conteúdos duvidosos na internet. Para tal prevê-se o seguinte plano de segurança:

1) **Segurança física da rede**: Instalar sensores de porta aberta e câmaras de vídeo vigilância na sala de equipamentos onde contêm o data-center bem como em outros locais com equipamentos de comunicação.
2) **Segurança de acesso a rede wi-fi**: Implementação de Hotspot, para atribuição de credenciais de acesso, para cada utilizador, limitando o número de dispositivos a serem usado através do endereço MAC.
3) **Segurança da rede cabeada**: Implementação de Port Security, (segurança nas portas dos Switches), para a filtragem de acesso a rede de equipamentos com endereço MAC não autorizados, permitindo somente endereços MAC autorizados. Todas as tomadas de rede necessitam de registo para serem utilizadas.

4) **Segurança com VLAN´s**: Divisão da rede em sub-redes, de modo que a comunicação entre outros sectores de VLAN seja restrita.
5) **Segurança de aplicações** - Utilização de políticas de grupo GPO (Group Policy), a fim de controlar em parte o que os utilizadores podem ou não fazer em um computador, restringir determinadas acções que podem representar potenciais riscos a segurança onde destacam-se:

Tabela 3 - Restrições de acções dos utilizadores

Directivas	Utilizadores	Procedimento
Acesso a internet	Todos utilizadores da rede	Configuração de firewall por meio de regras de entrada e saída.
Acesso a voz	Directores e áreas de recepção	Limitar o número de telefones por gabinete.
Acesso a impressoras	Todos utilizadores da rede	Partilhar as impressoras na rede.
Acesso a central de CCTV	Administrador da rede	Aumentar o nível de segurança física do local onde a central funciona.
Backup	Administrador da rede	Implementação de servidor de arquivos.

2.5. Alteração dos diagramas (lógico e físico)

2.5.1. Proposta de alteração do diagrama lógico

Com o objectivo de reestruturar a rede existente na Delegação Provincial do MININT/HLA, propõe-se a seguinte alteração do diagrama lógico:

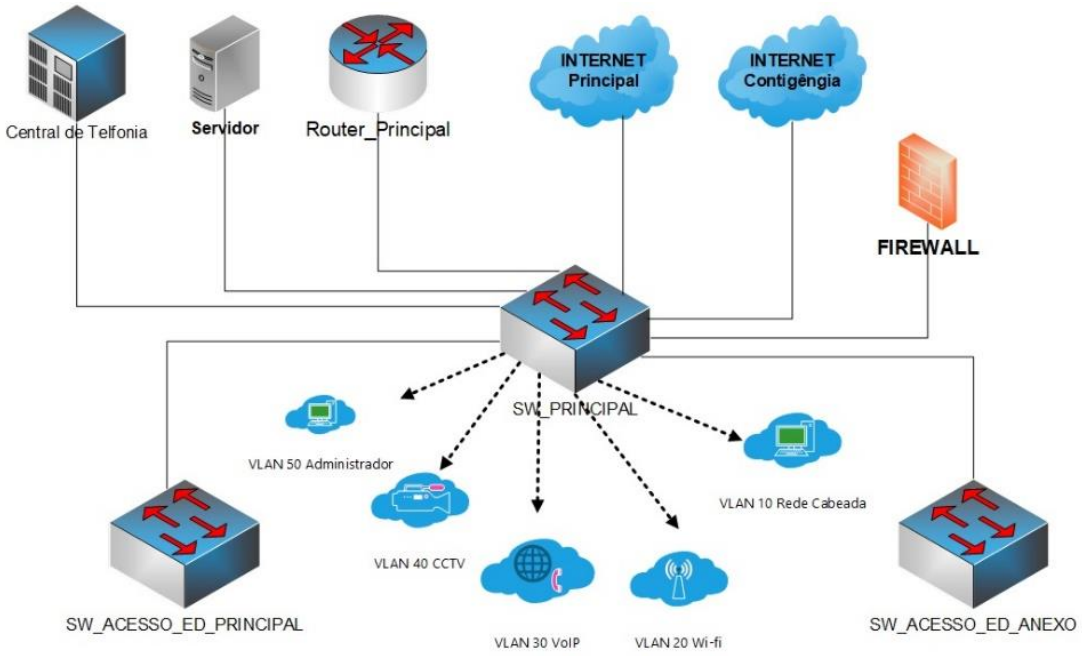


Figura 11 - Proposta de alteração do diagrama lógico

Com a alteração do diagrama lógico, a rede será constituída pelo seguinte:

- **Central de telefonia IP**: trata-se de uma tecnologia que utiliza o sistema VoIP (Voz sobre IP), por meio do qual a rede de dados trabalha de maneira similar à telefonia fixa. Permite o uso de ramais virtuais em qualquer aparelho que tenha acesso à internet, que pode ser um smartphone, computador ou tablet (Leucotron, 2020).
- **Internet** fornecida por uma ISP, para permitir o acesso a páginas web, bem como o funcionamento de alguns serviços na rede.
- **Router principal** que tem a responsabilidade de efectuar o acesso exterior (internet) como ao interior (pontos de distribuição);
- **Firewall** para gestão da rede e controlo do tráfego interno e externo;
- **Switch de distribuição**, sendo através deste que foi feito a segmentação da rede por intermédio da criação de VLANs, possibilitando a comunicação dos dispositivos locais com o roteador principal. É partir deste equipamento onde está conectado os switches de acesso bem o ponto de acesso wi-fi.
- **Switches de acesso**, com vista a interligar cada estação de trabalho ou cliente disponível na rede com os equipamentos de rede no armário de distribuição, é neste ponto onde fez-se a configuração de VLANs de modos a segmentá-los a rede para que haja maior controlo, desta feita, o recurso a VLAN permite agrupar vários dispositivos disponíveis em uma única rede lógica.
- **Servidor,** para processamento e execução de solicitações feitas pelos utilizadores através de softwares, bases de dados, envio e recepção de informações como e-mails e outros (Kriger, 2022).
- **VLANs** da rede cabeada, CCTV, Voz e Wi-fi, de modos a proporcionar uma infra-estrutura de rede convergente.

Para o presente diagrama, adoptou-se a topologia estrela, com vista a proporcionar melhor segurança a rede, tanto a nível da firewall com os recursos de restrição de entrada e saída, como a nível do roteador com a configuração de algumas regras de NAT.

Tabela de endereçamento

No âmbito de endereçamento, a rede não contava com nenhuma tabela de endereçamento, pelo que representava um grande problema aos gestores da rede.

