ESCUELA POLITÉCNICA DEL EJÉRCITO
EXTENSIÓN LATACUNGA

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

"DISEÑO E IMPLEMENTACIÓN DE UNA RED SEGURA DE DATOS PARA LA DIRECCIÓN DE LA INDUSTRIA AERONÁUTICA DE LA FUERZA AÉREA (DIAF)"

ANGEL TOBÍAS CHICAIZA CRUZ
ALEX SANTIAGO PEREZ VARGAS

TESIS PRESENTADA COMO REQUISITO PREVIO A LA OBTENCIÓN DEL GRADO DE

INGENIERO EN SISTEMAS E INFORMÁTICA

AÑO 2012

ESCUELA POLITÉCNICA DEL EJÉRCITO
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, Ángel Tobías Chicaiza Cruz
Alex Santiago Pérez Vargas

DECLARAMOS QUE:

El proyecto de grado denominado: "DISEÑO E IMPLEMENTACIÓN DE UNA RED SEGURA DE DATOS PARA LA DIRECCIÓN DE LA INDUSTRIA AERONÁUTICA DE LA FUERZA AÉREA (DIAF)" declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y , que se ha consultado las referencias bibliográficas que se incluyen en este documento.
En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto en mención.

Latacunga, 09 de Agosto del 2012

Ángel T. Chicaiza C.	Alex S. Pérez V.
C.I. 1803303609	C.I. 1803880416

ESCUELA POLITÉCNICA DEL EJÉRCITO

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

CERTIFICACIÓN

Se certifica que el presente trabajo fue desarrollado por los Sres. Ángel Tobías Chicaiza Cruz y Alex Santiago Pérez Vargas, bajo nuestra supervisión.

_____

Ing. César Naranjo
DIRECTOR DE PROYECTO

_____

Ing. Patricio Espinel
CODIRECTOR DE PROYECTO

_____

Ing. Santiago Jácome
DIRECTOR DE CARRERA

_____

Dr. Rodrigo Vaca
SECRETARIO ACADEMICO

ESCUELA POLITÉCNICA DEL EJÉRCITO
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Nosotros, Ángel Tobías Chicaiza Cruz
Alex Santiago Pérez Vargas

Autorizamos a la Escuela Politécnica del Ejército la publicidad, en la biblioteca virtual de la Institución del trabajo "DISEÑO E IMPLEMENTACIÓN DE UNA RED SEGURA DE DATOS PARA LA DIRECCIÓN DE LA INDUSTRIA AERONÁUTICA DE LA FUERZA AÉREA (DIAF)", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Latacunga, 09 de Agosto del 2012

Ángel T. Chicaiza C.	Alex S. Pérez V.
C.I. 1803303609	C.I. 1803880416

DEDICATORIA

Primeramente a Dios.

Por el esfuerzo diario y compartido, por las horas de paciencia y compresión, por el apoyo económico y por el infinito amor que tienen los padres para con sus hijos , a mi hija por haberme dado fuerzas para superarme y además ser ella quien me impulsa a ser cada día mejor siendo un ejemplo a seguir y que siempre piense que debe ser superior que su padre, a mi esposa por ser parte de mi vida un soporte en momentos difíciles dedico este proyecto de titulación a ellos, Cumanda, Damaris, Andrea y Ángel que Dios les bendiga mucho.

Este proyecto va dedicado con amor y todo el empeño a todas las personas que han intervenido directamente o indirectamente en mi vida, por eso muchas gracias a todos nunca los defraudare.

Tobías

DEDICATORIA

Mi tesis la dedico con todo amor y cariño.

A ti Dios que me diste la oportunidad de vivir y regalarme una maravillosa familia.

Con mucho cariño principalmente a mis padres que me dieron la vida y han estado conmigo en todo momento. Gracias por todo Papá y Mamá por su comprensión y haberme dado una carrera para mi futuro y por creer en mí, aunque hemos pasados momentos difíciles siempre han estado apoyándome y brindándome todo su amor, por todo esto les agradezco de todo corazón el que estén a mi lado.

A mis hermanos Cristian y Paola, por su constante amor inexplicable para mi superación personal y siempre me han apoyado incondicionalmente.

A todos las personas que de una u otra forma colaboraron por hacer de este sueño una realidad.

A todos ellos
Muchas gracias de todo corazón.

Alex

ÍNDICE

DECLARACIÓN DE RESPONSABILIDAD ii

ESCUELA POLITÉCNICA DEL EJÉRCITO iii

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA iii

CERTIFICACIÓN iii

AUTORIZACIÓN iv

DEDICATORIA v

ÍNDICE vii

RESUMEN 1

SUMMARY 2

CAPÍTULO 1 3

REDES DE DATOS 3

1.1. INTRODUCCIÓN 3

1.2. REDES 4

1.3. COMPONENTES DE REDES 5

1.3.1 Software de Aplicaciones 5

1.3.2 Software de Red 6

1.3.3. Hardware de Red 7

1.4. TIPOS DE REDES 8

1.5. CLASIFICACIÓN POR SU EXTENSIÓN O DISTRIBUCIÓN GEOGRÁFICA 9

1.5.1. Segmento de Red 9

1.5.2. Redes Pan 10

1.5.3. Redes LAN 10

1.5.4. Redes Can 16

1.5.5. Redes Man 17
1.5.6. Redes WAN 18
1.6. CLASIFICACIÓN POR SU DISTRIBUCIÓN LÓGICA 20
1.6.1. Cliente-Servidor 20
1.6.2. Tipo de Servidores 21
1.7. TOPOLOGÍAS 25
1.7.1. Criterios para Establecer una Topología 25
1.7.2. Clasificación de Redes por su Topologías 26
1.8. MEDIOS DE TRANSMISIÓN 34
1.8.1. Medio Guiado 34
1.8.2. Medio No Guiado 41
1.9. DIRECCIONAMIENTO IP 49
1.10. TIPOS DE DIRECCIONES IP 49
1.11. CARACTERÍSTICAS DE LAS REDES DE DATOS 51
1.12. DISPOSITIVOS DE NETWORKING 53
1.13. CLASIFICACIÓN DE DISPOSITIVOS DE NETWORKING 54
1.13.1. Dispositivos de Usuario Final 54
1.13.2. Dispositivos de Red 54
1.14. VENTAJAS Y DESVENTAJAS DE LAS REDES DE DATOS 56
1.15. MODELO OSI (INTERCONEXIÓN DE SISTEMAS ABIERTOS) 58
1.15.1. Capas del Modelo OSI 59
1.16. MODELO TCP/IP 59
1.16.1. Capas del Modelo TCP/IP 59
1.17. SISTEMA DE CABLEADO ESTRUCTURADO 63

1.17.1. Definición 63
1.17.2. Objetivos de un Sistema de Cableado Estructurado 64
1.17.3. Elementos de un Sistema de Cableado Estructurado 65
1.17.4. Especificación Global 65
1.17.5. Certificar Cableado Estructurado 75
1.18. Normas y Estándares 75
1.18.1. ISO 76
1.18.2. IEC 77
1.18.3. CENELEC 77
1.18.4. AS/NZS 77
1.18.5. CSA 77
1.18.6. IEEE 77
1.18.7. ANSI 81
CAPÍTULO 2 82
SEGURIDADES EN REDES 82
2. INTRODUCCIÓN 82
2.1. OBJETIVO DE LAS SEGURIDADES 82
2.1.1. DEFINICIÓN DE LA SEGURIDAD EN REDES 84
2.1.2. CLASIFICACIÓN DE LAS AMENAZAS EN LA SEGURIDAD DE LAS REDES 86
2.1.3. MÉTODOS DE SEGURIDAD PARA LA RED 87
2.1.4. RECOMENDACIONES DE SEGURIDAD PARA LA RED 88
2.2. MECANISMOS DE SEGURIDAD EN LAS REDES 90
2.2.1. ANTIVIRUS 90

2.2.2. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS) 91
2.2.3. REDES VIRTUALES PRIVADAS (VPN) 94
2.2.4. FIREWALLS 95
2.2.5. OTRAS OPCIONES QUE SE PUEDEN IMPLANTAR 96
2.3. VIOLACIONES A LAS SEGURIDADES EN REDES 97
2.3.1. INTRUSOS 97
2.3.2. GUSANOS (WORMS) 97
2.3.3. TROYANOS 98
2.3.4. VIRUS INFORMÁTICOS 99
2.3.5. SPAM (CORREO BASURA) Y SPYWARE (SOFTWARE ESPÍA) 105
2.3.6. CABALLOS DE TROYA 106
2.3.7. CRACKER 107
2.3.8. HACKERS 107
2.3.9. SEÑUELOS 107
2.3.10. SUPERZAPPING 108
2.3.11. PUERTAS FALSAS 108
2.3.12. BOMBAS LÓGICAS 108
2.3.13. VULNERABILIDADES EN REDES 108
2.3.14. Vulnerabilidad en los Sistemas Operativos 109
2.3.15. Vulnerabilidad en los Protocolos de Comunicación 110
2.3.16. Vulnerabilidad en el Protocolo TCP 110
2.3.17. Vulnerabilidad de Kerberos 111
2.3.18. Vulnerabilidad de PKINIT 112
2.3.19. Tipos de Ataques en la Redes 112

2.4. POLÍTICAS DE SEGURIDAD EN LAS REDES 116
2.4.1. GENERALIDADES 117
2.4.2. CONCEPTO 117
2.4.3. OBJETIVO 118
2.4.4. ELEMENTOS DE LAS POLÍTICAS 120
2.4.5. PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD 121
2.4.6. COMPONENTES DE UNA POLÍTICA DE SEGURIDAD 122
2.4.7. ESTRATEGIAS DE SEGURIDAD 123
2.4.8. A QUIENES VAN DIRIGIDAS LAS POLÍTICAS 125
2.5. FIREWALLS 126
2.5.1. INTRODUCCIÓN 126
2.5.2. FUNCIONAMIENO DEL FIREWALL 128
2.5.3. COMPONENTEL FIREWALL 130
2.5.4. CARACTERÍSTICAS DE LOS FIREWALLS 132
2.5.5. VENTAJAS Y DESVENTAJAS EN LOS FIREWALLS 134
2.5.6. POLÍTICAS DE UN FIREWALL 137
2.5.7. TIPOS DE FIREWALLS 137
2.5.8. BENEFICIOS DEL FIREWALL EN EL USO DEL INTERNET 140
CAPÍTULO 3 142
DISEÑO E IMPLEMENTACIÓN DE LA RED PARA LA DIRECCIÓN DE LA INDUSTRIA AERONÁUTICA DE LA FUERZA AÉREA (DIAF). 142
3.1. INTRODUCCIÓN 142
3.2. UBICACIÓN 143
3.3. OBJETIVOS 144

3.4. REQUERIMIENTOS DE LA DIAF 145
3.5. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA DIAF 145
3.5.1. SERVICIOS DE DATOS SOBRE MPLS 147
3.5.2. HARDWARE Y SOFTWARE 148
3.6. PROPUESTA 151
3.7. PRESUPUESTO PARA LA IMPLEMENTACIÓN DE LA RED 152
3.8. DISEÑO DE LA TOPOLOGÍA DE LA RED DE DATOS 154
3.9. DISEÑO DE LA RED 156
3.9.1. SUBSISTEMA ÁREA DE TRABAJO 156
3.9.2. SUBSISTEMA HORIZONTAL 159
3.9.3. SUBSISTEMA CUARTO DE TELECOMUNICACIONES 161
3.9.4. IDENTIFICACIÓN DE LOS PUNTOS DE LA RED 165
3.10. PLANOS DE LOS CENTROS PRODUCTIVOS CIMAM Y CEMA 166
3.10.1. PLANO DEL CENTRO PRODUCTIVO CIMAM 167
3.11. IMPLEMENTACIÓN Y PRUEBAS DE FUNCIONAMIENTO DE LA RED DE DATOS DELL CIMAM 173
3.11.1. IMPLEMENTACIÓN 173
3.11.2. INSTALACIÓN DEL SOFTWARE DE ADMINISTRACIÓN Y SEGURIDAD 180
3.11.3. CONFIGURACIONES 181
3.12. RESUMEN TÉCNICO 188
CAPÍTULO 4 190
CONCLUSIONES Y RECOMENDACIONES 190
4.1. CONCLUSIONES 190

4.2. RECOMENDACIONES 191
BIBLIOGRAFÍA 192
Anexo A: 198
DISEÑO DEL TENDIDO DEL CABLEADO ESTRUCTURADO 198
Anexo B: 204
CONFIGURACIONES EN EL SISTEMA OPERATIVO 204
Pasos para configurar Active Directory 204
Pasos para Configurar Cuentas de Usuario 211
Pasos de Configuración de Grupo 214
Configuración de DNS en Windows 2003 Server 216
Configuración de Recursos Compartidos en Windows 2003 Server 221
Anexo C: 225
Configuración del Outlook en Microsoft Office 2007 226
Configuración de Cuenta de Correo en Outlook 226
Anexo D: 229
Configuración del dispositivo Server Printer 230
Configuración del Server Printer 230
Anexo E: 232
Configuración del Access Point DWL 232
Configuración del Access Point 232
Anexo F: 235
Configuración del Firewall NetCyclón 235
Configuración del Firewall 235
Anexo G: 253

Imágenes del Cableado Estructurado 253

Anexo: H 255

Imágenes del Hangar CIMAM 256

Anexo: I 258

Certificado de Finalización y Aceptación del Proyecto 258

ÍNDICE DE FIGURAS

FIGURA 1. 1: RED DE DATOS 5
FIGURA 1. 2: SOFTWARE DE APLICACIÓN 6
FIGURA 1. 3: SOFTWARE DE RED 7
FIGURA 1. 4: HARDWARE DE RED 8
FIGURA 1. 5: SEGMENTO DE RED DE DATOS 9
FIGURA 1. 6: RED DE DATOS PAN 10
FIGURA 1. 7: RED DE DATOS LAN 11
FIGURA 1. 8: DISPOSITIVOS DE RED DE DATOS 12
FIGURA 1. 9: TECNOLOGÍA ETHERNET 13
FIGURA 1. 10: TECNOLOGÍA TOKEN-RING 14
FIGURA 1. 11: TECNOLOGÍA FDDI 14
FIGURA 1. 12: TECNOLOGÍA ATM 15
FIGURA 1. 13: TECNOLOGÍA FRAME RELAY 16
FIGURA 1. 14: RED DE TIPO CAN 17
FIGURA 1. 15: RED DE DATOS MAN 17
FIGURA 1. 16: RED DE DATOS WAN 18
FIGURA 1. 17: DISPOSITIVOS DE RED DE DATOS WAN 19
FIGURA 1. 18: SERVIDOR DE ARCHIVOS 22
FIGURA 1. 19: SERVIDOR DE IMPRESIÓN 22
FIGURA 1. 20: SERVIDOR DE COMUNICACIONES 23
FIGURA 1. 21: SERVIDOR DE BASE DE DATOS 23
FIGURA 1. 22: SERVIDOR DE CORREO ELECTRÓNICO 24
FIGURA 1. 23: SERVIDOR DE ACCESO REMOTO 24
FIGURA 1. 24: TOPOLOGÍA BUS 27
FIGURA 1. 25: TOPOLOGÍA ESTRELLA 28
FIGURA 1. 26: TOPOLOGÍA ANILLO 29

FIGURA 1. 27: TOPOLOGÍA ÁRBOL 30
FIGURA 1. 28: TOPOLOGÍA MALLA 31
FIGURA 1. 29: TOPOLOGÍA CELULAR 32
FIGURA 1. 30: TOPOLOGÍA AD – HOC 33
FIGURA 1. 31: TOPOLOGÍA INFRAESTRUCTURA 33
FIGURA 1. 32: TOPOLOGÍA MANAGED 34
FIGURA 1. 33: PARTES CABLE COAXIAL 35
FIGURA 1. 34: PARTES CABLE UTP 36
FIGURA 1. 35: PARTES CABLE UTP APANTALLADO 38
FIGURA 1. 36: PARTES CABLE FIBRA ÓPTICA 40
FIGURA 1. 37: TECNOLOGÍAS DE REDES INALÁMBRICAS 42
FIGURA 1. 38: RED LAN INALÁMBRICA 42
FIGURA 1. 39: RED MICROONDAS 43
FIGURA 1. 40: RED SATÉLITE 44
FIGURA 1. 41: RED INFRARROJO 45
FIGURA 1. 42: RED WIMAX 46
FIGURA 1. 43: DISPOSITIVOS DE USUARIO FINAL 54
FIGURA 1. 44: DISPOSITIVOS DE RED 55
FIGURA 1. 45: CAPAS DEL MODELO OSI 59
FIGURA 1. 46: CAPAS DEL MODELO TCP/IP 60
FIGURA 1. 47: ELEMENTOS DE UN SISTEMA DE CABLEADO ESTRUCTURADO 65
FIGURA 1. 48: CABLEADO HORIZONTAL 69
FIGURA 1. 49: CABLEADO BACKBONE 72
FIGURA 1. 50: MAPA CONCEPTUAL DE NORMAS 76

FIGURA 2. 1 : PIRÁMIDE DONDE SE INDICA CÓMO SE ARTICULAN LAS CONTRAMEDIDAS 85
FIGURA 2. 2: PERÍMETRO DE SEGURIDAD 127
FIGURA 2. 3: EL FIREWALL ACTÚA COMO UN PUNTO DE CIERRE QUE MONITOREA Y RECHAZA 129
FIGURA 2. 4: RUTEADOR FILTRA PAQUETES 130
FIGURA 2. 5: GATEWAY A NIVEL-CIRCUITO 131
FIGURA 2. 6: DUAL-HOMED HOST 131

FIGURA 2. 7: SCREENED HOST 132

FIGURA 3. 1: CENTRO PRODUCTIVO CIMAM 143
FIGURA 3. 2: RED IP/MPLS 148
FIGURA 3. 3: SERVIDOR 149
FIGURA 3. 4: ESTACIÓN DE TRABAJO 150
FIGURA 3. 5: SWITCH 150
FIGURA 3. 6: ACCESS POINT 151
FIGURA 3. 7: DIAGRAMA DE ENLACE DE LA RED DE DATOS DIAF 155
FIGURA 3. 8: ÁREA DE TRABAJO 157
FIGURA 3. 9: TOPOLOGÍA DEL CABLEADO HORIZONTAL 159
FIGURA 3. 10: ESQUEMA DE CABLEADO HORIZONTAL 160
FIGURA 3. 11: DISTANCIAS MÁXIMAS PARA EL CABLEADO HORIZONTAL 160
FIGURA 3. 12: RACK 44 UR 162
FIGURA 3. 13: PATCH PANEL DE 24 PUERTOS DE 19 PULGADAS DE ANCHO 163
FIGURA 3. 14: PLANO FÍSICO DE RED CENTRO CIMAM 167
FIGURA 3. 15: PLANO FÍSICO DE RED HANGARCIMAM 168
FIGURA 3. 16: PLANO FÍSICO DE RED HANGAR CEMA 171
FIGURA 3. 17: CANALETA DOBLE INSTALADA EN EL CIMAM 174
FIGURA 3. 18: INSTALACIÓN DE CABLES PARA EL SISTEMA ELÉCTRICO 174
FIGURA 3. 19: INSTALACIÓN DEL CABLE UTP CAT 5E 175
FIGURA 3. 20: INSTALACIÓN DE FACEPLATES Y PONCHADO DE JACK . 176
FIGURA 3. 21: INSTALACIÓN DE CABLE UTP EN EL PATCH PANEL Y PONCHADORA 177
FIGURA 3. 22: EQUIPO PROBADOR DE CABLE REMOTO 178
FIGURA 3. 23: EQUIPO CERTIFICADOR AGILENT WIRESCOPE 350 179

FIGURA 3. 24: PANTALLA QUE SE VISUALIZA EN EL EQUIPO DE CERTIFICACIÓN. 180

ÍNDICE DE TABLAS

TABLA 1. 1: TECNOLOGÍAS DE REDES WAN 20
TABLA 1. 2: DISTANCIAS PERMITIDAS ENTRE DISPOSITIVOS EN FUNCIÓN AL TIPO DE CABLEADO. 38
TABLA 1. 3: TECNOLOGÍAS INALÁMBRICAS 48
TABLA 1. 4: PROTOCOLO IPV4 Y IPV6 51
TABLA 1. 5: COMPARATIVO ENTRE MODELOS DE REFERENCIA OSI VS TCP/IP 60
TABLA 1. 6: CARACTERÍSTICAS, VENTAJAS Y DESVENTAJAS DE LOS MODELOS OSI Y TCP/IP 62

TABLA 3. 1: DISTRIBUCIÓN DEPARTAMENTO CIMAM 144
TABLA 3. 2: DISTRIBUCIÓN DEPARTAMENTO CEMA 144
TABLA 3. 3: CARACTERÍSTICAS DEL SERVIDOR 148
TABLA 3. 4: PRESUPUESTO PARA LA IMPLEMENTACIÓN DE LA RED 153
TABLA 3. 5: DISTRIBUCIÓN DE PUNTOS DE RED EN EL CENTRO CIMAM 157
TABLA 3. 6: DISTRIBUCIÓN DE PUNTOS DE RED EN EL CENTRO CEMA 158
TABLA 3. 7: RESUMEN DE LOS MATERIALES PARA CABLEADO ESTRUCTURADO 163
TABLA 3. 8: PUNTOS DE DATOS, NOMENCLATURA, DISTANCIA APROXIMADA Y DIRECCIONES IP 165
TABLA 3. 9: HARDWARE CENTRO CIMAM 169
TABLA 3. 10: SOFTWARE CENTRO PRODUCTIVO CIMAM 170

TABLA 3. 11: HARDWARE CENTRO CEMA.....171
TABLA 3. 12: SOFTWARE CENTRO PRODUCTIVO CEMA 172

RESUMEN

El presente trabajo tiene como finalidad describir de forma detallada la investigación que se llevó a cabo en lo que respecta al DISEÑO E IMPLEMENTACIÓN DE UNA RED SEGURA DE DATOS PARA LA DIRECCIÓN DE LA INDUSTRIA AERONÁUTICA DE LA FUERZA AÉREA (DIAF), que se consigue compartir información entre sus dependencias, disponer la conectividad de equipos informáticos, los usuarios pueden intercambiar información y los departamentos pueden cumplir con los servicios ofertados, generando gran cantidad de información que siempre se halla disponible en el momento requerido, produciendo que la alta gerencia experimente facilidades para tomar decisiones oportunas y adecuadas.

Este documento a la vez servirá de guía para informar sobre el Sistema de Red de Datos de los Centros Productivos CIMAM y CEMA. El desarrollo de este proyecto de investigación se lo ha realizado por capítulos los cuales se detallan su contenido a continuación:

Capítulo I, se detalla información referente a Redes de Datos, como su introducción, definición, tipos de redes, características y estructuras de las redes, ventajas y desventajas, redes inalámbricas, topologías, estándares de redes.

Capítulo II, se explica las seguridades en las redes, describiendo: introducción, mecanismos de seguridades en la red, violaciones a las seguridades, políticas, firewalls.

En el capítulo III referente al Diseño e Implementación de la Red se detalla cada uno de las fases utilizadas para implementar la red como: análisis de la situación actual de la DIAF, Diseño de la Topología de la Red implementado con el Sistema de Seguridad, Implementación de la Red, Instalación del software de Administración, Configuraciones, Pruebas, Resumen Técnico General del Sistema de Seguridad.

Capítulo IV, están las conclusiones y recomendaciones que se han obtenido de acuerdo a este estudio.

SUMMARY

This paper aims to describe in detail there search conducted in regard to DESIGN AND IMPLEMENTATION OF ASECURE NETWORK ADDRESS DATA FOR AVIATION INDUSTRY OF THE AIR FORCE (DIAF), which is achieved by sharing information between their agencies, have computer connectivity, users can exchange information and departments can carry out the services offered, and generating large amount of information is always available when required, leading to top management experience facilities timely and appropriate decisions.

This document will guide both to inform the Data Network System Centers CIMAM Productive and CEMA. The development of this research project it has been done by chapter which are listed the contents below:

Chapter I is detailed information on Data Networks, as its introduction, definition, types of networks, characteristics and network structures, advantages and disadvantages, wireless networks, topologies, network standards.

Chapter II explains the assurances in the networks, describing: Introduction, assurance mechanisms in the network, securities violations, policies, and firewalls.

In Chapter III relating to Design and Implementation of Network detailing each of the phases used to implement the network as: analysis of the current situation DIAF Design of Network Topology implemented with the Security System, Implementation of the Network Management Software Installation, Configuration, Testing, and Technical Summary General Security System.

Chapters IV are the conclusions and recommendations that have been obtained according to this study.

CAPÍTULO 1

REDES DE DATOS

1.1. INTRODUCCIÓN

El desarrollo del hombre desde el nivel físico de su evolución, pasando por su crecimiento en las áreas sociales y científicas hasta llegar a la era moderna se ha visto apoyado por herramientas que extendieron su funcionalidad y poder como ser viviente. Sintiéndose consciente de su habilidad creativa, metódicamente elaboró procedimientos para organizar su conocimiento, sus recursos y manipular su entorno para su comodidad, impulsando las ciencias y mejorando su nivel de vida a costo de sacrificar el desarrollo natural de su ambiente, produciendo así todos los adelantos que un gran sector de la población conoce: automóviles, aeroplanos, trasatlánticos, teléfonos, televisiones[1], etc.

En el transcurso de todo este desarrollo, también evolucionó dentro del sector tecnológico el cómputo electrónico. Este nació con los primeros ordenadores en la década de los años 40, porque la necesidad del momento era extender la rapidez del cerebro humano para realizar algunos cálculos aritméticos y procedimientos repetitivos. Este esfuerzo para continuar avanzando, se reflejó en el desarrollo de las redes de datos.

Las Redes de Datos han tenido grandes avances a través del tiempo, hasta nuestros días con los avances de la informática, que hoy hace posible la comunicación por internet.

[1] http://www.monografias.com/trabajos40/redes-informaticas/redes-informaticas.shtml

Estos avances traen grandes ventajas a las empresas e instituciones, no existe la menor duda que el avance de la tecnología y de los medios de transporte, han permitido que cada día el mundo sea más accesible. Las nuevas características de los mercados financieros, la Tecnología de la Información y Telecomunicaciones (Tics) permiten que los principales mercados financieros y bursátiles del mundo se comuniquen en forma instantánea y que los operadores puedan efectuar sus operaciones como si estuvieran en los recintos y con la seguridad que le ofrecen las Telecomunicaciones[2].

El desarrollo de la computación y su integración[3] con las telecomunicaciones en la Informática han propiciado el surgimiento de nuevas formas de comunicación, que son aceptadas cada vez por más personas. El desarrollo de las redes informáticas posibilito su conexión mutua y finalmente, la existencia de Internet, una red de redes gracias a la cual, una computadora puede intercambiar fácilmente información con otras situadas en regiones lejanas del planeta.

1.2. REDES

Una red es un conjunto de dispositivos físicos (hardware) y de programas (software), mediante la cual se puede comunicar computadoras para compartir recursos (discos, impresoras, programas, etc.) así como trabajo (tiempo de cálculo, procesamiento de datos etc.), su objetivo es hacer que todos los programas, datos, video, voz y equipos estén disponibles para cualquier miembro de la red que así lo solicite, sin importar la localización física del recurso y del usuario tomando en cuenta medidas de seguridad.

[2] Es una técnica que consiste en la transmisión de un mensaje desde un punto hacia otro, usualmente con la característica adicional de ser bidireccional. La telefonía, la radio, la televisión y la transmisión de datos a través de computadoras son parte del sector de las telecomunicaciones.
[3] http://monografias.com/trabajos15/computadoras.shtml

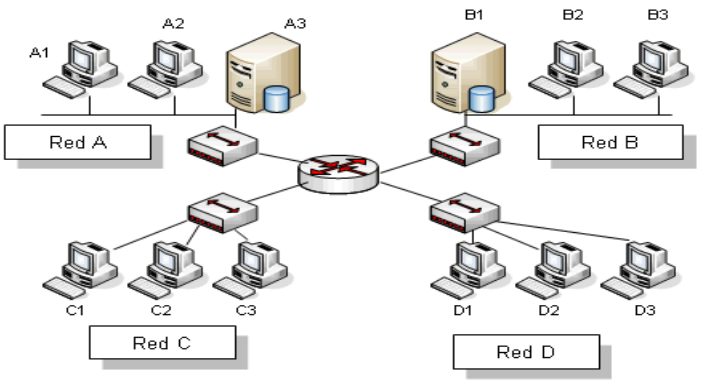


Figura 1. 1: Red de Datos

1.3. COMPONENTES DE REDES

Los componentes de una red son elementos que cumplen funciones específicas como la conexión entre varias estaciones de trabajo, y se utilizan dependiendo de las características físicas (hardware) que tienen. Para poder formar una red de datos se requieren de tres niveles de componentes:

1.3.1 Software de Aplicaciones

Está formado por programas informáticos que se comunican con los usuarios de la red y permiten compartir información (archivos de bases de datos, de documentos, gráficos, vídeos, etc.) y recursos (impresoras, unidades de disco, etc.).

Un tipo de software de aplicaciones se denomina cliente-servidor. Las computadoras cliente envían peticiones de información o de uso de recursos a otras computadoras, llamadas servidores, que controlan el flujo de datos y la ejecución de las aplicaciones a través de la red.

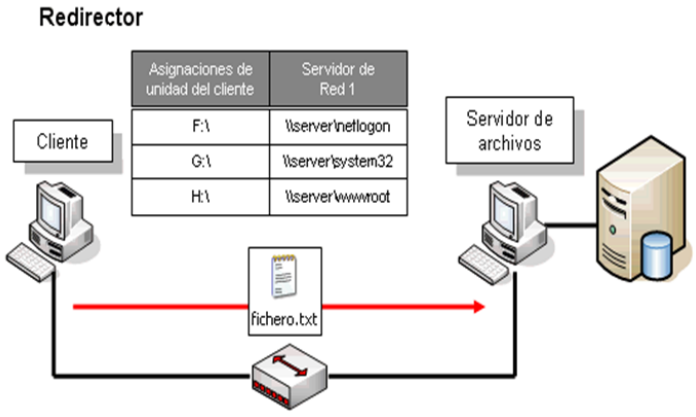


Figura 1. 2: Software de Aplicación

1.3.2 Software de Red

Consiste en programas informáticos que establecen protocolos o normas, para que las computadoras se comuniquen entre sí. Estos protocolos se aplican enviando y recibiendo grupos de datos formateados denominados paquetes. Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigir el movimiento de paquetes a través de la red física y minimizar las posibilidades de colisión[4] entre paquetes enviados simultáneamente.

[4] Colisión.- Situación que ocurre cuando dos o más dispositivos intentan enviar una señal a través de un mismo canal al mismo tiempo.

Figura 1. 3: Software de Red

1.3.3. Hardware de Red

Está formado por los componentes físicos que enlazan las computadoras. Dos componentes importantes son los medios de transmisión que transportan las señales de los ordenadores (cables estándar o de fibra óptica, aunque también hay redes sin cables que realizan la transmisión por infrarrojos o por radiofrecuencia) y el adaptador de red, que permite acceder al medio físico que conecta a los ordenadores, recibir paquetes desde el software de red y transmitir instrucciones y peticiones a otras computadoras. La información se transfiere en forma de dígitos binarios o bits (uno y cero), que pueden ser procesados por los circuitos electrónicos de los ordenadores.

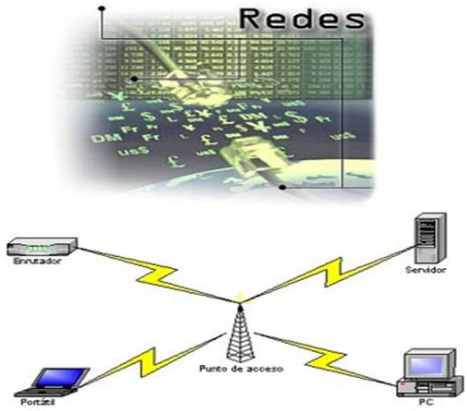


Figura 1. 4: Hardware de Red

1.4. TIPOS DE REDES

En el mundo de las Telecomunicaciones existen varios tipos de redes que se clasifican de la siguiente manera:

- **Redes de Datos.-** Compañías de beepers, compañías celulares de datos (SMS), proveedores de Internet, Voz paquetizada (VoIP).
- **Redes de Video.-** Compañías de cable TV, Estaciones televisoras.
- **Redes de Voz.-** Compañías telefónicas, compañías celulares.
- **Redes de Audio.-** Rockolas digitales, audio por Internet, música por satélite.
- **Redes de Multimedia.-** Compañías que explotan voz, datos, video simultáneamente.

Existen varios tipos de redes, las cuales se clasifican de acuerdo a su extensión, distribución lógica y topologías.

1.5. CLASIFICACIÓN POR SU EXTENSIÓN O DISTRIBUCIÓN GEOGRÁFICA

Las Redes de computadoras se clasifican por su extensión física en que se ubican sus componentes, desde una aula hasta una ciudad, un país o incluso el planeta. Dicha clasificación determinará los medios físicos y protocolos requeridos para su operación, por ello se ha definido seis tipos:

1.5.1. Segmento de Red

Es definido como el hardware o una dirección de red especificada, por ejemplo en un segmento de red se puede incluir todas las estaciones de trabajo conectadas a una tarjeta de interfaz de red de un servidor.

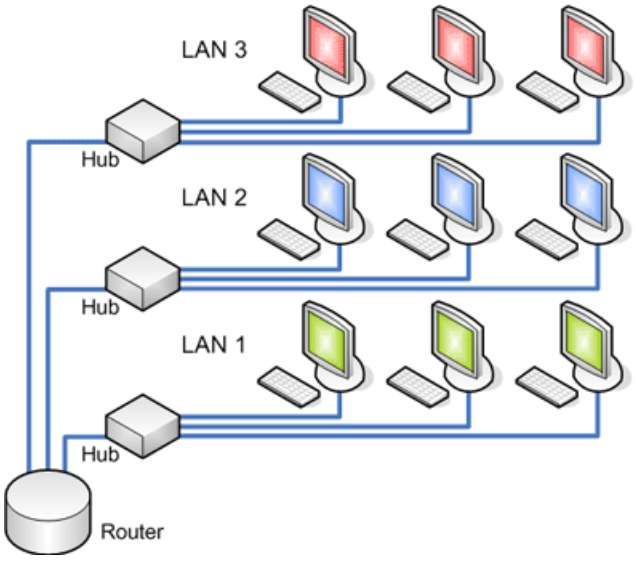


Figura 1. 5: Segmento de Red de Datos

1.5.2. Redes PAN

Las Redes PAN (Red de Administración Personal).-Son redes pequeñas, las cuales están conformadas hasta por ocho equipos, por ejemplo: un café internet.

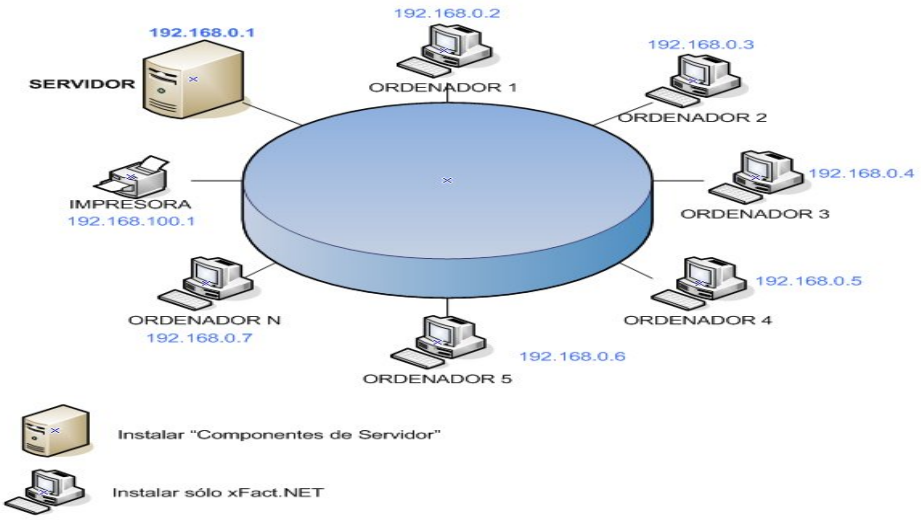


Figura 1. 6: Red de Datos Pan

1.5.3. Redes LAN

Las Redes LAN (Redes de área local).- Es un segmento de red que tiene conectadas estaciones de trabajo y servidores o un conjunto de segmentos de red interconectados, generalmente dentro de una misma zona, por ejemplo: un edificio.

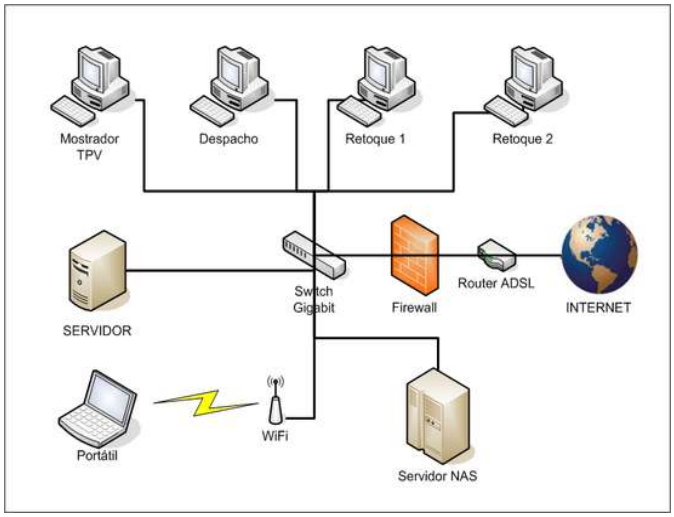


Figura 1. 7: Red de Datos LAN

Características

- Están restringidas en tamaño, las computadoras se distribuyen dentro de la LAN para obtener mayor velocidad en las comunicaciones dentro de un conjunto de edificios.

- Tienen diversas topologías. La topología o la forma de conexión de la red, depende de algunos aspectos como la distancia entre las computadoras y el medio de comunicación entre ellas ya que este determina la velocidad del sistema.

Dispositivos de Redes LAN

Los dispositivos de Redes LAN y los medios son los elementos físicos o hardware de la red, que tienen como objetivo transmitir y recibir información. El hardware es generalmente el componente visible de la plataforma de red, como una computadora portátil o personal, un Switch, o el cableado que se usa para conectar estos

dispositivos. Estos dispositivos constituyen la interfaz entre la red humana y la red de comunicación subyacente.

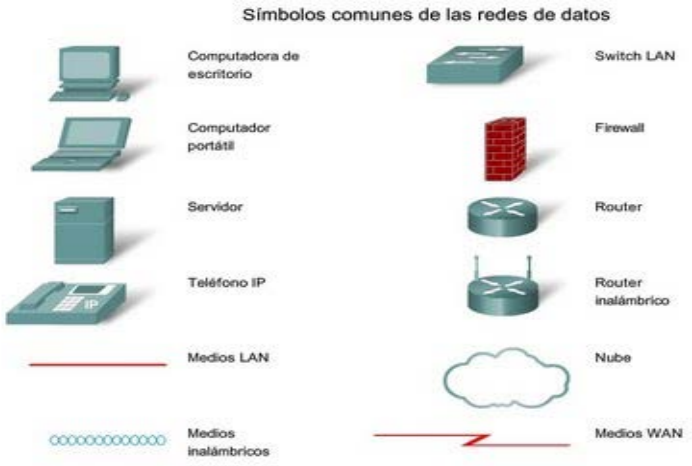
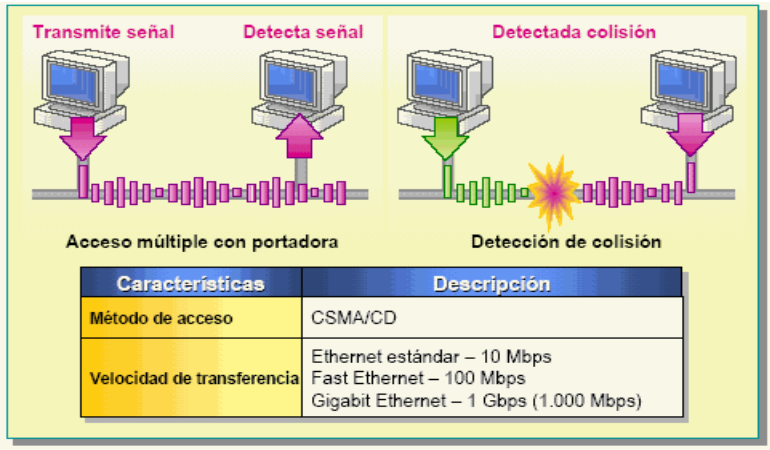


Figura 1. 8: Dispositivos de Red de Datos

Las tecnologías que se utilizan en las Redes LAN son:

a. **Ethernet.-** El protocolo de red Ethernet fue diseñado originalmente por Digital, Intel y Xerox por lo cual, la especificación original se conoce como Ethernet DIX. Posteriormente, IEEE ha definido el estándar Ethernet 802.3. Es el método de conexión más extendido en la actualidad. La velocidad de transmisión de datos en Ethernet es de 10Mbits/s. En el caso del protocolo Ethernet/IEEE 802.3, el acceso al medio se controla con un sistema conocido como CSMA/CD (Carrier Sense Multiple Access with Collision Detection, Detección de Portadora con Acceso Múltiple y Detección de Colisiones), cuyo principio de funcionamiento consiste en que una estación, para transmitir, debe detectar la presencia de una señal portadora y, si existe, comienza a transmitir. Si dos estaciones empiezan a transmitir al mismo tiempo, se produce una colisión y ambas deben repetir la transmisión, para lo cual esperan un tiempo aleatorio antes de repetir, evitando de

este modo una nueva colisión, ya que ambas no seleccionarán el mismo tiempo de espera.



Características	Descripción
Método de acceso	CSMA/CD
Velocidad de transferencia	Ethernet estándar – 10 Mbps Fast Ethernet – 100 Mbps Gigabit Ethernet – 1 Gbps (1.000 Mbps)

Figura 1. 9: Tecnología Ethernet

Hoy en día se puede hacer la siguiente clasificación de las redes de protocolo Ethernet:

- Ethernet: Hasta 10 Mbps.
- Fast Ethernet: Hasta 100 Mbps.
- Gigabit Ethernet: Hasta 1000 Mbps.
- 10 Gigabit Ethernet.

b. Token Ring.- Las redes basadas en protocolos de paso de testigo (Token passing) basan el control de acceso al medio en la posesión de un testigo. Éste es un paquete con un contenido especial que permite transmitir a la estación que lo tiene. Cuando ninguna estación necesita transmitir, el testigo va circulando por la red de una a otra estación. Cuando una estación transmite una determinada cantidad de información debe pasar el testigo a la siguiente. Las redes de tipo

Token ring tienen una topología en anillo y están definidas en la especificación IEEE 802.5 para la velocidad de transmisión de 4 Mbps.

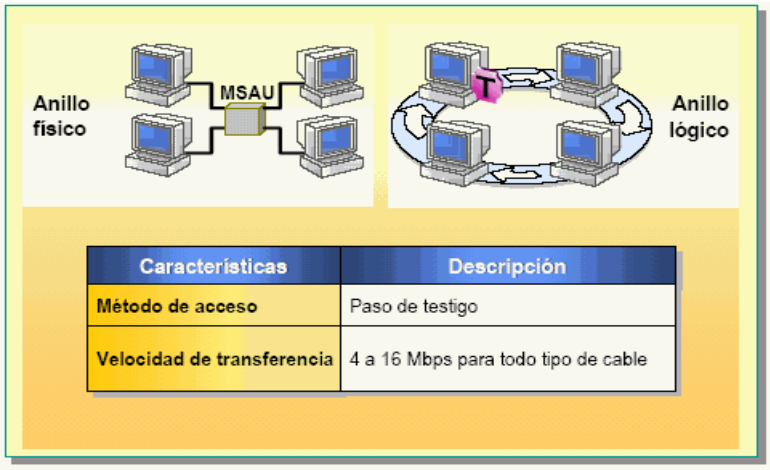


Figura 1. 10: Tecnología Token-Ring

c. FDDI (Fiber Distributed Data Interface). -Es una especificación de red sobre fibra óptica con topología de doble anillo, control de acceso al medio por paso de testigo y una velocidad de transmisión de 100 Mbits/s. Esta especificación estaba destinada a sustituir a la Ethernet pero el retraso en terminar las especificaciones por parte de los comités y los avances en otras tecnologías, principalmente Ethernet, la han relegado a unas pocas aplicaciones como interconexión de edificios.