De modos a superar esta dificuldade, propomos a seguinte tabela de endereçamento:

Tabela 4 - Tabela de endereçamento

Rede Privada - 192.168.0.0/24						
Designação	**VLAN ID**	**Hosts p/ocupar**	**Sub-rede**	**Pool DHCP**	**Broadcast**	**Máscara**
Rede Cabeada	VLAN 10	250	192.168.0.0/24	192.168.0.1 - 254	192.168.0.255	255.255.255.0
Wi-fi	VLAN 20	240	192.168.1.0/24	192.168.1.1 - 254	192.168.1.255	255.255.255.0
VoIP	VLAN 30	34	192.168.2.0/26	192.168.2.1 – 62	192.168.2.63	255.255.255.192
CCTV	VLAN 40	30	192.168.2.64/27	192.168.2.65 - 126	192.168.2.127	255.255.255.224
Admin	VLAN 50	10	192.168.2.128/28	192.168.2.129 - 142	192.168.2.143	255.255.255.240
Rede Pública Principal – 66.10.11.0/24						
R. Principal	VLAN 70	4	66.10.11.0/29	66.10.11.1 - 6	66.10.11.7	255.255.255.248
Rede Pública de Contigência - 66.10.11.0/24						
R. Contigência	VLAN 80	2	66.10.11.8/30	66.10.11.9 - 10	66.10.11.11	255.255.255.252

2.5.2. Proposta de alteração do diagrama físico da rede

Apesar de que um dos objectivos do presente estudo é a implementação de serviços inexistentes na rede, considerou-se necessário propor algumas remodelações no cabeamento de modos a garantir que o hardware tenha a robustez necessária para suportar os sistemas que serão implementados, assim sendo, propomos as seguintes alterações no diagrama físico da rede:

Alteração do diagrama físico do edifício anexo

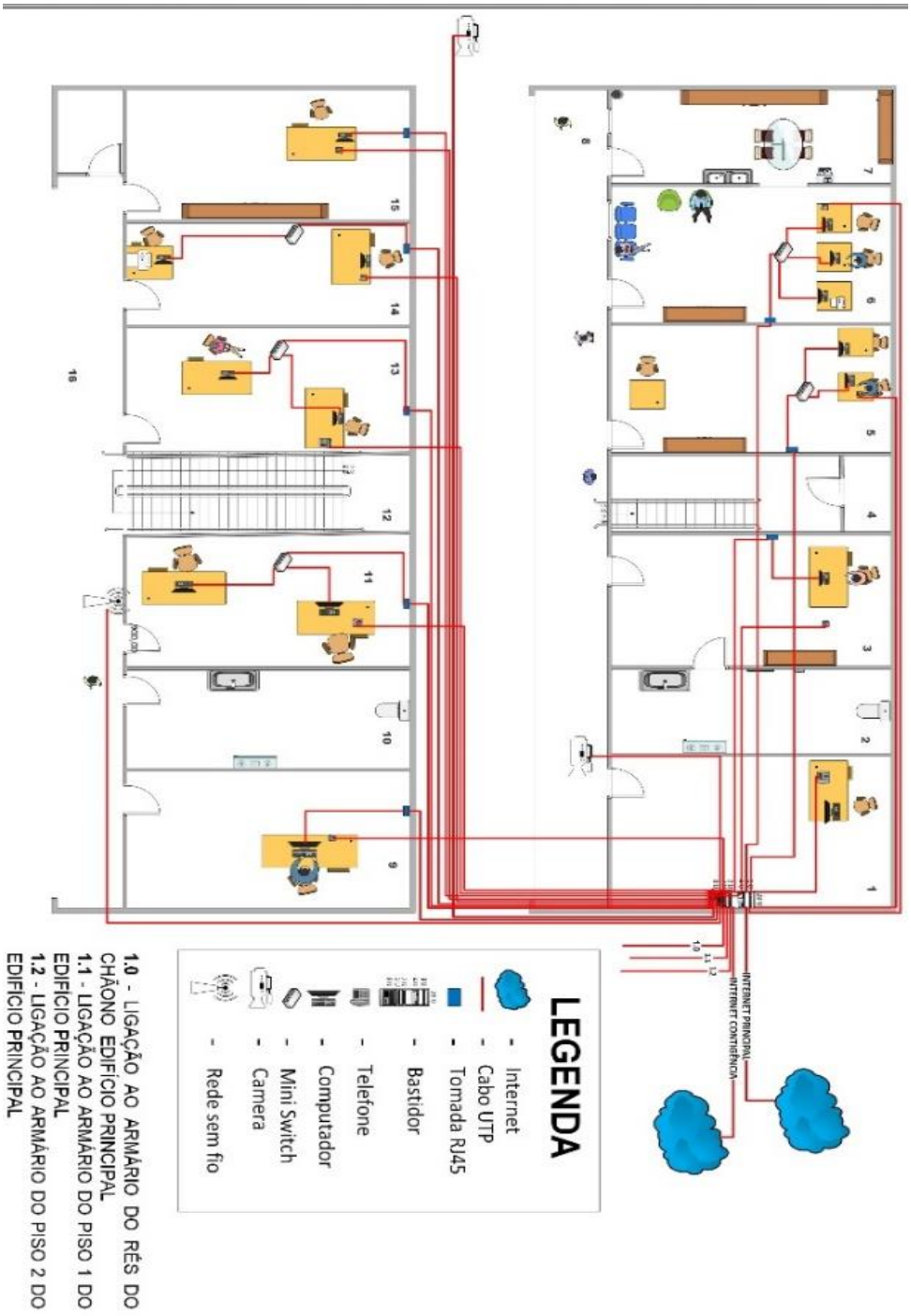


Figura 12 - Alteração do diagrama físico do edifício anexo

Conforme a figura 13, propõem-se a colocação de um Data Center (centro de dados) que é o espaço dedicado à instalação de todos os sistemas de armazenamento de dados, a serem configurados no armário principal, bem como boa parte dos equipamentos activos da rede que permitem a comunicação de dados entre os sistemas existentes e a comunicação desses dados para o exterior, isto é, uma

estrutura que envolve um grande volume de recursos e tecnologias para prover serviços de processamento, onde serão alocados o painel de ligação, modens das provedoras de internet, switch principal e entre outros, para garantir o bom funcionamento da rede.

Propõem-se igualmente a implementação de uma central de telefonia IP no armário principal, feito isso, será possível que os administradores da rede efectuem o gestão das chamadas. Quanto a central de gestão do sistema de CCTV, propõem-se que seja alocada no armário principal, uma vez que para monitoramento do mesmo bastará um computador com acesso a VLAN CCTV e assim aceder a qualquer câmera configurada na rede.

Para a segurança física dos equipamentos propõem-se que a sala de equipamentos tenha acesso limitado, bem como seja instalado sensores de porta aberta e o monitoramento por câmeras de vigilância.