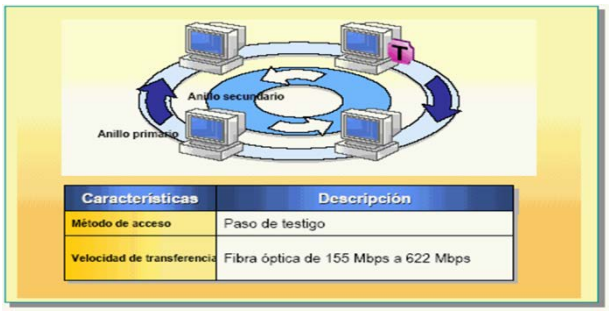
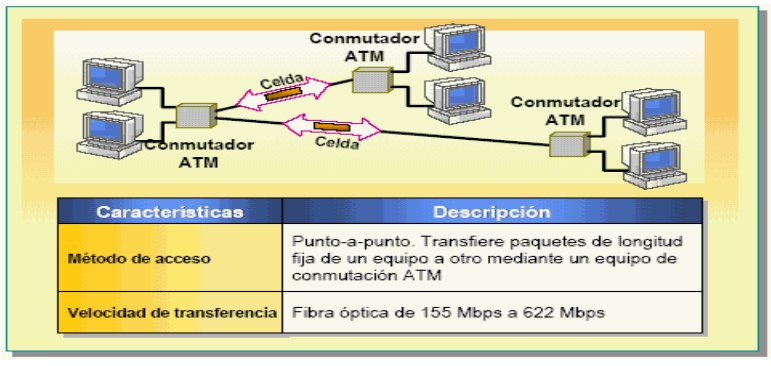


Figura 1. 11: Tecnología FDDI

d. ATM (Modo de Transferencia Asincrónica).- Es una red de conmutación de paquetes que envía paquetes (celdas atm) de longitud fija a través de Lans o Wans, en lugar de paquetes de longitud variable utilizados en otras tecnologías. Los paquetes de longitud fija, o celdas, son paquetes de datos que contienen únicamente información básica de la ruta, permitiendo a los dispositivos de conmutación enrutar el paquete rápidamente. La comunicación tiene lugar sobre un sistema punto-a-punto que proporciona una ruta de datos virtual y permanente entre cada estación. Una red ATM utiliza el método de acceso PUNTO-A-PUNTO, que transfiere paquetes (celdas ATM) de longitud fija de un equipo a otro mediante un equipo de conmutación ATM. El resultado es una tecnología que transmite un paquete de datos pequeño y compacto a una gran velocidad. En una red ATM se encuentra entre 155 y 622 Mbps.

Su alta velocidad permite transmitir voz, vídeo en tiempo real, audio con calidad CD, imágenes y transmisiones de datos del orden de megabytes.

Utilizando ATM, se puede enviar datos desde una oficina principal a una ubicación remota. Los datos viajan desde una LAN sobre una línea digital a un conmutador ATM y dentro de la red ATM. Pasa a través de la red ATM y llega a otro conmutador ATM en la LAN de destino.



Características	Descripción
Método de acceso	Punto-a-punto. Transfiere paquetes de longitud fija de un equipo a otro mediante un equipo de conmutación ATM
Velocidad de transferencia	Fibra óptica de 155 Mbps a 622 Mbps

Figura 1. 12: Tecnología ATM

e. **FRAME RELAY.**-Es una red de conmutación de paquetes que envía paquetes de longitud variable sobre Lans o Wans, los paquetes de longitud variable, o tramas, son paquetes de datos que contienen información de direccionamiento adicional y gestión de errores necesaria para su distribución. Frame Relay utiliza un método de acceso punto-a-punto, que transfiere paquetes de tamaño variable directamente de un equipo a otro, en lugar de entre varios equipos y periféricos, permite una transferencia de datos que puede ser tan rápida como el proveedor pueda soportar a través de líneas digitales. Ha sido especialmente adaptado para velocidades de hasta 2.048 Mbps, aunque nada le impide superarlas.

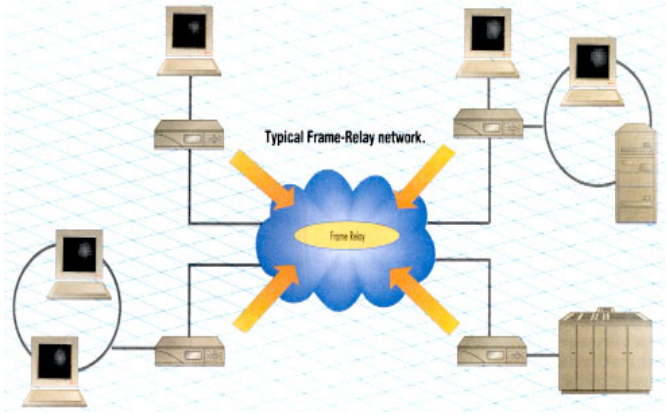


Figura 1. 13: Tecnología FRAME RELAY

1.5.4. Redes CAN

Las Redes CAN (Red de área de Campus).- Es una colección de LANs dispersadas geográficamente dentro de un campus universitario, oficinas de gobierno o industrias pertenecientes a una misma entidad en un área delimitada en kilómetros.

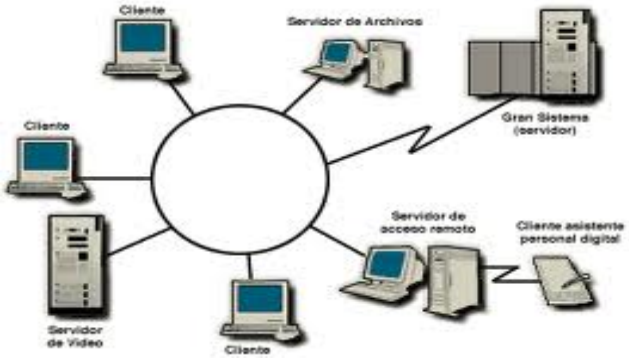


Figura 1. 14: Red de Tipo CAN

1.5.5. Redes MAN

Las Redes MAN (Redes de área Metropolitana).- Comprenden una ubicación geográfica determinada "ciudad, municipio", los enlaces se realizan mediante diversas instalaciones públicas y privadas como el sistema telefónico o los suplidores de sistemas de comunicación por microondas o medios ópticos y su distancia de cobertura es mayor de 4kmts.

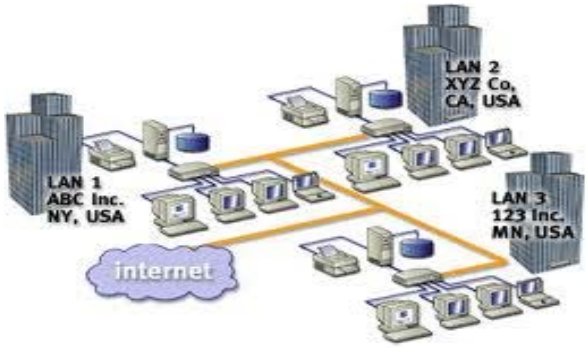


Figura 1. 15: Red de Datos MAN

Características

- Se extienden sobre áreas geográficas de tipo urbano, como una ciudad.
- Son implementadas por los proveedores de servicio de Internet.

- Estas redes son de alto rendimiento.

1.5.6. Redes WAN

Las RedesWAN (Redes de área Extensa).- Son redes punto a punto que interconectan países y continentes. Al tener que recorrer una gran distancia sus velocidades son menores que en las LAN aunque son capaces de transportar una mayor cantidad de datos. El alcance es una gran área geográfica, los enlaces se realizan con instalaciones de telecomunicaciones públicas y privadas además por microondas y satélites como por ejemplo: un país o un continente.

Figura 1. 16: Red de Datos WAN

Características

- Su uso de comunicación es privada.
- Posibilidades de conectarse con otras redes.
- La transmisión de datos es generalmente por fibra óptica[5] y satélites.

[5] Es un conductor de ondas en forma de filamento, generalmente de vidrio o de materiales plásticos. La fibra óptica es capaz de dirigir la luz, emitida por un láser o un LED, a lo largo de su longitud usando la reflexión total interna.

Dispositivos de Redes WAN

Cada computadora necesita el "hardware" para transmitir y recibir información. Es el dispositivo que conecta la computadora u otro equipo de red con el medio físico.

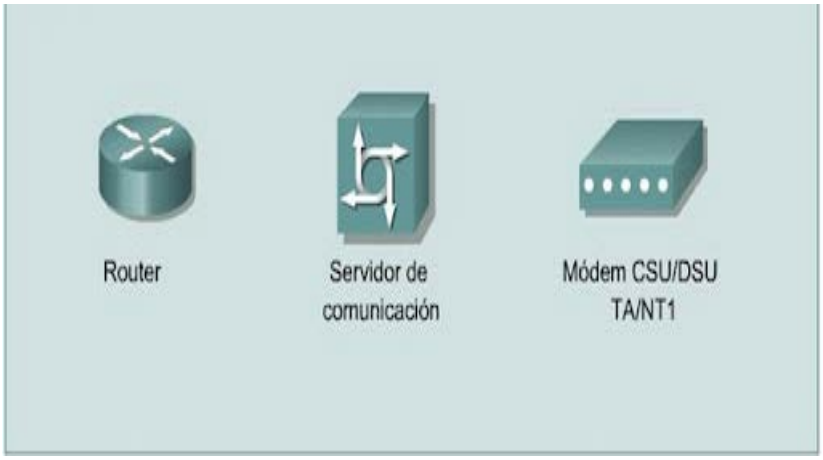


Figura 1. 17: Dispositivos de Red de Datos WAN

La tecnología de redes es utilizada actualmente para ofrecer un servicio veloz y eficiente. Las diferentes tecnologías de redes ofrecen ventajas para los usuarios. Varían en su velocidad de transferencia y el método de acceso que utilizan.

La tecnología de conexión que se utiliza en WAN son:

- Módems
- Red Digital de Servicios Integrados (RDSI)
- Línea de Suscripción digital (DSL-Digital Subscribe Line)
- Frame Relay

Tabla 1. 1: Tecnologías de Redes WAN

Tipo de Servicio WAN	Usuario Típico	Ancho de Banda
Modem	Individuos	56 Kbps = 0,056 Mbps
RDSI	Pequeñas instituciones (escuelas), WAN confiables	128 Kbps = 0,128 Mbps
Frame Relay	Entidades de mayor envergadura	56 Kbps - 1544 Kbps = 0,056 Mbps - 1,544 Mbps
T1	Entidades de mayor envergadura	1,544 Mbps
T3	Entidades de mayor envergadura	44,736 Mbps
E1	Entidades de mayor envergadura	2,048 Mbps
E3	Entidades de mayor envergadura	34,368 Mbps
STS-1 (OC-1)	Compañías telefónicas; backbones de las empresas de transmisión de datos	51,840 Mbps
STS-3 (OC-3)	Compañías telefónicas; backbones de las empresas de transmisión de datos	155,251 Mbps
STS-48 (OC-48)	Compañías telefónicas; backbones de las empresas de transmisión de datos	2,488320 Gbps

1.6. CLASIFICACIÓN POR SU DISTRIBUCIÓN LÓGICA

Esta clasificación consiste básicamente en un conjunto de computadoras de las cuales hay un computador llamado servidor encargada de administrar los recursos, dar servicios y compartir información con las demás computadoras llamadas clientes.

1.6.1. Cliente-Servidor

Las Redes Cliente-Servidor se usan en entornos LAN mayores, incluyendo colegios y universidades. En este enfoque de la conectividad, la red se compone de uno o más servidores especializados y varios clientes diferentes, los servidores están diseñados

para proporcionar servicios centralizados y los clientes son los diferentes nodos en la red. En un entorno Cliente- Servidor, las PCs conectadas a la red puede llamarse clientes, nodos o estaciones de trabajo.

1.6.2. Tipo de Servidores

Los servidores aluden a una computadora remota a la que los navegadores le solicitan datos desde otras computadoras. Los servidores pueden almacenar información en forma de páginas web en formato HTML[6] que después envían a los usuarios que las piden por medio del protocolo HTTP[7]. Tipos de servidores que existen:

- **Servidor de Archivos.-** Un servidor de archivos proporciona una ubicación central en la red, en la que puede almacenar y compartir los archivos con usuarios de la red. Cuando los usuarios necesiten un archivo importante, como un plan de proyecto, podrán tener acceso al archivo del servidor de archivos en lugar de tener que pasarlo entre distintos equipos.

[6] Lenguaje de Marcado de Hipertexto.- Es el lenguaje de marcado predominante para la elaboración de páginas web.
[7] Protocolo de Transferencia de Hipertexto.- Es el método más común de intercambio de información en la Word Wide web, el método mediante el cual se transfieren las páginas web a un ordenador.

Figura 1. 18: Servidor de Archivos

- **Servidor de Impresión.-** Es un concentrador, que conecta una impresora a red, para que cualquier PC pueda acceder a ella e imprimir trabajos, sin depender de otro PC para poder utilizarla, como es el caso de las impresoras compartidas.

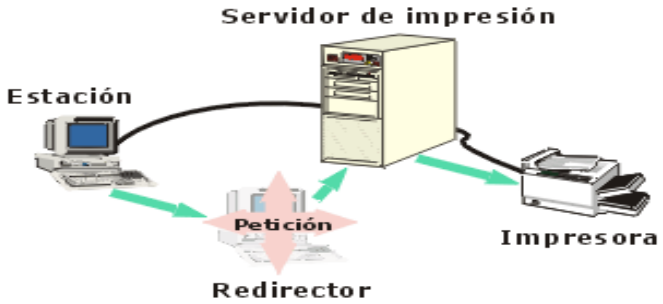


Figura 1. 19: Servidor de Impresión

- **Servidor de Comunicaciones.-** Un servidor de comunicación es una combinación de hardware y software que permite el acceso remoto[8] a herramientas o información que generalmente residen en una red de dispositivos.

[8] En redes de computadoras, acceder desde una computadora a un recurso ubicado físicamente en otra computadora, a través de una red local o externa (como internet).

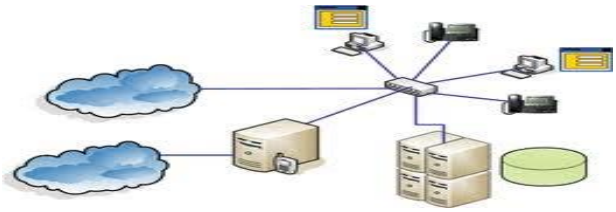


Figura 1. 20: Servidor de Comunicaciones

- **Servidor de Base de Datos.-** Un servidor de base de Datos es un programa que provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.

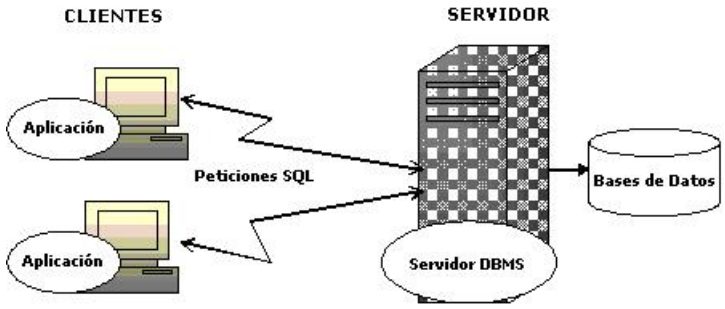


Figura 1. 21: Servidor de Base de Datos

- **Servidor de Correo Electrónico.-** Es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente.

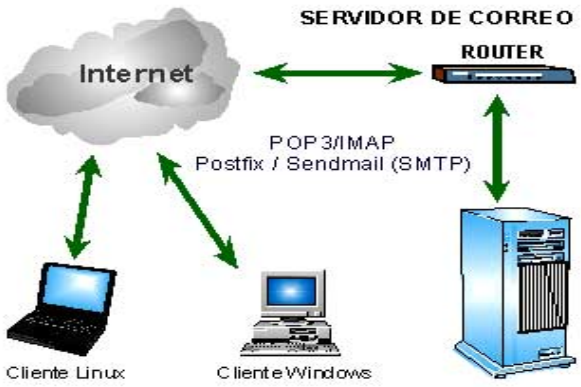


Figura 1. 22: Servidor de Correo Electrónico

- **Servidor de Acceso Remoto.-** Estos servidores permiten la administración del acceso a internet en una determinada red. De esta forma, se puede negar el acceso a ciertos sitios web. Por otro lado, ofrece servicios de seguridad y controla las líneas de módem de los canales de comunicación de las redes para que las peticiones sean conectadas con las redes cuya posición es remota.

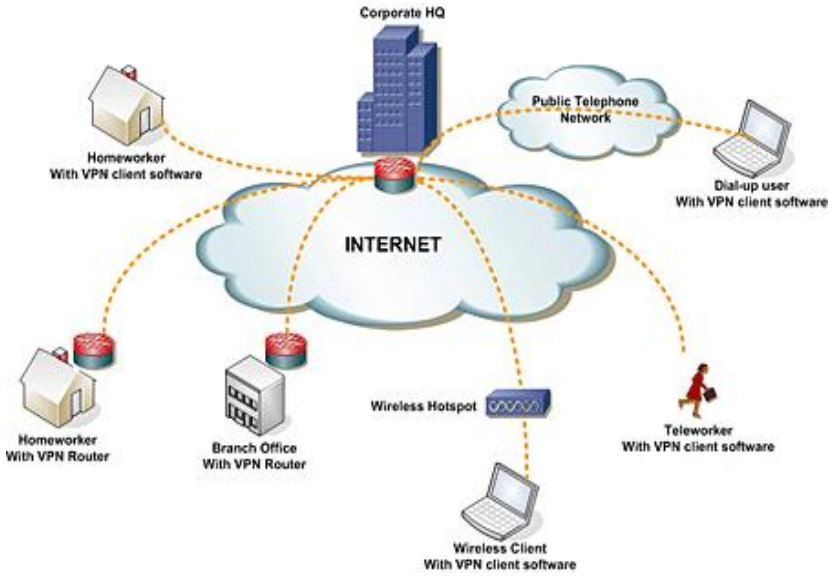


Figura 1. 23: Servidor de Acceso Remoto

1.7. TOPOLOGÍAS

Hay varias maneras de conectar dos o más computadoras en red. Para ello se utilizan cuatro elementos fundamentales: servidores de archivos, estaciones de trabajo, tarjetas de red y cables. A ellos se les suman los elementos propios de cada cableado, así como los manuales y el software de red, a efectos de la instalación y mantenimiento.

La manera en que están conectados no es arbitraria, sino que siguen estándares físicos llamados topologías. Dependiendo de la topología será la distribución física de la red y dispositivos conectados a la misma, así como también las características de ciertos aspectos de la red como: velocidad de transmisión de datos y confiabilidad del conexionado.

La configuración de una red, recoge tres campos: físico, eléctrico y lógico. El nivel físico y eléctrico se entiende como la configuración del cableado entre máquinas o dispositivos de control o comunicación. Llamado también topología física, es la forma que adopta un plano esquemático del cableado o estructura física de la red.
Cuando se habla de la configuración lógica (topología lógica) hay que pensar en cómo se trata la información dentro de nuestra red, como se dirige de un sitio a otro o como la recoge cada estación; Es decir es la forma de como la red reconoce a cada conexión de estación de trabajo.

1.7.1. Criterios para Establecer una Topología

Para establecer la topología de red se debe analizar los siguientes parámetros.

- **Fiabilidad.-** Proporciona la máxima fiabilidad y seguridad posible, para garantizar la recepción correcta de toda la información que soporta la red de datos.
- **Costos.-** Proporciona el tráfico de datos más económico entre el transmisor y el receptor en una red.
- **Respuesta.-** Proporciona el tiempo de respuesta óptimo y un caudal eficaz o ancho de banda, que sea máximo.

1.7.2. Clasificación de Redes por su Topología

Las topologías de red se clasifican en:

a. Topología Lineal o Bus

Topología de red en la que todas las estaciones están conectadas a un único canal de comunicaciones por medio de unidades interfaz y derivadores. Las estaciones utilizan este canal para comunicarse con el resto. La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los hosts queden desconectados. La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información.

Ventajas

- Es la más barata
- Apta para oficinas medianas y pequeñas

Desventajas

- Si se tiene demasiadas computadoras conectadas a la vez, la eficiencia baja notablemente.
- Es posible que dos computadoras intenten transmitir al mismo tiempo provocando lo que se denomina “colisión”, y por lo tanto se produce un reintento de transmisión.
- Un corte en cualquier punto del cable interrumpe la red.

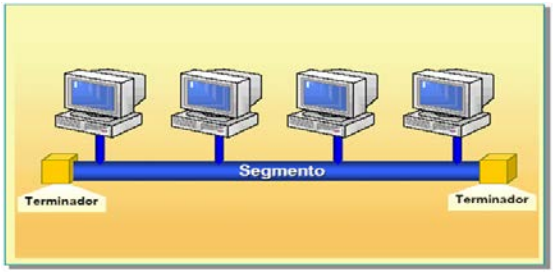


Figura 1. 24: Topología Bus

b. Topología Estrella

En este esquema todas las estaciones están conectadas a un concentrador o Switch con cable por computadora. Para futuras ampliaciones pueden colocarse otros Switch en cascada dando lugar a la estrella jerárquica.

Por ejemplo en la estructura Cliente-Servidor está conectado al Switch activo, de este a los pasivos y finalmente a las estaciones de trabajo.

Ventajas

- La ausencia de colisiones en la transmisión y diálogo directo de cada estación con el servidor.
- La caída de una estación no anula la red.

Desventajas

- Baja transmisión de datos

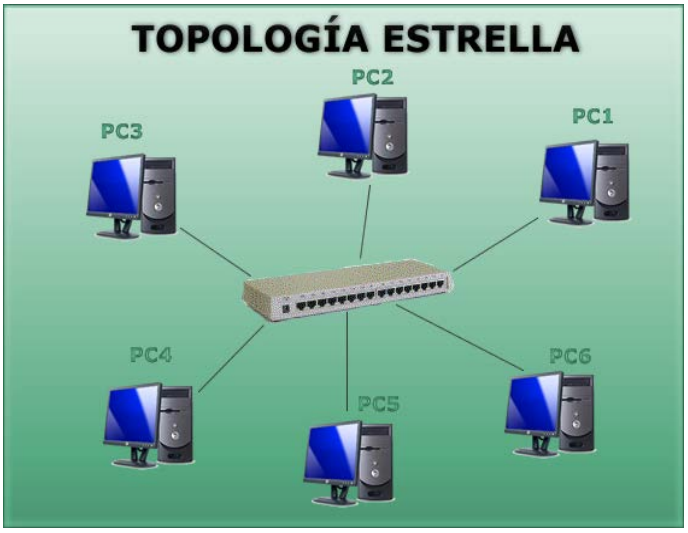


Figura 1. 25: Topología Estrella

c. Topología Anillo (Token Ring)

Es un desarrollo de IBM que consiste en conectar cada estación con otra dos formando un anillo.

Los servidores pueden estar en cualquier lugar del anillo y la información es pasada en un único sentido de una a otra estación hasta que alcanza su destino. Cada estación

que recibe el TOKEN regenera la señal por toda la red. Si la terminal quiere transmitir pide el TOKEN y hasta que lo tiene puede transmitir. Si no está la señal la pasa a la siguiente en el anillo y sigue circulando hasta que alguna pide permiso para transmitir.

Ventajas

- No existe colisiones, pues cada paquete tiene una cabecera o TOKEN que identifica al destino.

Desventaja

- La caída de una estación interrumpe toda la red. Actualmente no hay conexiones físicas entre estaciones, sino que existen centrales de cableado o MAU[9] que implementa la lógica de anillo sin que estén conectadas entre sí evitando las caídas.
- Es cara, llegando a costar una placa de red lo que una estación de trabajo.

Figura 1. 26: Topología Anillo

[9] Unidad de Acceso a Múltiples Estaciones.- Es un dispositivo Multi-puerto del equipamiento en el que se conectan las estaciones de trabajo.

d. Topología Árbol

En esta topología es una generalización del tipo bus, el árbol tiene su primer nodo[10] en la raíz y se expande hacia fuera utilizando ramas, en donde se conectan las demás terminales.

Esta topología permite que la red se expanda y al mismo tiempo asegura que nada más existe una ruta de datos entre dos terminales cualesquiera.

Figura 1. 27: Topología Árbol

e. Topología Malla

Es una combinación de más de una topología, como podría ser un bus combinado con una estrella. Este tipo de topología es común en lugares en donde tenían una red bus y luego la fueron expandiendo en estrella.

Son complicadas para detectar su conexión por parte del servicio técnico para su reparación.

[10] Es un punto de intersección, conexión o unión de varios elementos que confluyen en el mismo lugar.

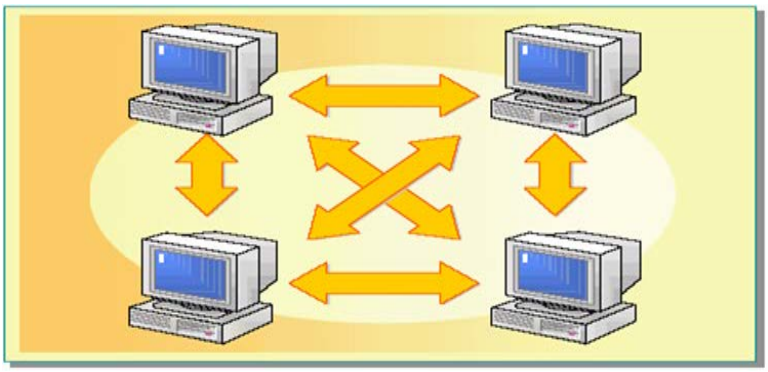


Figura 1. 28: Topología Malla

Dentro de estas topologías se encuentra:

e.1. Topología Anillo en Estrella.- Se utilizan con el fin de facilitar la administración de la red. Físicamente la red es una estrella centralizada en un concentrador, mientras que a nivel lógico la red es anillo.

e.2. Topología Bus en Estrella.- El fin es igual al anterior. En este caso la red es un bus que se cable físicamente como una estrella mediante el uso de concentradores.

e.3. Topología Estrella Jerárquica.- Esta estructura se utiliza en la mayor parte de redes locales actuales. Por medio de concentradores dispuestos en cascadas para formar una red jerárquica.

f. Topología Celular

La topología celular está compuesta por áreas circulares o hexagonales, cada una de las cuales tiene un nodo individual en el centro. La topología celular es un área geográfica dividida en regiones (celdas) para los fines de la tecnología inalámbrica. En esta tecnología no existen enlaces físicos; sólo hay ondas electromagnéticas.

La ventaja de una topología celular (inalámbrica) es que no existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites).

Las desventajas son que las señales se encuentran presentes en cualquier lugar de la celda y, de ese modo, pueden sufrir disturbios y violaciones de seguridad. Como norma, las topologías basadas en celdas se integran con otras topologías, ya sea que usen la atmósfera o los satélites.

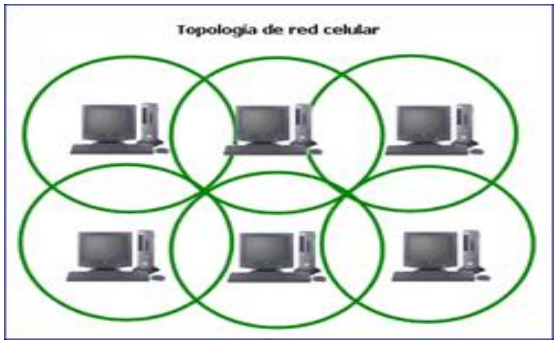


Figura 1. 29: Topología Celular

g. Topología de una WLAN

Se define como topología a la disposición lógica o a la disposición física de una red. Las topologías lógicas en redes WLAN son:

g.1. Topología Ad – hoc.- Cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red Peer to Peer o de igual a igual, para lo cual sólo se necesita disponer de un SSID (Suele denominar de manera familiar el nombre de la red wireless que da servicio un Punto de Acceso) igual para todos los nodos y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento. A

más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre sí.

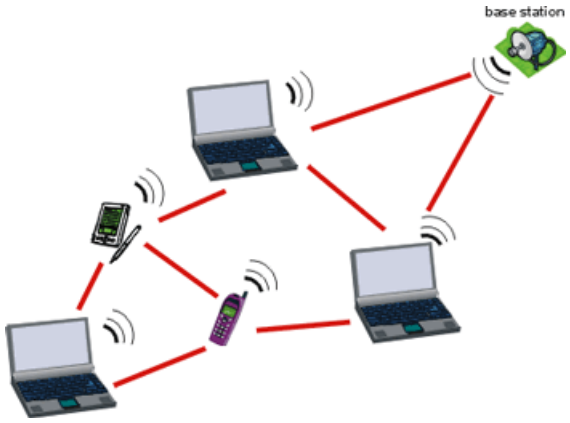


Figura 1. 30: Topología Ad – hoc

g.2. Topología en Infraestructura.- Existe un nodo central llamado Punto de Acceso WiFi que sirve de enlace para todos los demás (es decir, las Tarjetas de Red WiFi). Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del Punto de Acceso.

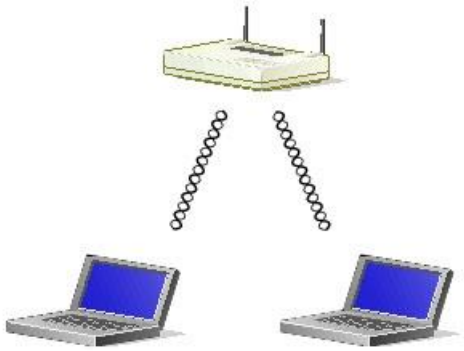


Figura 1. 31: Topología Infraestructura

g.3. Topología Modo Managed.- Es el modo en el que la Tarjeta de Red se conecta al Punto de Acceso para que éste último, le sirva de "concentrador". En este caso la Tarjeta de Red solo se comunicará con ese Punto de Acceso.

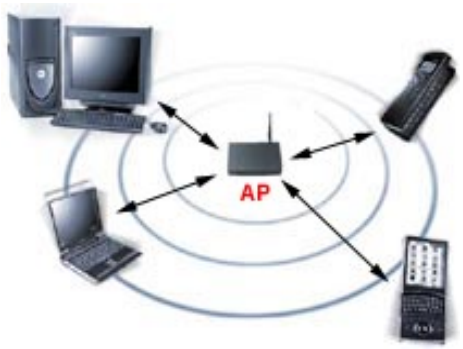


Figura 1. 32: Topología Managed

1.8. MEDIOS DE TRANSMISIÓN

Actualmente, la gran mayoría de las redes están conectadas por algún tipo de cableado, que actúa como medio de transmisión por donde pasan las señales entre los equipos. Hay disponibles una gran cantidad de tipos de cables para cubrir las necesidades y tamaños de las diferentes redes, desde las más pequeñas a las más grandes.

Existen dos medios de transmisión: guiados y no guiados.

1.8.1. Medio Guiado

Los medios de transmisión guiados están constituidos por un cable que se encarga de la conducción de las señales desde un extremo al otro.

Existen una gran cantidad de tipos de cables. Algunos fabricantes de cables publican unos catálogos con más de 2.000 tipos diferentes que se pueden agrupar en tres

grupos principales que conectan la mayoría de las redes: Cable coaxial, Cable de par trenzado (apantallado y no apantallado) y Cable de fibra óptica.

a. Cable Coaxial

Presenta propiedades mucho más favorables frente a interferencias y a la longitud de la línea de datos, de modo que el ancho de banda[11] puede ser mayor. Esto permite una mayor concentración de las transmisiones analógicas o más capacidad de las transmisiones digitales.

El cable coaxial está estructurado por los siguientes componentes de la siguiente manera:

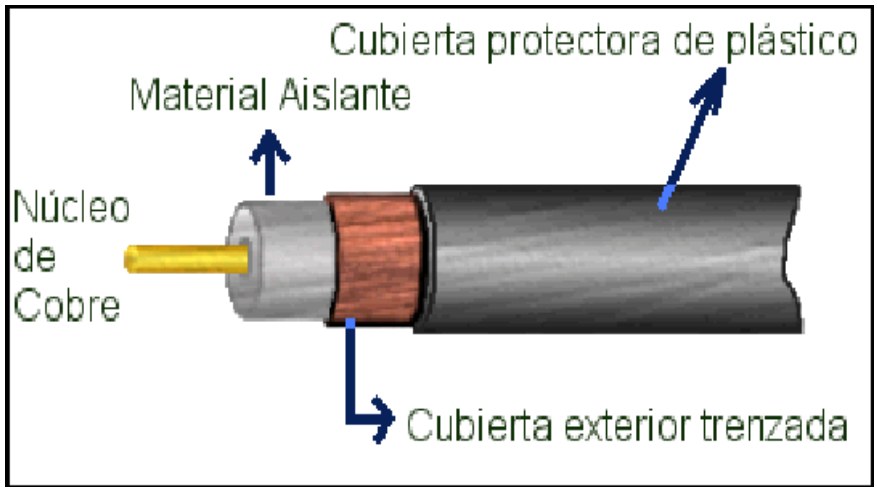


Figura 1. 33: Partes Cable Coaxial

[11] Ancho de Banda.- Es la cantidad de información o de datosque se puedeenviar a través de unaconexión de red en un período de tiempo dado.

b. Cable Par Trenzado

El cable par trenzado está compuesto de conductores de cobre aislados por papel o plástico y trenzados en pares. Esos pares son después trenzados en grupos llamados unidades, y estas unidades son a su vez trenzados hasta tener el cable terminado que se cubre por lo general por plástico. El trenzado de los pares de cable y de las unidades disminuye el ruido de interferencia, mejor conocido como diafonía. Existen dos tipos:

b.1. Par Trenzado No Apantallado (UTP).- Son cables de pares trenzados sin ningún tipo de pantalla adicional y con una impedancia característica de 100 ohmios. El conector más frecuente con el UTP es el RJ-45, también se puede usar RJ-11, DB-25, DB-11, dependiendo del adaptador de red y su aplicación.

Figura 1. 34: Partes Cable UTP

Características

- Es el más difundido en redes de área local LAN.
- Es muy usado en redes con arquitectura Ethernet y Token ring.
- El juego de conectores y fichas usadas en este cableado son muy prácticas, seguras, resistentes y económicas.

- Es el más liviano y flexible, es muy fácil de instalar y mantener.
- La distancia máxima que puede alcanzar la señal transmitida a través del cableado sin necesidad de usar repetidores que restauren la señal, a una velocidad de 10 Mbps (Megabits por segundo), con arquitectura Ethernet y topología en Estrella es de 90 metros. Con arquitectura Token Ring y topología en Anillo-Estrella se pueden alcanzar distancias de 100 metros.

Ventajas

- Es de fácil instalación y es el medio más barato.
- No llenan los conductos fácilmente, punto especialmente importante en instalaciones antiguas.
- Está considerado como el transporte más rápido dentro de la tecnología de cobre.

Desventajas

- Es más propenso al ruido y las interferencias que otros tipos de cable.
- La distancia final (sin repetidores) es más corta.

b.2. Par Trenzado Apantallado (STP)

Este tipo de cable combina las dos técnicas de apantallamiento y de cancelación mediante el trenzado del cable. Cada par de cable se envuelve en una hoja metálica. Los cuatro pares de cables se envuelven globalmente en una hoja metálica que finalmente se recubre con la cubierta protectora.

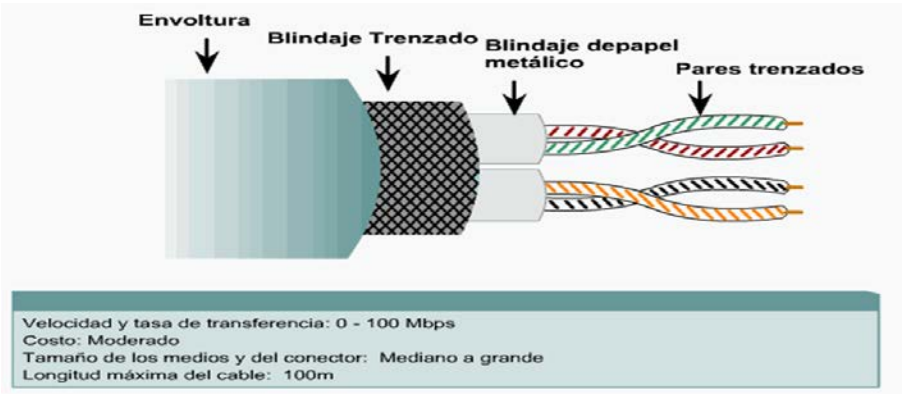


Figura 1. 35: Partes Cable UTP Apantallado

Ventajas

- STP reduce el ruido originado dentro del cable (diafonía) y fuera del cable.

Desventajas

- Es más costoso y difícil de instalar.
- Es más rígido y de mayor sección.

Tabla 1. 2: Distancias Permitidas entre Dispositivos en Función al Tipo de Cableado.

Categoría Obtenida	Topologías soportadas	Velocidad Max. De Transferencia	Distancias Máximas entre Repetidores por Norma	Requerimientos Mínimos de Materiales a Utilizar	Estado
Cat. 5	Inferiores y Fast Ethernet	100 Mbits.	90 mts. + 10 mts. En Patch Cords	Cable UTP y conectores Categoría 5 de 100 - 150 MHz	Sujeta a Descontinuarse
Cat. 5e	Inferiores y ATM	165 Mbits.	90 mts. + 10 mts. En Patch Cords	Cable UTP / FTP y conectores Categoría 5e de 150 - 350 MHz	Sujeta a Descontinuarse

Cat. 6	Inferiores y Gigabit Ethernet	1000 Mbits.	90 mts. + 10 mts. En Patch Cords Con cable de cobre Cat. 6. 1 Km. En Fibra Multimodo 2 Km. En Fibra Monomodo	Cable de cobre y conectores Categoría 6 de 1 - 250 MHz y/o Fibra Óptica	Actual
Cat. 6ª	Inferiores y Gigabit Ethernet	1000 Mbits.	90 mts. + 10 mts. En Patch Cords Con cable de cobre Cat. 6A. 1 Km. En Fibra Multimodo 2 Km. En Fibra Monomodo	Cable de cobre y conectores Categoría 6A de 1 - 500 MHz y/o Fibra Óptica	Punta Tecnológica
Cat. 7	Inferiores y Gigabit Ethernet	Mayor a 10 Gbits.	90 mts. + 10 mts. En Patch Cords Con cable de cobre Cat. 7. 1 Km. En Fibra Multimodo 2 Km. En Fibra Monomodo	Cable de cobre y conectores Categoría 7 de 1 - 600 MHz y/o Fibra Óptica	Punta Tecnológica
Cat. 7ª	Inferiores y Gigabit Ethernet	Mayor a 10 Gbits.	90 mts. + 10 mts. En Patch Cords Con cable de cobre Cat. 7A. 1 Km. En Fibra Multimodo 2 Km. En Fibra Monomodo	Cable de cobre y conectores Categoría 7A de 1 - 1000 MHz y/o Fibra Óptica	Punta Tecnológica

c. Cable de Fibra Óptica

Es un filamento de vidrio sumamente delgado diseñado para la transmisión de la luz. Las fibras ópticas poseen enormes capacidades de transmisión, del orden de miles de millones de bits por segundo.

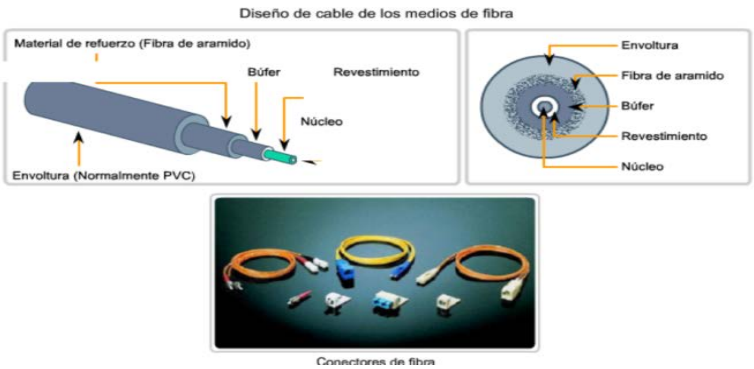


Figura 1. 36: Partes Cable Fibra Óptica

Como características de la fibra se puede destacar que son compactas, ligeras, con bajas perdidas de señal, amplia capacidad de transmisión y un alto grado de confiablidad ya que son inmunes a las interferencias electromagnéticas de radiofrecuencia. Las fibras ópticas no conducen señales eléctricas, conducen rayos luminosos, por lo tanto son ideales para incorporarse en cables sin ningún componente conductivo y pueden usarse en condiciones peligrosas de alta tensión.

Su principal desventaja es el costo que resulta superior al resto de los tipos de cables. Con la utilización del cable de fibra óptica se logran distancias de transmisión del orden de los 2,4 kmts y velocidades que llegan hasta el orden de los Gigabits por segundo.

c.1. Tipos de Fibra Óptica

Actualmente se utilizan dos tipos de fibras ópticas para la transmisión de datos:

- **Mono modo:** Cuando el valor de la apertura numérica es inferior a 2,405, un único modo electromagnético viaja a través de la línea y por tanto esta se denomina Mono modo. Solo se propagan los rayos paralelos al eje de la fibra óptica, consiguiendo el rendimiento máximo, en concreto un ancho de banda

de hasta 50GHz. Este tipo de fibras necesitan el empleo de emisores laser para la inyección de la luz, lo que proporciona un gran ancho de banda y una baja atenuación con la distancia, por lo que son utilizadas en redes metropolitanas y redes de área extensa. Por el contrario, resultan más caras de producir y el equipamiento es más sofisticado. Puede operar con velocidades de hasta los 622 Mbps y tiene un alcance de transmisión de hasta 100Km.

- **Multimodo:** Cuando el valor de la apertura numérica es superior a 2.405, se transmiten varios modos electromagnéticos por la fibra, denominándose por este motivo fibra Multimodo.

  Las fibras Multimodo son las más utilizadas en las redes locales por su bajo coste. Los diámetros más frecuentes 62,5/125 y 100/140 micras. Las distancias de transmisión en este tipo de fibras están alrededor de los 2,4 Kmts y se utiliza a diferentes velocidades: 10Mbps, 16Mbps, 100Mbps y 155Mbps.

1.8.2. Medio No Guiado

Los medios de transmisión no guiados son los que no confinan las señales mediante ningún tipo de cable, sino que las señales se propagan libremente a través del medio.

Los medios no guiados proporcionan el soporte de la comunicación pero no dirigen la señal por un camino concreto.

a. Redes Inalámbricas

Hoy día las redes inalámbricas hacen más simple muchas operaciones que se realizan en sitios donde no hay cableado. No significa que estas vayan a remplazar las redes

cableadas. Pero muchas de las redes inalámbricas son más veloces, en algún momento se espera que éstas lleguen a alcanzar hasta los 100 Mbps. Las inalámbricas no necesitan hacer su conexión mediante un alambre, sino que también se puede hacer por el uso de satélites, un láser y microondas.

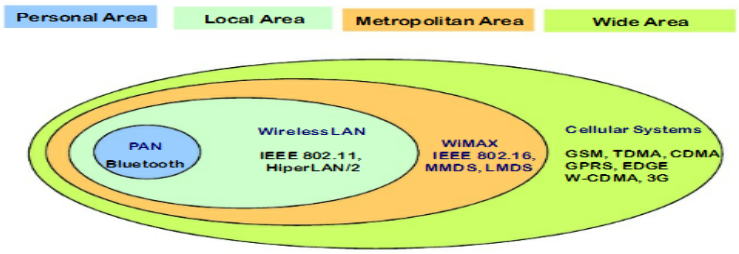


Figura 1. 37: Tecnologías de Redes Inalámbricas

b. Redes LAN Inalámbricas (WLAN)

Las redes LAN inalámbricas no requieren cables para transmitir señales, sino que utilizan ondas de radio o infrarrojos para enviar paquetes (conjunto de datos) a través del aire. Es una de las tecnologías de comunicación inalámbrica mediante ondas más utilizada hoy en día. WIFI, también llamada WLAN (wireless LAN, red inalámbrica) o estándar IEEE 802.11.

Figura 1. 38: Red LAN Inalámbrica

La mayoría de las redes LAN inalámbricas utilizan tecnología de espectro distribuido, la cual ofrece un ancho de banda limitado generalmente inferior a 11Mbps, el cual es compartido con otros dispositivos del espectro.

c. Microondas Terrestres

La distancia máxima entre antenas sin ningún obstáculo es de 7,14 km. El uso principal de este tipo de transmisión se da en las telecomunicaciones de largas distancias, se presenta como alternativa del cable coaxial y la fibra óptica.
Los principales usos de las microondas terrestres son para la transmisión de televisión, voz y para enlazar punto a punto dos edificios. La banda de frecuencia va desde 2 a 40 GHz.

Figura 1. 39: Red Microondas

d. Microondas Por Satélite

El satélite funciona como un espejo donde la señal rebota, su principal función es la de amplificar la señal corregirla y retransmitirla a una o más antenas.

Estos satélites son geoestacionarios, es decir se encuentra fijo para un observador que está en la tierra. Las comunicaciones satelitales se utilizan principalmente para la

difusión de televisión, transmisiones telefónicas de larga distancia y redes privadas entre otras. También se usan para proporcionar enlaces punto a punto entre las centrales telefónicas en las redes públicas. El rango de frecuencia está comprendido entre 1 y 10 GHz.

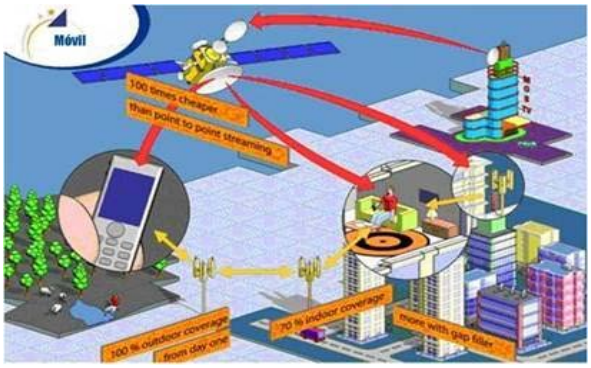


Figura 1. 40: Red Satélite

e. Infrarrojo

Los infrarrojos son útiles para las conexiones locales punto a punto, así como para aplicaciones multipunto dentro de un área de cobertura limitada, ejemplo: una habitación.

El espectro infrarrojo a diferencia de las microondas no tiene problemas de interferencia o seguridad, tampoco tiene problemas de asignación de frecuencia, ya que estas bandas no necesitan permiso. La velocidad de transmisión alcanza los 10 Mbps y tiene un rango de alcance corto.

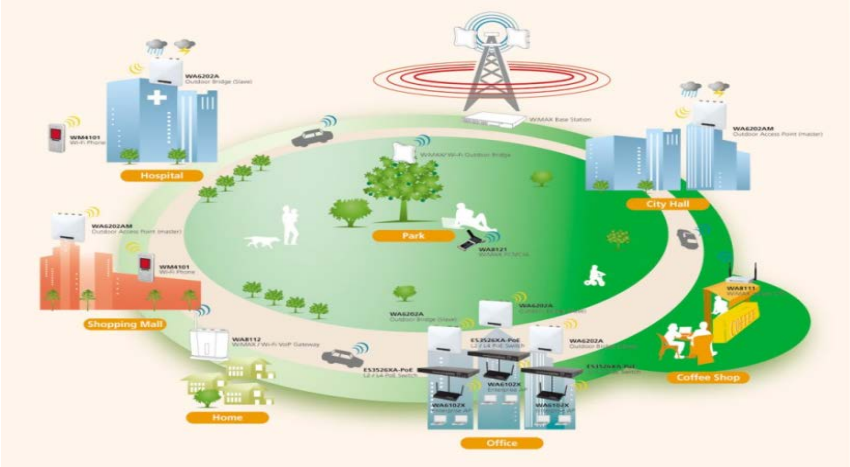


Figura 1. 41: Red Infrarrojo

f. Radio

Las ondas de radio son fáciles de generar, pueden viajar distancias largas y penetrar edificios sin problemas, de modo que se utilizan mucho en la comunicación, tanto en interiores como exteriores; son menos sensibles a la atenuación producida por la lluvia y son utilizadas para la transmisión de voz.

Estas ondas de radio también son omnidireccionales[12], lo que significa que viajan en todas las direcciones a partir de la fuente, por lo que no es necesario que el transmisor y el receptor se encuentren alineados físicamente. Comprenden un rango de frecuencias que oscila entre los 30 MHz y 1 GHz.

g. Láser

La tecnología óptica láser punto a punto se utiliza para conectar redes en áreas metropolitanas. Permite conectar redes que se encuentran separadas desde unos pocos metros hasta 4 o 5 kilómetros. Esta tecnología utiliza el espectro no licenciado

[12] Se puede orientar o utilizar en cualquier dirección o sentido.

mediante rayos de luz infrarroja y se pueden alcanzar velocidades de hasta 1500 Mbps.

h. Red WiMAX

Una Red WiMAX es la creación de una estructura de red implementando como base principal la utilización de tecnología inalámbrica WiMAX (802.16d - 802.16e) como forma para que los equipos se conecten entre sí y a internet.

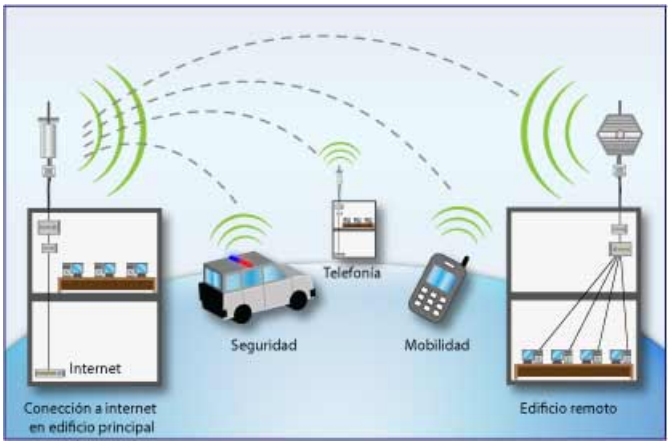


Figura 1. 42: Red WiMAX

Una definición breve sería como si existiera un enchufe de red en cualquier punto dentro de la zona de cobertura WiMAX.

h.1. Utilidades de la Red WiMAX

Las Redes WiMAX pueden tener muchas utilidades prácticas para todo tipo de entidades, empresas o negocios.

- Acceder a una red empresarial desde cualquier punto.

- Acceder a Internet sin necesidad de cables.
- Conectarse sin cables con un PC, un portátil, una PDA, un teléfono móvil con conexión WiMAX.
- Servicio de HotSpot para acceso restringido por tiempo o volumen.
- Acceder a servicios de VoIP sin cables.

h.2. Tipos de redes Inalámbricas WiMAX

Dependiendo de su finalidad, las redes WiMAX se pueden diferenciar en dos tipos diferentes. Diferenciando el tipo de equipos que se conectaran a ellas:

- **WiMAX Fijo.-** WiMAX, en el estándar IEEE 802.16-2004, fue diseñado para el acceso fijo. En esta forma de red al que se refirió como "fijo inalámbrico" se denomina de esta manera porque se utiliza una antena, colocada en un lugar estratégico del suscriptor. Esta antena se ubica generalmente en el techo de una habitación mástil, parecido a un plato de la televisión del satélite. También se ocupa de instalaciones interiores, en cuyo caso no necesita ser tan robusto como al aire libre.

  Se podría indicar que WiMAX Fijo, indicado en el estándar IEEE 802.16-2004, es una solución inalámbrica para acceso a Internet de banda ancha (también conocido como Internet Rural). WiMAX acceso fijo funciona desde 2.5-GHz autorizado, 3.5-GHz y 5.8-GHz exento de licencia. Esta tecnología provee una alternativa inalámbrica al módem cable y al ADSL.

- **WiMAX Móvil.-** WiMAX, en una posterior revisión de su estándar IEEE 902.16-2004, la IEEE 802.16e, se enfoca hacia el mercado móvil añadiendo

portabilidad y capacidad para clientes móviles con capacidades de conexión WiMAX (IEEE 802.16e).

Los dispositivos equipados con WiMAX que cumpla el estándar IEEE 802.16e usan Acceso Múltiple por División Ortogonal de Frecuencia (OFDMA), similar a OFDM en que divide en las subportadoras múltiples. OFDMA, sin embargo, va un paso más allá agrupando subportadoras múltiples en subcanales. Una sola estación cliente del suscriptor podría usar todos los subcanales dentro del periodo de la transmisión.

Tabla 1. 3: Tecnologías Inalámbricas

	WPAN	**WLAN**	**WMAN**	**WWAN**
TECNOLOGÍA	Bluetooth Ultra Wide Band Zig Bee	802.11b 802.11 a 802.11 g 802.11 n	802.16 802.16 a 802.16 e	GSM GPRS CDMA 2.5 G 3 G 4G
TASA DE DATOS	Tasa de Datos medias (1 a 2 Mbps)	Tasas de Datos altas (11 Mbps a 200 + Mbps)	Muy altas tasas de Datos (350 + Mbps)	Tasas de Datos de bajas a medias, (10 Kbps a 2.4 Mbps)
Rango	Rango muy corto 3m	Rango Corto 100 m	Rango medio 50 Km	Rango Global
Conectividad	Laptop a Pc a periféricos	Computador a computador y la internet	LAN o computador a una línea cableada de alta velocidad de internet	Da Smart Phones y PDas a Wans y al internet

1.9. DIRECCIONAMIENTO IP

Cada host TCI/IP se identifica mediante una dirección IP lógica que señala la ubicación de un equipo en la red.

La dirección IP identifica la localización de un sistema en la red. Equivale a una dirección de una calle y número de portal. Es decir, es única. No pueden existir en la misma ciudad dos calles con el mismo nombre y números de portal.

Cada dirección IP tiene dos partes. Una de ellas, identifica a la RED y la otra identifica a la máquina dentro de esa red. Todas las máquinas que pertenecen a la misma red requieren el mismo número de RED el cual debe ser además único en Internet. El número de máquina, identifica a una Workstation, servidor, routers o cualquier otra máquina TCP/IP dentro de la red. El número de máquina (número de host) debe ser único para esa red. Cada host TCP/IP, por tanto, queda identificado por una dirección IP que debe ser única.

1.10. TIPOS DE DIRECCIONES IP

Hay dos tipos de direcciones IP que se pueden utilizar en una red. La versión sobre la que internet y la mayoría de los routers están configurados es IPv4 (Protocolo de Internet versión 4). Esta versión utiliza direcciones de 32 bits, lo que limita la cantidad de direcciones a 4.294.967.296 direcciones únicas posibles. Algunas de estas direcciones, 290 millones aproximadamente, están reservadas para propósitos especiales. Debido al crecimiento popular de internet ha habido preocupación de que el conjunto de direcciones posibles puedan agotarse en el futuro. Con esto en mente, una nueva versión de direcciones IP fue desarrollado y se llama IPv6 (Protocolo de Internet versión 6), que cambiaría el tamaño de las direcciones de 32 bits a direcciones de 128 bits. Este cambio permitiría una asignación más generosa de

direcciones IP a las redes sin ningún problema previsible con la cantidad de direcciones disponibles. Sin embargo, para poder utilizar direcciones IPv6, routers y hardware existente tendrían que ser actualizados o configurados para utilizar esta nueva versión de direcciones IP.

- **IPv4.-** Fue la primera versión de Protocolo de Internet de uso masivo y todavía se utiliza en la mayoría del tráfico actualde Internet. Existen más de 4.000 millones de direcciones IPv4. Si bien son muchísimas, no son infinitas.

- **IPv6.-** Es un sistema de numeración más nuevo que, entre otras ventajas, brinda un espacio de direcciones mucho mayor que IPv4. Se lanzó en 1999 y se supone que satisfará ampliamente las necesidades futuras de direcciones IP del mundo.

La principal diferencia entre IPv4 e IPv6 reside en la cantidad de direcciones IP. Hay algo más de 4.000.000.000 de direcciones IPv4. En cambio, existen más de 340.000.000.000.000.000.000.000.000.000.000.000.000 de direcciones IPv6.

El funcionamiento técnico de Internet es el mismo con ambas versiones, y es probable que ambas sigan operando simultáneamente en las redes por mucho tiempo más. En la actualidad, la mayoría de las redes que usan IPv6 admiten tanto direcciones IPv4 como IPv6 en sus redes.

Tabla 1. 4: Protocolo IPV4 Y IPV6

	Protocolo de Internet versión 4 (IPv4)	Protocolo de Internet versión 6 (IPv6)
Lanzado en	1981	1999
Tamaño de las direcciones	Número de 32 bits	Número de 128 bits
Formato de las direcciones	Notación decimal con puntos: 192.149.252.76	Notación hexadecimal: 3FFE:F200:0234:AB00:0 123:4567:8901:ABCD
Notación de prefijos	192.149.0.0/24	3FFE:F200:0234::/48
Cantidad de direcciones	2^{32} = ~4,000,000,000	2^{128} = ~340,000,000, 000,000,000,000,000, 000,000,000,000,000

Cada dirección IP consta de un ID de red y de un ID de host.

- **ID de Red,** también conocido como dirección de red, identifica los sistemas que se encuentran localizados en la misma red física. El ID de red debe ser único para toda la IntraRed.

- **ID de Host,** también conocido como dirección del host identifica a cada host TCP/IP existente dentro de la red.

1.11. CARACTERÍSTICAS DE LAS REDES DE DATOS

Características

Los sistemas operativos sofisticados de red ofrecen un amplio rango de servicios.

- Comparte uno o varios medios de transmisión comunes.

- Alta velocidad de transferencia. Esta se incrementa cada día más, por el uso de tecnologías cada vez más sofisticadas.
- Flexibilidad. Un concepto cada vez más importante, y debe ser entendido, por la capacidad de las redes para adaptarse a las necesidades de los usuarios.
- Confiabilidad. Término discutido que plantea el grado de seguridad de los datos, expresado por las facilidades y medios de que disponen las redes.
- Seguridad. En la infraestructura de red y de sus componentes dentro de los ambientes e instalaciones.
- Operatividad. Soportado sobre principio de fácil instalación y manipulación de los componentes de la red informática.

Razones para Instalar Redes de Datos

Desde sus inicios una de las razones para instalar redes era compartir recursos, como discos, impresoras y trazadores. Ahora existen además otras razones:

- **Disponibilidad Del Software De Redes.-** El disponer de un software multiusuario de calidad que se ajuste a las necesidades de la empresa. Por ejemplo: Se puede diseñar un sistema de puntos de venta ligado a una red local concreta. El software de redes puede bajar los costos si se necesitan muchas copias del software.
- **Trabajo en Común.-** Conectar un conjunto de computadoras personales formando una red que permita que un grupo o equipo de personas involucrados en proyectos similares puedan comunicarse fácilmente y compartir programas o archivos de un mismo proyecto.
- **Actualización Del Software.-** Si el software se almacena de forma centralizada en un servidor es mucho más fácil actualizarlo. En lugar de tener que actualizarlo

individualmente en cada uno de los PC de los usuarios, pues el administrador tendrá que actualizar la única copia almacenada en el servidor.

- **Copia De Seguridad De Los Datos.-** Las copias de seguridad son más simples, ya que los datos están centralizados.
- **Ventajas en el Control de los Datos.-** Como los datos se encuentran centralizados en el servidor, resulta mucho más fácil controlarlos y recuperarlos. Los usuarios pueden transferir sus archivos vía red antes que usar los dispositivos de almacenamiento magnéticos.
- **Uso Compartido De Las Impresoras De Calidad.-** Algunos periféricos de calidad de alto costo pueden ser compartidos por los integrantes de la red. Entre estos: impresoras láser de alta calidad, etc.
- **Correo Electrónico Y Difusión De Mensajes.-** El correo electrónico permite que los usuarios se comuniquen más fácilmente entre sí. A cada usuario se le puede asignar un buzón de correo en el servidor. Los otros usuarios dejan sus mensajes en el buzón y el usuario los lee cuando los ve en la red. Se pueden convenir reuniones y establecer calendarios.
- **Ampliación Del Uso Con Terminales no inteligentes.-** Una vez montada la red local, pasa a ser más barato el automatizar el trabajo de más empleados por medio del uso de terminales no inteligentes en una red.
- **Seguridad.-** La seguridad de los datos puede conseguirse por medio de los servidores que posean métodos de control, tanto software como hardware. Los terminales no inteligentes impiden que los usuarios puedan extraer copias de datos para llevárselos fuera del edificio.

1.12. DISPOSITIVOS DE NETWORKING

Los dispositivos de Networking son todos aquellos que se conectan de forma directa a un segmento de red.

1.13. CLASIFICACIÓN DE DISPOSITIVOS DE NETWORKING

Estos dispositivos están clasificados en dos grandes grupos:

1.13.1. Dispositivos de Usuario Final

Incluyen los computadores, impresoras, escáneres, y demás dispositivos que brindan servicios directamente al usuario. A los dispositivos de usuario final que están conectados entre sí se les conoce como host, estos dispositivos pueden funcionar sin necesidad de estar conectados a un dispositivo de red pero sus capacidades se ven sumamente limitadas.

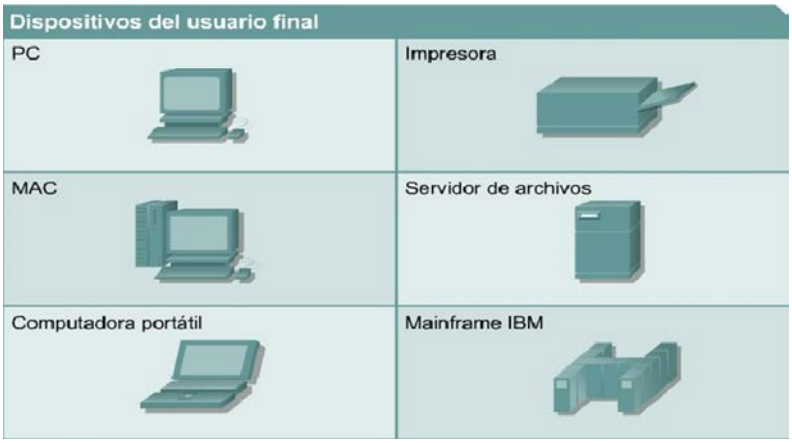


Figura 1. 43: Dispositivos de Usuario Final

1.13.2. Dispositivos de Red

Los dispositivos de red son los que conectan los dispositivos de usuario final posibilitando la comunicación entre ellos.

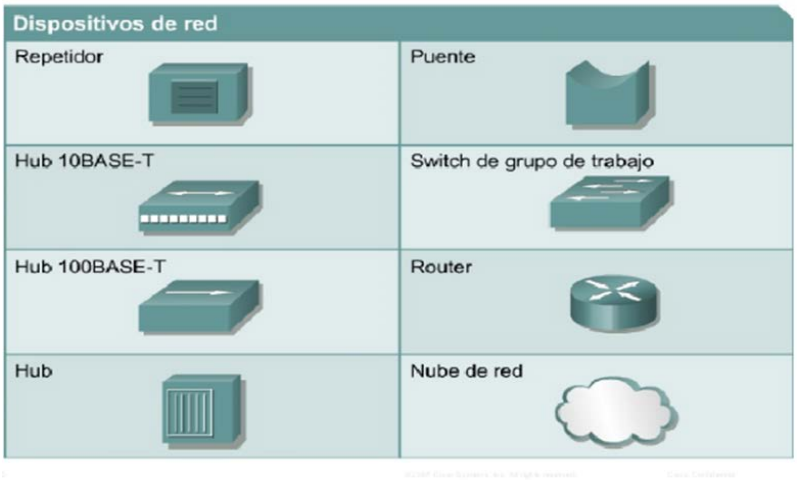


Figura 1. 44: Dispositivos de Red

- **Repetidores.-** Es un dispositivo de red que se utiliza para regenerar la señal tanto analógicas como digitales que se distorsionan a causa de pérdidas en la transmisión producidas por la atenuación, este dispositivo trabaja a nivel de capa física del modelo OSI[13] tiene dos puertos y permite extender la red, un repetidor no toma decisiones inteligentes acerca del envío de paquetes como lo hace un Router o puente.

- **Hubs.-** Permiten que la red trate un grupo de hosts como si fuera una sola unidad. Esto sucede de manera pasiva, sin interferir en la transmisión de datos. Los Hubs activos no sólo concentran hosts, sino que además regeneran señales, estos dispositivos trabajan en la capa física y tienen más puertos que un repetidor.

- **Puentes.-** Convierten los formatos de transmisión de datos de la red además de realizar la administración básica de la transmisión de datos. Los puentes, tal como su nombre lo indica, proporcionan las conexiones entre

[13]OSI (Modelo de Interconexión de Sistemas Abiertos)

LAN. Los puentes no sólo conectan las LAN, sino que además verifican los datos para determinar si les corresponde o no cruzar el puente. Esto aumenta la eficiencia de cada parte de la red. Trabajan a nivel de la capa de enlace de datos del modelo OSI, segmentan la red por puertos y son dispositivos pasivos.

- **Switch.-** Agregan inteligencia a la administración de transferencia de datos. No sólo son capaces de determinar si los datos deben permanecer o no en una LAN, sino que pueden transferir los datos únicamente a la conexión que necesita esos datos. Otra diferencia entre un puente y un Switch es que un Switch no convierte formatos de transmisión de datos, trabajan en la capa de enlace de datos y tienen más interfaces.

- **Routers.-** Los Routers pueden regenerar señales, concentrar múltiples conexiones, convertir formatos de transmisión de datos, y manejar transferencias de datos. También pueden conectarse a una WAN, lo que les permite conectar redes LAN que se encuentran separadas por grandes distancias. Ninguno de los demás dispositivos puede proporcionar este tipo de conexión. Trabajan en la capa de red del modelo OSI segmentan la red por puerto a nivel de capa 2 y 3.

1.14. VENTAJAS Y DESVENTAJAS DE LAS REDES DE DATOS

Ventajas

- Mayor facilidad en la comunicación entre usuarios
- Reducción en el presupuesto para software
- Reducción en el presupuesto para hardware

- Posibilidad de organizar grupos de trabajo
- Mejoras en la administración de los equipos y programas
- Mejoras en la integridad de los datos
- Mayor seguridad para acceder a la información
- Compartir recursos especialmente información (los datos)
- Proveer la confiabilidad
- Permite la disponibilidad de programas y equipos para cualquiera de la red que así lo soliciten sin importar la localización física del recurso y del usuario.
- Permite al usuario poder acceder a una misma información sin problemas llevándolo de un equipo a otro.
- Centralización del control: Los accesos, recursos y la integridad de los datos son controlados por el servidor de forma que un programa cliente defectuoso o no autorizado no pueda dañar el sistema. Esta centralización también facilita la tarea de poner al día datos u otros recursos.
- Escalabilidad: Se puede aumentar la capacidad de clientes y servidores por separado. Cualquier elemento puede ser aumentado (o mejorado) en cualquier momento, o se pueden añadir nuevos nodos a la red (clientes y/o servidores).
- Fácil mantenimiento: Al estar distribuidas las funciones y responsabilidades entre varios ordenadores independientes, es posible remplazar, reparar, actualizar, o incluso trasladar un servidor, mientras que sus clientes no se verán afectados por ese cambio (o se afectarán mínimamente). Esta independencia de los cambios también se conoce como encapsulación.

Desventajas

- Mayor riesgo en seguridad (tanto interna como externa, haciendo referencia a virus y hackers[14].
- Costo elevado de implementación.
- La congestión del tráfico ha sido siempre un problema en el paradigma de Cliente/Servidor. Cuando una gran cantidad de clientes envían peticiones simultáneas al mismo servidor, puede ser que cause muchos problemas para éste (a mayor número de clientes, más problemas para el servidor).
- El software y el hardware de un servidor son generalmente muy determinantes. Un hardware regular de un computador personal puede no poder servir a cierta cantidad de clientes. Normalmente se necesita software y hardware específico, sobre todo en el lado del servidor, para satisfacer el trabajo. Por supuesto, esto aumentará el costo.

1.15. MODELO OSI (INTERCONEXIÓN DE SISTEMAS ABIERTOS)

OSI Interconexión de sistemas abiertos fue propuesto por la ISO como una norma o modelo para explicar cómo debe trabajar una red y enlazar sistemas abiertos.

Este modelo consta de siete capas, las cuales se encargan desde establecer la conexión física y vigilar que los datos enviados no se pierdan o dañen, hasta controlar que los datos sean correctamente interpretados por diferentes aplicaciones.

Para el usuario final el proceso de verificación realizado por estas capas es transparente, sobre todo por la rapidez con que se realizan.

[14]Hacker.- Se autodefine como una persona que sólo desea conocer el funcionamiento interno de los sistemas informáticos, ayudando a mejorarlos en el caso de que detecte fallos en su seguridad.
Cracker.- Es también un apasionado del mundo informático. La principal diferencia consiste en que la finalidad del cracker es dañar sistemas y ordenadores.

1.15.1. Capas del Modelo OSI

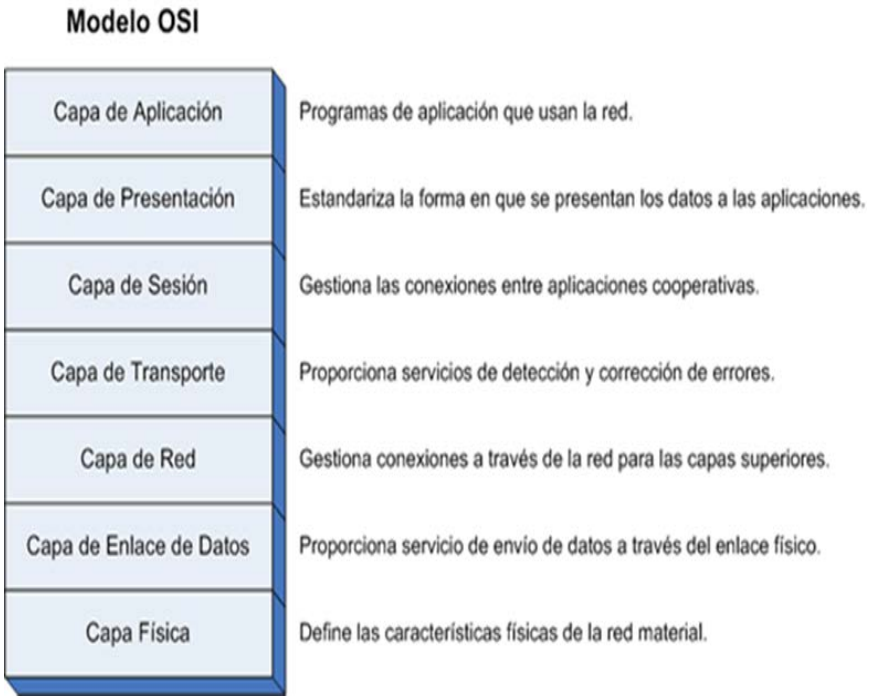


Figura 1. 45: Capas del modelo OSI

1.16. MODELO TCP/IP

El principal objetivo de TCP/IP fue la de interconectar un conjunto de redes heterogéneas a la cual se puede referir como una Internetwork o Internet.

1.16.1. Capas del Modelo TCP/IP

El siguiente cuadro hace referencia a las capas del modelo TCP/IP partiendo de las capas del modelo OSI.

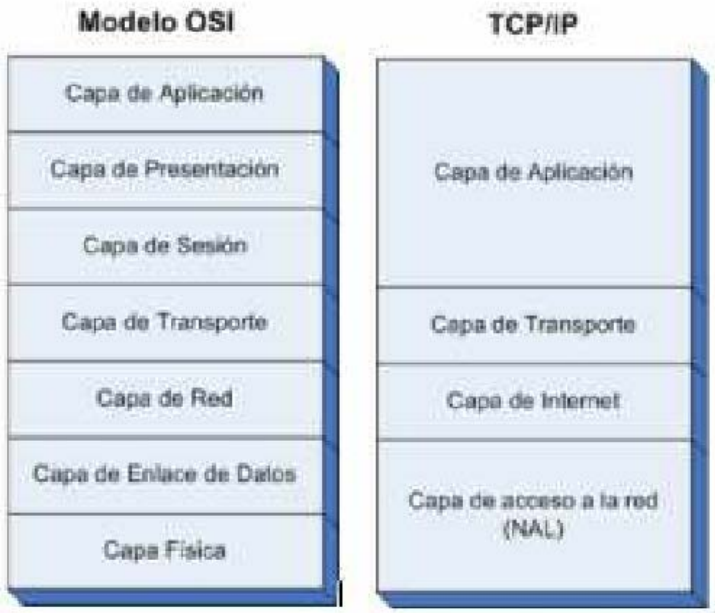


Figura 1. 46: Capas del modelo TCP/IP

Tabla 1. 5: Comparativo entre modelos de referencia OSI VS TCP/IP

MODELO DE REFERENCIA OSI	MODELO DE REFERENCIA TCP/IP
El modelo OSI consiste en siete capas, las cuales son: **1. La Capa de Aplicación:** Esta provee el acceso al entorno OSI para los usuarios y los servicios de información distribuida. **2. La Capa de Presentación:** Proporciona independencia a los procesos de aplicación respecto a las diferencias existentes en las representaciones de los datos. **3. La Capa de Sesión:** Facilita el control de la comunicación entre las aplicaciones; establece, gestiona y cierra las conexiones entre las aplicaciones cooperadoras (nivel lógico).	El protocolo TCP/IP se divide en 5 capas, a saber: • **La Capa de Aplicación:** En esta capa se encuentra toda la lógica necesaria para posibilitar las distintas aplicaciones del usuario. • **La Capa de Origen-Destino:** También llamada Capa de Transporte, es la que tiene aquellos procedimientos que garantizan una transmisión segura. • **La Capa de Internet:** En las situaciones en las que los dispositivos están conectados a redes diferentes, se necesitarán una serie de procedimientos que permitan que los datos atraviesen esas redes, para ello se hace uso de

4. **La Capa de Transporte:** Ofrece seguridad, transferencia transparente de datos entre los puntos interconectados y además establece los procedimientos de recuperación de errores y control de flujo origen-destino. 5. **La Capa de Red:** Da a las capas superiores independencia en lo que se refiere a las técnicas de conmutación y de transmisión utilizadas para conectar los sistemas, es responsable del establecimiento, mantenimiento y cierre de las conexiones (nivel hardware). 6. **La Capa de Enlace de Datos:** Suministra un servicio de transferencia de datos seguro a través del medio físico enviando bloques de datos, llevando a cabo la sincronización, el control de errores y el de flujo de información que se requiere. 7. **La Capa Física:** Encargada de la transmisión de cadenas de bits no estructuradas sobre el medio físico, se relaciona con las características mecánicas, eléctricas, funcionales y procedimientos para acceder al medio físico.	esta capa, en otras palabras, el objetivo de esta capa es el de comunicar computadoras en redes distintas. • **La Capa de Acceso a la Red:** Es la responsable del intercambio de datos entre el sistema final y la red a la cual se está conectado, el emisor debe proporcionar a la red la dirección de destino. Se encuentra relacionada con el acceso y el encaminamiento de los datos a través de la red. • **La Capa Física:** Define la interfaz física entre el dispositivo de transmisión de datos (por ejemplo, la estación del trabajo del computador) y el medio de transmisión o red. Esta capa se encarga de la especificación de las características del medio de transmisión, la naturaleza de las señales, la velocidad de los datos y cuestiones afines.

Tabla 1. 6: Características, Ventajas y Desventajas de los modelos OSI Y TCP/IP

<table>
<tr><td rowspan="4">MODELOS DE REFERENCIA</td><td rowspan="3">OSI</td><td>Características:

OSI define claramente las diferencias entre los servicios, las interfaces, y los protocolos.

• Servicio: lo que un nivel hace
• Interfaz: cómo se pueden acceder los servicios
• Protocolo: la implementación de los servicios

TCP/IP no tiene esta clara separación.</td></tr>
<tr><td>Ventajas:
Proporciona a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red utilizados por las empresas a nivel mundial.</td></tr>
<tr><td>Desventajas:
• Las capas contienen demasiadas actividades redundantes, por ejemplo, el control de errores se integra en casi todas las capas siendo que tener un único control en la capa de aplicación o presentación sería suficiente.
• La gran cantidad de código que fue necesario para implantar el modelo OSI y su consecuente lentitud hizo que la palabra OSI fuera interpretada como "calidad pobre", lo que contrastó con TCP/IP que se implantó exitosamente en el operativo UNIX y era gratis.</td></tr>
<tr><td></td><td>Características:
• Estándar en EE.UU. desde 1983
• Dispone de las mejores herramientas para crear grandes redes de ordenadores
• Independencia del fabricante</td></tr>
</table>

	TCP/IP	**Ventajas:** • En caminable • Imprescindible para Internet • Soporta múltiples tecnologías • Puede funcionar en máquinas de todo tamaño (multiplataforma)
		Desventajas: • El modelo no distingue bien entre servicios, interfaces y protocolos, lo cual afecta al diseño de nuevas tecnologías en base a TCP/IP. • Peor rendimiento para uso en servidores de fichero e impresión

1.17. SISTEMA DE CABLEADO ESTRUCTURADO

1.17.1. Definición

Un sistema de Cableado Estructurada es mucho más que un simple conjunto de cables, es la interconexión de diferentes tecnologías mediante una forma ordenada y planeada. El cableado Estructurado representa la columna vertebral de cualquier edificio, oficina o plantas industriales. Hoy en día las soluciones de cableado utilizan el mismo cable para los servicios de telecomunicaciones de voz, datos, imagen, control y seguridad.

De esta manera, un Sistema de Cableado Estructurado debe ser compatible con todas las aplicaciones y normas de conexión manteniendo una relación razonable entre el costo y prestaciones para otorgarle funcionalidad y flexibilidad al sistema.

Un sistema Unificado de Cableado estructurado es un Sistema de Cableado Integral con sus cables y conectores estandarizados, capaz de cubrir las necesidades de todos los ocupantes de un edificio, siendo este un sistema abierto capaz de dar cabida a las distintas tecnologías así de incorporar diferentes tipos de equipos presentes y futuros según vayan siendo necesarios lo que lo convierte en un sistema Universal.

Los Sistemas de Cableado Estructurado deben emplear una Arquitectura de Sistemas Abiertos (OSA) y soportar aplicaciones basadas en estándares logrando efectuar movimientos y adiciones de tal manera que la administración y mantenimiento sea muy simplificado.

1.17.2. Objetivos de un Sistema de Cableado Estructurado

- Cubrir las necesidades y requisitos de todos los usuarios.
- Permitir las modificaciones y ampliaciones necesarias para soportar cualquier servicio e incorporar tecnologías en un periodo mínimo de 10 años, sin necesidad de re cablear el edificio.
- Proveer un sistema total de transporte de información a través de un medio común.
- Minimizar el impacto de los cambios para el cliente, ya que los cambios y alteraciones del diseño pueden hacerse sin mayores variaciones en el cableado de la instalación.
- Expansión de redes locales y otras aplicaciones nuevas.
- Fácil redistribución de las estaciones de trabajo mediante el cambio de las interconexiones dentro de las áreas de distribución.
- Otorgar compatibilidad con todos los sistemas existentes y dar una garantía de futuro basado en una arquitectura abierta, la misma que permanecerá así mientras dure la vida útil de las instalaciones.

1.17.3. Elementos de un Sistema de Cableado Estructurado

Figura 1. 47: Elementos de un Sistema de Cableado Estructurado

1.17.4. Especificación Global

Son los requerimientos generales del Sistema de Cableado como la topología, la categoría del sistema, la selección del medio de comunicación, el tipo de polarización y secuencia, las políticas y procedimientos a emplearse dentro del sistema y todo esto está sujeto normas y estándares.

a. Área de Trabajo

El cableado del área de trabajo se entiende desde la boca de telecomunicaciones conector del cableado horizontal hasta el equipo, que queda fuera de este estándar. Para los objetivos de planificación, si no se conocen las especificaciones exactas, el espacio estimado para cada área de trabajo es de 10 metros cuadrados, lo que significa un área aproximada de 3m x 3m.

El cableado del área de trabajo puede tener un máximo de 5m y puede variar su forma dependiendo de la aplicación. El cableado generalmente es no permanente y se diseña de forma tal de ser relativamente fácil su cambio.

- **Cuarto de Telecomunicaciones**

  La función principal del cuarto de telecomunicaciones es la terminación del cableado horizontal y de Backbone[15].

  Debe tener la capacidad de contener los equipos de telecomunicaciones, las terminaciones de cables y las interconexiones asociadas.

  El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información como televisión por cable, alarmas, seguridad, audio y otros sistemas de telecomunicaciones. Todo edificio debe contar con un cuarto de telecomunicaciones, no hay un límite máximo de TR.

  En el cuarto de telecomunicaciones se debe tener ciertas consideraciones:

- **Altura**

  La altura mínima recomendada del cielo raso es de 2.6 metros.

[15] Backbone.- Es el principal conducto que permite comunicar segmentos entre sí.

- **Ductos**

Se recomienda por lo menos tres ductos de 100 milímetros (4 pulgadas) para la distribución del cable del Backbone.

- **Puertas**

Las puertas de acceso deben ser de apertura completa, con llave y de al menos 91 centímetros de ancho y 2 metros de alto. La puerta debe ser removible y abrir hacia fuera (o lado a lado). La puerta debe abrir al ras del piso y no debe tener postes centrales.

- **Polvo y Electricidad Estática**

Se debe evitar polvo y la electricidad estática utilizando piso de concreto, terrazo, loza o similar (no utilizar alfombra).

- **Control Ambiental**

En cuartos que no tienen equipo electrónico la temperatura del cuarto de telecomunicaciones debe mantenerse continuamente entre 10 y 35 grados centígrados.

- **Cielos Falsos**

Se debe evitar el uso de cielos falsos en los cuartos de telecomunicaciones.

- **Prevención de Inundaciones**

Los cuartos de telecomunicaciones deben estar libres de cualquier amenaza de inundación y haber regaderas contra incendio.

- **Iluminación**

Los cuartos deben de estar bien iluminados, se recomienda que la iluminación deba estar a un mínimo de 2.6m del piso.

- **Seguridad**

Se debe mantener el cuarto de telecomunicaciones con llave y asignarlas al personal de operación.

b. Cuarto de Equipos

El cuarto de equipos provee un ambiente controlado central para albergar el equipamiento de telecomunicaciones los puntos de interconexión/ distribuidores, hardware de conectividad, empalmes, las facilidades de puesta a tierra y anclaje y los aparatos de protección. Un cuarto de equipos puede proveer tan bien algunas o todas las funciones de un cuarto de telecomunicaciones.

- **Entrada de Facilidades**

Es la entrada de servicios de telecomunicaciones al edificio. Puede contener las canalizaciones del Backbone, líneas telefónicas que vinculan con otros edificios.

c. Cableado Horizontal

Cableado Horizontal se extiende desde el área de trabajo hasta el cuarto de telecomunicaciones.

El cableado horizontal incluye:

- Las salidas (cajas, canaletas, conectores) de telecomunicaciones en el área de trabajo.
- Cables y conectores de transmisión instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones.
- Panales de empate (Patch) y cables de empate utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

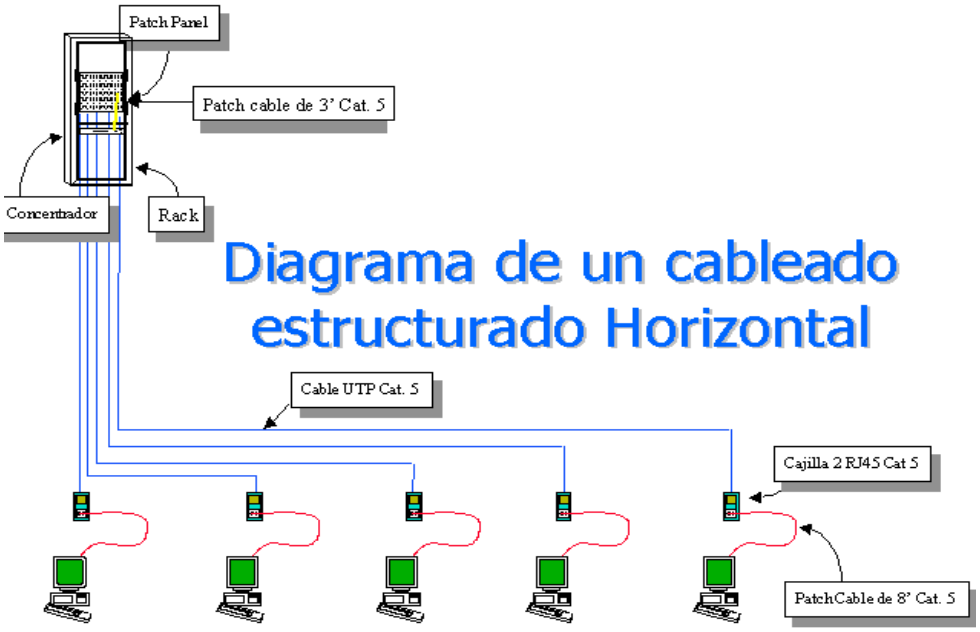


Figura 1. 48: Cableado Horizontal

- **Diseño**

El cableado horizontal deberá diseñarse para ser capaz de manejar diversas aplicaciones de usuario incluyendo:

- Comunicación de voz (teléfono).
- Comunicación de datos.
- Redes de área local
- El diseñador también debe considerar incorporar otros sistemas de información del edificio como sistemas de televisión por cable, control ambiental, seguridad, audio, alarmas y sonido.

- **Topología**

El cable horizontal se debe implementar en una topología de estrella. Cada salida del área de trabajo de telecomunicaciones debe estar conectada directamente al cuarto de telecomunicaciones.

- **Manejo de Cable**

El destrenzado de pares individuales en los conectores y paneles de empate debe ser menor a 1.25 cm y el radio de doblado del cable no debe ser menor a cuatro veces el diámetro del cable.

- **Distancia del Cable**

La distancia horizontal máxima es de 90 metros independiente del cable utilizado.

Este es la distancia desde el área de trabajo de telecomunicaciones hasta el cuarto de telecomunicaciones. Al establecer la distancia máxima se hace la previsión de 10 metros adicionales para la distancia combinada de cables de empate 3 metros y cables utilizados para conectar equipo en el área de trabajo de telecomunicaciones y el cuarto de telecomunicaciones.

- **Interferencia Electromagnética**

Al establecer la ruta del cableado se debe evitar cualquier tipo de cables eléctrico conectado a diferentes dispositivos, para esto es recomendable buscar una nueva ruta para el cableado estructurado.

- **Rutas y Espacios Horizontales**

Las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal, vertical y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones.

d. Cableado Vertical

Proporciona interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del Backbone incluye la conexión vertical entre pisos en edificios de varios pisos.
El cable de Backbone incluye medios de transmisión (cable), puntos principales y terminaciones mecánicas.