Proposta para o armário principal

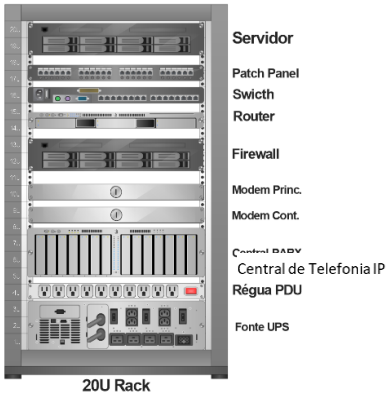


Figura 13 - Proposta para o armário principal

Tabelas de conexão do armário principal

Tabela 5 - Tabela de conexão do armário principal

Tabela de conexão do bastidor principal				
Ocupado por	**Local (Tomada) Painel de Ligação**	**Porta Switch**	**ID Switch**	**VLAN**
RT-PRINCIPAL	P-PRINCIPAL-PL-01	FE0/1	SW-DT-1	50-ADM
SERVIDOR-01	P-PRINCIPAL-PL-02	FE0/2	SW-DT-1	50-ADM
SERVIDOR-VOIP	P-PRINCIPAL-PL-03	FE0/3	SW-DT-1	50-ADM
FIREWALL	P-PRINCIPAL-PL-04	FE0/4	SW-DT-1	50-ADM
MODEM-PRINCIPAL	P-PRINCIPAL-PL-5	FE0/5	SW-DT-1	50-ADM
MODEM-CONTINGENCIA	P-PRINCIPAL-PL-06	FE0/6	SW-DT-1	50-ADM
SW-ED. ANEXO	P-PRINCIPAL-PL-07	FE0/7	SW-DT-1	50-ADM
SW-ED. PRINCIPAL-P0	P-PRINCIPAL-PL-08	FE0/8	SW-DT-1	50-ADM
SW-ED. PRINCIPAL-P1	P-PRINCIPAL-PL-09	FE0/9	SW-DT-1	50-ADM
SW-ED. PRINCIPAL-P2	P-PRINCIPAL-PL-10	FE0/10	SW-DT-1	50-ADM

Legenda: RT – Router; SW – Swicth; Ed – Edifício, P – Painel; PL – Painel de ligação; DT – Distribuição; ADM – Administrador;

Tabela de conexões do armário do edifício anexo

Tabela 6 - Tabela de conexão do edifício anexo

Tabela de conexão do bastidor do edifício anexo				
Ocupado por	**Local (Tomada) Painel de Ligação**	**Porta Switch**	**ID Switch**	**VLAN**
SW-DT-1	P-ANEXO-PL-01	FE0/1	SW - ED.ANEXO	50-ADM
WI-FI-ED-ANEXO	P-ANEXO-PL-02	FE0/2	SW - ED.ANEXO	50-ADM
ED-ANEXO-CCTV1	P-ANEXO-PL-03	FE0/3	SW - ED.ANEXO	40-CCTV
PC-0-ED-ANEXO	P-ANEXO-PL-04	FE0/4	SW - ED.ANEXO	10-RD CAB
PC-1-ED-ANEXO	P-ANEXO-PL-5	FE0/5	SW - ED.ANEXO	10-RD CAB
IP-PHONE-0	P-ANEXO-PL-06	FE0/6	SW - ED.ANEXO	30-VOIP
IP-PHONE-1	P-ANEXO-PL-07	FE0/7	SW - ED.ANEXO	30-VOIP
IMPRESORA-0	P-ANEXO-PL-24	FE0/24	SW - ED.ANEXO	10-RD CAB

Legenda: SW-DT – Swicth de Distribuição; Ed – Edifício, PC – Computador; P – Painel; PL – Painel de ligação; FE – Fast Ethernet; RD CAB – Rede cabeada; ADM – Administrador;

Alteração do diagrama físico do edifício principal piso 0

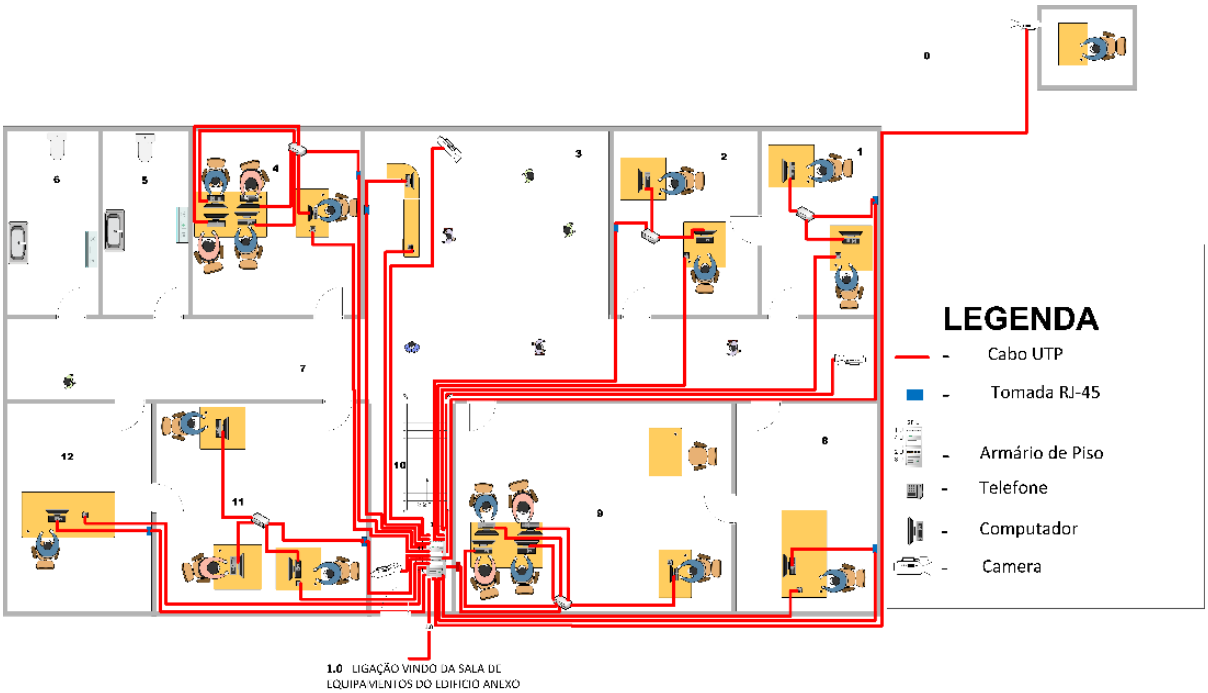


Figura 14 - Alteração do diagrama físico do edifício principal piso 0

Para o piso 0 do edifício principal, propõem-se a instalação de um armário de piso no compartimento nº10, conforme a figura 14, para recepção do sinal vindo do armário principal, de modos a se efectuar o controlo e distribuição eficaz do sinal aos demais equipamentos neste piso. Para atender as solicitações de utilizadores a rede

wireless, será instalado um access point no armário proposto. Para a segurança física do armário propõem-se a instalação de sensores de porta aberta e o monitoramento por câmeras de vigilância.