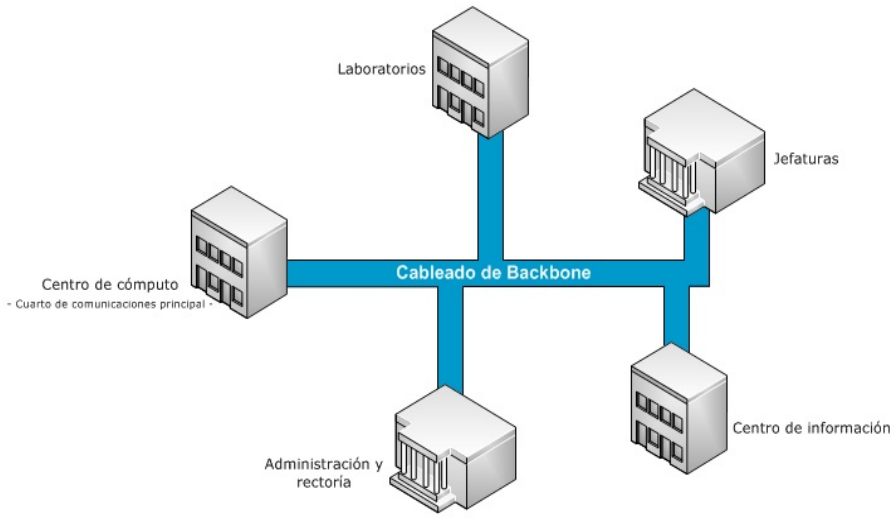


Figura 1. 49: Cableado Backbone

- **Topología**

Tiene una topología de estrella jerárquica es decir, se interconectan los gabinetes con uno que se define como centro de la estrella, en donde se ubica el equipamiento electrónico más complejo.

- **Tipo y Distancia del Cable**

  - Fibra óptica Multimodo 62.5/125 µm para aplicaciones hasta 2.000m.
  - Fibra óptica Mono modo 8.5/125 µm para aplicaciones hasta 3.000m.
  - Cable UTP para aplicaciones de voz hasta 800m.
  - Cable UTP, siempre que la distancia máxima entre el recurso y el terminal de usuario, no excedan de 100 metros.

- **Manejo de Cable**

Es importante destacar que debe presentarse un especial cuidado en la selección de estos cables, ya que además de cumplir las especificaciones de la norma por el medio en el que se instalan, deben asegurar la debida protección frente a agentes externos como humedad, roedores y perturbaciones eléctricas o electromagnéticas en el caso de que salgan al exterior de los edificios.

- **Sistema de Puesto a Tierra**

Es un componente importante de cualquier sistema de cableado estructurado moderno, el gabinete deberá disponer de una toma de tierra, conectada a la tierra general de la instalación eléctrica, para efectuar las conexiones de todo equipamiento. Los cables de tierra de seguridad serán puestos a tierra en el subsuelo.

- **Cableado de Campus**

El diseño del cableado de campus viene a ser la parte final del Diseño del Sistema de Cableado y se hace necesario cuando se desea integrar más de un edificio dentro de un mismo sistema. Al iniciar con esta parte se debe ya tener establecidos el número de salidas de comunicaciones y de distribuidores de planta por cada edificio, la situación de los distribuidores de planta, la situación del distribuidor principal por cada edificio, las tecnologías de cableado utilizadas en la parte vertical y horizontal del Sistema de Cableado, así como las rutas y medios de conducción del cable a utilizarse incluidas la distancias del mismo.

- **Indicación Dentro de Planos y Esquemas**

Se debe realizar un diagrama esquemático del Campus a implementarse situando los diferentes edificios con sus respectivos distribuidores principales, también se debe incluir los conductos disponibles para pasos de cable, las posibles rutas aéreas y las fuentes de radiación electromagnética.

- **Distribuidor de Campus**

En primer lugar se deberá establecer el mejor lugar para situar el distribuidor de Campus que viene a ser el distribuidor principal de todo el Sistema de Cableado estructurado.

Los factores que determinan la ubicación del distribuidor de Campus serán:

- Proximidad a la sala general de comunicaciones o centro general de proceso de datos.
- Proximidad al punto de acceso a la red pública.
- La relación coste/eficacia de la instalación.
- Influencias de radiación electromagnética.
- Seguridad
- Accesibilidad y espacio disponible.
- Proximidad a los ductos, medios de conducción y rutas áreas posibles.
- Estética.

Es muy conveniente integrar el distribuidor de campus en uno de los distribuidores de edificio con mayor centralización con el fin de acotar las rutas a seguir para interconectar los diferentes edificios del campus pero no se debe olvidar la accesibilidad a la red pública y evitar las fuentes de radiación electromagnética.

1.17.5. Certificar Cableado Estructurado

Un cableado estructurado puede o no ser certificado, es decir se puede realizar el servicio de certificar que el cableado cumple con todas las normas que se requieren (EIA/TIA 568A/B, TSB 67 entre otras normas) para la transmisión de datos a través de materiales categoría 5e o superior instalados de manera adecuado.

La certificación del cableado la emiten los fabricantes de los materiales utilizados para la realización del cableado y certifican, tanto la calidad de sus materiales, como la correcta mano de obra aplicada sobre la instalación de los mismos; esta certificación garantiza el buen funcionamiento del cableado.

Se puede certificar cuando la totalidad de los materiales son categoría 5e (inclusive la canaleta y/o ducteria). Para empresas pequeñas no es muy recomendable realizar esta erogación, ya que es considerable; y, un cableado que utilice materiales categoría 5e, excepto la ducteria (instalada de manera adecuada), puede tener el mismo rendimiento que un cableado certificado categoría 5e, a un menor costo.

1.18. Normas y Estándares

Los estándares son escritos y aprobados por comités formados por profesionales de la industria sobre la cual actúan dichos estándares, estos comités tienen representantes

de fabricantes, gobierno, universidades y consultores independientes quienes poseen un interés especial en la forma en que los productos y servicios son ofrecidos.

Los estándares y organizaciones que rigen la construcción de la infraestructura de un Sistema de Cableado Estructurado se muestra en el siguiente esquema:

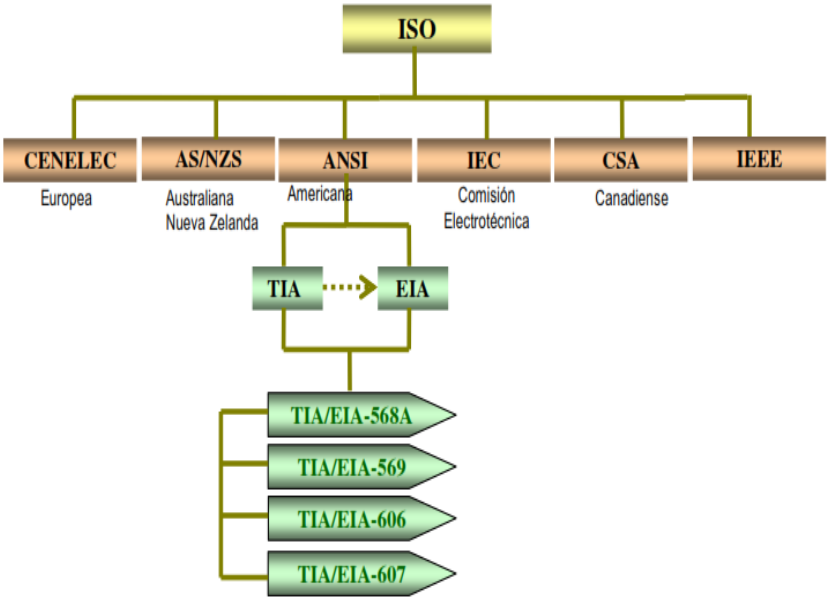


Figura 1. 50: Mapa Conceptual de Normas

1.18.1. ISO

Organización Internacional para Estandarización, es la principal organización de estándares internacional para sistemas de telecomunicaciones.

1.18.2. IEC

Comisión Internacional Electrotécnica, es una organización que certifica componentes según su desempeño eléctrico. Junto con la ISO, la IEC desarrolla el estándar ISO/IEC 1181 (Cableado genérico para áreas de clientes).

1.18.3. CENELEC

Comité Europeo para la estandarización Electrotécnica, desarrollo el estándar EN50173 utilizando en algunas partes de Europa.

1.18.4. AS/NZS

Estándar de Australia Nueva Zelanda, desarrollo un estándar similar llamado AZ/NZS3080.

1.18.5. CSA

Asociación Canadiense de Estándares, desarrollo el CSA T529, un estándar similar al ISO/IEC 11801, utilizado en Canadá.

1.18.6. IEEE

Instituto de Ingenieros Eléctricos y Electrónicos, organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y redes. Los estándares IEEE son de mayor importancia para las LAN de la actualidad.

- **IEEE 802.1.-** Cubre la administración de redes y otros aspectos relacionados con la LAN.

- **IEE 802.2.-** Protocolo de LAN de IEEE que especifica una implementación de la subcapa LLC (Control de Enlace Lógico) de la capa de enlace de datos. IEEE maneja errores, control de flujo y la interfaz de servicio de la capa de red. Se utiliza en las LAN IEEE 802.3 e IEEE 802.5.

- **IEEE 802.3.-** Protocolo de IEEE para LAN que especifica la implementación de las capas física y de la subcapa MAC[16] de la capa de enlace de datos. IEEE 802.3 utiliza el acceso CSMA/CD[17] a varias velocidades a través de diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican implementaciones para Fast Ethernet. Las variaciones físicas de las especificaciones IEEE 802.3 original incluyen 10Base2, 10Base5, 10BaseF, 10BaseT. Las variaciones físicas para Fast Ethernet incluyen 100BaseTX y 100BaseFx.

- **IEEE 802.4.-** Define una red en bus por paso de testigo. El testigo no es más que una trama de control que informa del permiso que tiene una estación para usar los recursos de la red. Ninguna estación puede transmitir mientras no recibe el testigo que la habilita para hacerlo.

- **IEEE 802.5.-** Protocolo de LAN IEEE que especifica la implementación de la capa física y de la subcapa MAC de la capa de enlace de datos. IEEE 802.5 usa de acceso de transmisión de Token a 4 Mbps o 16 Mbps en

[16] MAC (Control de Acceso al Medio)
[17] CSMA/CD (Acceso múltiple con detección de portadora y detección de colisiones), tiene la capacidad de detectar los errores que resulten al transmitir simultáneamente varias estaciones.

cableado STP o UTP y de punto de vista funcional y operacional es equivalente a Token Ring de IBM.

- **IEEE 802.11.-** Estándar para redes inalámbricas con línea visual. Es aplicada a Lans inalámbrica y proporciona 1 o 2 Mbps de transmisión en la banda de 2.4 GHz que usa cualquier frecuencia.

- **IEEE 802.11ª.-** Estándar superior al 802.11b, pues permite velocidades teóricas máximas de hasta 54 Mbps, apoyándose en la banda de los 5GHz. A su vez, elimina el problema de las interferencias múltiples que existen en la banda de los 2,4 GHz (hornos microondas, teléfonos digitales DECT, BlueTooth). Es aplicada a una LANs inalámbrica. La especificación esta aplicada a los sistemas de ATM inalámbricos.

  - **IEEE 802.11b**

  Extensión de 802.11 para proporcionar 11 Mbps usando DSSS. También conocido comúnmente como Wi-Fi (Wireless Fidelity). Es el estándar más utilizado en las comunidades inalámbricas.

  - **IEEE 802.11e**

  Estándar encargado de diferenciar entre video-voz-datos. Su único inconveniente es el encarecimiento de los equipos.

- **IEEE 802.11g.-** Utiliza la banda de 2,4 GHz, pero permite transmitir sobre ella a velocidades teóricas de 54 Mbps.

- **IEEE 802.11i.-** Está dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Cifrado Avanzado). Se implementa en WPA2.

- **IEEE 802.11n.-** La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO Multiple Input – Multiple Output, que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas.

  A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

- **IEEE 802.11w.-** Todavía no concluido. TGw está trabajando en mejorar la capa del control de acceso del medio de IEEE 802.11 para aumentar la seguridad de los protocolos de autenticación y codificación. Las LANs inalámbricas envían la información del sistema en tramas desprotegidos, que los hace vulnerables. Este estándar podrá proteger las redes contra la

interrupción causada por los sistemas malévolos que crean peticiones desasociadas que parecen ser enviadas por el equipo válido. Se intenta extender la protección que aporta el estándar 802.11i más allá de los datos hasta las tramas de gestión, responsables de las principales operaciones de una red. Estas extensiones tendrán interacciones con IEEE 802.11r e IEEE 802.11u.

1.18.7. ANSI

Instituto Nacional Americano de Estándares, es una organización que posee otros comités que reportan a ella, incluyendo:

- TIA (Asociación de la Industria de Telecomunicaciones).
- EIA (Asociación de la Industria Electrónica).

CAPÍTULO 2

SEGURIDADES EN REDES

2. INTRODUCCIÓN

Actualmente, debido a que el uso de Internet se encuentra en aumento, cada vez más compañías permiten a sus socios y proveedores acceder a sus sistemas de información, por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. La seguridad en las redes resulta esencial en este entorno, sobre todo si se puede acceder a esta desde cualquier computador, que eventualmente está expuesta y es muy vulnerable a las amenazas de personas no autorizadas que lograrían acceder a la red.

Las contramedidas que deben implementarse no sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas. Para que un sistema de red sea seguro, deben identificarse las posibles amenazas y por lo tanto, conocer y prever el curso de acción del enemigo.

2.1. OBJETIVO DE LAS SEGURIDADES

El objetivo de la seguridad en redes es describir cuales son los métodos más comunes que se utilizan para incidir ataques a la seguridad informática de una organización, y qué medidas se puedan implementar para la defensa, ya que es importante conocer cómo pueden atacar y qué soluciones se tienen para prevenir, detectar y reparar un siniestro de este tipo. Los ataques pueden servir a varios objetivos incluyendo fraude,

extorsión, robo de información, o simplemente el desafío de acceder a un sistema. Esto puede ser realizado por empleados internos de la organización que abusan de sus permisos de acceso, o por agentes externos que acceden remotamente o interceptan el tráfico de red.

A su vez, es una de las preocupaciones principales del administrador encargado de la red, debido a que en la reciente actualidad existen peligros de ataques y virus informáticos que son altamente maliciosos, y diariamente aparecen novedosas técnicas de ataques que pueden explotar un sistema de red mal protegida. Por tal motivo, es necesario desarrollar mecanismos o sistemas que protejan la red. El Internet mediante la utilización de filtros equipados se puede evitar automáticamente que un usuario no autorizado pueda acceder a la red. Lo recomendable es, además de contar con un programa anti-virus, disponer de un buen Firewall, con lo que se consiguen muchos beneficios:

- Impedir que personas no autorizadas intervengan en el sistema con fines malignos.
- Los Firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.
- Evitar que los usuarios realicen operaciones involuntarias que puedan dañar el sistema.
- Se han convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a

Internet por medio de un "traductor de direcciones", el cual puede alojarse en el Firewall.

- Asegurar los datos mediante la previsión de fallas.
- Garantizar que no se interrumpan los servicios.
- El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreo.
- Los Firewalls manejan el acceso entre dos redes, y si no existiera, todas las computadoras de la red estarían expuestos a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna.

2.1.1. DEFINICIÓN DE LA SEGURIDAD EN REDES

La Seguridad en las redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo planificado. En la seguridad de un sistema informático, hay tres conceptos[18] que entran en discusión: la vulnerabilidad o inseguridad, las amenazas y las contramedidas.

- **La Vulnerabilidad.-** Por vulnerabilidad se entiende la exposición latente a un riesgo. Es un punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático.

[18]http://www.conectronica.com/seguridad/analisis-en-torno-a-la-vulnerabilidad-de-informacion

- **Las Amenazas.-** Son un posible peligro del sistema. Puede ser una persona (hacker) o un programa (virus, caballo de Troya). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.

- **Las Contramedidas.-** Técnicas de protección del sistema contra las amenazas. La seguridad informática se encarga de la identificación de las vulnerabilidades del sistema y del establecimiento de contramedidas que evitan que las distintas amenazas posibles exploten dichas vulnerabilidades. Una regla de la seguridad informática es que: "No existe ningún sistema completamente seguro". Existen sistemas más o menos seguros, y más o menos vulnerables, pero la seguridad nunca es absoluta. No se puede hablar de un sistema informático totalmente seguro, sino más bien de uno en el que no se conocen tipos de ataques que puedan vulnerarlo, debido a que se han establecido medidas contra ellos. Las contramedidas que deben implementarse no sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas.

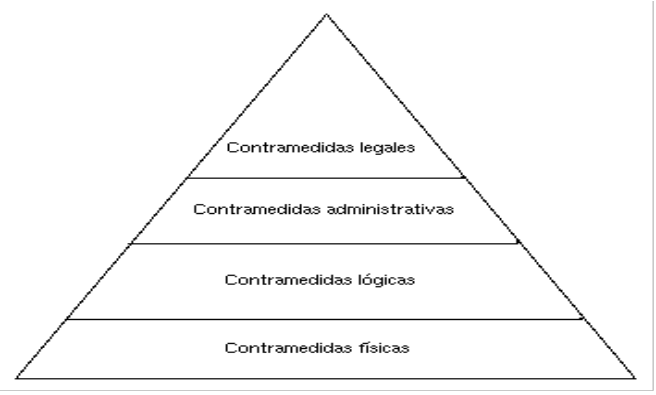


Figura 2. 1 : Pirámide donde se indica cómo se articulan las contramedidas En un sistema de seguridad informática.

2.1.2. CLASIFICACIÓN DE LAS AMENAZAS EN LA SEGURIDAD DE LAS REDES

Se entiende por amenaza una condición del entorno del sistema de información (persona, maquina, suceso o idea) que, dada una oportunidad, podrá dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

Las amenazas a la seguridad en redes se pueden clasificar en cuatro categorías:

a. Amenaza no Estructurada

Suelen ser originadas por personas inexpertas que utilizan herramientas de piratería e Internet. Algunas de estas personas suelen obrar de mala manera, pero la mayoría se ve arrastrada por los retos intelectuales que suelen conocerse como script kiddies[19], que suponen una amenaza a la seguridad de las redes. Ya que pueden introducir un virus en la red, sin ser conscientes de las consecuencias que pueden provocar.

b. Amenaza Estructurada

Son causadas por personas mucho más competentes a nivel técnico que los script kiddies, ya que conocen los diseños de los sistemas y sus puntos débiles. Pueden entender y crear scripts piratas que penetren en el sistema y además suelen dirigirse a un destino o grupo específico.

[19] Script kiddies término utilizado para describir a aquellas personas sin habilidad para programar, que utilizan programas desarrollados por otros para atacar sistemas de computadoras y redes.

c. Amenaza Externa

Suelen ser causadas por personas ajenas a la propia empresa, pero que no tienen acceso autorizado a los sistemas o a la red de la empresa. Por lo general entran en una red desde Internet o desde servidores de acceso telefónico, un atacante de este tipo tiene que realizar ciertos pasos para poder conocer que es lo que hay en ella y buscar la manera de acceder. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

d. Amenaza Interna

Habitualmente, son causadas por personas que tienen acceso autorizado a la red. Según las estadísticas, la mayor parte de incidentes de seguridad proviene de este tipo de amenazas. Generalmente estas amenazas pueden ser más serias que las externas por varias razones:

- Los usuarios conocen la red y saben cómo es su funcionamiento.
- Tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo.
- Los IPS[20] y Firewalls son mecanismos no efectivos en amenazas internas.

2.1.3. MÉTODOS DE SEGURIDAD PARA LA RED

Toda organización debe estar a la vanguardia de los procesos de cambio. Donde disponer de información continua, confiable y en tiempo real.

La irrupción de la tecnología basada en la comunicación a través de la red ha proporcionado nuevos métodos para el desarrollo de seguridades en las redes.

[20] IPS (Sistema de Prevención de Intrusos).- Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Para obtener una seguridad adecuada hay que tener en cuenta tres factores principales:

- **Método de Prevención.-** La prevención se encarga de preparar el equipo para recibir los ataques, mantener una buena política de seguridad y poder reaccionar al momento, para así evitar el ataque. Un ejemplo de prevención son los firewalls ya que ayudan a evitar el ataque. Dentro de prevención se encuentra también todo lo que se refiere a realizar unas buenas copias de seguridad, mantener diferentes equipos encargándose de la seguridad a la vez, etc.

- **Método de Detección.-** La detección se encarga de descubrir los ataques en el momento que se están realizando, y así poder contrarrestarlos debidamente. Un ejemplo de detección sería un IDS[21] bien configurado, que sepa al momento lo que está ocurriendo y alerte debidamente del suceso en tiempo real.

- **Método de Recuperación.-** Consiste en recuperar todo el equipo como se encontraba en un principio borrando el ataque para poder continuar normalmente. Dentro de la recuperación se puede encontrar también la localización del atacante.

2.1.4. RECOMENDACIONES DE SEGURIDAD PARA LA RED

Para que un sistema de red sea seguro se debe tomar en cuenta algunos factores, como los que se cita a continuación:

[21] IDS (Sistema de Detección de Intrusos).- Es un programa usado para detectar accesos desautorizados a un computador o a una red.

- Dar acceso al sistema sólo a los usuarios que vayan a hacer uso del equipo, y otorgarles los mínimos privilegios necesarios, vigilando después desde dónde se conectan para controlar posibles intrusiones, si surgen en lugares sospechosos.
- Habilitar sólo aquellos puertos y servicios que se van a usar, por ejemplo: el Ftp, Telnet, Mail y configurarlos de una manera correcta.
- Hacer uso de NIS (Network Information Services, que permite la compartición de ficheros de passwd, hosts) y NFS (Sistema de archivos de red), sólo cuando sea imprescindible, dados los problemas de configuración que suponen.
- Disponer de las últimas versiones de servidores Web, así como de sistemas operativos en constante evolución y actualización.
- Conservar las listas de correo que informan de los problemas detectados en programas y sistemas operativos, así como de los parches a esos bugs.
- La aplicación inadecuada de los parches para las vulnerabilidades de software pueden causar inoperatividad del sistema, crear debilidades en la seguridad y alterar los componentes críticos del sistema o la información. Además pueden dejar desprotegidos los sistemas informáticos y exponerlos al uso indebido por parte de personas no autorizadas, como los hackers informáticos. Siguiendo consistentemente los procedimientos de administración de parches, se podrá reducir los riesgos asociados a las vulnerabilidades de software.
- Es recomendable aplicar una buena contraseña que tenga por lo menos ocho caracteres que incluyan tanto letras como números. Una política que pida a los usuarios que cambien sus contraseñas con frecuencia, también reduce el riesgo de una violación a los sistemas.

La seguridad de redes es un nivel que garantiza que el funcionamiento de todas las máquinas de una red sea óptimo y que todos los usuarios de estas máquinas posean los derechos que les han sido concedidos, así se puede restringir que personas no autorizadas intervengan en el sistema con fines malignos y evitar que los usuarios realicen operaciones involuntarias que puedan dañar el sistema, donde también se aseguren los datos mediante la previsión de fallas que garanticen que no se interrumpan los servicios.

2.2. MECANISMOS DE SEGURIDAD EN LAS REDES

Los mecanismos adecuados para que la información de una organización o empresa sea segura, dependen de la protección que el usuario aplique para el uso normal del equipo. Esto se consigue con las garantías de confidencialidad que garantiza que la información sea accesible, protegiendo la integridad y totalidad de la información y sus métodos de proceso. También asegura la disponibilidad que garantiza a los usuarios autorizados acceso a la información y los recursos. Las amenazas actuales son más frecuentes y avanzadas en sus métodos de propagación como en los daños que causan. La complejidad de las amenazas en cuanto al ataque y a la propagación, junto a la creciente diversidad de las redes, indican que las medidas de seguridad por si solas ya no son adecuadas. Por dicha razones se deben implementar medidas de seguridad en todos los puntos vulnerables de un sistema de red, como son servidores y clientes, para establecer una completa línea de defensa de múltiples capas o denominada protección total.

Existen elementos que son indispensables en la seguridad de las redes, tales como:

2.2.1. ANTIVIRUS

Consiste en brindar protección contra archivos que ingresen a la red, a través del correo electrónico, descargas de internet, etc., los antivirus son una herramienta

simple cuyo objetivo es detectar y eliminar virus informáticos, para garantizar que nada peligroso ingrese a la red.

Los virus informáticos son programas de computadora que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras. Infecta "entidades ejecutables": cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador ejecute. Se programa en lenguaje ensamblador y por lo tanto, requiere algunos conocimientos del funcionamiento interno de la computadora.
Los daños que los virus causan a los sistemas informáticos son[22]:

- Pérdidas de información (evaluable y actuable según el caso).
- Horas de contención (horas de paradas productivas, pérdida productiva, tiempos de contención o reinstalación, cuantificables según el caso y horas de asesoría externa).
- Pérdida de imagen (valor no cuantificable).

El software antivirus no solo debe proteger los servidores y las estaciones de trabajo, sino también los firewalls y aplicaciones importantes como servidores web y correo electrónico. Para evitar la acción de la mayoría de los virus actuales, debe actualizar el software antivirus de forma periódica. La mayoría de los tipos de software antivirus se pueden configurar para que se actualicen de forma automática.

2.2.2. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

Un sistema de detección de intrusos o IDS, es un programa usado para la detectar accesos no autorizados a un computador o una red. Su función consiste en monitorear

[22] http://www.microsoft.com/spain/protect/computer/basics/antivirus.mspx

constantemente el tráfico de la red en busca de actividades sospechosas o ataque directos, que pueden dar ataques de habilidosos hackers que usan herramientas sofisticadas para la incursión dentro de la red, donde se debe actuar de una forma inmediata ante dicho evento. La detección de intrusos es especialmente útil cuando se utiliza conjuntamente con un firewall, convirtiéndose en una herramienta muy poderosa, los datos forzosamente deberán pasar por este tramo, donde serán bloqueados antes de acceder a la red. Los IDS buscan patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre la red o host.

a. Tipos de IDS

Existen tres tipos de sistemas de detección de intrusos[23]:

- HIDS (HostIDS): El principio de funcionamiento del HIDS, depende del éxito de los intrusos, que generalmente dejaron rastros de sus actividades en un equipo atacado. El HIDS intenta detectar tales modificaciones en el equipo afectado.
- NIDS (NetworkIDS): Está basado en la red, detectando ataques a todo el segmento conformado. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.
- DIDS (DistributedIDS): Sistema basado en la arquitectura cliente-servidor, compuesto por una serie de NIDS, que actúan como sensores centralizando la información de posibles ataques en una unidad central, que son almacenados o recuperados en una base de datos, es una estructura habitual en redes privadas virtuales.

[23] http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos

b. Características del IDS

Los IDS pueden prevenir y sobretodo dar la alerta anticipada ante cualquier actividad sospechosa. No están diseñados para detener un ataque, aunque sí pueden generar ciertos tipos de respuesta ante éstos.

Aumentan la seguridad de un sistema, vigilan el tráfico de una red, examinan los paquetes analizándolos en busca de datos sospechosos y detectan las primeras fases de cualquier ataque como pueden ser el análisis de la red, barrido de puertos, etc. Supervisan la actividad del sistema y del usuario para luego analizarla en cuanto a problemas como ataques al nombre del usuario por usuarios no autorizados o paquetes de información que contengan códigos malignos.

Revisan la integridad de la información fundamental y archivos del sistema para asegurarse que los usuarios no autorizados no la han alterado. Inspeccionan las configuraciones del hardware y software de un sistema a fin de señalar proactivamente los aspectos vulnerables de la red como características o errores que aumenten la posibilidad de daños por acción de los hackers o accidentes.

Buscan patrones anormales de actividad en el intercambio rutinario de la información en la red. Protegen un sistema operativo de toda actividad del usuario que sea una violación de las políticas de seguridad de la red. El software para la detección de intrusiones no sabe automáticamente qué constituye una violación de forma que debe configurarse de acuerdo a las políticas individuales de seguridad. Después de completar cada uno de los pasos anteriores, el software alertará si detecta una violación de la seguridad.

2.2.3. REDES VIRTUALES PRIVADAS (VPN)

Las redes virtuales privadas protegen las conexiones remotas más allá del perímetro para poder establecer comunicaciones seguras a través del Internet.

a. Características de las VPN

- **Autenticación y autorización:**Que persona tiene al acceso al sistema y el nivel de permisos que debe tener, verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.
- **Integridad:** Que los datos enviados, antes deben ser cifrados para que así no puedan ser leídos.
- **Confidencialidad:** Dado que solo pueden ser interpretado por nadie más que los destinarios de la misma.
- **Administración de claves:** Las VPN deben actualizar las claves de cifrado para los usuarios que pertenecen a la red.

b. Tipos de Conexión de las VPN[24]

Existen tres conexiones en VPN:

- **Conexión de Acceso Remoto:** Es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y este se autentifica al servidor de acceso remoto.
- **Conexión Router a Router:** Es realizada por un Router, y esta a su vez se conecta a una red privada. El Router que realiza la llamada se autentifica

[24] http://es.wikipedia.org/wiki/Red_privada_virtual

ante el Router que responde y este a su vez se autentica ante el Router que realiza la llamada y también sirve para la intranet.

- **Conexión Firewall a Firewall:** En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

c. Ventajas de las VPN

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costos y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.
- Son utilizadas más en campus de universidades

2.2.4. FIREWALLS

El firewall es un dispositivo que funciona como cortafuegos, permitiendo o denegando las transmisiones de una red a la otra, utilizado como un dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial, para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser: la web, correo electrónico o el IRC[25], dependiendo del servicio, el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente, y dependiendo de su dirección puede permitirla o no. Son una importante línea de defensa de la red y de toda la información para garantizar que no sucedan accesos no autorizados.

[25] IRC (Internet Relay Chat).- Es un protocolo de comunicación en tiempo real basado en texto, que permite debates entre dos o más personas.

2.2.5. OTRAS OPCIONES QUE SE PUEDEN IMPLANTAR

- Creación de políticas de seguridad: Se debe establecer cuáles son los recursos más valiosos de información, derechos y permisos de acceso a la misma dado en los usuarios y administradores que se describe que se va o está tratando de proteger. Además se deben determinar normas para el acceso remoto. Las políticas de seguridad son una parte fundamental de cualquier esquema de seguridad eficiente.
- Actualizar parches: Es necesario actualizar los sistemas operativos, aplicaciones y productos de seguridad con los últimos parches para asegurar muchas puertas abiertas frente a las amenazas que han sido usadas para difundirse y dañar los sistemas o programas de la red. Los parches de seguridad son especialmente usados en aplicaciones que interactúan con el internet.
- Configuración del disco: Permite realizar copias y recuperarlo a su estado inicial seguro y poder confiar en la integridad de la información, de esta manera se mejora la planeación de la preparación de desastres, ya que se pueden recuperar si se producen daños, se aplica cuando ya se ha producido alguna alteración dentro del sistema.
- Restricción y control en el acceso a la red: Es importante asignar únicamente los permisos que el usuario necesita para acceder a la red, que es el punto más vulnerable en cualquier red.
- Reforzar la administración de las contraseñas: Es elemental que los usuarios cambien con frecuencias sus contraseñas y tengan cuidado de no anunciarlas públicamente cuando un usuario es incapaz de mantener en secreto, una clave de acceso o información confidencial, también instruir a los usuarios para que conozcan sus funciones en la relación con el mantenimiento de la seguridad informática. Es por tal motivo que tiene

una gran importancia el impulsar una cultura de concientización a los usuarios acerca de los peligros acerca de este tema.

2.3. VIOLACIONES A LAS SEGURIDADES EN REDES

Es el falseamiento, es decir, la modificación previa a la introducción de los datos en el sistema informático o en una red.

Actualmente, cuando se habla de violaciones a la seguridad en las redes de computadoras, se hace una gran referencia a Internet, pues es dentro de esa red de alcance mundial que se producen con mayor frecuencia los ataques a nuestras computadoras. De esta forma, se tiene posibles violaciones de seguridad a un sistema, o sea, varias amenazas.

2.3.1. INTRUSOS

Los intrusos en las violaciones de las redes, son personas o programas que consigue acceder a los datos, archivos o carpetas de los cuales no tiene acceso permitido, cuyo único propósito es invadir la privacidad de tu computadora, posiblemente dejando daños y alterando el software del equipo.

2.3.2. GUSANOS (WORMS)

Son programas que constantemente viajan a través de un sistema informático interconectado, sin dañar necesariamente el hardware o el software de los sistemas que visitan. Su función principal es viajar en secreto a través de equipos anfitriones recopilando cierto tipo de información programada (tal como los archivos de password) para enviarla a un equipo determinado al cual el creador del virus tiene acceso, tiene la propiedad de duplicarse a sí mismo. Los gusanos usan las partes

automáticas de un sistema operativo que generalmente son invisibles al usuario, se basan en una red de computadoras para enviar copias de sí mismos a otras computadoras, utilizando el Internet como medio de propagación.
Existen básicamente 3 métodos de propagación en los gusanos:

- **Correo electrónico.-** Se envía una copia de sí mismo a todos los usuarios que parecen en las libretas de direcciones que encuentra en el computador dónde se ha instalado.

- **Mecanismos basados en RPC (Remote Procedure Call).-** Ejecuta una copia de sí mismo en todos los sistemas que aparecen en la tabla de rutas.

- **Mecanismos basados en RLOGIN.-** El gusano se conecta como usuario en otros sistemas y una vez en ellos, se copia y ejecuta de un sistema a otro.

2.3.3. TROYANOS

Son programas que simplemente facilita el control remoto de un computador, también denominados "malware" y realmente no son más que aplicaciones de gestión remota, que por ser totalmente gratuitos están muy difundidos y suelen utilizarse para el acceso a otros computadores de la red sin el debido permiso. Están habitualmente ocultos dentro de otro programa, e-mail, fichero, etc. Se ejecutan automáticamente, haciendo copias de sí mismos dentro de otros programas a los que infectan. Dependiendo del modo en que atacan y se propagan reciben un nombre, este clase de virus pueden ser altamente peligrosos, porque se ocultan dentro de otro para evitar ser detectado, e instalarse de forma permanente en el sistema. Este tipo de software no suele realizar acciones destructivas por sí mismo, pero entre muchas otras funciones, tienen la capacidad de capturar datos, generalmente contraseñas e información

privada, enviándolos a otro sitio. Otra de sus funciones es dejar indefenso el sistema, abriendo brechas en la seguridad, de esta forma se puede tomar el control total de forma remota, como si realmente se estuviera trabajando delante de la pantalla. Estos programas son llamados espías, pues recolectan información del usuario con fines que pueden ser maliciosos. Algunos programas antivirus los detectan como virus o como caballos de Troya (o simplemente troyanos).

2.3.4. VIRUS INFORMÁTICOS

Los virus informáticos son programas que se introducen de forma oculta en un computador para ejecutar acciones no deseadas por sus usuarios. Se dice que es un programa parásito porque consiste en atacar archivos. Su objetivo es alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, remplazan archivos ejecutables por otros infectados con el código de este, que pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos. Tienen diferentes finalidades: algunos sólo infectan, otros alteran datos, otros los eliminan, algunos sólo muestran mensajes. Pero el fin último de todos ellos es el mismo: adjuntarse a un programa o archivo de forma que pueda propagarse, infectando los ordenadores a medida que viaja de un ordenador a otro.

Módulos de Reproducción de los Virus

Es importante destacar que el potencial del daño de un virus informático no depende de su complejidad pero si del entorno donde interactúa. Se pueden distinguir tres módulos principales de un virus informático:

- **Módulo de Reproducción.-** Se encargan de manejar las rutinas de "parasitación" de entidades ejecutables (o archivos de datos, en el caso de los virus macro) a fin de que el virus pueda ejecutarse discretamente. Pudiendo, de esta manera, tomar control del sistema e infectar otras entidades permitiendo se traslade de una computadora a otra a través de algunos de estos archivos.
- **Módulo de Ataque.-** Es optativo y está encargado de manejar las rutinas de daño adicional del virus. Por ejemplo, existen virus que además de producir daños muy pronunciados, tiene un módulo de ataque que se activa cuando el reloj de la computadora indica una fecha determinada. En estas condiciones la rutina actúa sobre la información del disco duro volviéndola inutilizable.
- **Módulo de Defensa.-** Tiene la misión de proteger al virus y, como el módulo de ataque, puede estar o no presente en la estructura. Sus rutinas apuntan a evitar todo aquello que provoque la eliminación del virus y retardar su detección.

Los virus informáticos son los causantes de innumerables daños tanto en software como el hardware.

Daño en el Software

- Modificación de programas para que dejen de funcionar correctamente.
- Modificar datos.
- Eliminar programas, datos o archivos.
- Hacer que el sistema funcione lentamente, es decir colgar el sistema.
- Acabar con el espacio libre en el disco duro.

Daño en el Hardware

- Borrado del BIOS.

Formas de propagación de los virus

- Memoria Flash u otro medio de almacenamiento removible.
- Redes de computadoras.
- Mensajes de correo electrónico.
- Software descargado de Internet.

Señales que indican la presencia de virus

- Cambios en la longitud de los programas.
- Cambios en la fecha y/u hora de los archivos.
- Retardos al cargar un programa.
- Operación más lenta del sistema.
- Reducción de la capacidad en memoria y/o disco duro.
- Mensajes de error inusuales.
- Actividad extraña en la pantalla.
- Fallas en la ejecución de los programas.
- Fallas al reiniciar el equipo.
- Unirse a un programa instalado en el ordenador permitiendo su propagación.
- Mostrar en la pantalla mensajes o imágenes humorísticas, generalmente molestas.
- Ralentizar o bloquear el ordenador.

- Destruir la información almacenada en el disco, en algunos casos vital para el sistema, que impedirá el funcionamiento del equipo.
- Molestar al usuario cerrando ventanas, moviendo el ratón, etc.

Clasificación de los virus[26]

Los virus se pueden clasificar de la siguiente forma:

- **Virus residentes.-** La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De esta manera, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados.
- **Virus de acción directa.-** Al contrario que los residentes, estos virus no permanecen en memoria, por lo tanto, su objetivo principal es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos.
- **Virus de sobre-escritura.-** Se caracterizan por destruir la información contenida en los ficheros que infectan, haciéndolo que queden total o parcialmente inservibles.
- **Virus de boot o de arranque.-** Infectan el sector de booteo o arranque de discos duros o diskettes. Las PC se infectan cuando se arranca el equipo con el diskette infectado, siempre y cuando el setup de la PC esté programado para arrancar primero desde el drive A. Si por el contrario el setup inicia primero desde el disco duro, no es necesario preocuparse por este tipo de virus.

[26] http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico

- **Virus de macro.-** Los virus macro se esparcen fácilmente a través de archivos adjuntos de e-mails, unidades de almacenamiento magnéticas, programas obtenidos en Internet, transferencia de archivos y aplicaciones compartidas. Algunas macros son tan potentes que deben considerarse instrucciones de programación. Las macros del paquete Office, son en realidad un subconjunto de instrucciones de Visual Basic y son muy fáciles de crear. Pueden infectar diferentes puntos de un archivo en uso, por ejemplo, cuando éste se abre, se graba, se cierra o se borra. Este tipo de virus se activa al abrir un archivo infectado dentro del procesador de texto.
- **Virus de enlace o directorio.-** Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos.
- **Virus cifrados.-** Más que un tipo de virus, se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones. Estos virus se cifran a sí mismos para no ser detectados por los programas antivirus.
- **Virus polimórficos.-** Son virus que en cada infección que realizan se cifran de una forma distinta (utilizando diferentes algoritmos y claves de cifrado). De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas, por lo que suelen ser los virus más costosos de detectar.
- **Virus multipartites.-** Virus muy avanzados, que pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc.

- **Virus de Fichero.-** Infectan programas o ficheros ejecutables (ficheros con extensiones EXE y COM). Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos.
- **Virus FAT.-** Los virus que atacan a este elemento son especialmente peligrosos, ya que impedirán el acceso a ciertas partes del disco, donde se almacenan los ficheros críticos para el normal funcionamiento del ordenador.
- **Virus Bug-Ware.-** Son programas que en absoluto no son virus informáticos, sino fragmentos de código mal implementado, que debido a fallos lógicos, dañan el hardware o inutilizan los datos del computador. En realidad son programas con errores, pero funcionalmente el resultado es semejante al de los virus.
- **Virus de arquitectura cliente / servidor.-** La funcionalidad de estos virus consiste en hacer que la víctima del ataque ejecute un programa que corresponde al servidor del virus, lo que conduce a su auto instalación en el sistema a la espera de que el usuario conecte su computadora a Internet. En este grupo se incluyen de manera especial a los troyanos, que más que virus, son verdaderas aplicaciones cliente / servidor, por las cuales cualquier persona, y con la configuración adecuada, puede controlar los recursos de una PC a distancia y a través de una conexión a Internet.
- **Virus en archivos "fantasmas".-** Estos virus basan su principio en DOS (Sistema Operativo de Disco), al tener dos archivos con el mismo nombre, ejecuta primero el archivo con extensión COM y luego el punto EXE, siempre y cuando estos archivos se encuentren en el mismo directorio. Al infectar la computadora, el virus crea un archivo punto COM con el mismo nombre y en el mismo lugar que se encuentre el punto EXE. De este modo, se asegura que durante la

próxima ejecución, el sistema operativo arrancará el nuevo archivo punto COM creado por el virus y conteniendo el código viral, para luego ceder el control al archivo punto EXE.

- **Virus de e-mail.-** Dentro de este grupo, se incluyen dos tipos de virus: los que junto a un mail hacen llegar un archivo adjunto que necesariamente debe abrirse o ejecutarse para activar el virus, y también están los gusanos (worms) que aprovechan los agujeros de seguridad de programas de correo electrónico para infectar a las computadoras. Esta variedad difiere de los otros virus en el hecho de que no necesitan de la ejecución de un programa independiente para ser activados, sino que ingresan e infectan las PCs con la simple visualización del mail.
- **Virus de archivos ejecutables.-** Infectan los archivos que la PC toma como programas: ".EXE, *.DRV, *.DLL,*.BIN, *.OVL, *.SYS e incluso BAT". Pueden permanecer residentes en memoria durante mucho tiempo después de haber sido activados, en ese caso se dice que son virus residentes, o pueden ser virus de acción directa, que evitan quedar residentes en memoria y se replican o actúan contra el sistema sólo al ser ejecutado el programa infectado. Se dice que estos virus son virus de sobre-escritura, ya que corrompen al fichero donde se ubican.

2.3.5. SPAM (CORREO BASURA) Y SPYWARE (SOFTWARE ESPÍA)

Cuando se navega en Internet, se puede encontrar ventanas que sugieren instalar ciertos programas, o que ofrecen premios y regalos. Si se acepta, se expone a que se

instalen en el equipo aplicaciones de tipo spyware, adware o dialers[27]. Los daños o inconveniencias que pueden causar son los siguientes:

- Ocupan el ancho de banda en la conexión a Internet, haciendo la navegación más lenta.
- Obligan al usuario a visitar sitios indeseados, que pueden incluir juegos de azar, productos basura y hasta contenidos indecentes.
- La lenta conexión a Internet implica que el usuario pague más dinero por el servicio de conexión.
- Usuarios maliciosos pueden estar recibiendo información privada, que incluye números de tarjetas de crédito y contraseñas.
- Un virus se puede distribuir a todos sus contactos de correo electrónico.
- En resumen, cualquier persona puede estar espiando a otra que esté navegando en Internet.

2.3.6. CABALLOS DE TROYA

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuestos no autorizados y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto. Un ejemplo simple de un Caballo de Troya es un programa que hace las veces de una útil calculadora, pero, en la medida que es usada, borra o corrompe archivos del disco duro, sin que el usuario se percate.

[27] Dialers.- Son programas que se instalan en el ordenador y que, llaman a números de tarifación adicional sin que el usuario lo sepa.

2.3.7. CRACKER

Su principal objetivo es producir daños que en muchos casos suponen un problema de extrema gravedad para el administrador del sistema. Es una persona que mediante ingeniería inversa realiza: seriales, Keygens[28] y crack, los cuales sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original, done se viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

2.3.8. HACKERS

Este término normalmente es utilizado para identificar a una persona que únicamente accede a un sistema protegido sin intentar causar daños, especializado en penetrar en las bases de datos de sistemas informáticos estatales con el fin de obtener información secreta, que lo utiliza para un determinado objetivo. Tradicionalmente se considera Hacker al aficionado a la informática cuya afición es buscar defectos y puertas traseras para entrar en una red, el método más utilizado son los denominados: Caballos de Troya.

2.3.9. SEÑUELOS

Suelen ser programas diseñados para hacer caer en una trampa a los usuarios, cuando un usuario puede sustituir el login por un programa que si intenta entrar al root donde notifique el password. El intruso instala un programa que registre las teclas presionadas para después analizar la información en busca de password.

[28] Keygens programas generalmente ilegales, que al ejecutarse genera un código para que un determinado programa de software de pago en su versión de prueba pueda ofrecer los contenidos completos.

2.3.10. SUPERZAPPING

Se denomina Superzapping al uso no autorizado de un programa de editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un computador. El nombre proviene de una utilidad llamada SUPERZAP diseñada para Mainframes y que permite acceder a cualquier parte del computador y modificarlo

2.3.11. PUERTAS FALSAS

Es una práctica común en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc. Con el objeto de producir un atajo para ir corrigiendo los posibles errores. Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario estas rutinas no se eliminan del programa y proveen al hacker de accesos o facilidades en su labor si sabe descubrirlas.

2.3.12. BOMBAS LÓGICAS

Consiste en introducir un programa o rutina que en una fecha determinada destruirá o modificará la información, o provocará la caída del sistema.

2.3.13. VULNERABILIDADES EN REDES

Vulnerabilidad es definida como un fallo en el proyecto implementación o configuración de un sistema operativo que, cuando es descubierta por un atacante, resulta en la violación de la seguridad de un computador o un sistema computacional.

En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones. Las vulnerabilidades son el resultado de bugs o de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas, porque, en principio, no existe sistema totalmente seguro. Por lo tanto existen vulnerabilidades teóricas y vulnerabilidades reales.

Las vulnerabilidades en las aplicaciones suelen corregirse con parches, hotfixs o con cambios de versión. En tanto algunas otras requieren un cambio físico en un sistema informático, se descubren muy seguidos en grandes sistemas, y el hecho de que se publiquen rápidamente por todo internet (mucho antes de que exista una solución al problema), es motivo de debate. Mientras más conocida se haga una vulnerabilidad, más probabilidades de que existan piratas informáticos que quieren aprovecharse de ellas.

2.3.14. Vulnerabilidad en los Sistemas Operativos

La mayoría de los ataques se basan en fallos de diseño inherentes a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son solucionables en un corto plazo. La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos. Muchos sistemas están expuestos a los agujeros de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por varias razones, y miles de puertas invisibles que son descubiertas cada día en sistemas operativos, aplicaciones de software, protocolos de red, exploradores de Internet, correo electrónico y toda clase de servicios

informáticos disponibles. Los Sistemas operativos abiertos (como Unix y Linux) tienen agujeros más conocidos y controlados que aquellos que existen en sistemas operativos cerrados (como Windows). La importancia y ventaja del código abierto radica en miles de usuarios que analizan dicho código en busca de posibles bugs y ayudan a obtener soluciones en forma inmediata. Actualmente, se están descubriendo casi de forma continua, vulnerabilidades en los sistemas operativos Windows de Microsoft. Por esta razón, se editan parches para corregir las deficiencias del sistema Windows frente a posibles ataques maliciosos.

2.3.15. Vulnerabilidad en los Protocolos de Comunicación[29]

Los protocolos son como reglas de comunicación que permiten el flujo de información entre computadoras distintas que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas hablen el mismo idioma, por tal sentido, el protocolo TCP/IP fue creado para las comunicaciones en Internet. Para que cualquier computador se conecte a Internet, es necesario que tenga instalado este protocolo de comunicación.

2.3.16. Vulnerabilidad en el Protocolo TCP

La que sería una importante vulnerabilidad en el protocolo TCP, consiste en que cualquier atacante podría interrumpir a su antojo todas las conexiones realizadas entre servidores y Routers, causando un gran caos en Internet. Junto a IP, TCP es uno de los protocolos fundamentales para el funcionamiento de Internet. Y aunque aún existe cierta confusión sobre los detalles del problema, la mayoría de los escenarios afectados son tremendamente críticos. En principio serían todos aquellos que utilizan

[29] http://www.vsantivirus.com/ev-vul-tcp.htm

conexiones de larga duración y gran ancho de banda. Uno de los protocolos más afectados por esta vulnerabilidad en TCP, es el llamado BGP (Border Gateway Protocol), que se emplea para el intercambio de información de enrutamiento y el mantenimiento de las tablas de direcciones IP, y que hace uso intensivo de las conexiones TCP, sin utilizar ningún tipo de autenticación. Además del protocolo BGP, otros protocolos como DNS que es usado para la resolución de nombres, y todos los protocolos que utilizan cifrado SSL, también serían vulnerables.

Casi cualquier protocolo que se basa en la utilización de conexiones TCP persistentes en el tiempo, y cuyos puertos y direcciones IP puedan ser identificados, prácticamente todos los servicios de Internet conocidos, serían vulnerables. Por lo general cualquier protocolo que se base en la utilización de conexiones TCP persistentes a larga duración, que utilicen un puerto TCP de origen fácilmente identificable y con direcciones IP del origen y el destino identificables pueden llegar a ser vulnerables.

2.3.17. Vulnerabilidad de Kerberos

Kerberos.- Es el protocolo predefinido que proporciona la autenticación segura de usuario en Windows, siendo además un estándar de la industria. Existe una vulnerabilidad capaz de provocar una denegación de servicio en este protocolo. Esto permite que un atacante pueda enviar un mensaje especialmente modificado a un controlador de dominio, causando que el servicio responsable de la autenticación de usuarios en un directorio activo de dominio, deje de responder. Se ha detectado un problema de seguridad que podría permitir a un usuario malintencionado obtener acceso a información confidencial transmitida a través de un equipo basado en Microsoft Windows dentro de un entorno de dominio y realizar ataques por denegación de servicio contra los controladores del dominio. Puede mejorar la

protección del equipo con esta actualización de Microsoft. Tras instalar este elemento, es posible que deba reiniciar el equipo.

2.3.18. Vulnerabilidad de PKINIT

PKINIT.- Es el protocolo utilizado por el proceso de autenticación basado en claves públicas integrado con el sistema de control de acceso Kerberos de Windows. Existe una vulnerabilidad en este protocolo que puede permitir la revelación de información y el Spoofing[30] que es una falsificación de servidor. Un atacante puede interferir con cierta información que se envía a un controlador de dominio y potencialmente acceder a comunicación sensible de la red del cliente. Los usuarios pueden creer estar accediendo a un servidor confiable, cuando en realidad están en un servidor malicioso controlado por el atacante. Para que el ataque sea exitoso, el atacante debe inyectarse primero en el medio de una sesión de autenticación como intermediario entre el cliente y el controlador de dominio.

2.3.19. Tipos de Ataques en la Redes

Los ataques siempre se producen en Internet, a razón de varios ataques por minuto en cada equipo conectado. En su mayoría, se lanzan automáticamente desde equipos infectados (a través de virus, troyanos, gusanos, etc.) sin que el administrador conozca lo que está ocurriendo. Los ataques pueden ejecutarse por diversos motivos:

- Obtener acceso al sistema.
- Robar información, como secretos industriales o propiedad intelectual.
- Recopilar información personal acerca de un usuario.
- Conseguir información de cuentas bancarias.

[30] Spoofing uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

- Obtener información acerca de una organización (la compañía del usuario, etc.).
- Afectar el funcionamiento normal de un servicio.
- Utilizar el sistema de un usuario como un "rebote" para un ataque.

Los ataques se pueden producir en cualquier lugar, siempre y cuando exista una vulnerabilidad que se pueda aprovechar, existen varios tipos de ataques a una red, como son:

- **Ataque de Reconocimiento.-** Un intruso trata de descubrir sistemas, servicios y puntos débiles. Este reconocimiento tiene lugar cuando un usuario no autorizado trata de descubrir dispositivos, servicios disponibles y puntos débiles del sistema de red. También se conoce como recopilación de información y suele preceder a un acceso real o a un ataque de denegación de servicio.El intruso primero barre la red con pings para determinar que direcciones IP están activas y responden. Esto permite localizar información acerca de los servicios o puertos activos en las direcciones IP. Con dicha información, el intruso consulta los puertos de la aplicación con el fin de determinar el tipo y versión de la aplicación y del sistema operativo que se está ejecutando en el host de destino.
- **Ataque de Acceso.-** Un intruso ataca las redes o sistemas para recuperar datos, obtener acceso o incrementar sus privilegios de acceso personales. El acceso es un término muy amplio que hace referencia a la capacidad que tiene un origen completo de conectarse con un destino concreto. Luego de determinar el destino, el atacante usa algún software para llegar a él. Un ataque de acceso puede materializarse como recuperación y manipulación no autorizada de datos, un acceso al sistema o incremento de privilegios. Además

pueden ser utilizados para obtener el control de un sistema e instalar y ocultar software para que los hackers lo utilicen posteriormente.

- **Ataques de Denegación de Servicio (DOS).-** Tiene lugar cuando un atacante desactiva o corrompe las redes, los sistemas o los servicios para denegar el servicio a los usuarios. Esto implica que el sistema se colapse o que se vuelva lento hasta un punto que sea inutilizable. Estos ataques también pueden ser tan sencillos como borrar o corromper información necesaria. Generalmente, el ataque consiste en ejecutar un script o una herramienta. El atacante no necesita tener acceso previo al destino, sino solo una ruta a éste. Un ataque de denegación de servicio distribuida (DDOS) es aquel en el que el origen del ataque proviene de muchas computadoras, haciendo que sea muy complicado localizar y detener el origen.
- **Ataques de Modificación-Daño.-** Este tipo de ataques son los más peligrosos porque actúan sobre los datos o los programas instalados, modificando o borrando los archivos. Estos ataques necesitan primero de los anteriores para obtener la información necesaria de la red y normalmente es el objetivo final de un intruso, tiene efecto sobre el software o los datos del sistema con la finalidad de sustituir el original por un malicioso, y los archivos de datos de la víctima por otros que pueden llevar incorporados virus.
- **Ataque por Rebote.-** Cuando se ejecuta un ataque, el pirata informático siempre sabe que puede ser descubierto, por lo que generalmente privilegia los ataques por rebote, que consiste en atacar un equipo a través de otro para ocultar los rastros que podrían revelar la identidad del pirata (como su dirección IP) con el objetivo de utilizar los recursos del equipo atacado. Esto comprueba la importancia de proteger su red o PC, ya que podría terminar siendo cómplice de un ataque y, si las víctimas realizan una denuncia, la primera persona cuestionada será el propietario del equipo que se utilizó como rebote. Con el desarrollo de las redes inalámbricas, este tipo de situación

podría ser cada vez más común ya que estas redes no son demasiado seguras y los piratas ubicados en sus inmediaciones podrían usarlas para ejecutar un ataque.

- **Ataque de Autentificación.-** Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password. El atacante accede al sistema suplantando la identidad de algún usuario preferentemente el administrador con la información que se obtuvo del ataque de escaneo, y después va saltando por la red, aprovechando las relaciones de confianza entre las redes. En cada nueva red accesible el atacante realiza de nuevo escaneo para acceder como usuario legítimo y en conjunto desde el origen al destino pueden existir muchas estaciones, esto genera muchos problemas a la hora de rastrear.
- **Ataque de Escaneo.-** Los ataques de escaneo se realizan para la recopilación de información sobre posibles puertas de acceso a la red. Consisten en recopilar la información de que puertos están escuchando en la red para posteriormente acceder a los recursos a través de ellos, que es el encargado de utiliza puertos virtuales para realizar el envío y recepción de los datos por la red adoptando la estrategia cliente/servidor, escucha permanente por determinados puertos para recibir los datos que se van a transmitir de un equipo a otro.
- **Recuperación no autorizada de datos.-** Consiste en leer, escribir, copiar o trasladar archivos a los cuales el intruso no puede acceder. El intruso solo tendrá problemas cuando el archivo esté cifrado y no pueda ser leído.
- **Acceso no autorizado al sistema.-** La obtención de acceso a sistemas que incorporen cierta seguridad puede implicar la ejecución de un script o el uso de una herramienta que explote un punto débil de la aplicación o sistema que

está siendo atacado. Los puntos débiles del sistema operativo también pueden ser utilizados para proporcionar un acceso no autorizado al sistema.

- **Incremento no autorizado de los privilegios.-** Los usuarios legítimos con niveles muy bajos de privilegio o los intrusos que tienen un acceso muy restringido son los más propensos a realizar este tipo de ataque. El objetivo es obtener información o procedimientos de ejecución para los que no tiene acceso autorizado. Esto implica obtener acceso a la raíz en un sistema Unix e instalar un sniffer[31] para capturar el tráfico de la red, detectando los cuellos de botella y problemas que existan. El objetivo final consiste en localizar nombres de usuario y contraseñas que puedan ser utilizados para acceder a otro destino.

2.4. POLÍTICAS DE SEGURIDAD EN LAS REDES

Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización proviene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos.

Las políticas de seguridad en las redes han tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes de las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información. Se debe concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que

[31] Sniffer.- Es un programa de para monitorear y analizar el tráfico en una red de computadoras.

permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas, y es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

2.4.1. GENERALIDADES

Las políticas de seguridad surgen como una herramienta organizacional para concientizar a los usuarios de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la compañía, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del ambiente dinámico que rodea las organizaciones modernas.

2.4.2. CONCEPTO

Una política de seguridad informática es un conjunto de reglas y procedimientos que definen la manera en que una organización maneja, administra, protege, previene y asigna recursos para alcanzar el nivel de seguridad requerido sobre riesgos de diferentes daños, donde se debe tomar en cuenta:

- Todo está prohibido a menos que se permita explícitamente.
- Todo está permitido a menos que se prohíba explícitamente.

En ocasiones se utilizan combinaciones de éstas, para diferentes partes del sistema, La primera clave, asume que se puede obstruir cada uno de los servicios o aplicaciones deseadas. La segunda, indica que se puede desplazar cada servicio potencialmente peligroso y necesitará ser aislado básicamente caso por caso. Con esto, las políticas de seguridad se basarán en una conducción cuidadosa, analizando la seguridad y la asesoría en caso de riesgo que se presente.

No se puede considerar que una política de seguridad a la descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de lo que se desea proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus usuarios a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

2.4.3. OBJETIVO

El objetivo en las políticas de seguridad de red, hacen énfasis en proteger la red y la información de los sistemas de una manera adecuada, tratando de informar al mayor nivel de detalle a los usuarios, empleados y gerentes de las normas y mecanismos que deben cumplir y utilizar para salvaguardar los componentes de los sistemas de la organización, ya que la administración requiere que la información contenida en sus sistemas sea integra y que pueda tener la certeza para la toma de decisiones, como por ejemplo:

- Informar a los usuarios de la red sus obligaciones para proteger todos los recursos disponibles.

- Especificar los mecanismos a través de los cuales estos requerimientos pueden ser logrados.
- Proveer una guía que permitirá implementar, configurar y controlar los sistemas de la red para determinar su conformidad con la política.

Dentro de los objetivos regularmente se encuentran algunos elementos claves de la seguridad de la red:

Confidencialidad

Proteger la información de su revelación no autorizada, se debe garantizar que si un usuario desea que su información no sea vista por alguien más pueda lograrlo, debe poder decidir quiénes tienen derecho a obtener la información. Usualmente se manejan permisos de accesos individuales o grupales, y encriptamiento para transmisión en la red y para almacenamiento de información crítica.

Disponibilidad

Los recursos de información sean accesibles cuando estos sean necesarios, es garantizar el acceso a un servicio.

Integridad

Proteger la información de alteraciones no autorizadas por la organización. Los sistemas se deben poder checar en cuanto a su integridad, esto con el fin de detectar modificaciones que puedan afectar la seguridad, si el sistema se corrompe o es modificado, sería deseable detectar el origen del problema (quien lo modificó) y restituir la integridad (en muchos casos hay que reinstalar el sistema).

Control de Acceso

Los recursos del sistema son proporcionados o negados de acuerdo al tipo de usuario que los solicite, y dependiendo desde donde haga la solicitud, algunas veces sólo se permite uso parcial de los recursos, esto es común en sistemas de archivos, donde algunos usuarios solamente pueden leer, algunos otros leer y escribir, etc.

Identificación y Autentificación

Los usuarios deben identificarse y después comprobar que son quien dice ser. Lo más común es usar login y password. Además se podría usar un login y alguna identificación física como huellas digitales o analizadores de reconocimiento por voz.

Responsabilidad

Determinar qué individuo en la organización es responsable directo en cuanto a los recursos de cómputo e información.

2.4.4. ELEMENTOS DE LAS POLÍTICAS

Toda política de seguridad se debe orientar a las decisiones que tengan relación con la seguridad, para lo cual, se requiere la disposición de todos los usuarios de la empresa para lograr una visión conjunta de lo que se considera importante.
Las Políticas de Seguridad en las Redes deben considerar principalmente los siguientes elementos[32]:

[32] http://www.123innovationgroup.info/politicas_de_seguridad.htm

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Seriedad de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

2.4.5. PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD

Es muy importante que al momento de formular las políticas de seguridad, se consideren por lo menos los siguientes aspectos:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- Reunirse con los departamentos responsables de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.

- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos su área.
- Monitorear periódicamente los procedimientos y operaciones de la organización, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

2.4.6. COMPONENTES DE UNA POLÍTICA DE SEGURIDAD

Una política de seguridad debe hacer énfasis en cuatro aspectos fundamentales en una solución de seguridad:

- **Política de Privacidad.-** Define expectativas de privacidad con respecto a funciones como monitoreo, registro de actividades y acceso a recursos de la red.

- **Política de Acceso.-** Permite definir derechos de acceso y privilegios para proteger los objetivos clave de una pérdida o exposición mediante la especificación de guías de uso aceptables para los usuarios con respecto a conexiones externas, comunicación de datos, conexión de dispositivos a la red, incorporación de nuevo software a la red, etc.

- **Política de Autenticación.-** Establece un servicio de confiabilidad mediante alguna política de contraseñas o mecanismos de firmas digitales, estableciendo guías para la autenticación remota y el uso de dispositivos de autenticación.

- **Política de Administración de la Red.-** Describe como pueden manipular las tecnologías de los encargados de la administración interna y externa. De aquí surge la consideración de si la administración externa será soportada y, en tal caso, como será controlada.

Las empresas y organizaciones raramente mantienen sus servicios constantes, sino que continuamente introducen nuevas tecnologías para mejorarlos. Además, deben ser revisadas periódicamente para adaptarse a las necesidades de seguridad reales, ya que la introducción o modificación de algún recurso puede generar fallas en la arquitectura de seguridad actual.

2.4.7. ESTRATEGIAS DE SEGURIDAD

Al diseñar la política de seguridad de una red se deben llevar algunos puntos claves para poder lograr a cabo una estrategia de seguridad. Para establecer una estrategia adecuada es conveniente pensar una política de protección en los distintos niveles que esta debe abarcar, como por ejemplo:

- **La Estrategia Proactiva (proteger y proceder).-** O de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un

sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar esta estrategia.

- **Mínimos privilegios.-** Consiste en asignar a cada usuario el mínimo de privilegios que necesite. El objetivo es minimizar los daños en caso de que la cuenta de un usuario sea invadida, si un usuario quiera realizar actividades diferentes tiene que solicitar que se le asignen los privilegios correspondientes.
- **Seguridad basada en hosts.-** Los mecanismos de seguridad están en los hosts. Puede ser diferente en cada host, lo cual hace difícil su instalación y mantenimiento, si un host es atacado con éxito, peligra la seguridad de la red, ya que la mayoría de los usuarios tienen el mismo login y password en todos los hosts a los que tienen acceso.
- **Seguridad basada en la red.-** La seguridad se basa en controlar los accesos a los hosts desde la red, el método más común es la implementación de firewalls.
- **Simplicidad.-** Los sistemas muy complejos tienden a tener fallas y huecos de seguridad. La idea es mantener los sistemas tan simples como sea posible, eliminando funcionalidad innecesaria, donde los sistemas simples que tienen mucho tiempo, han sido tan depurados que prácticamente no tienen huecos de seguridad.
- **Falla segura.-** Los sistemas deben estar diseñados para que en caso de falla queden en un estado seguro. Por ejemplo en la red, en caso de falla se debe suspender el acceso a Internet.
- **Seguridad por Obscuridad.-** La estrategia es mantener un bajo perfil y tratar de pasar desapercibido, de modo que los atacantes no lo detecten.
- **Defensa en profundidad.-** Consiste en usar tantos mecanismos de seguridad como sea posible, colocándolos uno tras otro. Puede hacer muy compleja la utilización del sistema.

- **Check Point.-** Se hace pasar todo el tráfico de la red por un solo punto y se enfocan los esfuerzos de seguridad en ese punto. Además, se puede disminuir el rendimiento.
- **La Estrategia Reactiva (perseguir y procesar).-**O estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia Proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

2.4.8. A QUIENES VAN DIRIGIDAS LAS POLÍTICAS

Las políticas están dirigidas a todo el personal que labora en la organización y se deben apegar a estas. Cada uno de los empleados es responsable de su cumplimiento. Todas las organizaciones, sin importar su tamaño, ameritan contar con una política seguridad, para lo cual se debe asignar un presupuesto para la seguridad en la red, ya que siempre es necesaria, puesto que ayudan a poner orden en el caos. Deben de recibir el apoyo total de los directivos de la organización. Todo el personal tiene la responsabilidad de la seguridad. Las políticas deben ser claras, breves, posibles de cumplir, cooperativas, dinámicas y consistentes con la visión de la organización. Se debe asegurar que todo el personal entienda las políticas de seguridad de la organización, donde se resalte la importancia de contar y apegarse a las buenas prácticas de la seguridad dentro de la empresa.

Las políticas de seguridad son documentos de alto nivel que denota el compromiso de la gerencia con la seguridad en la red. Contiene la definición de la seguridad de la información bajo el punto de vista de cierta entidad, de tal modo que obliga a ser enriquecida y compatibilizada con otras políticas dependientes de ésta, con sus respectivos objetivos de seguridad y procedimientos. También, debe estar fácilmente

accesible de forma que los empleados conozcan de su existencia y entiendan su contenido, y sobre todo se debe designar un propietario que será el responsable de su mantenimiento y su actualización a cualquier cambio que se requiera, denominado ISO (Information Security Officer) quien es la persona responsable de mantener actualizadas las políticas, estándares y los controles para garantizar la protección de los activos de información de la organización.

2.5. FIREWALLS

2.5.1. INTRODUCCIÓN

La preocupación principal del administrador de red, son los múltiples accesos a internet, porque se desconoce lo que pasa en la transmisión de datos, si son virus, intrusos, espías.

Un firewall es un sistema que imponen una política de seguridad entre la red privada de la organización e Internet. Para lograr la efectividad de un firewall, todo el tráfico de información de Internet deberá pasar a través del mismo. Así, toda la información será inspeccionada mediante el uso de políticas de seguridad y monitoreo de los registro de seguridad. De esta manera que este dispositivo pueda permitir o denegar las transmisiones de una red a la otra, donde se crea un perímetro de defensa, diseñado para proteger toda la información, a fin de evitar que los intrusos puedan acceder a información confidencial. En otras palabras un firewall es un mecanismo para proteger redes confiables cuando se conectan a redes no confiables (como Internet).

Los Firewall son simplemente filtros que bloquean o admiten conexiones y transmisiones de información por Internet. Los filtros están diseñados para evitar que un usuario irreconocible ataque al equipo en la red y al mismo tiempo podrá ser

inmune a la acceso en la red. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, que primero se asegura si la comunicación es entrante o saliente. Los datos son analizados procedentes de Internet, eliminando el tráfico no deseado. Básicamente sólo permiten el tráfico de páginas web, cortando todos los demás servicios (Chat, Ftp, Telnet, Control Remoto, IRC, etc.), de esta forma protegen a los computadores frente a las posibles amenazas procedentes de Internet, dichos ataques pueden ocasionar el bloqueo del computador, la infección por un virus informático y el robo de datos o ficheros. Algunas aplicaciones pueden requerir que se abran ciertos puertos o conexiones del firewall. En estos casos conviene que los cambios introducidos sean lo más restrictivos que sea posible. Para el correcto funcionamiento de un firewall es necesario mantenerlo actualizado. Constantemente se descubren nuevas vulnerabilidades y se actualizan los programas de seguridad.

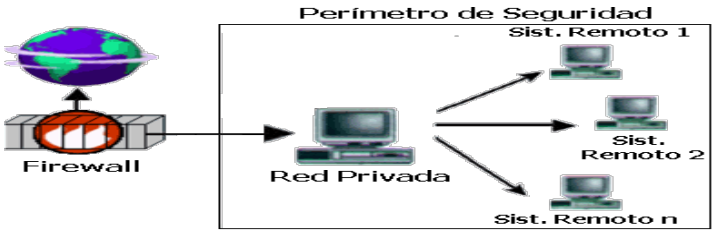


Figura 2. 2:Perímetro de Seguridad

Es importante aclarar que un firewall de Internet no es justamente un Ruteador, ni un servidor de defensa o una combinación de elementos que proveen seguridad para la red, sino una parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección

de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad.

2.5.2. FUNCIONAMIENO DEL FIREWALL[33]

Para poner a funcionar un sistema firewall es necesario tomar en cuenta los siguientes aspectos:

- Los Firewalls en Internet administran los accesos posibles de la Internet a la red privada. Si no se cuenta con este sistema, cada uno de los servidores de la red se exponen al ataque de otros servidores.
- El sistema opera en las capas superiores del modelo OSI y tiene información sobre las funciones de la aplicación en la que basan sus decisiones. También opera en las capas de red y transporte, en cuyo caso, examina los encabezados IP y TCP (paquetes entrantes y salientes), y rechaza o acepta paquetes con base en reglas de filtración de paquetes programadas. Así, el Firewall actúa como el punto de cierre que monitorea y rechaza el tráfico en la red en el nivel de la aplicación.

Todas las comunicaciones de Internet se realizan mediante el intercambio de paquetes de información, que son unidades mínimas de datos transmitidas por la red. El Firewall funciona definiendo una serie de autorizaciones para la comunicación, tanto de entrada como de salida, mediante reglas, las cuales se realizan teniendo en cuenta los puertos de comunicación, los programas o las IP de conexión, que pueden ser tanto restrictivas como permisivas, es decir, pueden ser reglas que denieguen o autoricen las comunicaciones (de entrada, de salida o ambas) a un determinado puerto, un determinado programa o una determinada IP.

[33] http://redescolar.ilce.edu.mx/redescolar/Revista/10/articulos/08.html

Los Firewalls también operan en las capas de red y transporte en cuyo caso examinan los encabezados IP y TCP, (paquetes entrantes y salientes), y rechazan o pasan paquetes con base a reglas de filtración de paquetes programables.

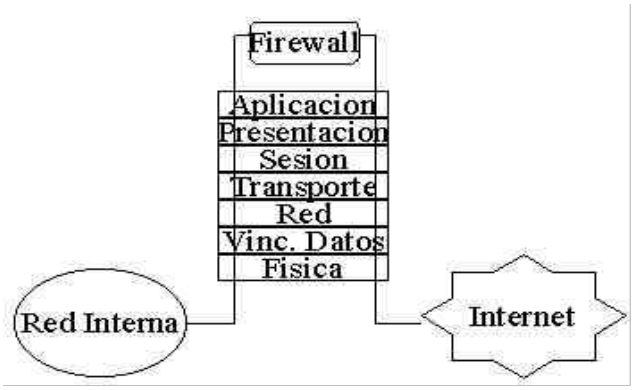


Figura 2. 3: El firewall actúa como un punto de cierre que monitorea y rechaza el tráfico de red a nivel de aplicación

Para que cada paquete pueda llegar a su destino, independientemente de donde se encuentren las máquinas que se comunican, debe llevar anexa la información referente a la dirección IP de cada máquina en comunicación, así como el puerto a través del que se comunican. La dirección IP de un dispositivo lo identifica de manera única dentro de una red. Un firewall intercepta todos y cada uno de los paquetes destinados o provenientes de un computador, y lo hace antes de que ningún otro servicio los pueda recibir. Es decir el firewall puede controlar de manera exhaustiva todas las comunicaciones de un sistema a través de Internet.

2.5.3. COMPONENTES FIREWALL[34]

Un Firewall típico está compuesto por una combinación de Ruteador filtrado de paquetes, Gateway a nivel de la capa de aplicación, Gateway a nivel-circuito, Dual-Homed Host y Screened Host.

La función del Ruteador toma las decisiones para cerrar y permite el paso de cada uno de los paquetes que son recibidos. Estos sistemas se basan en el examen de cada datagrama enviado y cuenta con regla de revisión de la información de los encabezados de las IP, si estos no corresponden a las reglas, se descarta o desplaza el paquete, en fin solo utilizan políticas por omisión (descartar o reenviar) ya que el filtro de paquetes es configurado típicamente como una lista de reglas basadas en campos del encabezado IP o del encabezado TCP.

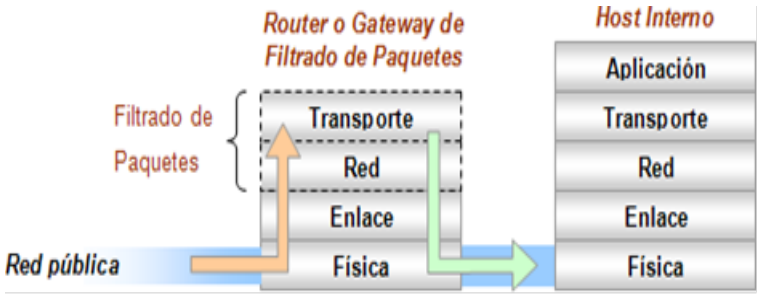


Figura 2. 4: Ruteador Filtra Paquetes

Por otra parte, los Gateway del nivel de aplicación permiten al administrador de red la implementación de una política de seguridad más estricta que la admite un Ruteador filtra-paquete, y es altamente mejor porque depende de una herramienta genérica que filtra paquetes para administrar la circulación de los servicios de Internet a través de Firewall. Se puede instalar en el Gateway un código de propósito especial “Servidor Proxy” para cada aplicación deseada. Este tipo de componentes son más seguro que

[34] http://redescolar.ilce.edu.mx/redescolar/Revista/10/articulos/08.html

los filtros de paquetes, por lo que solo necesitan revisar algunas aplicaciones permisibles, donde registran y auditan el tráfico entrante.

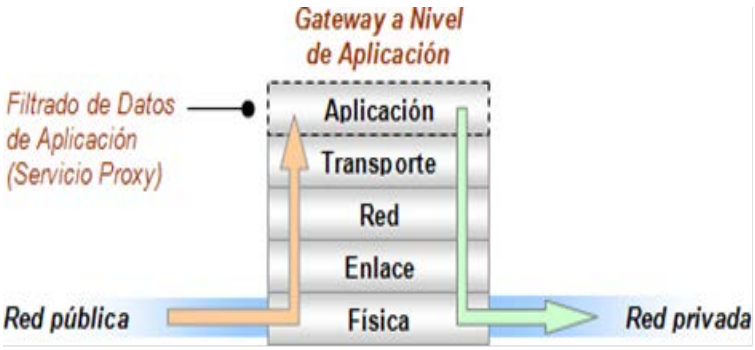


Figura 2. 5: Gateway a nivel-circuito

En cambio el Dual-Homed Host son dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el caso del Filtrado de Paquetes), por lo que se dice que actúan con el "IP-Forwarding desactivado". Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el Proxy atenderá su petición, y en función de la configuración impuesta en dicho Firewall, se conectará al servicio exterior solicitado y hará de puente entre este y el usuario interior. Es decir que se utilizan dos conexiones. Uno desde la máquina interior hasta el Firewall y el otro desde este hasta la máquina que albergue el servicio exterior.

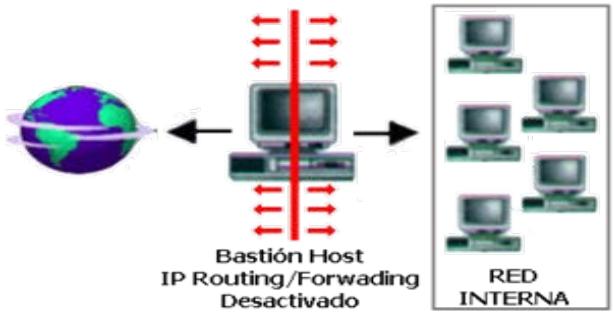


Figura 2. 6: Dual-Homed Host

Finalmente, el Screened Host combina un Router con un host bastión y el principal nivel de seguridad proviene del filtrado de paquetes. En el bastión, el único sistema accesible desde el exterior, se ejecuta en el Proxy de aplicaciones y en el Choke se filtran los paquetes considerados peligrosos y sólo se permiten un número reducido de servicios.

Figura 2. 7: Screened Host

2.5.4. CARACTERÍSTICAS DE LOS FIREWALLS

El Firewall le proporcionara la mayoría de las herramientas para complementar su seguridad en la red, mediante la imposición de políticas de seguridad, en el acceso alos recursos de la red y hacia la red externa, es importante establecer que un monitoreo constante del registro base, nos permitirá detectar un posible intruso y así proteger la información.

Entre las principales características de los Firewalls, destacan las siguientes:

- **Control de acceso a los recursos de la red.-** Al encargarse de filtrar, en un primer nivel, antes que lleguen los paquetes al resto de las computadoras de la red, el Firewall es idóneo para implementar en los controles de acceso; también, inspecciona y controla el tráfico entre la red local e Internet.

- **Protección de la Red.-** Mantiene alejados a los piratas informáticos (crackers) de la red al mismo tiempo que permite el acceso a todos los usuarios de la misma.

- **Concentra la seguridad.-** Facilita la labor a los responsables de seguridad, dado que su máxima preocupación es encarar los ataques externos y vigilar manteniendo un monitoreo, de tal manera que permite detectar y rechazar el trafico potencialmente peligroso.

- **Software.-** Provisto con un software de administración que puede identificar problemas que pudieran ocasionar bajo performance en la red, y es totalmente configurable, en donde se puede hacer filtrados por dirección IP, por dominios, por protocolos, por puertos, palabras o frases específicas.

- **Control del Uso en Internet.-** Permite bloquear el material no adecuado, determinar qué sitios puede visitar el usuario de la red interna y llevar un registro, a su vez optimiza el ancho de banda al controlar el acceso a Internet.

- **Genera Alarmas de Seguridad.-** El administrador del Firewall puede responder una alarma y examina regularmente los registros de base.

- **Audita y registra Internet.-** Autoriza al administrador de red justificar el gasto que implica la conexión a Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda.

- **Control y estadísticas.-** Permite controlar el uso de Internet en el ámbito interno, conocer los intentos de conexiones desde el exterior y detectar

actividades sospechosas, y administra los accesos provenientes de Internet hacia la red privada.

2.5.5. VENTAJAS Y DESVENTAJAS EN LOS FIREWALLS[35]

Ventajas

- Obviamente, la principal ventaja de un firewall es que permite la interconexión segura de una red privada con una red pública para aprovechar los beneficios que ésta ofrece, tales como:
- Pueden resultar en una reducción de costos si todo el software de seguridad puede ser situado en un único sistema firewall, en lugar de ser distribuido en cada servidor o máquina de la red privada.
- Los Firewalls manejan el acceso entre redes, y si no existiera, todas las computadoras de la red estarían expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna.
- Bloquea eficazmente los intentos de intrusión realizadas a través de redes inalámbricas (WiFi). Al producirse una intrusión de este tipo, aparece un aviso emergente que permitirá bloquear la intrusión de inmediato.
- Son el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, donde el administrador será el responsable de la revisión de estos monitoreo, ya que protege al computador de los ataques que se produzcan desde máquinas situadas en internet.
- Otra causa que ha hecho que el uso de Firewalls se haya convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las

[35] http://www.textoscientificos.com/redes/firewalls-distribuidos/firewalls

intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el Firewall.

- Los Firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.
- Los Firewalls también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad o para albergar los servicios WWW y FTP brindados.
- Prevenir el uso de troyanos que puedan existir en el sistema debido a que se hayan introducido a través de correo electrónico o en algún dispositivo de almacenamiento, y detectan patrones de ataques e identificar de dónde provienen.
- Evitan que un computador pueda ser un punto de entrada a una red privada virtual en el caso de utilizarlo para acceso remoto, también aseguran que un computador no se utiliza para atacar a otros.

Desventajas

Hay algunas limitaciones que los firewalls no pueden proteger al sistema, como pueden ser las amenazas de puntos de acceso alternativos no previstos (backdoors) y ataques originados en el interior de la red, como por ejemplo:

- El problema de los firewalls es que limitan el acceso desde y hacia Internet, pero es un precio que se debe pagar y es una cuestión de análisis de costo / beneficio al desarrollar una implementación de seguridad.

- Un Firewall no puede proteger contra aquellos ataques que se efectúen fuera de su punto de operación, en este caso: conexión dial-out sin restricciones que permita entrar a nuestra red protegida. El usuario puede hacer una conexión SLIP[36] o PPP[37] a Internet. Este tipo de conexiones derivan de la seguridad provista por un Firewall construido cuidadosamente, creando una puerta de ataque.
- El Firewall no puede proteger de las amenazas a las que lo sometan usuarios inconscientes.
- No puede proteger contra los ataques de la ingeniería social, en este caso, un cracker que quiera ser un supervisor o aquel que persuade a los usuarios menos sofisticados.
- No puede proteger de los ataques posibles a la red interna por virus informativos provenientes de archivos y software.
- Tampoco puede proteger contra los ataques en la transferencia de datos. Éstos ocurren cuando datos aparentemente inocuos son enviados o copiados a un servidor interno y ejecutados, abriendo la puerta al ataque.
- Sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa. Un Firewall "No es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir password o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta.

[36]Slip.- Es un estándar de transmisión de datagramas IP para líneas serie, reemplazado por el PPP.
[37] PPP (Protocolo Punto a Punto).- Es un protocolo de nivel de enlace para hacer conexión entre dos puntos (dos computadoras o nodos).

2.5.6. POLÍTICAS DE UN FIREWALL

Las políticas son el pilar fundamental de este sistema, informan a los usuarios de sus debidas responsabilidades, normas de acceso remoto o local, políticas de acceso a los recursos de la red, reglas de encriptación, normas de protección de virus y entrenamiento, por tal motivo se tiene las siguientes claves:

"No todo lo específicamente permitido está prohibido" y "No todo lo específicamente prohibido está permitido". La primera clave, asume que un Firewall puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas. La segunda, indica que el Firewall puede desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso. Para lo cual, la política de seguridad se basará en una conducción cuidadosa, analizando la seguridad y la asesoría en caso de riesgo.

2.5.7. TIPOS DE FIREWALLS

Se puede identificar tres grupos, en función de los criterios de diseño y el segmento de mercado al que apuntan, así se puede clasificar en:

a. Firewall por Hardware

Son equipos que están compuestos por software y hardware a la vez, para poder operar. Debido a su gran rendimiento, son utilizados en grandes empresas, y es necesario que sean administrados por personal técnico especializado. Como ventajas, se puede destacar que es una muy buena solución cuando se habla de una red, ya que permite hacer toda la configuración en un solo punto al que se conectan los ordenadores, también son independientes del PC, no es necesario configurarlos cada vez que se reinstale el sistema operativo, y no consumen recursos del sistema.

b. Firewall por Software

Esta clase de firewall son los más comunes y utilizados. Se trata de un software que se instala en un ordenador. Una ventaja es la flexibilidad que tienen, ya que permiten adaptarse al software y al hardware disponible, por lo que deben convivir con el sistema operativo, son más complicados de instalar y mantener, además del hecho que necesitan personal con conocimiento del producto y el sistema operativo. Hay modelos que protegen redes enteras y otros específicos para defender servidores.

c. Firewall Personales[38]

El término firewall personal se utiliza para los casos en que el área protegida se limita al ordenador en el que el firewall está instalado. Están diseñados para brindar la máxima seguridad posible, haciendo un balance entre el nivel de protección, facilidad de uso y mantenimiento. La mayoría tienen asistentes de configuración, así como también varias configuraciones predeterminadas que ayudan a mantener un alto nivel de seguridad sin perder su funcionalidad. Muchos de ellos poseen servicios de actualización automática y suman capacidades de detección de tráfico malicioso.

Un firewall personal permite controlar el acceso a la red de aplicaciones instaladas en el ordenador y prevenir notablemente los ataques de programas como los troyanos. También permiten subsanar y prevenir intrusiones de aplicaciones no autorizadas a conectarse a su ordenador.

c.1. Tipos de Firewall Personales

Estos son algunos firewalls para plataforma Windows:

[38] http://es.kioskea.net/contents/protect/firewall.php3

- **PortsLock.-** Es un firewall a nivel de usuario que controla los accesos a Windows NT/XP/2000. Una vez instalado el administrador puede asignar permisos a las conexiones, controlando que usuarios pueden acceder a los puertos TCP/IP con diferentes protocolos (STMP, POP3, FTP, HTTP, Telnet, etc.) dentro de una red, puede ser configurado para unos determinados días de la semana u horas en el sistema. También es posible establecer un conjunto de IPs aceptadas o rechazadas para las conexiones con los puertos TCP/UDP.

- **Per Systems.-** Es una barrera de protección frente a posibles ataques, muy rápido y que consume mucho menos recursos que otros Firewalls del mercado. Per Systems controla la ejecución y autorización de los servicios de Internet tales como los protocolos de Correo, sitios web, mensajería instantánea, así como los de redes de archivos compartidos. Se puede configurar reglas de permisos para aplicaciones que deseen transmitir datos a través de Internet y dar o bloquear el acceso independiente a una lista de programas. Además, bloquea eficientemente cualquier intento de ataque a una PC por hackers o intrusos de la red que manipulan troyanos o backdoors a través de los puertos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol). En definitiva, es una herramienta gratuita e imprescindible para navegar con seguridad.

- **Agnitum Outpost Firewall.-** Es un potente firewall destinado a proteger un computador de ataques externos. Sus prestaciones permiten mantener protegido un computador contra todo tipo de amenazas en Internet, como son cookies, publicidad intrusiva, virus de

correo electrónico, de una forma sencilla y sin consumir una gran cantidad de recursos.

- **MindSoft Firewall.-** Consigue una mayor sensibilidad a la hora de enfrentarse a posibles ataques y ofrece soluciones para evitarlos. Además es capaz de detectar todo tipo de virus de tipo troyano. Permite crear distintos niveles de seguridad, realizar filtros, bloquear direcciones (conexiones), bloquear puertos remotos y locales, etc.

- **ZoneAlarm.-** La utilidad básica de este programa es controlar cualquier acceso a un computador y los programas que se están ejecutando en él, actualmente se puede decir que es el arma más efectiva para evitar intrusos y virus. Una utilidad imprescindible al utilizar Internet. Dispone de diferentes niveles de seguridad que permiten desde no ser visible en Internet hasta deshabilitar NetBIOS o los recursos compartidos. Además, no consume muchos recursos, de modo que es válido para cualquier tipo de máquina.

2.5.8. BENEFICIOS DEL FIREWALL EN EL USO DEL INTERNET

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se expone al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la “Dureza” con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "Choke point" (embudo), manteniendo al margen los usuarios no autorizados (tal como: hackers, crackers y

espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran la red privada.

En conclusión, un FIREWALL proporcionara un sin número de las herramientas que son complementarias a la seguridad en la red, mediante la imposición de políticas de seguridad, en el acceso a los recursos de la red y hacia la red externa, para prevenir el acceso de usuarios no autorizados a los recursos computacionales en una red dentro de un esquema de conectividad a Internet. Es importante establecer que un monitoreo constante del registro base, que permitirá detectar un posible intruso y así proteger la información de una empresa.

CAPÍTULO 3

DISEÑO E IMPLEMENTACIÓN DE LA RED PARA LA DIRECCIÓN DE LA INDUSTRIA AERONÁUTICA DE LA FUERZA AÉREA (DIAF).

3.1. INTRODUCCIÓN

En la actualidad el manejo adecuado y eficiente de la información constituye una de las preocupaciones principales dentro de cualquier organización, sea esta de origen público o privado.

Existen métodos que hacen fácil la transmisión y recepción de información en la actualidad; uno de esos métodos constituye los sistemas de cableado estructurado y de redes inalámbricas enmarcados en las comunicaciones.
Para realizar el diseño de estos sistemas de comunicación, debe tenerse presente que cada red posee sus respectivas especificaciones de implementación.