Proposta para o armário do piso 0.

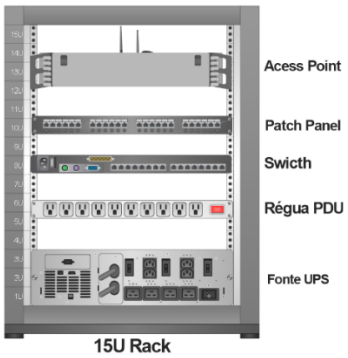


Figura 15 - Proposta para o armário do piso 0 edifício principal

Tabela de conexões do armário do edifício principal piso 0

Tabela 7 - Tabela de conexões do armário do edifício principal piso 0

Tabela de conexão do bastidor do edifício principal piso 0				
Ocupado por	**Local (Tomada) Painel de Ligação**	**Porta Switch**	**ID Switch**	**VLAN**
SW-DT-1	P-PISO 0 - PL-01	FE0/1	SW – ED-P-P0	50-ADM
WI-FI -ED-PRINCIPAL-PISO 0	P-PISO 0 -PL-02	FE0/2	SW – ED-P-P0	50-ADM
ED-P-PISO 0-CCTV2	P-PISO 0 -PL-03	FE0/3	SW – ED-P-P0	40-CCTV
PC-6-ED-P-PISO 0	P-PISO 0 -PL-04	FE0/4	SW – ED-P-P0	10-RD CAB
PC-7-ED-P-PISO 0	P-PISO 0 -PL-5	FE0/5	SW – ED-P-P0	10-RD CAB
IP-PHONE-2	P-PISO 0 -PL-06	FE0/6	SW – ED-P-P0	30-VOIP
IP-PHONE-3	P1-PL-07	FE0/7	SW - ED.ANEXO	30-VOIP

Legenda: SW-DT– Swicth de Distribuição; ED – Edifício; ED-P – Edifício Principal; FE – Fast Ethernet; PC – Computador; P – Painel; PL – Painel de ligação; RD CAB – Rede cabeada; ADM – Administrador;

Alteração do diagrama físico do edifício principal piso 1

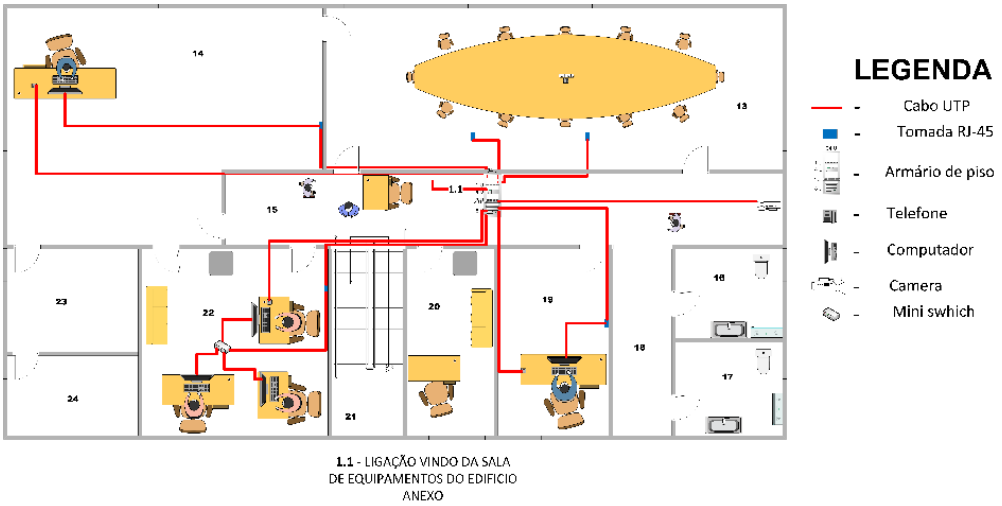


Figura 16 - Alteração do diagrama físico do edifício principal piso 1

As alterações feitas no piso 1, seguiram os mesmos principios do piso 0.

Proposta para o armário do piso 1

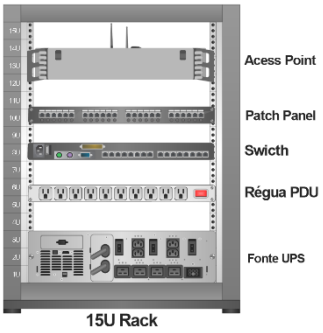


Figura 17 - Proposta para o armário do piso 1 edifício principal

Tabela de conexões do armário do edifício principal piso 1

Tabela 8 - Tabela de conexões do armário do edifício principal piso 1

Tabela de conexão do bastidor do edifício principal piso 1				
Ocupado por	**Local (Tomada) Painel de Ligação**	**Porta Switch**	**ID Switch**	**VLAN**
SW-DT-1	P-PISO 1 - PL-01	FE0/1	SW – ED-P-P1	50-ADM
WI-FI -ED-PRINCIPAL-PISO 1	P-PISO 1 -PL-02	FE0/2	SW – ED-P-P1	50-ADM
ED-P-PISO 1-CCTV3	P-PISO 1 -PL-03	FE0/3	SW – ED-P-P1	40-CCTV
PC-2-ED-P-PISO 1	P-PISO 1 -PL-04	FE0/4	SW – ED-P-P1	10-RD CAB
IMPRESSORA-1-ED-P-PISO 1	P-PISO 1 -PL-05	FE0/5	SW – ED-P-P1	10-RD CAB
IP-PHONE-4	P-PISO 1 -PL-06	FE0/6	SW – ED-P-P1	30-VOIP
IP-PHONE-5	P-PISO 1 -PL-07	FE0/7	SW – ED-P-P1	30-VOIP

Legenda: SW-DT– Swicth de Distribuição; ED – Edifício; ED-P – Edifício Principal; FE – Fast Ethernet; PC – Computador; P – Painel; PL – Painel de ligação; RD CAB – Rede cabeada; ADM – Administrador;