El diseño e implementación de la red para la DIRECCIÓN DE LA INDUSTRIA AERONÁUTICA DE LA FUERZA AÉREA (DIAF), aportará en la preservación de la confidencialidad, integridad y disponibilidad de la información en la red, a través de la utilización de un Firewall. Es decir garantizar que solo aquellas personas autorizadas accedan a la información y a los recursos de la red, cada vez que lo requieran. Manteniendo la integridad total de la información y los métodos de procesamiento. Además, minimizará los riesgos de seguridad a los cuales está expuesta la red interna frente a la gran red que es el Internet. De esta manera se reduce los riesgos de enfrentar problemas causados por cualquier tipo de filtraciones o virus.

3.2. UBICACIÓN

Dirección:

CALLE :	AV. AMAZONAS S/N Y ANTONIO CLAVIJO
PROVINCIA:	COTOPAXI
CANTON:	LATACUNGA:
TELEFONO:	2813208

Figura 3. 1: Centro Productivo CIMAM

La Dirección De La Industria Aeronáutica De La Fuerza Aérea (DIAF), cuenta con varios centros productivos CEMA (Centro de Mantenimiento Aeronáutico), CEMEFA (Centro de Mantenimiento Electrónico de la Fuerza Aérea), CIMAM (Centro de Ingeniería y Mantenimiento de Aviación Militar), y CETRACOM (Centro de Transporte de Combustible).

Se debe recalcar que el proyecto se basaráúnicamente en los centros productivos CEMA y CIMAM, ya que conforman el proceso inicial de obtención de la información, estos centros están integrados de la siguiente manera:

Tabla 3. 1: Distribución Departamento CIMAM

PLANTA BAJA	**PLANTA ALTA**
Aulas	Jefatura
Centro de Documentación	Secretaria General
Biblioteca	Aeronáutica
	Administrativo Logístico
	Electrónica
	Sistemas
	Sala de reuniones

Tabla 3. 2: Distribución Departamento CEMA

PLANTA ALTA
Jefatura
Secretaria General
Administrativo Logístico
Electrónica
Sala de reuniones

3.3. OBJETIVOS

- Proporcionar una infraestructura física y lógica capaz de proveer de acceso a la información y a los recursos de la red de datos.
- Facilitar la administración de la Red, con el objeto de asegurar una estabilidad de funcionamiento constante.

- Realizar satisfactoriamente la implementación de la red de cableado estructurado.
- Establecer políticas de seguridad mediante el firewall para la administración y el desempeño adecuado de la red de datos.
- Obtener una Red de Datos que se ajuste a las exigencias tecnológicas actuales.

3.4. REQUERIMIENTOS DE LA DIAF

Se requiere que la Red de la DIAF a diseñar e implementar administre 50 puntos de datos para los 30 PCs existentes y que a futuro se implementarán nuevos equipos electrónicos, que permitan compartir información y recursos así como también el acceso a internet entre otros.

3.5. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA DIAF

Los inconvenientes que se presentan en una red de datos cuando se improvisa el cableado son varios, tales como el desempeño muy lento de la red, o inclusive tiene caídas de servicio. Posibles colisiones de información, nula planeación de crecimiento, fácil acceso a poder alterar el cableado.

La DIAF carece de un sistema de seguridad para controlar y administrar la información de la red de datos, que si se le suma a la inadecuada configuración de los equipos de la red, se tiene como consecuencia lo siguiente:

- La imposibilidad de compartir los datos y recursos informáticos entre sus departamentos, provocando que la información no se halla disponible en el momento requerido.

- La falta de control en el acceso a URL’s o páginas WEB.
- La incorrecta protección de la información.
- El tráfico no deseado.
- La propagación de virus y amenazas provenientes del Internet.
- La mala administración de servicios, tales como: Correo Electrónico, Servidor Web, Servidores de Archivos e Impresoras.
- La inexistencia de cuentas de usuarios para el acceso autorizado a la red de datos, particularmente a la utilización del Internet.

Como medida o estrategia para superar los problemas citados, se puede utilizar hardware que ayude a mejorar el control de tráfico de la red, y poder aprovechar de una mejor manera todos los recursos de la misma. Con la instalación de un Firewall se podrá proteger, controlar y administrar toda la información de la red de datos, reduciendo así posibles problemas o riesgos. Además, con la configuración de los equipos activos de la red como son los Switch, Routers, Firewalls, Access Point, Servidor, pueden ofrecer una solución óptima para el funcionamiento eficaz de la red de datos.

La red de datos de la DIAF es de alta velocidad (Fast Ethernet) de acuerdo al estándar 100BASE-TX propuesto por el comité IEEE 802.3; este estándar define una red con una tasa de 100 Mbps en el cable UTP 5e que es utilizado de manera empírica en las conexiones actuales ya que no está instalado el cableado estructurado de acuerdo a las normas y estándares necesarios para su óptimo funcionamiento.

La red de datos actual posee:

- Servicios de datos sobre MPLS
- Servidor

- Estaciones de trabajo (Cableado no cumple con estándares y normas)
- Switch
- Access Point (D-Link)

3.5.1. SERVICIOS DE DATOS SOBRE MPLS

La tecnología para el enlace de datos utilizado en la DIAF es MPLS.
MPLS[39] (Multi-Protocol Label Switching) es un mecanismo de transporte de datos estándar creado por la IETF (Grupo Especial sobre Ingeniera de Internet). Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

Las VPN/IP basados en MPLS permiten ofrecer al cliente soluciones seguras y de calidad empresarial, fáciles de desplegar y de mantener y, notablemente, más económicas.

[39] Conmutación Multi-Protocolo mediante Etiquetas

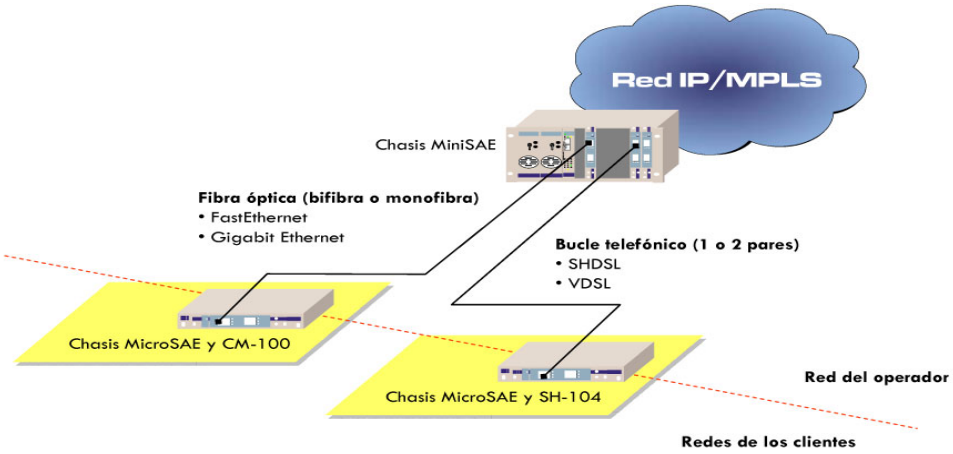


Figura 3. 2: Red IP/MPLS

3.5.2. HARDWARE Y SOFTWARE

- El Servidor de Comunicaciones es un dispositivo inteligente que realiza funciones de comunicaciones para los usuarios de la DIAF como administración de correo electrónico, administración del internet, entre otros. El servidor se encuentra ubicado en la Oficina de Sistemas.

  Las características del servidor son las siguientes:

Tabla 3. 3: Características del Servidor

MARCA	MODELO	PROCESADOR	MEMORIA RAM	DISCO DURO
HP	ProLiant ML150 G6 Servers	2 GHz	4 GB	1 TB

Figura 3. 3: Servidor HP

Este servidor se encuentra en óptimas condiciones, es decir cumple con todos los requerimientos que necesita la DIAF.

- **ESTACIONES DE TRABAJO**

  Las estaciones de trabajo no se hallan bien definidas ya que el cableado estructurado actual que se ocupa para el funcionamiento de los diferentes dispositivos de red está a punto de colapsar, y no se ha llevado ninguna planificación y estandarización de dicha red de datos.

  Cabe mencionar que los puntos de red están conectados directamente al Switch D'Link a su vez está conectado con el Switch 3 Com y este al servidor.

Figura 3. 4: Estación de Trabajo

- **SWITCHES**

Los Switch son dispositivos básicos para el estudio o diseño de una red LAN puesto que, estos equipos permitan enlazar a todos los servidores y estaciones o áreas de trabajo entre sí a través del cableado de la red.

En la actualidad los dispositivos utilizados por la DIAF son tres Switch, dos marca D'Link de 24 puertos cada uno y el otro de marca 3COM Súper Stack de 24 puertos.

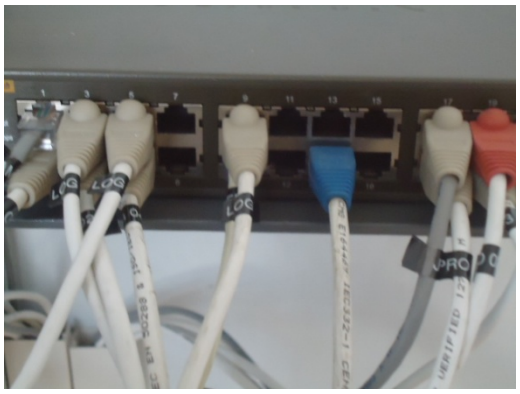


Figura 3. 5: Switch D´link

- **ACCESS POINT**

  Los Access Point son dispositivos que interconectan dispositivos de comunicación inalámbrica para formar una red inalámbrica.
  La DIAF dispone de dos Access Point en buenas condiciones y que serán útiles para el servicio de internet inalámbrico.

Figura 3. 6: Access Point

3.6. PROPUESTA

La propuesta se basa en la construcción de un cableado horizontal con topología estrella, es decir cada una de las salidas de telecomunicaciones distribuidas en las áreas de trabajo, están conectadas a un distribuidor de cables que estará ubicado en un cubículo existente en el cuarto de Datos de la DIAF.
Este proyecto plantea instalar dos Switch en cascada para que puedan ser parte de la red de datos. Además se instalará un rack en el cual se ubicara dos Patch Panel los Switch para la interconexión con los demás equipos.Se utilizará cable UTP categoría 5e. La propuesta abarca:

- Diagrama de la Red (por donde va el cableado).
- Esquema del Rack de comunicaciones.
- Identificación y etiquetado del cable.
- Certificación de Puntos.

- Instalación del Software de Administración (Active Directory, Cuentas de Usuarios).
- Configuraciones (Firewalls, Correo Electrónico, Access Point).
- Pruebas (Conectividad entre estaciones de trabajo).
- Resumen Técnico (Equipos de Telecomunicaciones).

El cableado estructurado para la DIAF se hará con cable categoría 5e de 4 pares por ser éste el medio más económico para la instalación por su diámetro muy pequeño, poco peso y un reducido radio de curvatura.

Los cables provenientes de cada punto serán conectados al Patch panel ubicado en el rack a través de conectores hembras RJ-45, permitiendo el uso de PatchCords para posterior conexión con el Switch.

La salida al usuario será a través de un cajetín rectangular más un Jack RJ-45 y face plate que estarán ubicados en un lugar adecuado para su conexión.

Se utilizarán PatchCords para conectar el Switch al Patch panel y para conectar las salidas de telecomunicaciones al área de trabajo.

3.7. PRESUPUESTO PARA LA IMPLEMENTACIÓN DE LA RED

Para la realización del Sistema de Cableado Estructurado la DIAF invirtió un presupuesto detallado en la siguiente tabla.

Tabla 3. 4: Presupuesto para la Implementación de la Red

DESCRIPCION	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Rack cerrado de 84''x19''	1	450	450
Patch Panel 24 puertos cat. 5e	3	98	294
Switch 24 puertos 10/100 Mbps	2	165	330
Cable UTP cat. 5e	2 rollos	180	360
Canaletas 60x40mm	30 metros	10	300
Canaletas 25x25mm	20 metros	12	240
Derivación en T 60x40 blanco	8	2	16
Unión 60x40 blanco	8	1	8
Ángulo plano 60x40 blanco	5	2	10
Tapa final 60x40 blanco	5	1	5
Face plate dobles blanco	16	1,50	24
Face plate un puerto blanco	4	1	4
Jack cat. 5e blanco	35	3	105
Caja sobrepuesta 40 mm blanca	15	1,60	24
Organizador 60x80	1	15	15
Patch Cords 3 pies cat. 5e	30	2	60
Patch Cords 7 pies cat. 5e	30	3,50	105
TOTAL	-	-	$ 2350

3.8. DISEÑO DE LA TOPOLOGÍA DE LA RED DE DATOS

El análisis que involucra el estudio, estará dirigido a definir el cableado estructurado desde el cuarto de Telecomunicaciones o data center hasta el área de trabajo, necesaria para el funcionamiento óptimo de cada dispositivo que opera en la red de datos.

Para tener una mejor visión de lo que se va a estudiar, se muestra en la Figura No. 3.7 el Diagrama del enlace de Red de la DIAF con sus respectivos Centros Productivos, además se indica en dicho gráfico las direcciones IP correspondientes a cada Centro que conforma la DIAF.

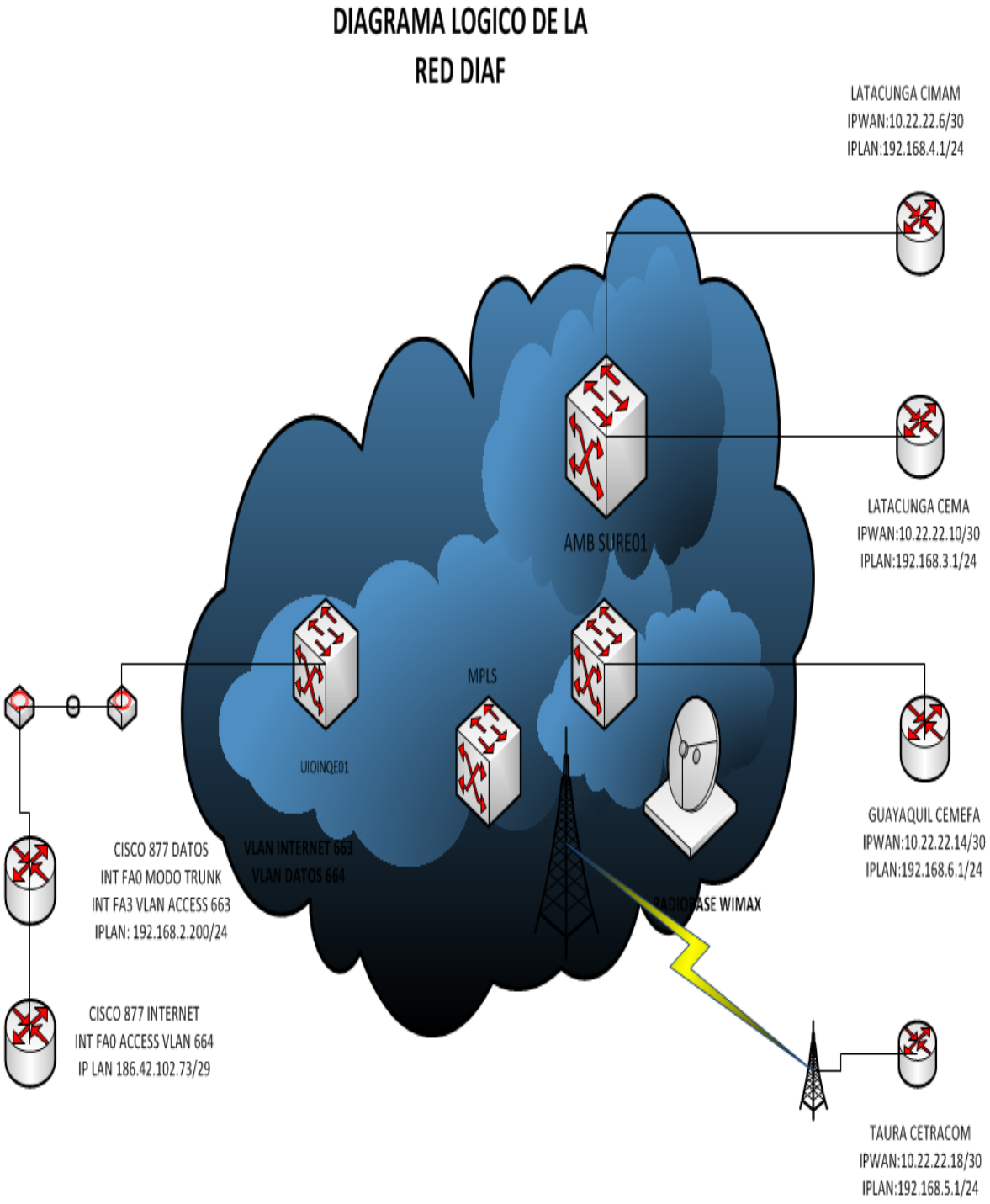


Figura 3. 7: Diagrama de Enlace de la Red de Datos DIAF

3.9. DISEÑO DE LA RED

El diseño de las redes de cableado estructurado, se fundamentará en las normas ANSI TIA/EIA 568-B, por ser las más adecuadas para adaptarse a los requerimientos actuales y futuras de la DIAF.

El cable UTP a utilizar será categoría 5e, el cual provee un ancho de banda de hasta 100 MHz en segmentos de 100m, los cuales son suficientes para las aplicaciones deseables.

Tomando en cuenta los elementos que se encuentran dentro de una red, el proceso de diseño de cada una de las redes a nivel pasivo se dividen en cuatro subsistemas:

- Subsistema Área de Trabajo.
- Subsistema Horizontal.
- Subsistema Cuarto de Telecomunicaciones y Cuarto de Equipos.
- Subsistema Vertical (Backbone).

Se especifica con más detalles en Anexo A.

3.9.1. SUBSISTEMA ÁREA DE TRABAJO

Dentro del área de trabajo se deben tener en cuenta las siguientes consideraciones:

- **Puntos De Red**

  El número de puntos por área de trabajo se determinó mediante visitas hechas a las oficinas de la DIAF y con la ayuda del personal de Sistemas e

Electrónica. Cada conector RJ-45 en los puestos de trabajo tiene la identificación correspondiente en el Rack.

Figura 3. 8: Cajetín RJ-45

El diseño de las redes de cada una de las áreas de trabajo de los centros CIMAM y CEMA se limitó a la distribución física de las salidas de información destinadas a servir a las diferentes áreas.

Tabla 3. 5: Distribución de puntos de red en el Centro CIMAM

CENTRO CIMAM	**PUNTOS DE DATOS**
PLANTA BAJA	
Aulas	5
Centro de Documentación	2
Biblioteca	2
PLANTA ALTA	
Jefatura	2
Secretaria General	1
Aeronáutica	4
Administrativo Logístico	3
Electrónica	5

Sistemas	5
Sala de Reuniones	3
Access Point	2
Impresora	1
TOTAL	**35**

Tabla 3. 6: Distribución de puntos de red en el Centro CEMA

CENTRO CEMA	**PUNTOS DE DATOS**
PLANTA BAJA	
Jefatura	1
Secretaria General	1
Administrativo Logístico	4
Electrónica	2
Sala de Reuniones	3
Access Point	1
Impresora	1
TOTAL	**13**

En la distribución de puntos de red que se indica en las tablas anteriores se detalla los puntos de datos que corresponden a las computadoras, equipos terminales (impresoras, Access Point) instalados en la red de datos.

Los puntos de red se ubicarán en tomas, compuestas por un cajetín, Jacks terminales y face plates. El cajetín que se empleará será el estandarizado para estos casos, y estará provisto de porta etiquetas con el fin de identificar la posición de terminación mecánica de las salidas de información respecto al panel de distribución de piso; en cada cajetín se colocará uno o hasta dos Jacks con sus face plates simples y dobles respectivamente dependiendo de su necesidad.

- **Patch Cords.-** Los cables de conexión (PatchCords) que se utilizaran en el área de trabajo para transmisión y recepción de voz y/o datos serán cables de red categoría 5e de 4 pares, con conectores (plug) RJ- 45 categorías 5e en los extremos cubiertos de sus respectivos cobertores.

  La longitud de los cables para realizar la conexión entre la salida de telecomunicaciones y la estación de trabajo, será de 7 pies (2.1336m), con lo cual se puede tener suficiente flexibilidad.

3.9.2. SUBSISTEMA HORIZONTAL

- **Topología.-** El cableado horizontal debe tener una topología de estrella, es decir, cada una de las salidas de Telecomunicaciones distribuidas en las áreas de trabajo, debe ser conectada a un distribuidor de cables que estará ubicado en la planta alta departamento de Sistemas, el cual debe estar instalado en el interior de un cuarto de telecomunicaciones. Ver Figura 3.9.

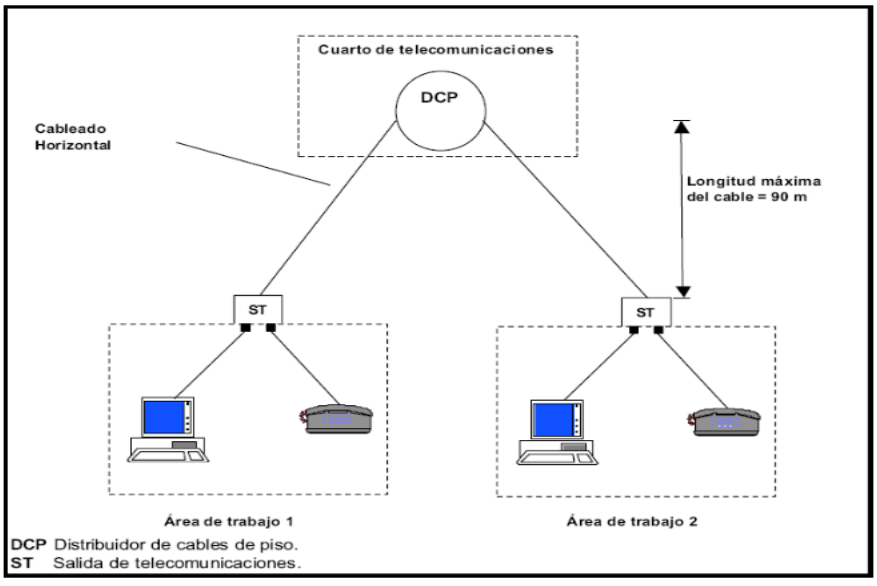


Figura 3. 9: Topología del Cableado Horizontal

- **Distancias Horizontales.-** La distancia máxima horizontal de cable de cobre permitida entre el distribuidor de cables de piso y la salida/conectar de telecomunicaciones, el conector para servicio de datos debe de ser RJ-45 hembra, compatible con el cable de cobre de 4 pares trenzados de 100 Ω, categoría 5e.

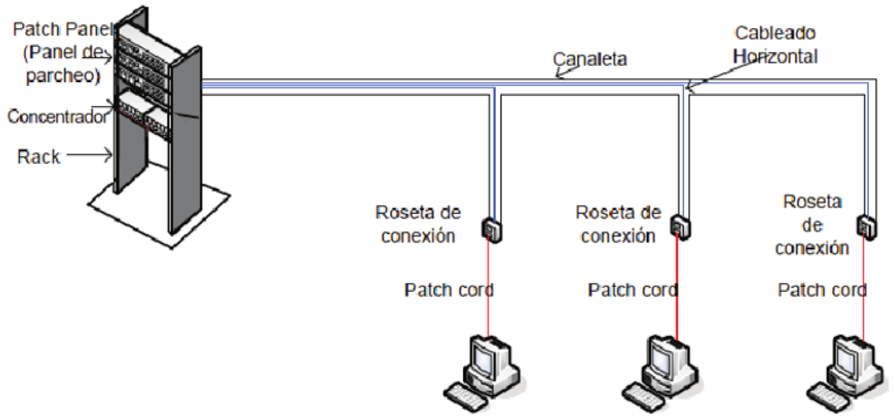


Figura 3. 10: Esquema de Cableado Horizontal

Para analizar el cableado horizontal es importante considerar los siguientes aspectos:

- **Cable.-** El medio de transmisión seleccionado es el UTP categoría 5e por su economía y por la facilidad de instalación que ofrece.
  Características:

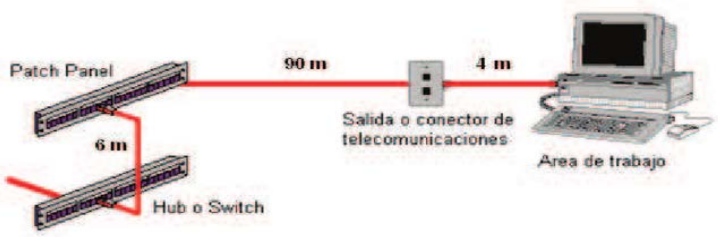


Figura 3. 11: Distancias máximas para el Cableado Horizontal

3.9.3. SUBSISTEMA CUARTO DE TELECOMUNICACIONES

Los equipos y distribuidores de cableado estructurado se deben instalar en áreas con acceso restringido de un edificio, denominados cuarto de equipos o cuarto de telecomunicaciones.

En el interior del cuarto de equipos debe existir al menos un extinguidor de fuegos portátil adecuado, el cual deberá estar colocado cerca del acceso al cuarto de equipos.

Como el cuarto de telecomunicaciones albergará en su interior equipos, se recomienda que tenga un sistema de aire acondicionado, con el objeto de mantener en su interior la temperatura y condiciones adecuadas para la operación de los equipos.

El sitio escogido para funcionar como cuarto de telecomunicaciones debe proporcionar todas las condiciones requeridas como son:

- **Rack.-** El closet de telecomunicaciones contará con un Rack, el mismo que será de tipo cerrado de piso hecho de acero con sus respectivos organizadores horizontales.

  La altura del rack útil será de 44Ur, su altura total será de 7 pies (84 pulgadas 0 2,1336m) y un ancho de 19 pulgadas (0,4826m) estándar. El rack tendrá dos organizadores verticales, y un número de organizadores horizontales que depende del número de Switch y de Patch Panels que poseerá el mismo.

  Además, en el rack se instalara 2 regletas multitoma de seis salidas eléctricas; cada salida electrónica funcionará a 110V.

Figura 3. 12: Rack 44

El rack se constituirá en distribuidor del sistema de voz y en el distribuidor del sistema de red de datos.

- **Patch Panel.-** Para el propósito de diseño en los Centros CIMAM, CEMA se utilizará tresPatchPanels de 24 puertos RJ-45 categoría 5e de 19 pulgadas de ancho, todos irán en el cuarto de telecomunicaciones ubicado en la planta alta del Centro Productivo CIMAM, con el fin de cubrir las salidas del sistema de datos (75 puntos de red); para la planta baja se distribuirá uno de 24 puertos y para la planta alta los otros dos de 24 puertos.

  Se utilizarán PatchPanels de 24 puertos para la mejor distribución de los cables ya que se contarían con 2 Switch, además en el Rack irá el equipo de enlace de red. También la suma de estos 3 paneles da 72 puertos, 42 puertos por encima de lo requerido (43 puertos), los cuales servirán en un futuro al momento de adicionar puntos de red.

Figura 3. 13: Patch Panel de 24 puertos de 19 pulgadas de ancho

- **Material Para El Cableado Estructurado**

Un resumen de los materiales necesarios para la instalación del sistema de cableado estructurado se muestra en la Tabla 3.7.

Tabla 3. 7: Resumen de los Materiales para Cableado Estructurado

Materiales para Cableado Estructurado	**CANTIDAD**		
	Planta Baja	**Planta Alta**	**TOTAL**
Patch Cords RJ-45 Cat5e 10 pies UTP (3.05metros)	5	15	20
Patch Cords RJ-45 Cat5e 7 pies UTP (2.13metros)	10	20	30
Rollos de cable UTP Cat5e	-	-	15

Azul para datos (305metros)			
Jack RJ-45 Cat5e	10	30	40
Rack cerrado de 84’’x19’’	-	-	1
Bandejas	-	-	3
Organizador de Rack Vertical	-	-	2
Organizador de Rack Horizontal	-	-	5
Patch Panel 24 Puertos	-	-	3
Cubierta para montaje superficial (Cajetín)	10	30	40
Face Plates simples	6	8	14
Face Plates dobles	8	12	20
Etiquetas para Face Plates	12	35	47
Nº. Canaletas 25x25mm	3	14	17
Nº. Canaletas 40x25mm	-	16	16
Nº. Canaletas 60x13mm	2	2	4
Nº. Canaletas 60x40mm	9	14	23
Nº. Canaletas 100x45mm	22	-	22
Nº. Canaletas 120x60mm	-	8	8

Algunos materiales no están mencionados en la tabla 3.6 debido a que estos pueden ser consumibles tales como accesorios para las canaletas, etiquetas o identificadores de cables, amarras, doble faz, entre otros.

Los rollos de cable UTP fueron calculados anteriormente al igual que las canaletas. Para ordenar estos cables en el Rack cerrado se utilizarán los PatchPanels, los organizadores verticales y horizontales y demás accesorios. Por cada Switch se utilizarán organizadores de 1Ur con sujetadores para los cables.

Las cubiertas de montaje, face plates, Jacks, etiquetas de identificación conformarán el punto de red físicamente, los cuales serán implementados en las áreas de trabajo.

El número de Jacks a incorporarse en un cajetín dependerá del tipo de toma: doble (2 Jacks), mixta (Jacks) y simple (1jack).

3.9.4. IDENTIFICACIÓN DE LOS PUNTOS DE LA RED

La tabla 3.8 muestra la dirección IP con la que está configurada cada una de las estaciones de trabajo, la nomenclatura está realizada de acuerdo a los departamentos y la longitud de los cables quedará determinada de acuerdo a las diferentes distancias que existen desde las áreas de trabajo al cuarto de Telecomunicaciones.

Tabla 3. 8: Puntos de Datos, Nomenclatura, distancia aproximada y direcciones IP

PUNTO DE DATOS	UBICACIÓN	IDENTIFICACIÓN	DIRECCIÓN IP	DISTANCIA TOTAL (m)
2	Gerencia	DG[1]	192.168.4.6	46,83
		DG[2]	192.168.4.7	44,23
5	Electrónica	DE[1]	192.168.4.11	44,23
		DE[2]	192.168.4.12	29,53
		DE[3]	192.168.4.13	29,53
		DE[4]	192.168.4.14	35,53
		DE[5]	192.168.4.15	32,53
		DA[1]	192.168.4.22	32,53

4	Aeronáutica	DA[2]	192.168.4.23	33,33
		DA[3]	192.168.4.24	38,43
		DA[4]	192.168.4.25	39,43
3	Logístico	DL[1]	192.168.4.26	40,83
		DL[2]	192.168.4.27	41,83
		DL[3]	192.168.4.28	43,23
5	Sistemas	DS[1]	192.168.4.16	20,33
		DS[2]	192.168.4.17	15,53
		DS[3]	192.168.4.1	10,33
		DS[4]	192.168.4.2	12,43
		DS[5]	192.168.4.4	13,43
1	Jefatura de Producción	DJP[1]	192.168.4.30	44,63
4	Producción	DP[1]	192.168.4.32	48,68
		DP[2]	192.168.4.33	48,43
		DP[3]	192.168.4.34	45,63
		DP[4]	192.168.4.35	41,83
1	Bodega	DB[1]	192.168.4.38	39,43
4	Logística	DLG[1]	192.168.4.40	44,23
		DLG[2]	192.168.4.41	45,23
		DLG[3]	192.168.4.42	46,63
		DLG[4]	192.168.4.43	47,63

3.10. PLANOS DE LOS CENTROS PRODUCTIVOS CIMAM Y CEMA

Los planos son representaciones graficas de un área, para poder realizar el cableado estructurado de una red de datos se debe de construir planos que identifiquen todos los puntos de red, acometidas etc.

3.10.1. PLANO DEL CENTRO PRODUCTIVO CIMAM

El Centro productivo CIMAM está compuesto por varios departamentos, dentro de este departamento se tiene configurada una red LAN con su respectivo cableado estructurado.

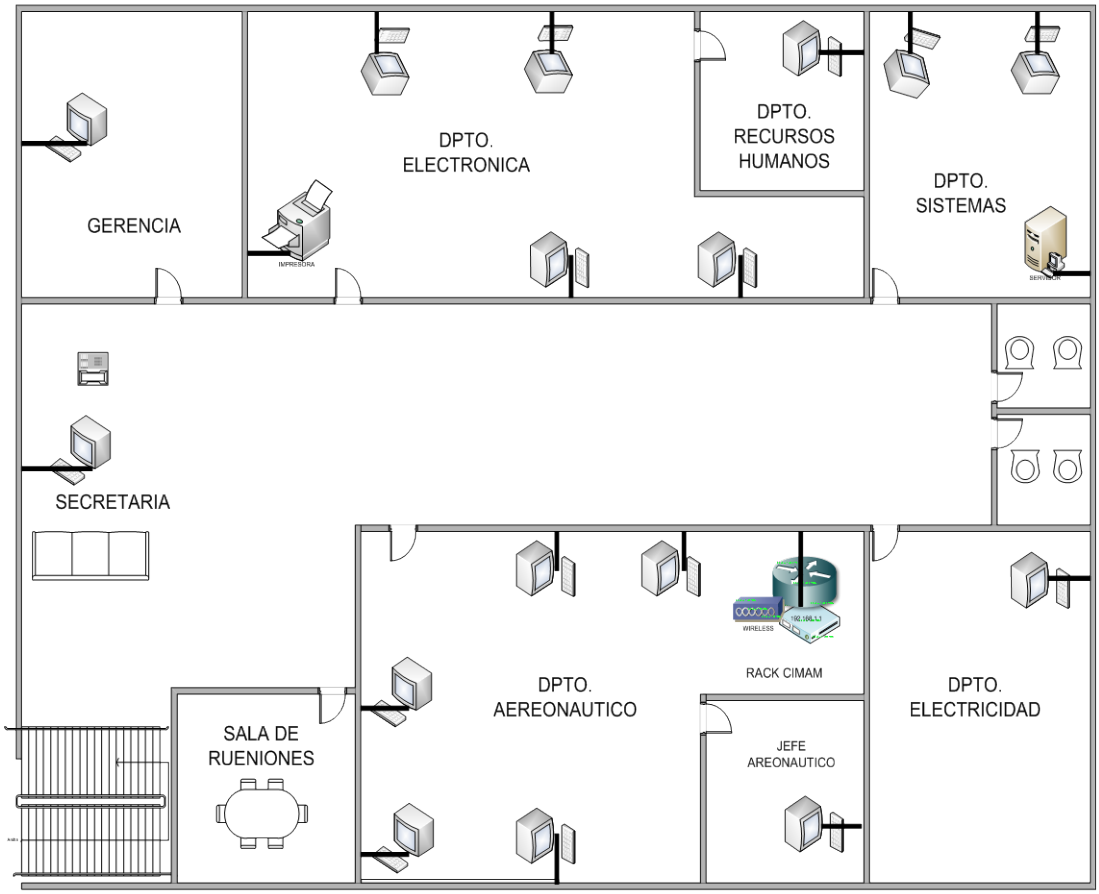


Figura 3. 14: Plano Físico de Red Centro CIMAM

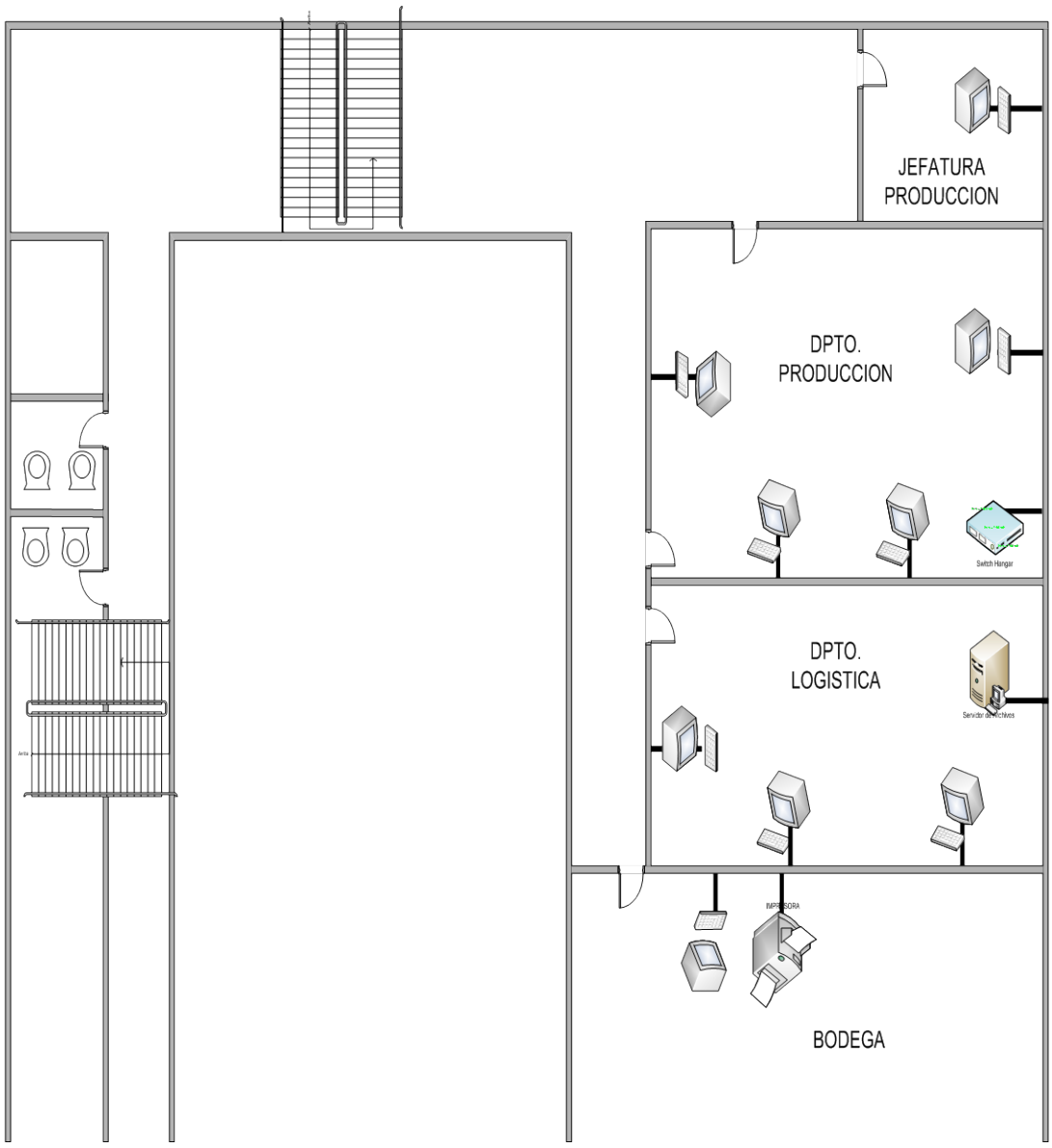


Figura 3. 15: Plano Físico de Red HANGARCIMAM

Cabe mencionar que el Centro Productivo CIMAM dispone en Hardware y Software lo siguiente:

Tabla 3. 9: Hardware Centro CIMAM

Nombre del Dispositivo	Características	Cantidad
Servidor	Marca: Hp Modelo: ProLiant ML150 G6 Servers Procesador: 2 GHz Memoria RAM: 4 GB Disco Duro: 1 TB	1
Switch	Marca: D'Link Modelo: DES-1024D 24 puertas RJ-45 10/100Mbps	2
Access Point	Marca: D'Link Modelo: DWL-2100AP Cobertura hasta 108Mbps - 2.4GHz Compatible con 802.11b y 802.11g	3
Impresora	Marca: Share Modelo:Sh520 Multifuncional Velocidad: B/N 43p.p.m	1
Impresora	Marca: HP Deskjet Modelo: 1000 (CH340B) Conectividad, estándar: 1 USB 2.0	2
PC	Marca: Clon Procesador : Pentium IV Velocidad 3,06 GHz Disco Duro: 120GB Memoria RAM: 512 Mb	15
PC	Marca: Clon Procesador : Pentium IV Velocidad 1,7 GHz	15

	Disco Duro: 40GB Memoria RAM: 512 Mb	

Tabla 3. 10: Software Centro Productivo CIMAM

Nombre del Paquete	Características
Sistema Operativo Microsoft Windows Server 2003 .Instalado en el Servidor	Versión: Standard Edition
Microsoft Office	Versión: Professional 2007
Sistema Operativo Microsoft Windows XP. Instalado en las estaciones de trabajo	Versión : Professional Service Pack 2
Antivirus	Karspesking
AutoCAD	Versión: 2010

3.10.2. PLANO DEL DEPARTAMENTO CEMA

El Departamento CEMA está compuesto por varios sub departamentos, dentro de este departamento se tiene configurada una red LAN con su respectivo cableado estructurado.

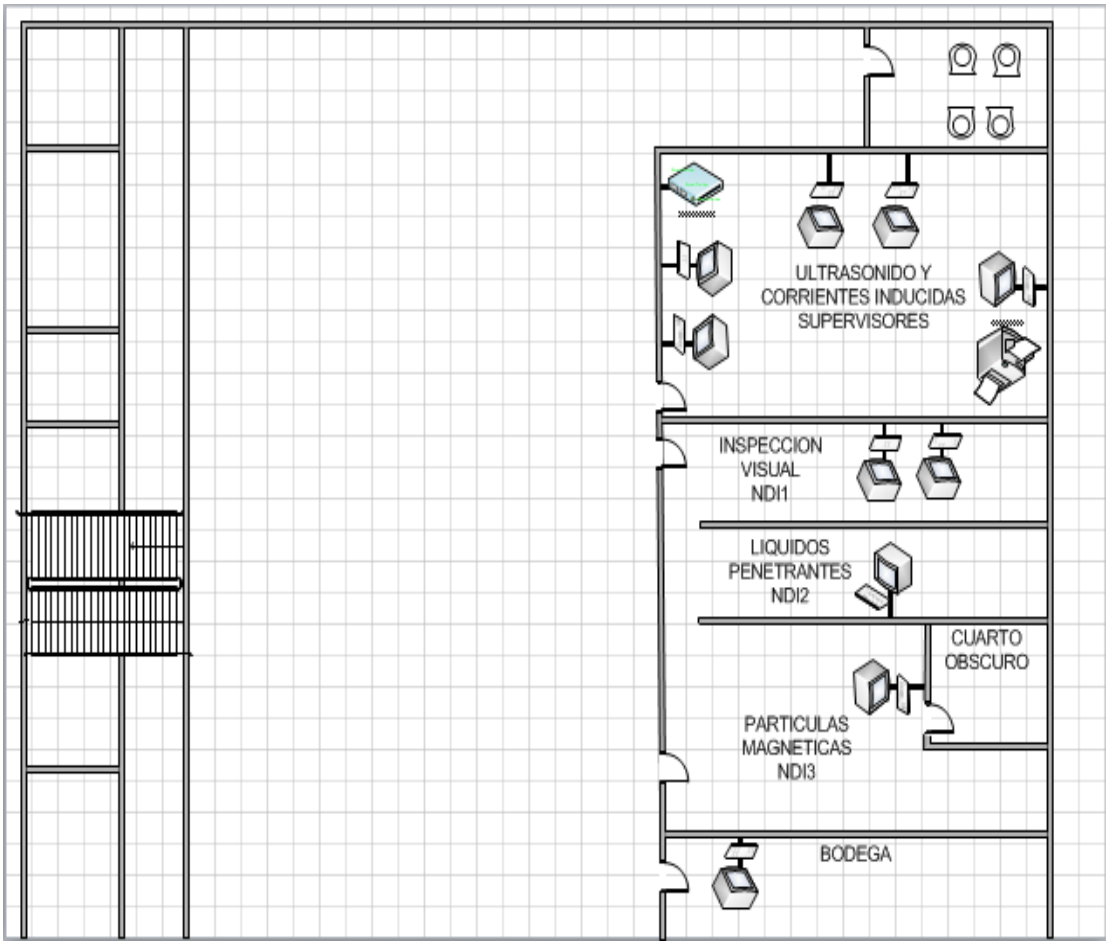


Figura 3. 16: Plano Físico de Red HANGAR CEMA

Cabe mencionar que el Centro Productivo CEMA dispone en Hardware y Software lo siguiente:

Tabla 3. 11: Hardware Centro CEMA

Nombre del Dispositivo	Características	Cantidad
Switch	Marca: D'Link Modelo: DES-1024D 24 puertas RJ-45 10/100Mbps	2
Access Point	Marca: D'Link	1

	Modelo: DWL-2100AP Cobertura hasta 108Mbps - 2.4GHz Compatible con 802.11b y 802.11g	
Impresora	Marca: HP Deskjet Modelo: 1000 (CH340B) Conectividad, estándar: 1 USB 2.0	2
PC	Marca: Clon Procesador : Pentium IV Velocidad 3,06 GHz Disco Duro: 120GB Memoria RAM: 512 Mb	10
PC	Marca: Clon Procesador : Pentium IV Velocidad 1,7 GHz Disco Duro: 40GB Memoria RAM: 512 Mb	15

Tabla 3. 12: Software Centro Productivo CEMA

Nombre del Paquete	**Características**
Sistema Operativo Microsoft Windows Server 2003 .Instalado en el Servidor	Versión: Standard Edition
Microsoft Office	Versión: Professional 2007
Sistema Operativo Microsoft Windows XP. Instalado en las estaciones de trabajo	Versión : Professional Service Pack 2
Antivirus	Karspesking
AutoCAD	Versión: 2010

3.11. IMPLEMENTACIÓN Y PRUEBAS DE FUNCIONAMIENTO DE LA RED DE DATOS DELL CIMAM

Las redes de Datos han pasado de ser patrimonio de solo algunos grandes grupos empresariales a popularizarse y extenderse a todos los ámbitos de la empresa e incluso a los entornos domésticos.
Por su parte los costos del equipamiento y los circuitos de comunicaciones se han reducido de forma drástica, fundamentalmente gracias al fenómeno Internet, permitiendo a cualquier empresa por pequeña que sea estar permanentemente "conectada", y acceder a la información desde cualquier lugar y en cualquier momento.

3.11.1. IMPLEMENTACIÓN

Luego de haber realizado el diseño de la Red de Datos, se inicia con el proceso de implementación, el mismo que consta de las siguientes etapas:

- **Instalación De Canaletas**

  Una vez que se ha coordinado los detalles de las distancias entre canaletas con el personal técnico se procedió a la colocación de canaletas 60x40mm con división (ver figura 3.12), a una separación de 1.90m medidos desde la pared y 1.51m entre canaletas.

  Se prestó especial atención a los radios de curvatura de forma que cumpla con las normativas revisadas anteriormente.
  Por las canaletas se guiaron los cables UTP Cat 5e y cables 12 AWG. Se utilizó este tipo de canaleta con división entre cables de datos y eléctricos

por la facilidad en la instalación y para lograr conservar la estética en el departamento productivo CIMAM.

Figura 3. 17: Canaleta instalada en el CIMAM

- **Instalación Del Sistema Eléctrico**

Después que se realizó la colocación de las canaletas se procedió a realizar la instalación del sistema eléctrico tomando en cuenta algunas consideraciones para la instalación de sistemas eléctricos.

Figura 3. 18: Instalación de cables para el Sistema Eléctrico

El sistema instalado cuenta con tres cables flexibles #12AWG para la polarización de la fase (negro), neutro (blanco) y tierra (verde), los cuales irán en un compartimiento de la canaleta, como se observa en la figura 3.18

- **Tendido Del Cable UTP Cat 5e**

Para proceder a realizar el tendido del cable UTP se miden las distancias desde donde va a ubicarse el punto de red (área de trabajo) hasta el Patch panel (ubicado en el rack de comunicaciones), siguiendo la ruta de la canaleta instalada previamente. Se empezó a cablear desde las salidas de telecomunicaciones más lejanas del Patch panel. Mientras se realiza el tendido del cable se sigue etiquetando cada cable en ambos extremos para identificarlos bien y de esta manera evitar posteriormente ponchar los cables en puntos equivocados.Al momento de realizar el tendido del cable es importante dejar una longitud adicional de cable a los extremos, la misma que servirá como margen de manipulación e instalación. Esta longitud adicional servirá también como seguridad en el caso de que sea necesario ponchar el cable nuevamente. Ver figura 3.19.

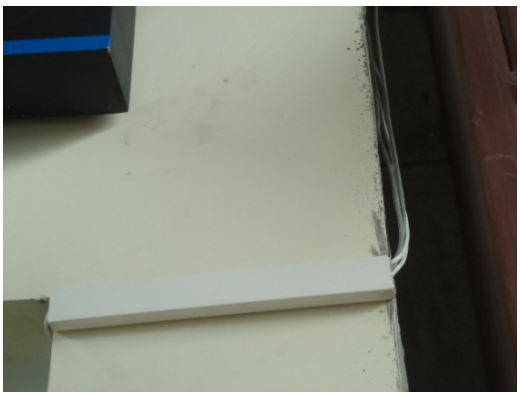


Figura 3. 19: Instalación del cable UTP Cat 5e

Además se debe tener mucho cuidado de no ejercer demasiada fuerza de tensión en los cables ni violar los radios de curvatura permitidos ya que esto puede afectar a las características de transmisión de los mismos.

- **Ponchado De Jacks e Instalación De Faceplates**

El ponchado de Jacks se lo hizo de acuerdo a la norma T568B. Antes de colocarlos en los Faceplates se revisó que hayan sido ponchados correctamente.

En la instalación de Faceplates se tomó muy en cuenta que los Jacks hayan sido colocados correctamente para que al momento de encajarlos en las cajas rectangulares y sujetarlos con los tornillos no se cause ningún daño al cable. Ver figura 3.20.

Figura 3. 20: Instalación de Faceplates y Ponchado de Jack

- **Montaje y Armado Del Rack Y Patch Panel**

En el montaje y armado del Rack de comunicaciones, es necesario dejar un espacio considerable para movilidad e instalación de componentes.

Esta distancia será medida desde la(s) pared(es) más cercana(s) hasta el Rack.El Patch panel debe ubicarse a una altura promedio de tal manera que brinde comodidad y holgura al momento de instalar los componentes.

Como primer paso se procedió a colocar el rack de piso, para posteriormente instalar los Switch, los Patch panel y los organizadores.

Una vez colocado el Patch panel se procedió a ponchar en la parte posterior del mismo de acuerdo a la norma T568B utilizada en toda la red de datos, para ello se utilizó la ponchadora de impacto 110. Ver figura 3.21.

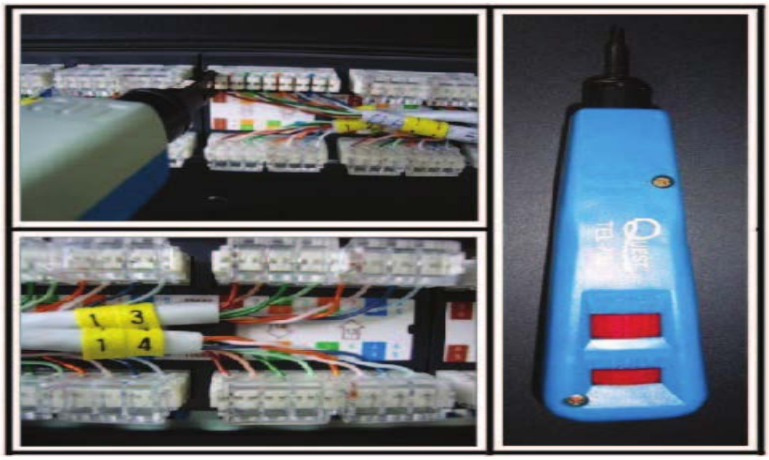


Figura 3. 21: Instalación de Cable UTP en el Patch Panel y Ponchadora

- **Pruebas De Continuidad Punto A Punto**

Una vez concluida la instalación de todos los elementos que conforman el Sistema de Cableado Estructurado se procedió a realizar las pruebas de continuidad para cada uno de los puntos de datos.

La prueba se realizó con la finalidad de verificar que exista continuidad en cada hilo que compone el par trenzado y así descartar circuitos abiertos, cortocircuitos, pares divididos y otros problemas de cableado estructurado. Para ello se utilizó un equipo probador de cable (Cable Tester) para redes LAN. Ver figura 3.22.

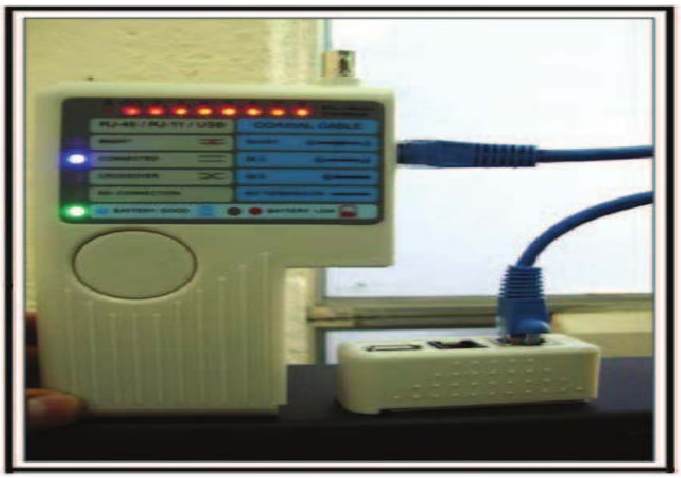


Figura 3. 22: Equipo probador de Cable Remoto

- **Certificación De Puntos**

Una vez testeado el cableado a fin de garantizar determinar continuidad, se puede proceder con las pruebas de certificación. Cabe mencionar que realizar una prueba no es lo mismo que obtener una certificación. La prueba es de funcionalidad y determina si el hilo puede transportar señal de punta a punta. La certificación o la verificación del rendimiento, es una declaración acerca de la productividad del cable que nos permite conocer la eficiencia con la que viaja la señal a través del medio físico, si la señal tiene o no interferencia, y si es lo suficiente fuerte como para llegar al extremo opuesto del cable, entre otros.

Para realizar la certificación de cada uno de los puntos del laboratorio se usó el equipo AgilentWireScope 350 (ver figura 3.23), este equipo realiza todas las pruebas de rendimiento necesarias para adherirse a los estándares ANSI/TIA/EIA-568-B.

Figura 3. 23: Equipo Certificador AgilentWireScope 350

Si el punto pasa la certificación la pantalla del equipo,como se muestra en la figura 3.24) y por el contrario si el punto no pasa la certificación la pantalla del equipo,como se muestra en la figura 3.24).

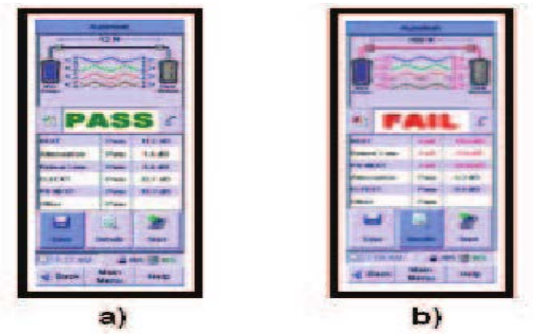


Figura 3. 24: Pantalla que se visualiza en el equipo de certificación.

3.11.2. INSTALACIÓN DEL SOFTWARE DE ADMINISTRACIÓN Y SEGURIDAD

El sistema de Administración aportará en la preservación de la confidencialidad, integridad y disponibilidad de la información de la red por lo cual se utilizó el Sistema Operativo Windows Server 2003, Standard Edition, debido a que proporciona un uso compartido inteligente de archivos e impresoras, conectividad a Internet más segura, administración centralizada de directivas de escritorio y soluciones Web para conectar a empleados, y clientes. Windows Server 2003, Standard Edition proporciona altos niveles de confiabilidad, escalabilidad y seguridad.

En el sistema de administración se configuró el servicio de DHCP (Protocolo de Configuración Dinámica de Host) que es útil para aquellas empresas/organizaciones que decidan que la configuración de red sea asignada automáticamente por un servidor de DHCP. De esta forma, a cualquier equipo que tenga las propiedades de red automáticas (sin IP fija) le será asignada una IP, una puerta de enlace, unas DNS, automáticamente por el servidor de DHCP.

Se configuró también el Active Directory, Cuentas de Usuario, Grupos, Dns, Recursos Compartidos.

Estos servicios se configuraron con el objetivo de unir los equipos de la red a un dominio específico.

Active Directory da a los usuarios de red acceso a los recursos permitidos en cualquier punto de la red mediante un único proceso de inicio de sesión proporcionando a los administradores de la red una vista jerárquica intuitiva de la red y un punto de administración único para todos sus objetos.

La implementación del sistema de seguridad, aportará en la integridad y disponibilidad de la información de la red, a través de la utilización de un Firewall. Es decir garantizar que solo aquellas personas autorizadas accedan a la información y a los recursos de la red, cada vez que lo requieran; manteniendo la exactitud y totalidad de la información y los métodos de procesamiento.

Además, minimizará los riesgos de seguridad a los cuales está expuesta la red interna frente a la gran red de internet. Reduciendo así, los riesgos de enfrentar problemas causados por cualquier tipo de virus.

Con más detalle se puede visualizar en Anexo B.

3.11.3. CONFIGURACIONES

Es un conjunto de datos que determina el valor de algunas variables de un programa o de un sistema operativo, estas opciones generalmente son cargadas en su inicio y en algunos casos se deberá reiniciar para poder ver los cambios, ya que el programa no podrá cargarlos mientras se esté ejecutando.

- **Configuración De Los Access Points**

  Los equipos para la instalación de la red inalámbrica son de Marca D-Link 2100AP, la adquisición de estos equipos fue tomada por decisión del Departamento de Sistemas de la DIAF por su fácil administración y su bajo costo comparada con otros equipos.

  Para el área de la Biblioteca, se requiere una señal inalámbrica, dicha área de trabajo necesita que satisfaga a un número de 10 usuarios.

  Para la configuración de los Access Point, la asignación de direcciones IP se implementó de una forma manual por políticas de la DIAF.

  Los equipos están configurados a partir de la dirección IP estática 192.168.4.180.

  Se especifica la configuración con más detalle en Anexo E.

- **Configuración De Server Printer**

  Para la utilización de Servidor de Impresión que tiene configurada una dirección IP estática se utiliza un dispositivo D-Link multiprotocolo serie DP-310P que permite conectar directamente la impresora a la red Ethernet, también administra el flujo de trabajos de impresión desde las estaciones de trabajo hacia la impresora que esté conectada, proporcionando un alto rendimiento en las tareas de impresión de dichos trabajos, obteniendo así una función de Print Server.

Se especifica la configuración con más detalle en Anexo D.

- **Configuración Del Outlook 2007**

Es un programa de organización ofimática y cliente de correo electrónico de Microsoft. Outlook 2007 integra correo electrónico, libretas de direcciones, calendarios, blocs de notas, listas de tareas, en un solo lugar, lo más importante, hace que esta información esté disponible cuando lo necesite. Las funciones más relevantes de este software son:

- Enviar, recibir, organizar y archivar mensajes de correo electrónico. También, puede filtrar el correo basura molesta.
- Enviar varios archivos como archivos adjuntos de mensajes y archivos adjuntos de vista previa que recibe de otras personas.
- Almacenar información de contacto en un formato fácilmente transferible que interactúa con el sistema de correo electrónico. Calendario de eventos, citas y reuniones, invitar a los asistentes, y reservar salas de conferencias, los proyectores, y otros recursos administrados.
- Ver las próximas citas y tareas, y recibir recordatorios para ellos.
- Seguimiento de las tareas por sí mismo o para otra persona, y el calendario para completar sus tareas.
- Compartir información de la programación con otras personas, dentro y fuera de su organización.
- Pista de las interacciones que tiene con otras personas.
- Organizar y localizar fácilmente la información en los mensajes, archivos adjuntos, calendarios, contactos y tareas.

Se especifica la configuración con más detalle en Anexo C.

- **Firewall Netcyclón**

  NetCyclón es una solución que agrega mucho valor a la infraestructura de comunicaciones de las empresas de cualquier dimensión, porque concentra en un mismo punto los servicios necesarios para garantizar un acceso al Internet y un manejo de correo electrónico seguros. El sistema fue concebido para abarcar las necesidades básicas de comunicación de datos de empresas pequeñas y medianas, en un esquema integrado “todo en uno”. Sin embargo se trata de una solución muy versátil, cuyas bondades han sido aprovechados por grandes organizaciones, al repartir sus servicios en varios dispositivos de hardware.

  La seguridad en las comunicaciones ha sido el objetivo central en el diseño de esta solución, así como poner al alcance de un vasto universo de usuarios, tecnología de punta con calidad. Con NetCyclon se asegura el perímetro de la red corporativa, se controla el contenido y la forma en la que los usuarios internos acceden a Internet, se acelera la navegación en el web, se protege el correo electrónico de males como los virus de correo y el Spam, y se habilita el acceso a las tecnologías más modernas de comunicaciones. Todo esto sin dejar de lado los estándares de la industria, lo que garantiza la integración de NetCyclon en cualquier ambiente de red.

  Todos los servicios que ofrece el NetCyclon pueden ser administrados gráficamente desde una interfaz amigable e intuitiva, lo que permite al personal de tecnología de las empresas concentrarse en su negocio

principal, y no dedicar esfuerzo innecesario a la configuración de sistemas complicados, que requieren un costoso entrenamiento particular.

Con NetCyclon se consigue controlar el acceso a Internet, gracias a sus notables funcionalidades de reportaría gráfica. Con estas herramientas, el administrador de red tendrá una visibilidad profunda de lo que ocurre con sus comunicaciones. Con los reportes web gráficos, el administrador conoce en tiempo real quién accede a qué sitios en Internet; qué tipo de conexiones en línea se encuentran establecidas; cómo se consume el ancho de banda WAN; así como el uso del servicio de correo electrónico. Los servicios de comunicaciones más importantes que ofrece NetCyclon son:

Control de Contenidos

- Listas Negras de URL's que pueden activarse o desactivarse.
- Generación de nuevas Listas Negras de URL's personalizadas.
- Listas Blancas de URL's totalmente confiables.
- Control de extensiones prohibidas.
- Control de Tipo MIME.
- Análisis Dinámico del contenido Web para el control de descarga.

Políticas de Navegación

- Regulación por día y hora de acceso al servicio de internet para cada usuario.

- Regulación para acceso restringido a URL's específicos por usuario, en un horario definido.

Protección Contra un Set Básico de Ataques

- Detección del Sistema Operativo.
- Anti Spoofing.
- Reducción de Riesgos de ataque de Denegación de servicios.
- Inundación de Bombas y paquetes de Sincronismo.
- Ataques de Paquetes Nulos.
- Ping de la Muerte.
- Protección contra el Escaneo de Puertos.

Antivirus

- Para correo Electrónico (entrante y saliente).
- Actualización Automática.

Servidor de Correo Electrónico

- Protocolos Soportados: SMTP, ESMTP, POP2, POP3, IMAP, IMAP4.
- Web mail.
- Control de tamaño de mensajes entrantes y salientes por usuario.

Servidor Web

- Soporta SSL , HTML, XML, SGML, PHP, JAVA SCRIPT
- Módulos para interacción con bases de datos.
- Múltiples dominios virtuales.

Servidor FTP

- Para transferencia de archivos desde y hacia el NetCyclón.

Servidor DHCP

- Asignación dinámica de direcciones IP por múltiples interfaces.
- Asignación estática de direcciones IP en función de la dirección MAC.

Reportes Gráficos Basados en la Web

- Reportes de navegación que indica quien accede a que sitios de Internet.
- Reporte de tipo de conexiones en línea se encuentran establecidas.
- Reporte del consumo de ancho de banda por interface.
- Reportes del uso de servicio de correo electrónico.

Se especifica la configuración con más detalle en Anexo F.

3.12. RESUMEN TÉCNICO

- La Red de la DIAF está constituida por una conexión directa de Internet proporcionada por la CNT, la misma que se conecta a un Switch de capa 2, a este se encuentra enlazado el Firewall SUPERMICRO a través de la interfaz WAN.
- La DIAF dispone de un servidor Web que tiene una entrada de Red Pública. La misma que tiene asignada una dirección IP estática dada por la CNT para el uso del servicio Web. Este servidor esta fuera del alcance de protección del firewall porque fue implementado después del desarrollo de sistema de seguridad de la red.
- En la interfaz interna se encuentra configurada la subred LAN de cada departamento. En la interfaz está habilitado direccionamiento Estático del Firewall, la misma que cada host tiene una dirección estática diferente.
- Cada estación de trabajo está registrada en el Firewall con su respectiva dirección IP asignada, para identificarle dentro del equipo. Y a la vez estas están incluidas en grupos de direcciones para facilitar el control y la administración de la red.
- De acuerdo a las necesidades de cada grupo de direcciones, está asignado un perfil de protección, el mismo que se encarga de proveer Antivirus, Control de Contenido, Políticas de Navegación, Control de Acceso al Servidor de Correo Electrónico, Servidor Proxy, Servidor de Archivos.
- Estos perfiles de protección están relacionados con las políticas de Firewall, las mismas que, según su configuración, se encargan permitir o denegar la conexión según las peticiones de cada usuario. Con el objetivo de proteger la red desde la interfaz interna hacia la externa.

- El Firewall Supermicro tiene una consola de administración basada en Web muy amigable e intuitiva para el administrador de la red, que facilita su configuración y administración.
- El enlace de la Matriz con las Sucursales es a través de una Red Privada Virtual
- La Red Privada Virtual está compuesta por tres tipos de conexión, los cuales son los siguientes: 1- RPV[40] de acceso remoto, 2- RPV sobre LAN y 3- RPV punto a punto. Esta red se caracteriza por tres tipos de conexiones, los cuales son los siguientes: Conexión RVP Router a Router, conexión de acceso remoto y conexión RPV firewall a firewall. Las grandes ventajas que nos brinda la VPN son la reducción de costos, facilidad de uso, confidencialidad y seguridad de los datos y la facilitación de comunicación entre los usuarios en diferentes localizaciones.
- El Firewall Supermicro instalado en el Cuarto de Datos de la DIAF está configurado y administrado con el Software NetCyclon.

Se especifica la configuración con más detalle en Anexo 7.

[40] Red Privada Virtual

CAPÍTULO 4
CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- La utilización del software de administración como NetCyclon permite brindar seguridad a la red de datos de los centros productivos CIMAM y CEMA, alcanzando el objetivo propuesto.
- Se realizó el cableado estructurado de la red de datos bajo la norma de calidad EIA/TIA 586-B, tomando en cuenta la estructura física y las necesidades de la DIAF en el que se instaló los equipos de telecomunicaciones, asegurando un funcionamiento óptimo de la red.
- Se garantiza la implementación y operabilidad del cableado de la red de datos de la DIAF, por la utilización del equipo de certificación llamado AgilentWireScope 350.
- La seguridad en redes de datos es una necesidad muy importante, debido a la información que por ellas se transmiten, por lo cual se utilizó tanto software como hardware, que permiten prevenir ataques informáticos y daños de información.
- Se evidencia la aplicación de mecanismos de seguridad en el sistema operativo Windows Server 2003, a través de la configuración del Active Directory, DNS, Cuentas de Usuarios y Directivas de Grupos.
- Con el uso del software de administración de la red se puede dar una serie de utilidades para mayor control y un adecuado funcionamiento de la red.
- La asignación de perfiles dentro de la red de datos de la DIAF potencia el trabajo colaborativo, haciendo el proceso más eficiente, propendiendo a la obtención de los objetivos de la Organización.

- El contar con la Red Inalámbrica permite reducir costos y a su vez que colapse la red cableada.
- Es necesario tener conocimientos sólidos en el manejo de redes de datos, sistemas operativos, configuraciones de dispositivos de red.
- Dada la extensión de la DIAF, y la cantidad de usuarios existente, es necesario centralizar el control de los recursos de los computadores de los usuarios finales de tal manera que éstos accedan únicamente a lo que realmente necesitan para realizar sus actividades de trabajo. En este sentido, la implementación de Active Directory.
- El desarrollo de la Red Ethernet con normas y estándares se encuentra en funcionamiento, la misma que proporciona servicios como correo electrónico, internet, entre otros.

4.2. RECOMENDACIONES

- Que la Universidad contemple dentro de sus políticas, establecer planes de relaciones institucionales que permitan que los estudiantes dispongan de opciones para hacer sus prácticas profesionales en instituciones públicas y privadas para contribuir a la consecución en la obtención del título universitario.
- Que la Universidad proponga espacios en los que se planifiquen talleres prácticos y apegados a la realidad laboral, en virtud de complementar la teoría práctica, permitiendo un mejor desenvolvimiento del estudiante en el campo laboral.
- Capacitar a los usuarios sobre el uso de la tecnología inalámbrica Wi-Fi para que hagan uso adecuado de la red y no se la subutilicen, permitiendo la ejecución de actividades relacionados con el mantenimiento preventivo y correctivo de la red inalámbrica.

- Los usuarios deben proteger sus archivos sensibles de confidencialidad, aplicar candados o seguridades.
- Es importante realizar la certificación de todo el sistema de cableado para comprobar que está operando de manera correcta y se encuentra en óptimas condiciones.
- Difundir el uso de herramientas de software libre ya que nuestro país no se puede dar el lujo de comprar licencias para todos los servidores que necesita implementar, reduciendo enormemente recursos económicos, obteniendo los mismos beneficios que nos brinda el software privativo.
- La utilización de estándares y equipos de certificación nos asegura la eficiencia, operabilidad, escalabilidad de la red de datos.
- En base al presupuesto destinado para el mantenimiento de la Red es necesario organizar un cronograma de mantenimiento anual de la red para que esta se encuentre siempre en óptimas condiciones.
- Se recomienda que los centros productivos CIMAM y CEMA, que se encuentran en Latacunga disponga de un proveedor de internet que actué como respaldo al momento que tenga problemas técnicos el proveedor contratado por la matriz Quito.
- Habilitar la administración del firewalls mediante usuarios remotos para que puedan acceder a la configuración desde cualquier parte del mundo, los cuales deberán estar registrados en el servidor principal de la Red.

BIBLIOGRAFÍA

- Stallings William, Comunicaciones y Redes de Computadores. Prentice Hall. 7ma. Edición
- Carballar, J. A. (Junio 2006). *FIREWALL La seguridad de la banda ancha.* Mexico: Alfaomega Grup Editorial S.A. de C.V.

- Goncalves, M. (Septiembre 2001). *Manual de Firewalls.* Mexico D.F.: McGraw-Hill Interamenricana, S.A. de C.V.
- Lipman, V. (2001). *Orange.* Recuperado el 12 de 05 de 2010, de file:///E:/diseno-de-una-red-propuesta.html
- Moya, J. M. (2001). *Redes y Servicios der Telecomunicaciones.* Madrid-España: Thomson Editores Spain araninfo S.A.
- Ochoa., C. A. (2003). *Monografias.com* . Recuperado el 19 de 5 de 2010, de Monografias.com : file:///C:/Documents%20and%20Settings/Tobias%20Chica/Escritorio/redes%C2%B4manuales/sein.shtml
- Stalling, W. (2002). *Comunicaciones y Redes de computadores.*Madrid: Prentice Hall.
- D. W. Davies, W. L. Price "Security for Computer Networks". John Wiley & Son Ltd. November 1989.
- Stallings, W. (2000). *Comunicaciones y Redes de Computadores.*Cataluña: Pearson Education, S.A.
- Tanenbaum, A. S. (1997). *Redes de Computadoras.* Mexico: Prentice-Hall HISPANOAMERICA S.A.
- Untiveros, S. (Julio de 2004). *Metodologias para Administrar Redes*. Recuperado el 11 de 05 de 2010, de AprendaRedes.
- PROFESORES TÉCNICOS DE FORMACIÓN PROFESIONAL, Sistemas y Aplicaciones Informaticas, 2da Edicion, 2006.
- INEI, Instituto Nacional de Estadística Informática, Introducción al Cableado Estructurado, Colección Cultura Informática, Diciembre 2002.
- RODRIGUEZ DURAN Luis, El Gran Libro del PC Interno, 2007.
- TOMASI Wayne, Sistemas de Comunicaciones Electrónicas, Edición 4, 2003.

INTERNET

- "Concepto sobre Medios de Transmisión, Fibra Óptica y Microondas". http://www.mitecnologico.com/Main/MediosDeTransmisionFibraOpticaMicroondas.
- "Topología de Redes" http://www.tecnologia.mendoza.edu.ar/comunicacion/topologia.htm
- "Arquitectura de Redes" http://arquitecturapc.blogspot.es/1207606620/
- "Redes Inalámbricas" http://tutorial.galeon.com/inalambrico.htm
- "Dispositivos de Redes" http://glendasnotepad.wordpress.com/2008/07/20/dispositivos-de-networking/
- "Aspectos Básicos de Redes" http://www.scribd.com/doc/23270783/1-3-Aspectos-Basicos-de-Networking http://www.monografias.com/trabajos30/conceptos-redes/conceptos-redes.shtml
- "Transmisión de Datos" http://www.mailxmail.com/curso-redes-transmicion-datos-1/transmision-datos-analogicos-digitales-perturbaciones
- "Tecnología Token_Ring"

  http://www.numina.net.uy/index.php?option=com_content&view=article&id=60&Itemid=65

- "Características Generales de un Sistema de Cableado Estructurado"

http://www.gennoa.com.ar/node/65.

- "Normas para Cableado Estructurado"

http://www.electronica.7p.com/cableado/estan.htm

- “TIA/EIA Normas para Cableado Estructurado”

“Elementos Principales de un Cableado Estructurado”

http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/458/10/Cap%C3%ADtulo%208_2.pdf.

- “Subsistemas de Cableado Estructurado”

http://www.reto.com.mx/subsistemas.php

- “Cableado Vertical”

http://www.parla.com.mx/cableadoestructurado.htm

- “Esquema de cableado Vertical”

http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/subs1.htm

- “Información General de Sistemas de Cableado Estructurado”

www.cableadoestructuradosenaipiales.blogspot.com

- “Información General del Cuarto de Telecomunicaciones”

http://www.slideshare.net/guesta4d883/cuarto-de-telecomunicaciones-1166154

- “Patch Panel Cat 5E”

www.americantechsupply.com

- “Área de Trabajo”

http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/areade.htm

- “Certificación de Redes”

http://elqui.dcsc.utfsm.cl/apuntes/redes/acceso-libre/pdf/1-2-Capa-Fisica_Coaxial-UTP.pdf.

- “Parámetros de Certificación de Redes”

http://support.novell.com/techcenter/articles/nc2000_08c.html

- “Conceptos Generales de redes de Datos”

http://www.it.uniovi.es/docencia/Telecomunicaciones/proyectos/material/PARTE%2011_Conceptos_Generales.pdf

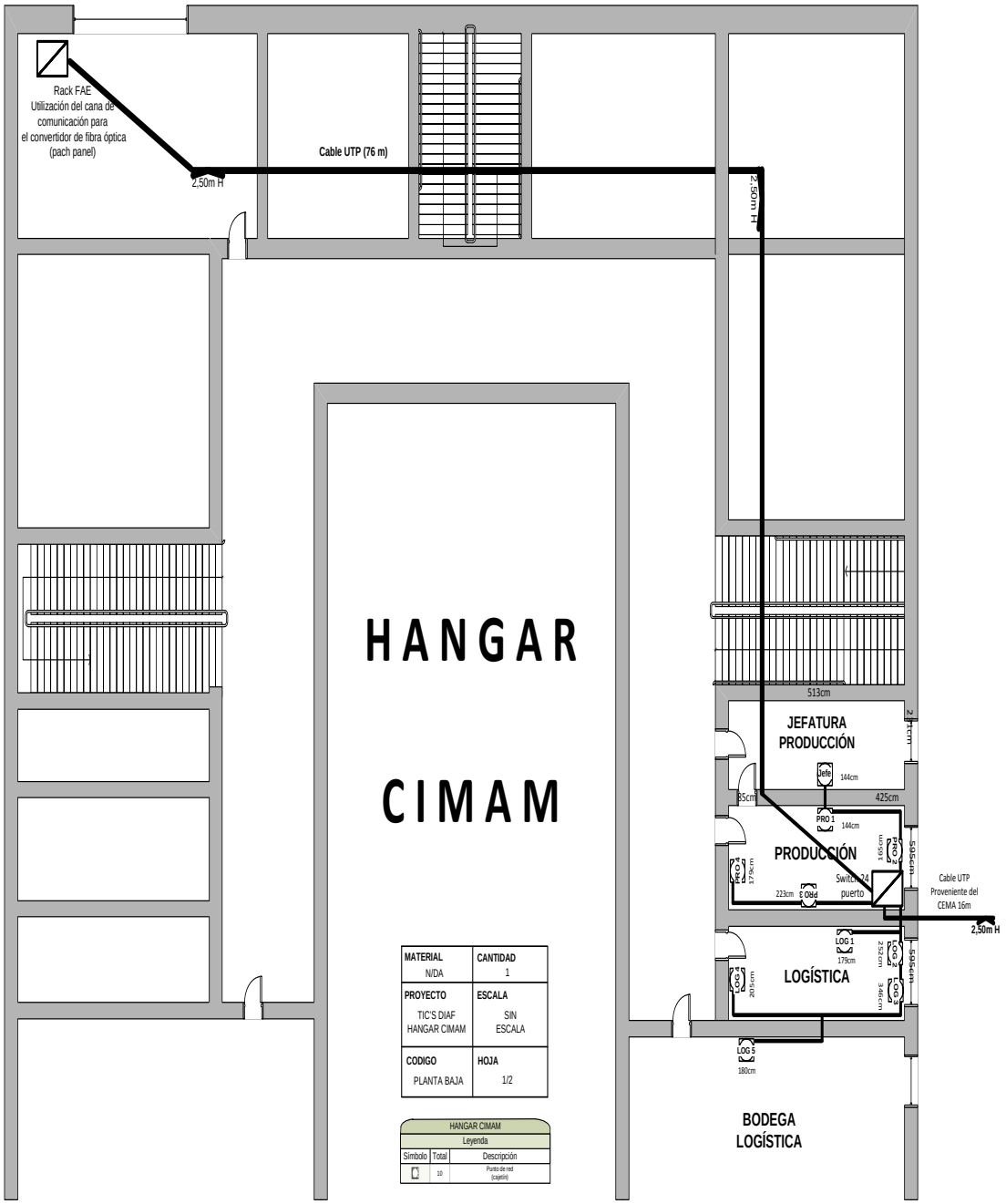
- “Redes de Computadoras”

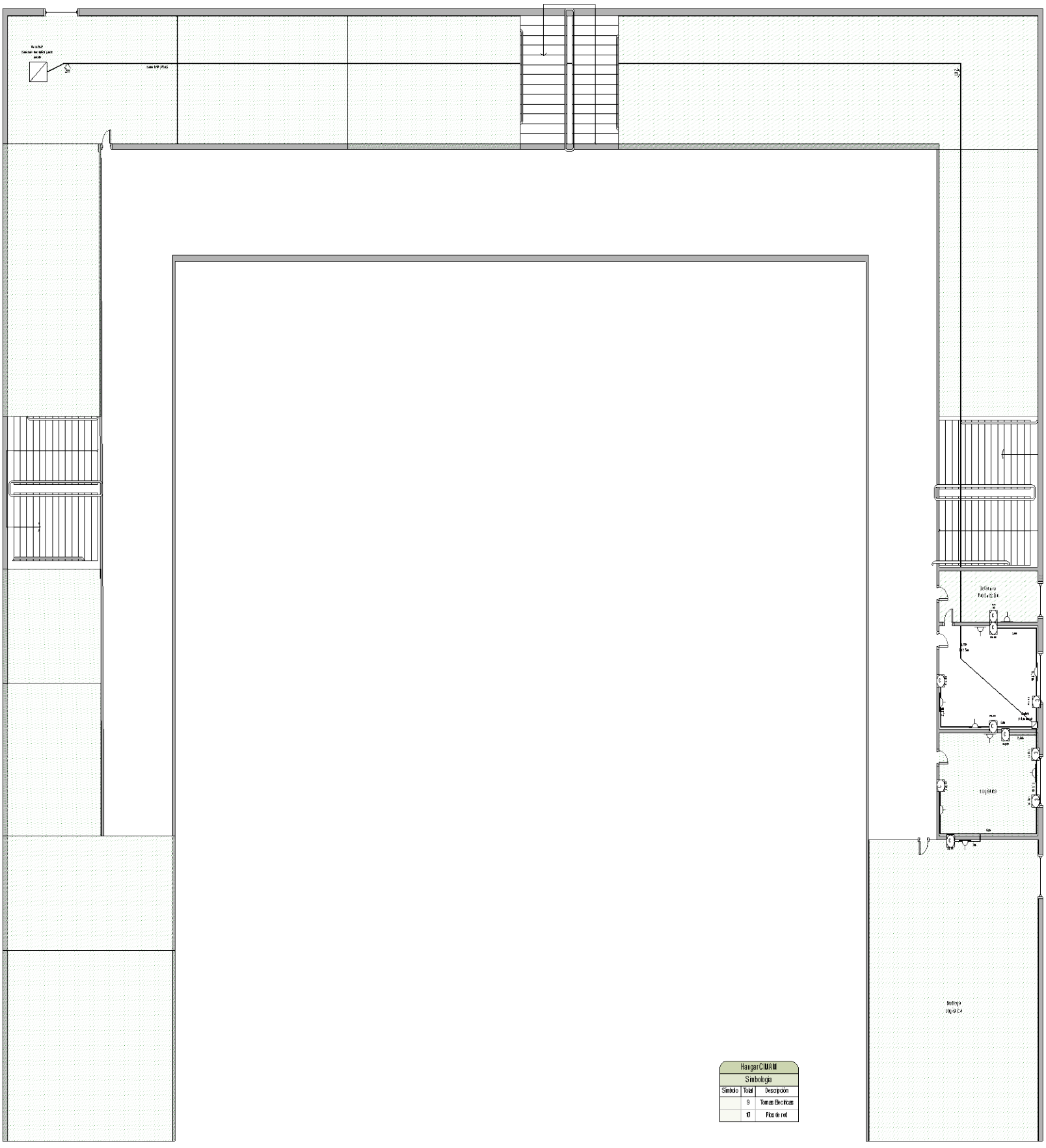
http://www.monografias.com/trabajos24/redes-computadoras/redes-computadoras.shtml.