Alteração do diagrama físico do edifício principal piso 2

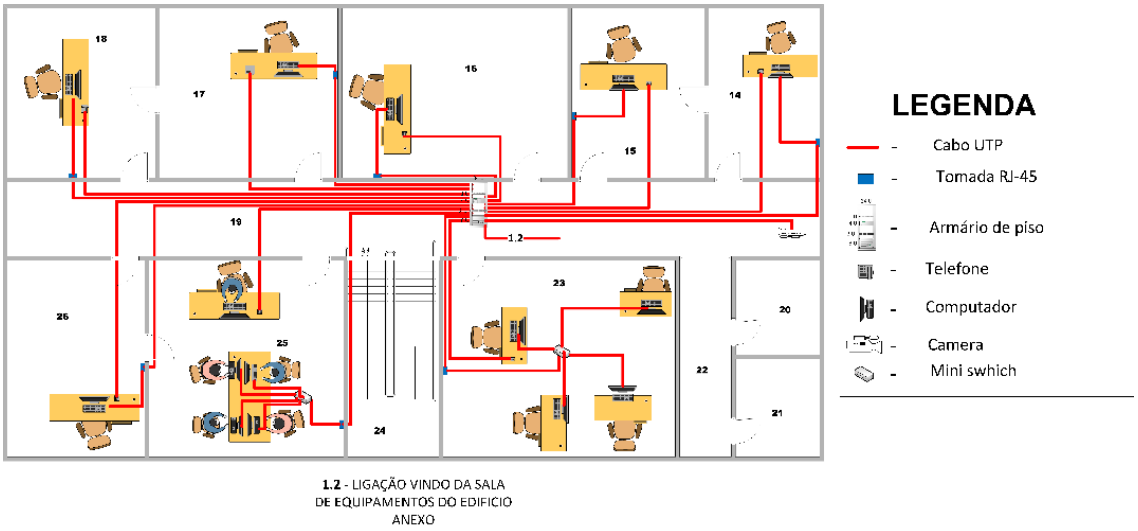


Figura 18 - Alteração do diagrama físico do edifício principal piso 2

Os princípios de alteração do diagrama físico feitas no piso 0 e 1, igualmente foram implementadas no piso 2.

Proposta para o armário do piso 2

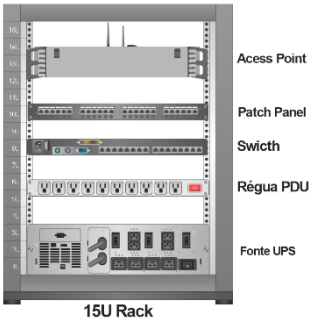


Figura 19 - Proposta para o armário do piso 2 edifício principal

Tabela de conexões do bastidor do edifício principal piso 2

Tabela 9 - Tabela de conexões do armário do edifício principal piso 2

Tabela de conexão do bastidor do edifício principal piso 2				
Ocupado por	**Local (Tomada) Painel de Ligação**	**Porta Switch**	**ID Switch**	**VLAN**
SW-DT-1	P-PISO 2 - PL-01	FE0/1	SW – ED-P-P2	50-ADM
WI-FI -ED-PRINCIPAL-PISO 2	P-PISO 2 -PL-02	FE0/2	SW – ED-P-P2	50-ADM
ED-P-PISO 1-CCTV3	P-PISO 2 -PL-03	FE0/3	SW – ED-P-P2	40-CCTV
PC-9-ED-P-PISO 2	P-PISO 2 -PL-04	FE0/4	SW – ED-P-P2	10-RD CAB
PC-10-ED-P-PISO 2	P-PISO 2 -PL-05	FE0/5	SW – ED-P-P2	10-RD CAB

IP-PHONE-6	P-PISO 2 -PL-06	FE0/6	SW – ED-P-P2	30-VOIP
IP-PHONE-7	P-PISO 2 -PL-07	FE0/7	SW – ED-P-P2	30-VOIP

Legenda: SW-DT– Swicth de Distribuição; ED – Edifício; ED-P – Edifício Principal; FE – Fast Ethernet; PC – Computador; P – Painel; PL – Painel de ligação; RD CAB – Rede cabeada; ADM – Administrador;

Como já temos estado a enfatizar ao longo do trabalho, o nosso projecto de reestruturação teve maior incidência na vertente lógica da rede, desta feita, como se pode constactar nas figuras 14, 16 e 18, as alterações feitas insidiram na subtituição completa da cablagem do CCTV, uma vez que a intenção é migrar do analógico para o digital, os cabos coaxiais usados até o momento serão todos substituídos por cabos UTP e as câmeras analógicas substituídas pelas câmeras IP. Os telefones analógicos serão substituídos por telefones IP, o que levará a substituição das tomadas RJ-11 actualmente existentes pelas RJ-45 que serviram para conectar todos os equipamentos existentes na rede.

A Cablagem anteriormente usada para o sinal de internet será aproveitada para trafegar em simultâneo Imagem, Dados e Voz, (Redes Convergentes).

2.6. Implementação do projecto no Cisco Packet Tracer

Neste ponto serão apresentadas considerações sobre a implementação do projecto, onde foi utilizado o simulador Cisco Packet Tracer, com vista a alcançar os objectivos específicos do presente trabalho científico. Para ter-se uma ideia da implementação da proposta foi usada uma ferramenta de simulação de rede, na qual fez-se as configurações dos serviços propostos na rede, cuja as configuração serão demonstradas nos anexos.

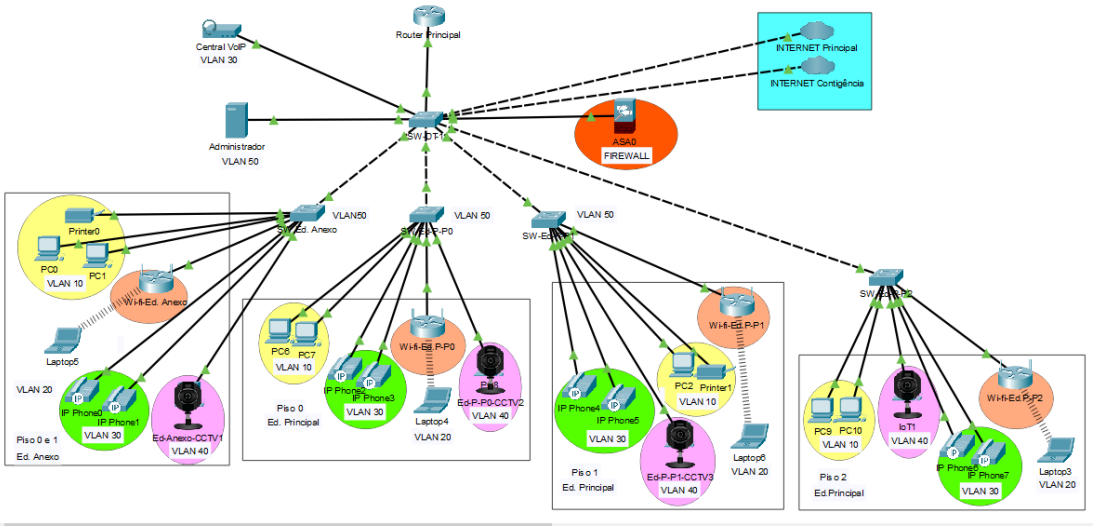


Figura 20 - Implementação do diagrama lógico no cisco packet tracer

CONCLUSÕES

CONCLUSÕES

Dada a natureza do estudo em causa e do campo de acção do mesmo, apresentou-se os principais argumentos literários que derão sustento aos objectivos inicialmente descriminados, na qual as aborgagem incidiram aos principais conceitos de protocolos, serviços de redes e o seu funcionamento convergente que de certo modo é importante numa infra-estrutura de rede e das instituições que fazem o uso destas, bem como a segurança em redes de computadores e a metodologia de projectos para concepção de uma infra-estrututa de rede;

O diagnóstico realizado, permitiu detectar que a rede da Delegação Provincial do MININT/HLA, possui várias inregularidades de cabeamento estruturado, bem como necessita da implementação de configurações de serviços que permitam dinamizar as actividades administrativas e operativas, em caso particular a comunicação entre utilizadores e do plano de segurança da rede lógica e física;

O projecto apresentado, reúne condições de implementação, pois, conforme a metodologia de projecto em foco, trará vários benefícios para a instituição nomeadamente um diagrama lógico com topologia adequada e que proporcione segurança da rede lógica e um fluxo de dados sem interrupções, partilha de recursos e informações, facilidade na comunicação entre os utilizadores, diagrama físico que possibilite mapear e organizar todos equipamentos na rede com base em normas de cabeamento estruturado, bem como a segurança física da rede.

Bibliografia

4infra. (9 de Dezembro de 2022). *O que é top-down*. Acesso em 17 de Setembro de 2023, disponível em 4infra: https://4infra.com.br/o-que-e-top-down/

Albini, L. C. (2014). *Rede de Computadores I.* Paraná.

Alctel. (04 de Fevereiro de 2020). *redes convergentes conheca as suas principais vantagens*. Acesso em 28 de Julho de 2023, disponível em alctel: https://www.alctel.com.br/redes-convergentes-conheca-as-suas-principais-vantagens/

Algar Telecom. (30 de Novembro de 2022). *tecnologia seguranca de rede*. Acesso em 2023 de Julho de 30, disponível em algartelecom: https://blog.algartelecom.com.br/tecnologia/seguranca-de-rede-2/

Alleasy. (03 de Julho de 2018). *seguranca-de-dados*. Acesso em 30 de Julho de 2023, disponível em alleasy: https://alleasy.com.br/seguranca-de-dados/

Amaral, A. F. (2012). *Rede de Computadores.* Colatina.

António, M. S. (2016). *Reestruturação e Optimização da Rede de Computadores dosCaminhos-de-Ferro de Moçâmedes (CFM) – Sede Lubango.* Lubango.

Aragão, J. W., & Neta, M. A. (2017). *Metologia Cientifica.* Salvador.

Aramuni, J. P., & Maia, L. C. (2020). O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa. *toZ: novas práticas em informação e conhecimento*, pp. 7(1), 31-37. Acesso em 29 de Julho de 2023, disponível em https://revistas.ufpr.br/atoz/article/view/64640/40229

Barral, A. O., Cardoso, K. B., & De Souza, J. M. (2018). *Redes Convergentes: VoD Aplicado ao Ensino por meio de implementação de Software Livre.*

Buscape. (09 de Dezembro de 2022). *Vírus no celular: como saber se o smartphone foi infectado*. Acesso em 05 de Novembro de 2023, disponível em Buscape: https://www.buscape.com.br/celular/conteudo/virus-no-celular

Camolacande, A. E., & Monteiro, M. C. (2020). *Projecto de Reestruturação da Rede de Computadores da Escola de Magistério Primário Nº137 do Nambambi - Lubango.* Lubango.

Cassanga , A. P., & Guelepete, L. C. (2023). *Melhoria da Segurança da Rede de Computadores no Instituto Superior de Ciências da Educação da Huíla.*

Cisco. (18 de Novembro de 2020). *network address translation nat*. Acesso em 01 de Agosto de 2023, disponível em Cisco: https://www.cisco.com/c/pt_br/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

Conceição, E. C. (2006). *Redes Locais de Computadores um Visão Global e Prática.* Palmarejo.

Costa, J. (2010). *Apostila de Redes de Computadores.* São Paulo.

Coutinho, T. (13 de Julho de 2023). *Redes de Computadores: sistema capaz de interconectar o mundo*. Acesso em 31 de Dezembro de 2023, disponível em voitto.com: https://www.voitto.com.br/blog/artigo/redes-de-computadores

CXtec. (2022). *O que é o CISCO Adaptive Security Appliance (ASA)?* Acesso em 04 de Novembro de 2023, disponível em CXtec: https://www.cxtec.com/blog/what-is-cisco-asa-security-appliance/

Da Costa, I. F., De Almeida, D. C., De Almeida, B. F., & Perreira, A. F. (11 de Novembro de 2022). Um Estudo Sobre Implementação de um Projecto de Rede Convergente no Âmbito Hospital. pp. 484-494. Acesso em 28 de Julho de 2023, disponível em https://www.periodicorease.pro.br/rease/article/view/7555/2950

Da Silva, M. A. (2022). *Análise e classificação de problemas de transmissão de dados em redes de computadores.*

Dechechi, G. A., Fernado, V., Penha, J. d., Paixão, G. d., de Oliveira, J. C., de Oliveira, P. L., & Rehme, R. (Janeiro/Dezembro de 2020). Segurança da Informação: Um Estudo de Caso. pp. 68-80. Acesso em 29 de Julho de 2023, disponível em http://chamadosfatecpr.com.br/revista/index.php/fatec/article/view/11/24

DEVMEDIA. (2019). *Projeto de redes de computadores: abordagem top-down - Revista Infra Magazine 8*. Acesso em 17 de Setembro de 2023, disponível em DEVMEDIA: https://www.devmedia.com.br/projeto-de-redes-de-computadores-abordagem-top-down-revista-infra-magazine-8/26300

Dias, D. (20 de Agosto de 2012). *modelo de rede hierarquica parte 1 de 2*. Acesso em 29 de Julho de 2023, disponível em Comuntadores: https://www.comutadores.com.br/modelo-de-rede-hierarquica-parte-1-de-2/

Downing, D. A., Covington, M. A., & Covingnton, M. M. (2001). *Dicionário de Termos Informáticos e da Internet* (1ª ed.). Lisboa: Paralelo Editora Lda.

FastFormat. (1 de Agosto de 2018). Acesso em 13 de Junho de 2023, disponível em FastFormat: https://blog.fastformat.co/o-que-e-e-quais-sao-os-metodos-cientificos/

Fernandes, M. (2019). *seguranca de rede*. Acesso em 30 de Julho de 2023, disponível em starti: https://blog.starti.com.br/seguranca-de-rede/

Fontana, F., & Pereira, A. C. (2023). *Pesquisa Documental.* Editora Chefe Profª Drª Antonella Carvalho de Oliveira Assistente Editoral.

Forouzan, B. A. (2010). *Comunicação de Dados e Redes de Computadores* (4ª ed.). São Paulo: AMGH Editora Ltda.

França, M. C. (2010). *Redes de Computadores.*

Grupo Técnico para implementação do SISP - Sistema Integrado de Segurança Pública. (2022). *Implementação do Sistema Integrado de Segurança Pública de Angola sua importância oara a manutençõ da ordem e traquilidade pública.* Luanda.

Heerdt, M. L., & Vilson, L. (2022). *Metodologia científica e da pesquisa: livro didático.*

ISO. (2022). *iso std iso/iec 27002 ed/3 v2 en*. Acesso em 29 de Julho de 2023, disponível em ISO: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en

Júnior, J. F. (11 de Maio de 2023). *Qual é a importância de segurança em redes de computadores?* Acesso em 19 de Abril de 2024, disponível em Linkedin:

https://www.linkedin.com/pulse/qual-%C3%A9-import%C3%A2ncia-de-seguran%C3%A7a-em-redes-computadores-fumo-j%C3%BAnior-

Koche, J. C. (2011). *Fundamentos de Metodologia Cientifica: teoria da ciência e iniciação à pesquisa.* Petrópolis, RJ : Editora Vozes.

Kriger, D. (02 de Fevereiro de 2022). *servidor*. Acesso em 08 de Novembro de 2023, disponível em Kenzie: https://kenzie.com.br/blog/servidor/

Leucotron. (17 de Junho de 2020). *Tipos de PABX: a diferença entre o analógico, digital, IP e híbrido*. Acesso em 08 de 11 de 2023, disponível em Leucotron: https://blog.leucotron.com.br/tipos-de-pabx-a-diferenca-entre-o-analogico-digital-ip-e-hibrido/

Library. (01 de Maio de 2022). Acesso em 29 de Julho de 2023, disponível em Library: https://1library.org/article/modelo-tr%C3%AAs-camadas-cisco-filippetti-ccna-guia-completo.q2933grz

Lima, A. (20 de Fevereiro de 2022). *Importância da Rede de Computadores*. Acesso em 31 de Dezembro de 2023, disponível em acervolima.com: https://acervolima.com/importancia-da-rede-de-computadores/

Lima, Y. F. (2018). *Capitulo I - Introdução às Redes de Computador.*

Luciano, M. L., & do Nascimento, J. V. (2021). PRINCÍPIO E FUNCIONAMENTO DA TECNOLOGIA VOIP. *In Congresso de Tecnologia-Fatec Mococa*, pp. Vol. 4, No. 1. Acesso em 29 de Julho de 2023, disponível em https://congresso.fatecmococa.edu.br/index.php/congresso/article/view/166/60

Manhice, R. O. (2022). *Desenvolvimento de Políticas de Segurança da Informação para Faculdade de Engenharia da UEM (FEUEM).* Maputo.

Marconi, M. d., & Lakatos, E. M. (2001). *Fundamentos de Metodologia Cientifica* (Vol. 4ª). São Paulo: Editora Atlas S. A.

Martins, R. X. (2002). *Introdução a Rede de Computadores.* Varginha, Minas Gerais.

Net, C. (29 de Junho de 2022). *qos quality of service para roteadores e switches*. Acesso em 29 de Julho de 2023, disponível em https://www.controle.net/faq/qos-quality-of-service-para-roteadores-e-switches

Neto, C. C., Vargas, A. A., Chapetta, M. d., & Ferreira, C. T. (2019). ARQUITETURA TCP/IP Empregada em Redes Interconectadas. Acesso em 15 de Junho de 2023, disponível em http://www.revista.universo.edu.br/index.php?journal=1reta2&page=article&op=view&path%5B%5D=7635&path%5B%5D=3792

Oliveira, C. (05 de Fevereiro de 2024). *Estatística Descritiva: uma técnica que não pode faltar na análise exploratória de dados*. Acesso em 19 de Abril de 2024, disponível em Linkedin: https://pt.linkedin.com/pulse/estat%C3%ADstica-descritiva-uma-t%C3%A9cnica-que-n%C3%A3o-pode-na-de-carla-fqc3f

Oliveira, M. F. (2011). *Metodologia Cientifica: um manual para a realização de pesquisas em administração.*

Paula, A. (22 de Julho de 2022). *sistemas de deteccao e prevencao de intrusao*. Acesso em 01 de Agosto de 2023, disponível em pcguia: https://www.pcguia.pt/2022/08/sistemas-de-deteccao-e-prevencao-de-intrusao/

Paula, T. d. (19 de Agosto de 2019). *Técnicas de Amostragem*. Acesso em 30 de Dezembro de 2023, disponível em capcs.uerj.br: http://www.capcs.uerj.br/tecnicas-de-amostragem/

Pocinho, M. (2009). *Estatística Teorias e Exercicios Passo-a-Passo* (Vol. I).

Raymundo, R. T. (10 de Dezembro de 2020). *Técnicas para recolha de dados*. Acesso em 19 de Seetembro de 2023, disponível em Viacarreira: https://viacarreira.com/tecnicas-para-coleta-de-dados/

Ricardo Tombesi Macedo, R. F. (2018). *Redes de Computadores.* Santa Maria: Universidade Federal de Santa Maria.

Roffé, C. R. (2022). *1 Video (37 min e 29 segundos). 2 - Soluções de Cabeamento Estruturado*. Acesso em 02 de Maio de 2023, disponível em publicado no EAD CCNA.

Sabóia , F. R. (2021). *Implementação de uma rede wi-fi infraestruturada para os alunos do IFPI-CATZS.* Acesso em 01 de Agosto de 2023, disponível em

http://bia.ifpi.edu.br:8080/jspui/bitstream/123456789/495/2/2021_tcc_frosaboia.pdf

Sduty CCNA. (Junho de 17 de 2013). *port security*. Acesso em 01 de Agosto de 2023, disponível em study ccna: https://study-ccna.com/port-security/

Services, O. (2019). Acesso em 16 de Maio de 2023, disponível em https://www.opservices.com.br/protocolos-de-rede/

Significados. (2023). Acesso em 23 de Julho de 2023, disponível em Significados: https://www.significados.com.br/link/

Silva, J. F. (14 de Dezembro de 2022). *A Importância das Redes de Computadores para as Empresas*. Acesso em 31 de Dezembro de 2023, disponível em Meu Artigo: https://meuartigo.brasilescola.uol.com.br/informatica/a-importancia-das-redes-de-computadores-para-as-empresas.htm

Silva, R. S. (27 de Dezembro de 2022). *Diferença entre método e técnica de pesquisa social*. Acesso em 30 de Dezembro de 2023, disponível em cafecomsociologia.com: https://cafecomsociologia.com/diferenca-entre-metodo-e-tecnica-de-pesquisa-social/

Stallings, W. (2015). *Criptografia e Segurança de Redes: Princípios e Práticas* (6ª ed.).

Tanenbaum, A. S., & Wetherall , D. (2011). *Redes de Computador* (5ª ed.). São Paulo: Pearson Prentice Hall.

TOTVS. (03 de Abril de 2023). *Governança digital: o que é, objetivos, desafios e mais*. Acesso em 31 de Dezembro de 2023, disponível em totvs.com: https://www.totvs.com/blog/gestao-para-assinatura-de-documentos/governanca-digital/

Transparency, A. (06 de Outubro de 2022). *quais sao algumas vantagens e desvantagens de uma organizacao hierarquica*. Acesso em 28 de Julho de 2023, disponível em Angola Transparency: https://angolatransparency.blog/quais-sao-algumas-vantagens-e-desvantagens-de-uma-organizacao-hierarquica/

Unyleya. (s.d.). *Unyleya*. Acesso em 17 de Maio de 2023, disponível em https://blog.unyleya.edu.br/inicie-sua-carreira/infraestrutura-de-redes/

Vasconcelos, L., & Vasconcelos, M. (2007). *Ligando Micros em Rede.* Rio de Janeiro: Márcio Bergami de Carvalho.

White, C. M. (2012). *Redes de Computadores e Comunicação de Dados.* São Paulo: Cengage Learning.

Xtech. (2017). *Firewall Cisco ASA : Compreendendo os oito comandos básicos*. Acesso em 04 de Novembro de 2023, disponível em Xtech: https://xtech.com.br/Blog/Firewall-Cisco-Asa-Compreendendo-Os-Oito-Comandos-Basicos/b/32/

ANEXOS

ANEXO 1

Instituto Superior De Ciências De Educação da Huíla

ISCED-HUÍLA

Inquérito aos administradores da rede de computadores da Delegação Provincial do MININT/HLA.

Trabalho de Licenciatura a ser desenvolvido por Dinilson Filipe Tiago Tchiwana e José Marcos Luciano, estudantes finalistas do 4º ano do curso de Informática Educativa do ISCED HUÍLA, com o tema "**Reestruturação da Rede de Computadores da Delegação Provincial do Ministério do Interior na Huíla**". Este inquérito tem como objectivo a recolha de informações, para diagnosticar possíveis problemas na rede de computadores da Delegação Provincial do MININT/HLA e sugerir a reestruturação da mesma com a implementação de serviços, não só. Comprometemo-nos a respeitar o anonimato e a confidencialidade dos dados, apenas para estudos académicos, pelo que a identidade será sempre salvaguardada. Agradecemos a vossa colaboração.

Identificação do inquirido

Função/Categoria_____

Questionário

A informação é o activo mais importante de uma instituição e precisa ser protegida de maneira a assegurar a sua integridade, disponibilidade e confidencialidade.

Assinale com um X

1) **Na execução das suas actividades diárias enquanto técnico de rede, tem alguma tarefa que considere bastante desafiadora?**
   a) Sim ☐
   b) Não ☐

   Se sim, qual?

   a) Diagnóstico de problemas na rede ☐
   b) Configuração de serviços na rede ☐
   c) Manutenção preventiva na rede ☐
   d) Manutenção correctiva ☐
   e) Outro ☐
2) **Tem sido possível aceder normalmente a qualquer website quando está conectado à rede da Delegação Provincial do Ministério do Interior na Huíla?**
   a) Sim ☐
   b) Não ☐
3) **Qual é a avaliação que faz do funcionamento do serviço de telefonia em paralelo com os demais serviços da rede?**
   a) Harmonioso ☐
   b) Interferências entre ambos ☐
   c) Outros ☐
4) **Quais são as principais debilidades que já foram possíveis identificar na rede da Delegação Provincial do MININT/HLA?**
   a) Latência ☐
   b) Indisponibilidade de serviços ☐
   c) Carência de equipamentos ☐
   ☐

d) Outro

5) **Na sua opinião, melhorias podem ser feitas na rede da Delegação Provincial do MININT/HLA?**

a) Sim ☐

b) Não ☐

Se sim, quais?

a) Implementação de serviços ☐

b) Aquisição de equipamentos ☐

c) Outro ☐

Muito Obrigado!

ANEXO 2

Instituto Superior De Ciências De Educação da Huíla

ISCED-HUÍLA

Inquérito aos funcionários administrativos da Delegação Provincial do MININT/HLA.

Trabalho de Licenciatura a ser desenvolvido por Dinilson Filipe Tiago Tchiwana e José Marcos Luciano, estudantes finalistas do 4º ano do curso de Informática Educativa do ISCED HUÍLA, com o tema "**Reestruturação da Rede de Computadores da Delegação Provincial do Ministério do Interior na Huíla**". Este inquérito tem como objectivo a recolha de informações, para diagnosticar possíveis problemas na rede de computadores da Delegação Provincial do MININT/HLA e sugerir a reestruturação da mesma com a implementação de serviços, não só. Comprometemo-nos a respeitar o anonimato e a confidencialidade dos dados, apenas para estudos académicos, pelo que a identidade será sempre salvaguardada. Agradecemos a vossa colaboração.

Identificação do inquirido

Função/Categoria_____

Questionário

A informação é o activo mais importante de uma instituição e precisa ser protegida de maneira a assegurar a sua integridade, disponibilidade e confidencialidade.

1) **Com que frequência se conecta a rede da Delegação Provincial do MININT/HLA?**
   a) Todos os dias laborais ☐
   b) Quando necessário ☐
   c) Raramente ☐
2) **Como é que avalia a velocidade da Internet na Delegação Provincial do MININT?**
   a) Muito lenta ☐
   b) Lenta ☐
   c) Normal ☐
   d) Rápida ☐
   e) Muito rápida
3) **Para além de usar a internet, quais as razões que levam a conectar-se a rede?**
   a) Partilha de ficheiros offline com colegas de trabalho ☐
   b) Acesso a dispositivos fisicamente distantes ☐
   c) Outro ☐
4) **Já alguma vez notou alguma anomalia em seu dispositivo depois de ter estado conectado à rede da Delegação Provincial do MININT/HLA?**
   a) Sim ☐
   b) Não ☐

   Se sim, qual?

   a) Lentidão do dispositivo ☐
   b) Dificuldades em aceder aplicações ☐
   c) Aquecimento do dispositivo acima do normal ☐

d) Excesso de anúncios no navegador ☐

5) **Tem sido possível aceder normalmente a qualquer website quando está conectado à rede da Delegação Provincial do MININT/HLA?**

a) Sim ☐
b) Não ☐

6) **Já alguma vez notou uma inexplicável perda de sinal?**

a) Sim ☐
b) Não ☐

Se sim, por quanto tempo?

a) Alguns segundos ☐
b) Alguns minutos ☐
c) Mais de uma hora ☐
d) Vários dias ☐

7) **Já tentou usar a internet enquanto alguém no seu gabinete usava o telefone fixo da rede? Se sim, o que aconteceu?**

a) Sim ☐
b) Não ☐

Se sim, o que aconteceu?

a) Nada ☐
b) Falha na comunicação por voz via telefone ☐
c) Falha no sinal da internet ☐
d) Outro ☐

Muito Obrigado!