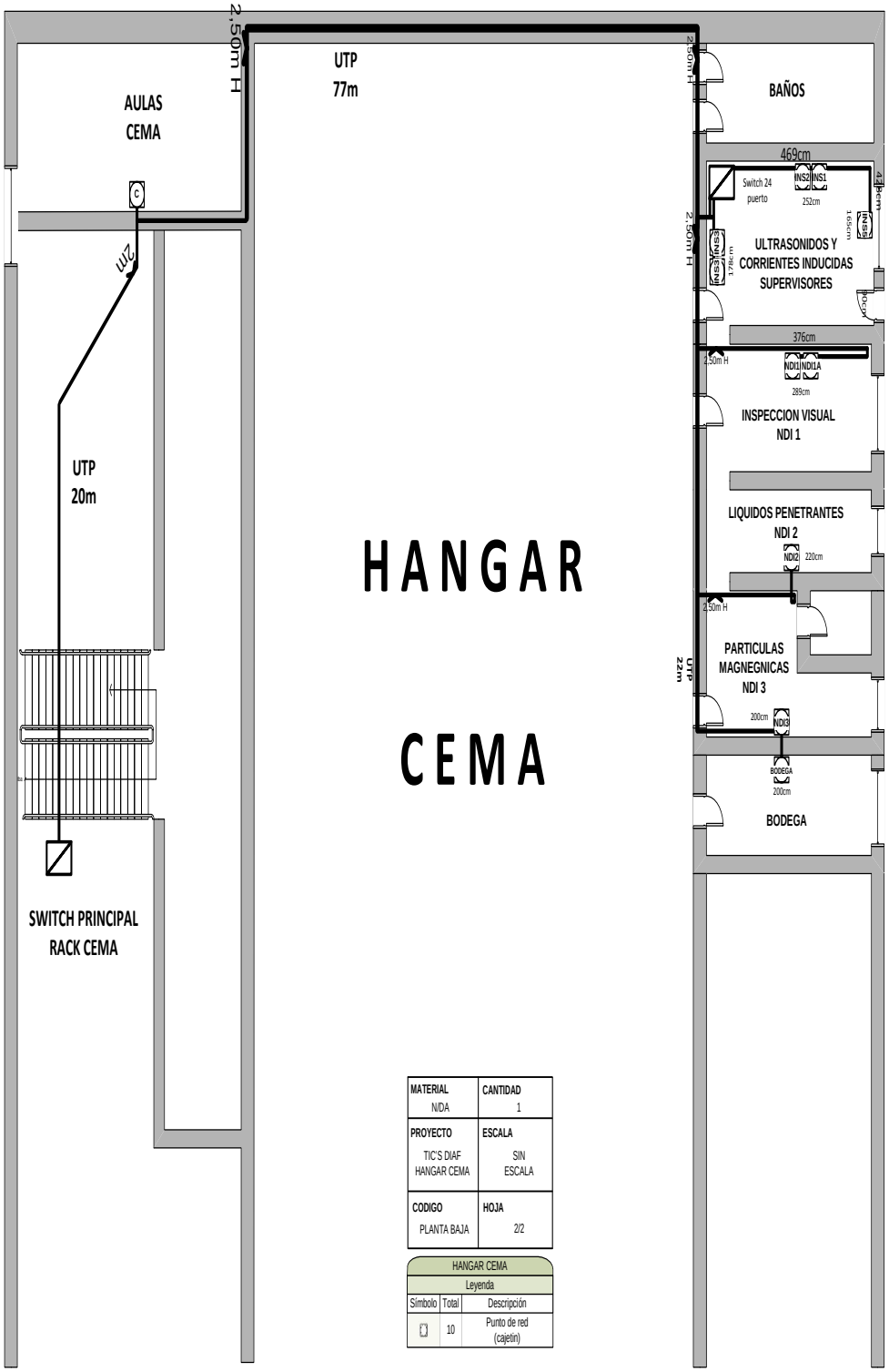
ANEXOS

Anexo A:

DISEÑO DEL TENDIDO DEL CABLEADO ESTRUCTURADO




Hangar CIMAM
Simbología
Símbolo
Total
Descripción
9
Tomas Electricas
10
Ptos de red



MATERIAL	CANTIDAD
NIDA	1
PROYECTO	**ESCALA**
TIC'S DIAF HANGAR CEMA	SIN ESCALA
CODIGO	**HOJA**
PLANTA BAJA	2/2

HANGAR CEMA		
Leyenda		
Símbolo	Total	Descripción
	10	Punto de red (cajetin)

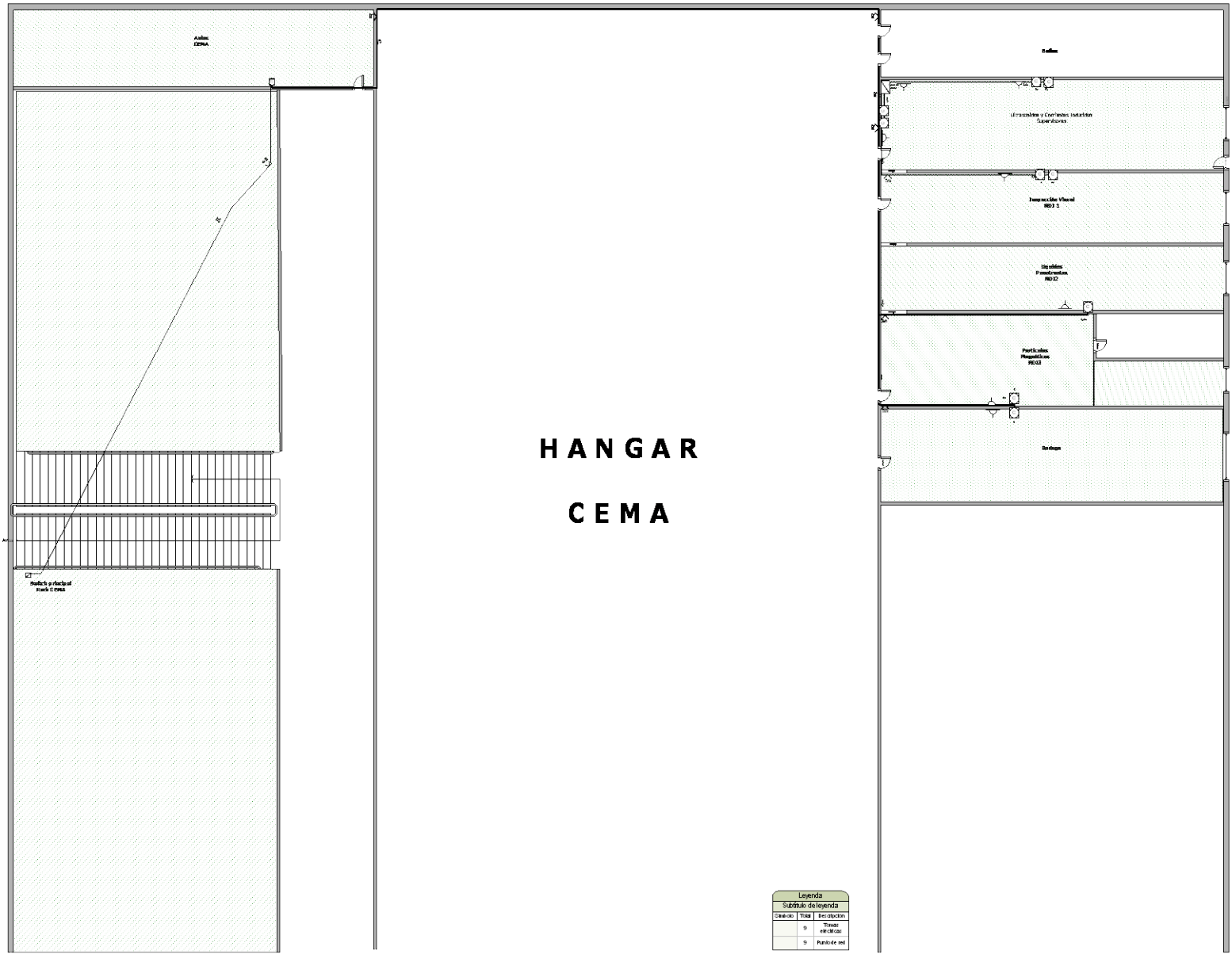
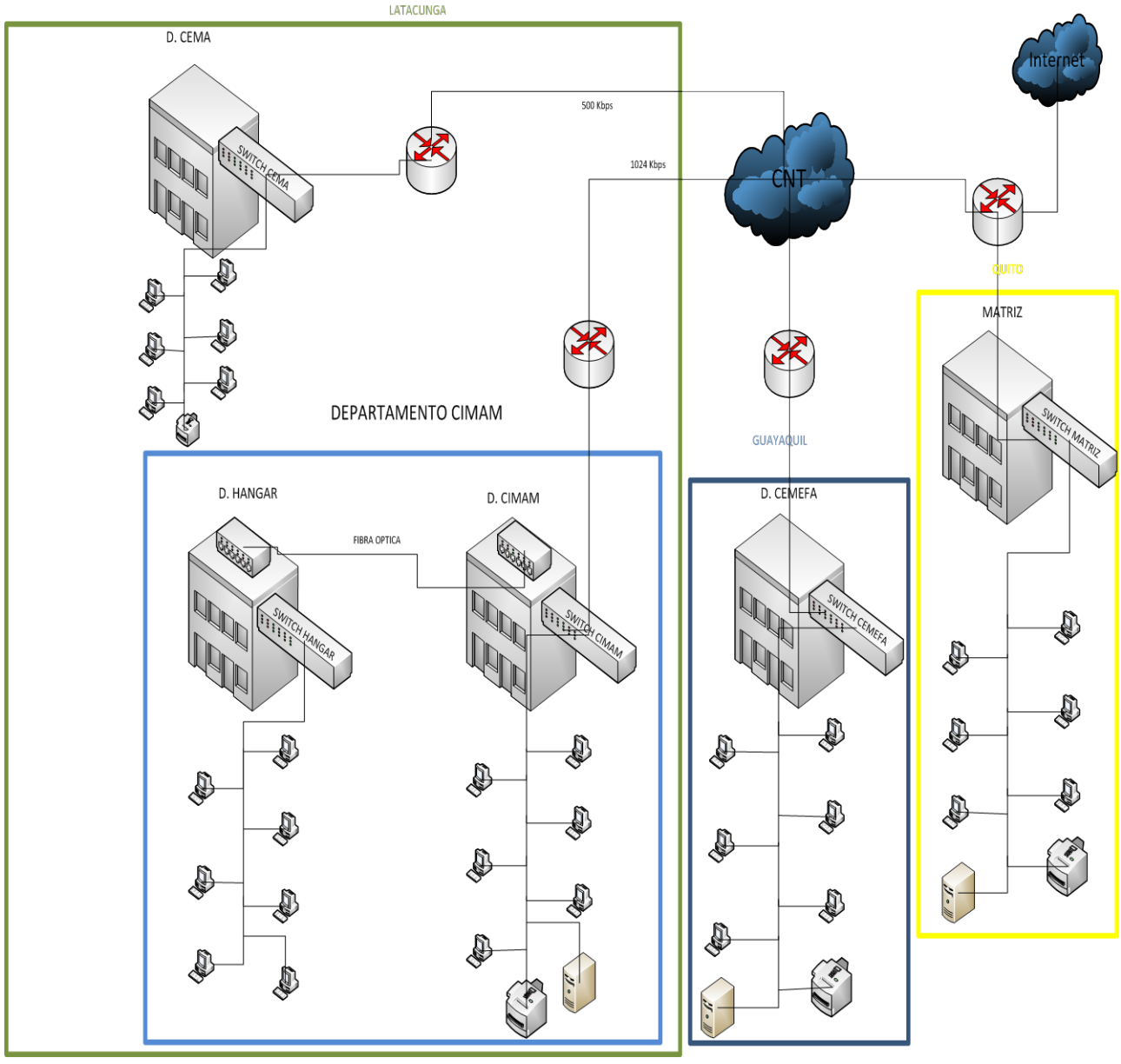
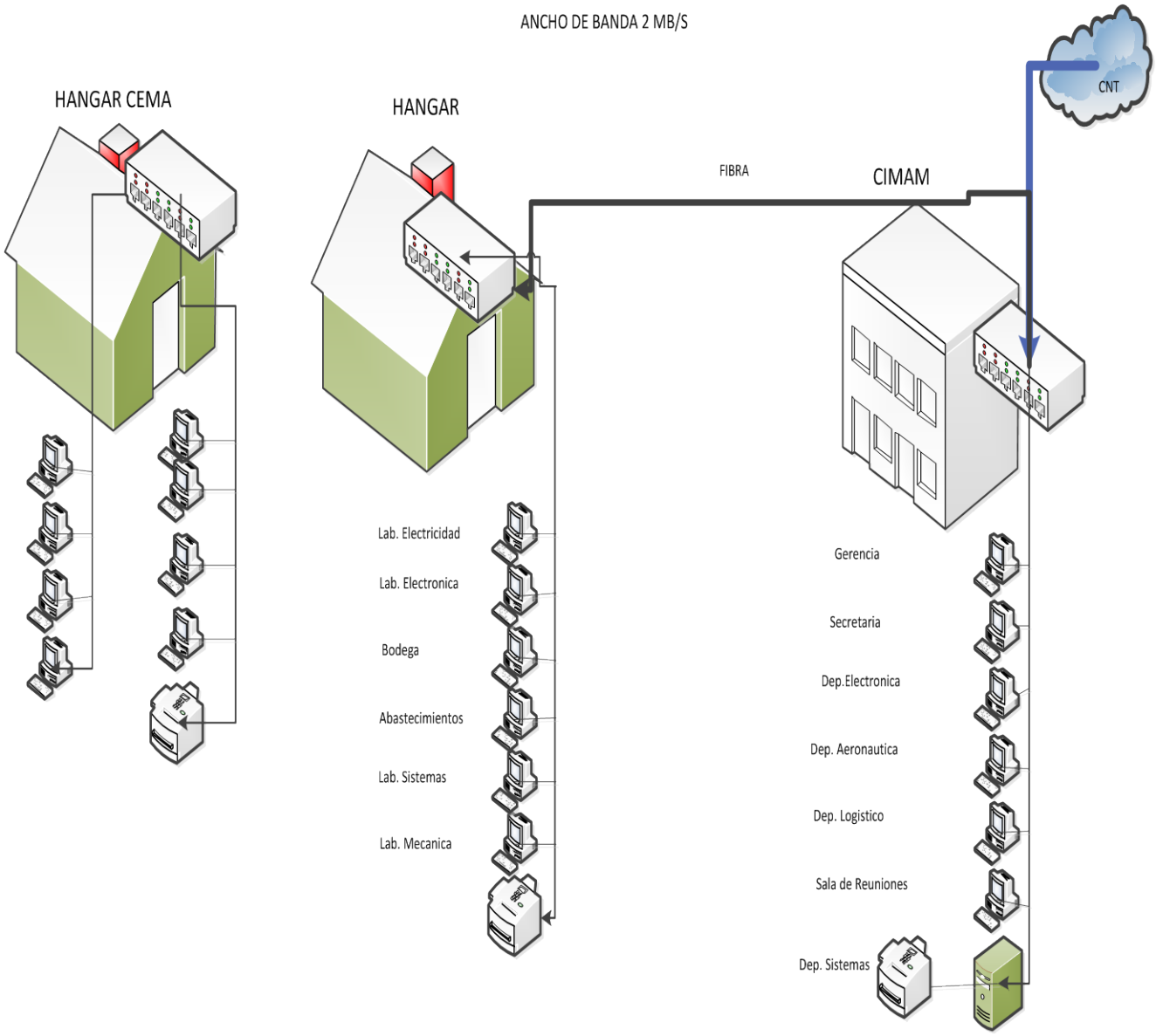

Aulas
CEMA
Radios
Ultrasonidos y Corrientes Inducidas
Superficiales
Inspección Visual
NDI 1
Líquidos
Penetrantes
NDI 2
Partículas
Magnéticas
NDI 3
Recibos
HANGAR
CEMA
Leyenda
Subtítulo de leyenda
Símbolo
Total
Descripción
9
Tomas
eléctricas
9
Puntos de red

DIAGRAMA DE CONEXIONES DEL CENTRO CIMAM CEMA



RED DE DATOS DE LA DIAF

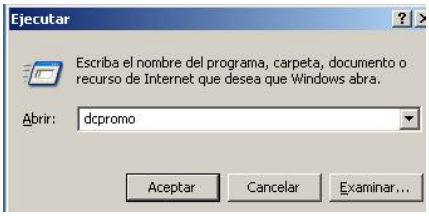


Anexo B:

CONFIGURACIONES EN EL SISTEMA OPERATIVO

Pasos para configurar Active Directory

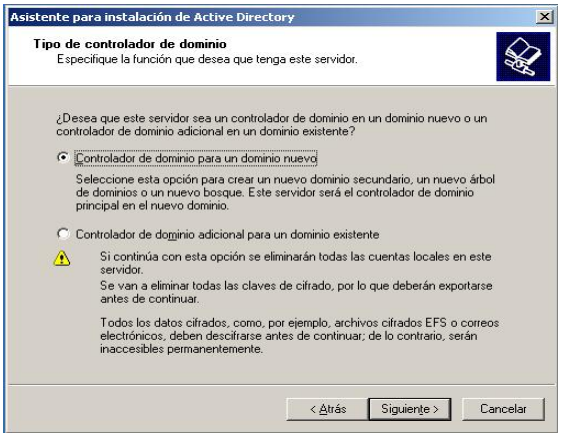
1. Dar click en ejecutar, escribimos dcpromo y seleccionamos en aceptar como se ve en la figura.



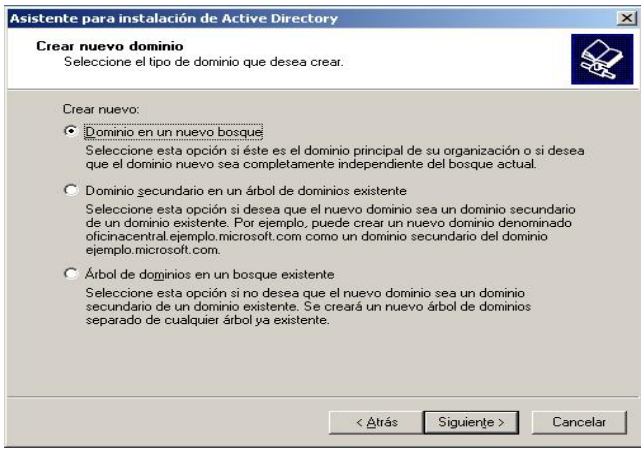
2. En esta ventana para instalación simplemente se elige la opción siguiente como se ve en la figura.

3. A continuación aparece una nueva ventana de compatibilidad de sistema operativo y aceptando las condiciones, se da click en la opción siguiente como se ve en la figura.

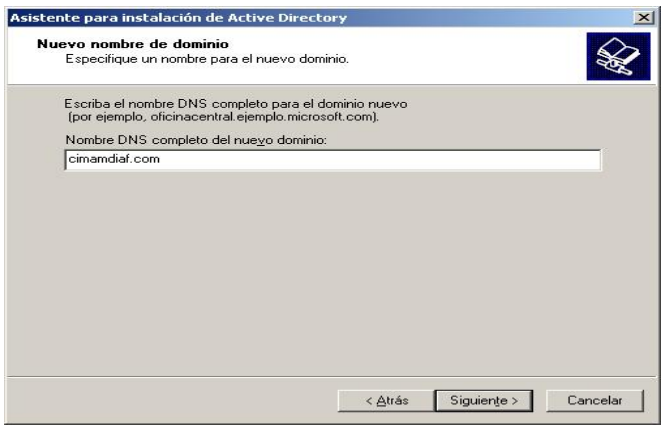
4. En esta ventana de tipo de controlador de dominio, se selecciona la opción controlador de dominio para un dominio nuevo y se escoge la opción siguiente como se ve en la figura



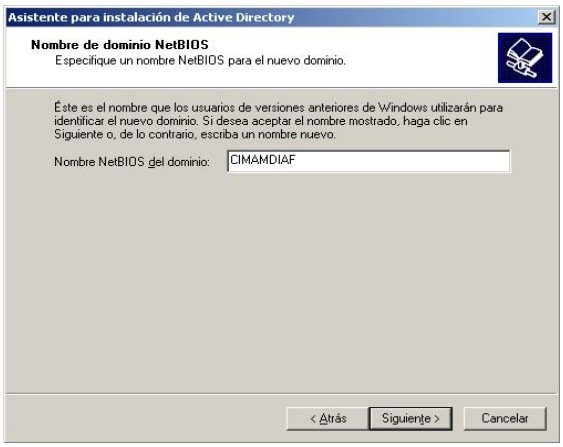
5. En la ventana crear nuevo dominio se elige la opción dominio de un nuevo bosque y se presiona siguiente como se ve en la figura.



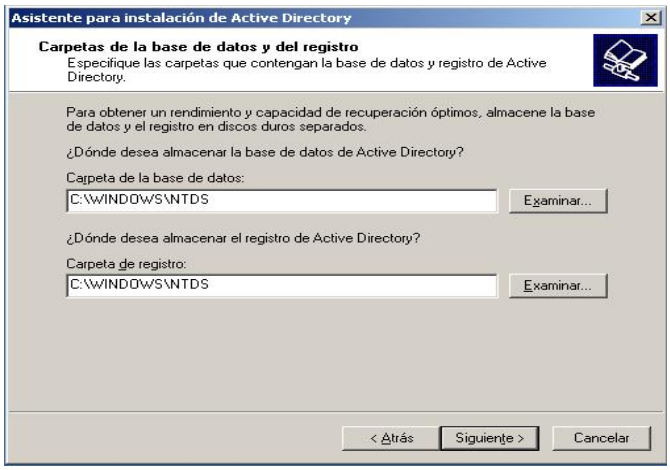
6. Se presenta una nueva ventana para nuevo nombre de dominio, se procede a escribir cimamdiaf.com y se selecciona la opción siguiente como se ve en la figura.



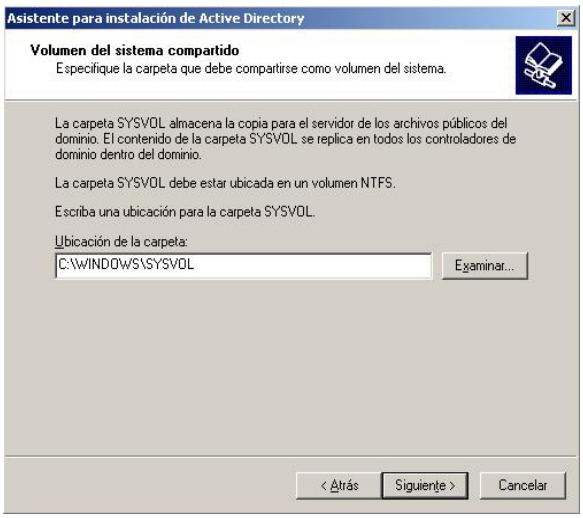
7. En la nueva ventana de dominio NetBIOS, se escribe CIMAMDIAF y se selecciona la opción siguiente como se ve en la figura.



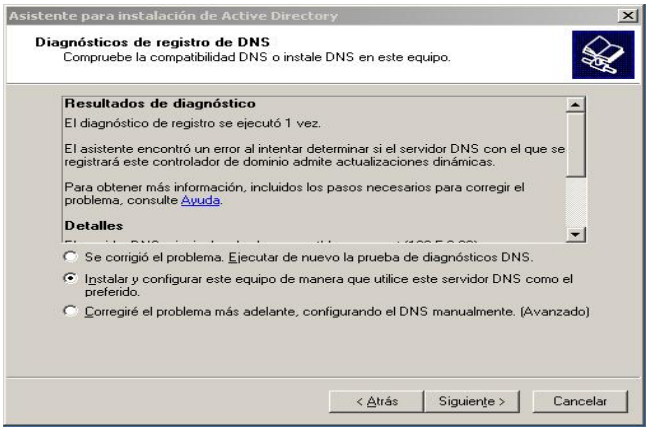
8. Se presenta una nueva ventana de Carpeta de la base de datos y del registro; presentando dos preguntas, en la primera se procede a escribir C: \WINDOWS\NTDS, en la segunda se escribe C:\WINDOWS\NTDS seleccionando la opción siguiente como se ve en la figura.



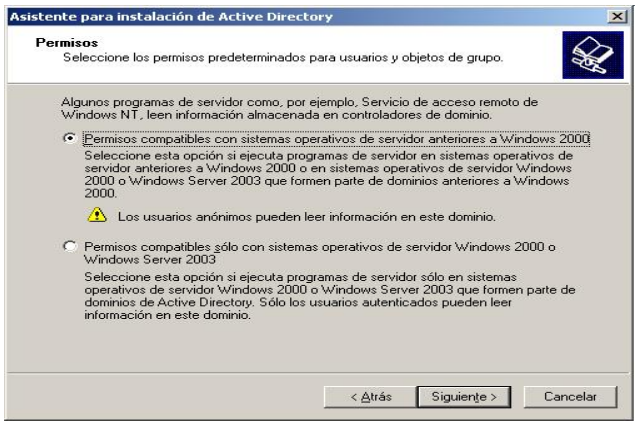
9. En esta ventana aparece la opción: volumen del sistema compartido en la cual y dar click en siguiente como se ve en la figura.



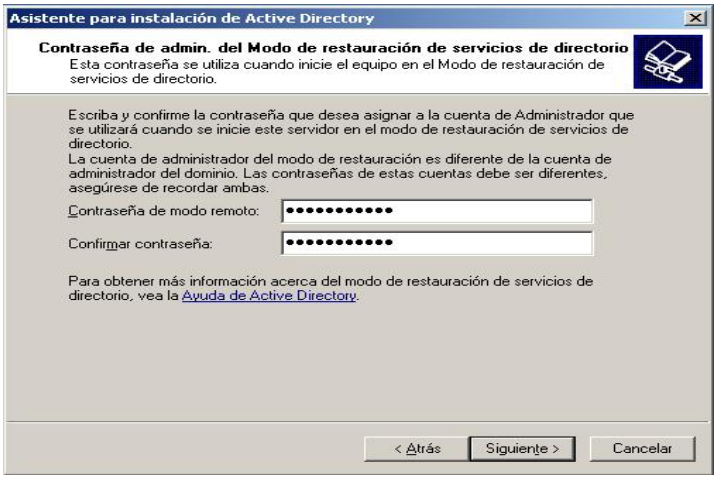
10. Se nos presenta la ventana de diagnósticos de registros de DNS con tres opciones en la cual se escoge: instalar y configurar este equipo seleccionando la opción siguiente como se ve en la figura.



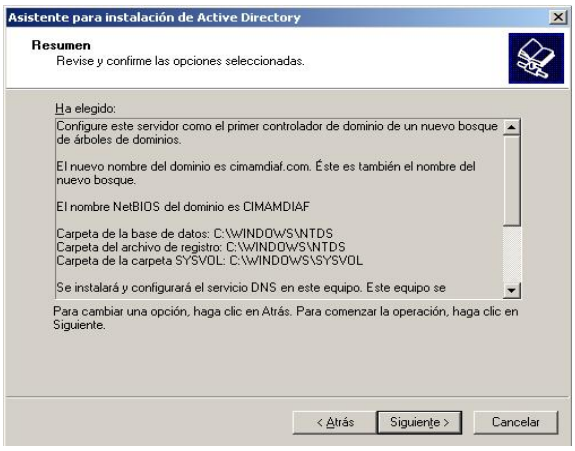
11. A continuación se nos presenta los permisos con dos opciones en la cual se selecciona la opción: permisos compatibles con sistemas operativos y dar click en siguiente como se ve en la figura.



12. Se nos presenta una nueva ventana en la cual se procede a escribir y verificar la contraseña y dar click en siguiente como se ve en la figura.



13. A continuación se nos presenta el resumen para revisar y confirmar los datos seleccionado; verificando los datos se procede a dar un click en la opción siguiente como se ve en la figura.



14. En la nueva ventana se espera a que el Active Directory se haya configurado hasta presentar una respuesta como se ve en la figura.

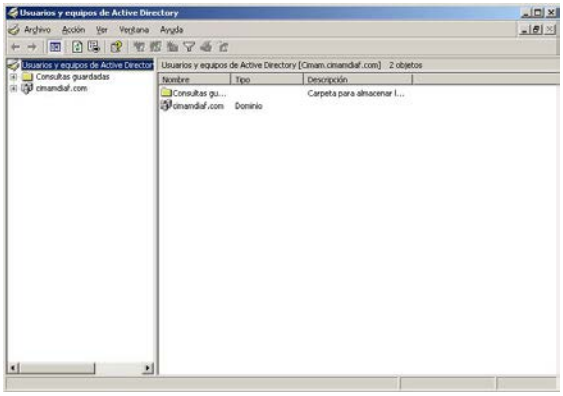
15. Finalmente el Active Directory se ha instalado con todos los datos confirmados del dominio cimamdiaf.com y para concluir dar click en la opción finalizar como se ve en la figura.

16. Por último se reinicia Windows para que surtan efecto los cambios realizados para el Active Directory.

Pasos para Configurar Cuentas de Usuario

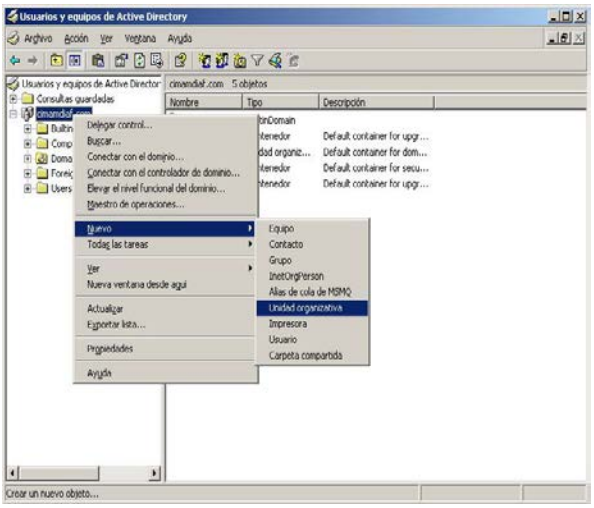
1. Lo primero que se hace es ir a, todos los programas, herramientas administrativas, usuarios y equipos de Active Directory tal y como se ve en la figura.

2. Aquí se ve la consola, desde donde se realiza todos los pasos necesarios, para crear la cuenta como se ve en la figura.

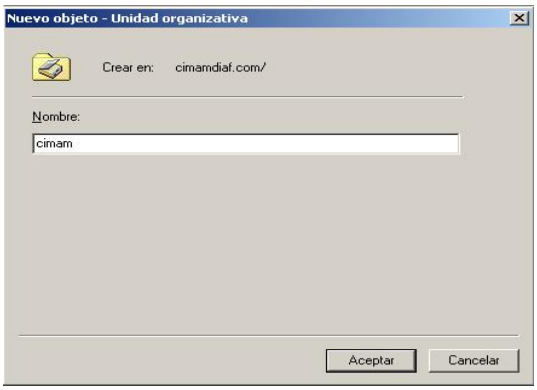


3. Lo primero que aquí se hace será crear una unidad organizativa, para introducir dentro las cuentas y grupos de usuario que nos interese, pudiendo introducir más

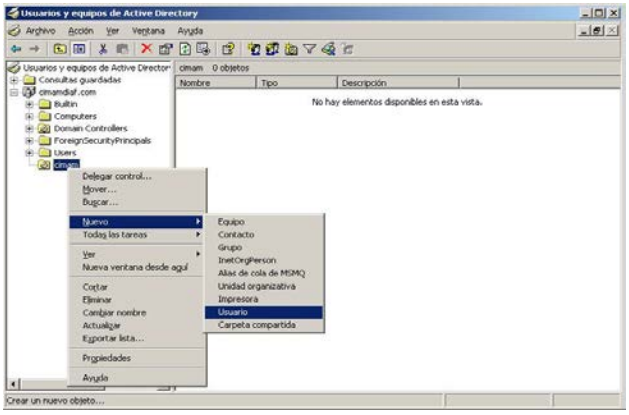
tipos de objetos. Pulsar en el botón derecho del ratón en el nombre del dominio, se escoge nuevo, unidad organizativa como se ve en la figura.



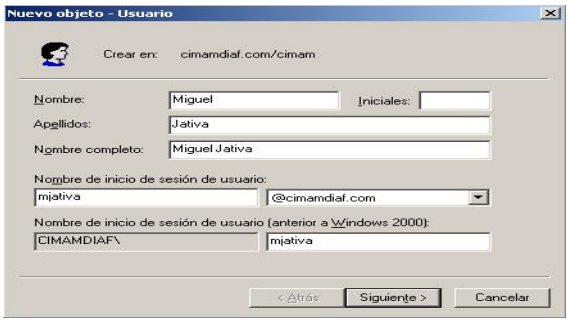
4. Se escoge el nombre a la unidad organizativa. Pulsar en el botón aceptar como se ve en la figura.



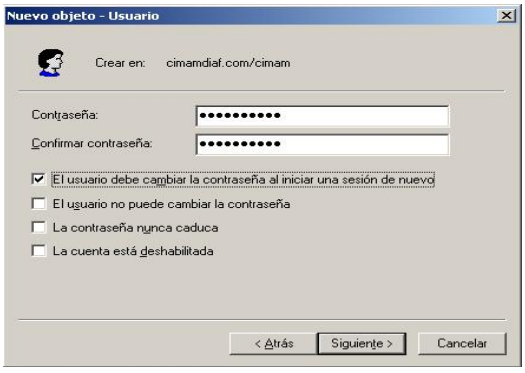
5. Dentro de la unidad organizativa se crea nuestra cuenta de usuario. Para ello se pulsa con el botón derecho del ratón se seleccionar nuevo usuario como se ve en la figura.



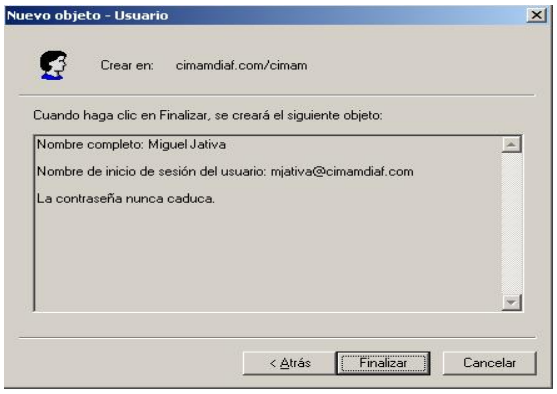
6. Introducir los datos, como mínimo el nombre de usuario y el nombre de inicio de sesión y pulsar en el botón siguiente como se ve en la figura.



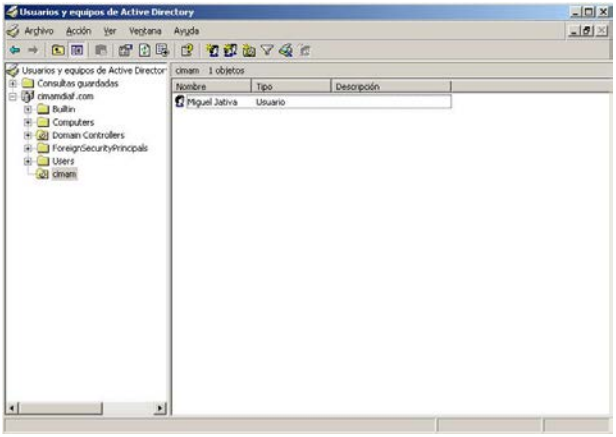
7. Digitar la contraseña dos veces y escogemos las opciones que se necesita, después pulsar siguiente como se ve en la figura.



8. A continuación se presenta una pantalla con todos los datos confirmados y dar click en Finalizar como se ve en la figura.

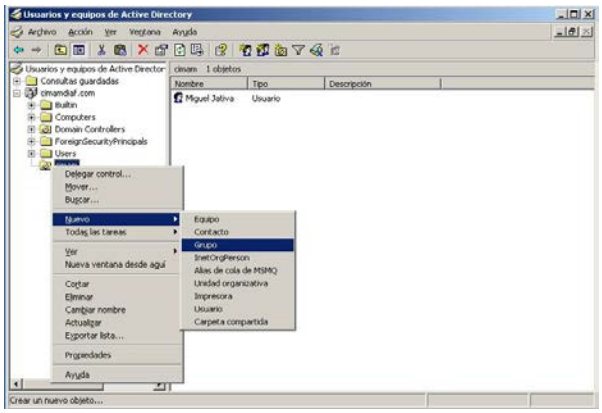


9. En la carpeta CIMAM se encuentra los datos del usuario creado como se ve en la figura.

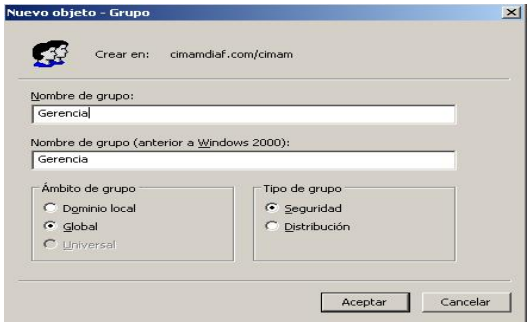


Pasos de Configuración de Grupo

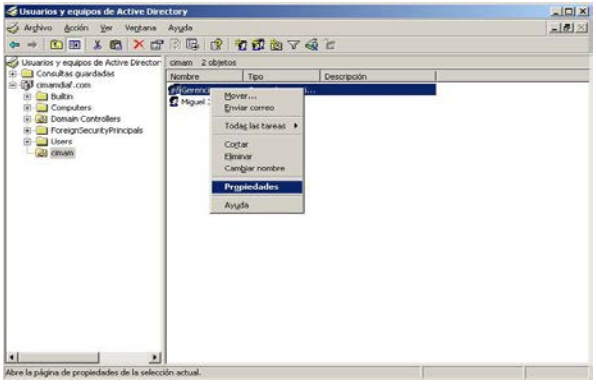
1. Pulsar con el botón derecho del mouse, en el área en blanco de nuestra unidad organizativa, y elegir nuevo grupo como se ve en la figura.



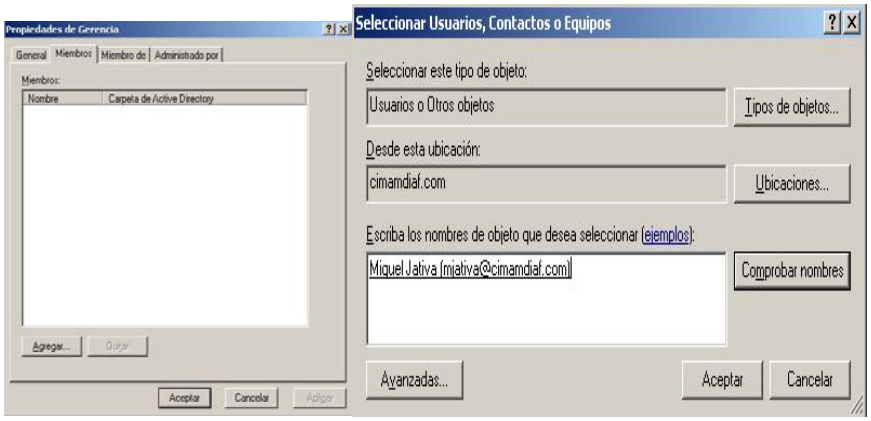
2. Colocar el nombre del grupo y pulsar el botón de aceptar como se ve en la figura.



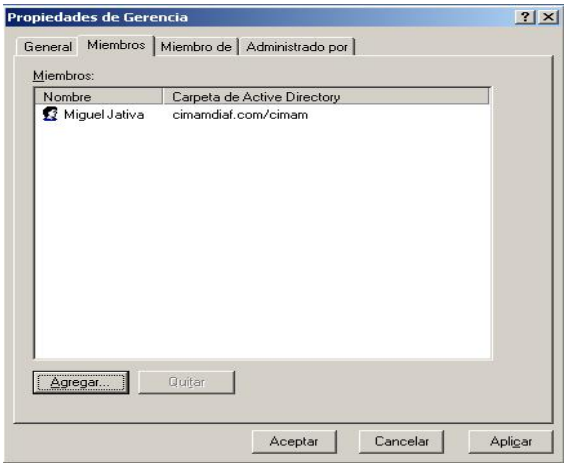
3. Con esto se tiene el grupo creado, pero un grupo vacío de poco nos sirve, así que se introduce los usuarios que pertenecen a este grupo. Para ello se pulsa con el botón derecho sobre el grupo y escoger propiedades como se ve en la figura.



4. En la pestaña de miembros, se pulsa en el botón agregar, e introducir los nombres de los usuarios y pulsar aceptar como se ve en la figura.



5. Observar que el usuario está introducido y volver a pulsar aceptar como se ve en la figura.

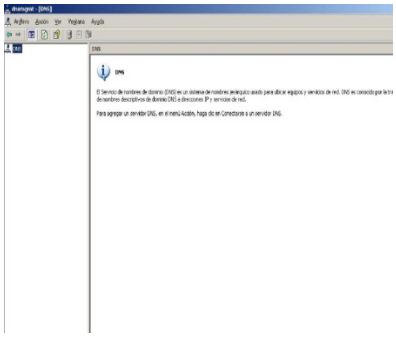


6. Con esto se ha terminado de introducir los usuarios en nuestro grupo.

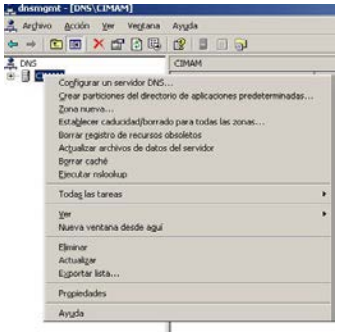
Configuración de DNS en Windows 2003 Server

1. Haga click en Inicio, seleccione Programas, haga click en Herramientas administrativas y, a continuación, en DNS como se ve en la figura.

2. Aparece la venta del servidor DNS como se ve en la figura.

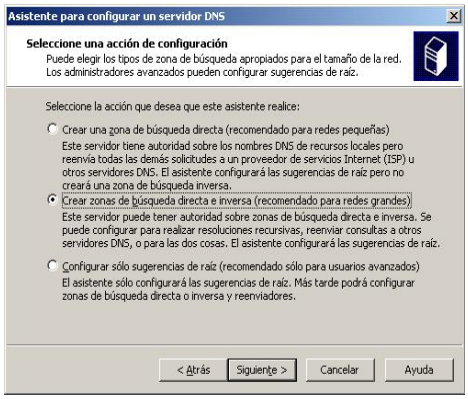


3. Dar un click secundario en servidor CIMAMy se selecciona configurar un servidor DNS como se ve en la figura.

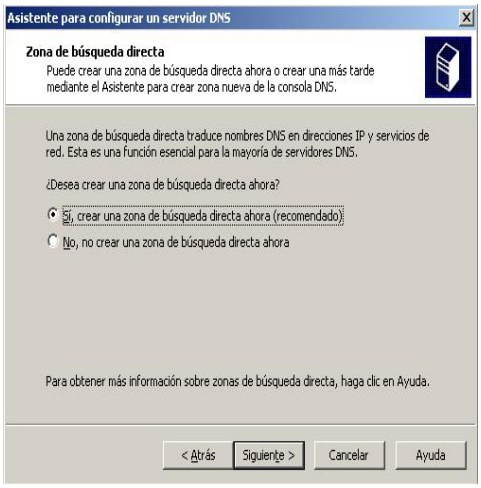


4. Aparece la siguiente ventana como se ve en la figura.

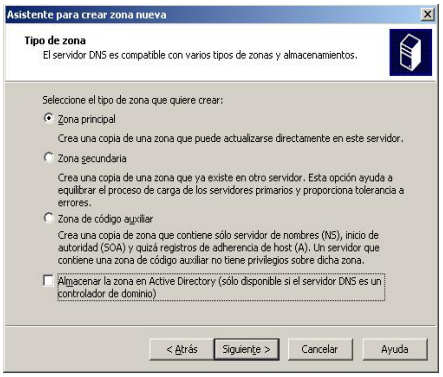
5. Seleccionar la opción de configuración como se ve en la figura.



6. Se visualiza la ventana de zona de búsqueda y seleccionar la opción Si como se ve en la figura.



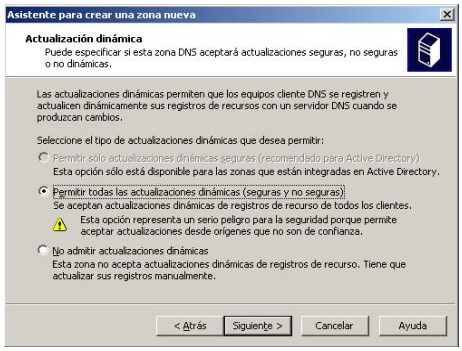
7. Se visualiza la ventana asistente para crear zona nueva y se procede a crear Zona principal como se ve en la figura.



8. Proceder a ingresar el nombre de la zona nueva y dar un click en el botón siguiente como se ve en la figura

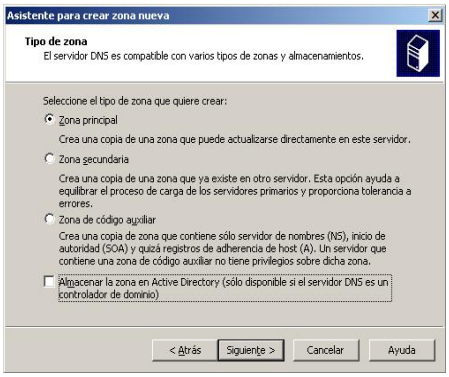
9. Se presenta la zona creada como se ve en la figura.

10. A continuación se visualiza la ventana que nos permitirá activar las actualizaciones dinámicas como se ve en la figura.

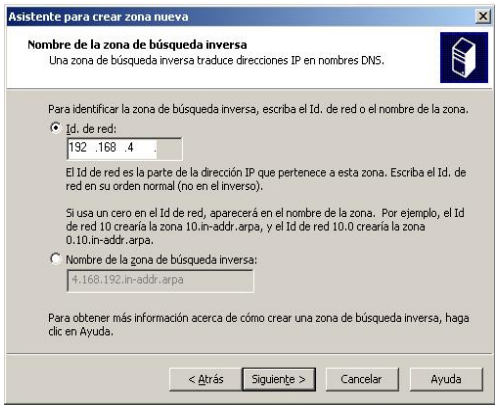


11. Se visualiza el asistente de zona de búsqueda inversa y seleccionar la opción Si crear zona inversa y pulsar en el botón siguiente como se ve en la figura.

12. A continuación se visualiza el asistente para crear nueva zona inversa, pulsar en siguiente como se ve en la figura.



13. Se presenta la ventana de zona inversa donde aparece la dirección IP de la maquina en forma inversa como se ve en la figura.



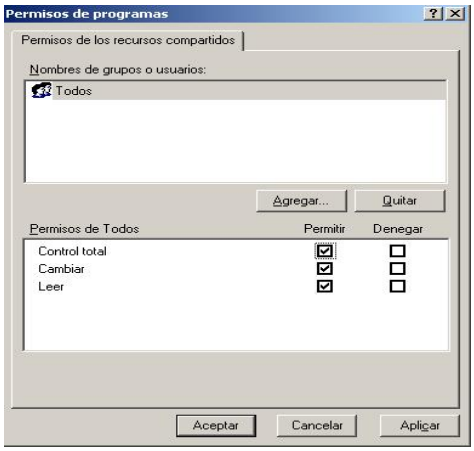
14. Finalmente se visualiza los parámetros de la configuración del servidor DNS y pulsar en el botón Finalizar como se ve en la figura.

Configuración de Recursos Compartidos en Windows 2003 Server

1. Seleccionar la carpeta que se quiere compartir, dar click en el botón derecho del mouse y elegir la opción de compartir y seguridad como se ve en la figura.

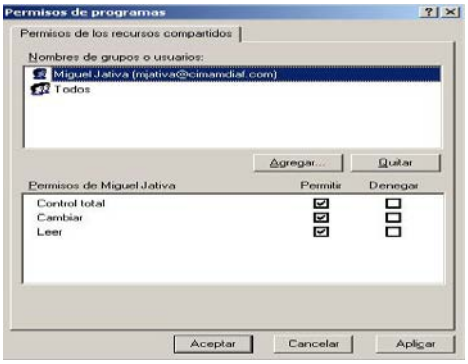
2. Click en la ficha compartir y seleccionar compartir esta carpeta. Pulsar sobre el botón de permisos y en la ventana que nos aparece se pulsa en el botón quitar para eliminar el grupo todos. Dejando nombres de grupos o usuarios vacío como se ve en la figura.

3. A continuación se pulsa en el botón agregar como se ve en la figura.

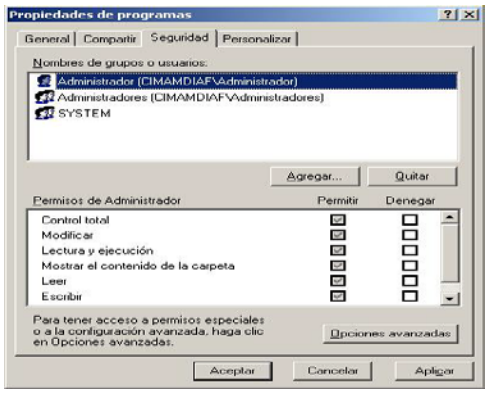


4. Se visualiza la ventana donde contiene los usuarios existentes como se ve en la figura.

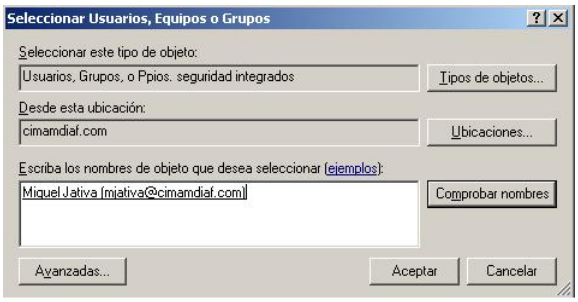
5. En la siguiente ventana aparece el nombre del usuario, se asigna los permisos que el administrador le designe como se ve en la figura.



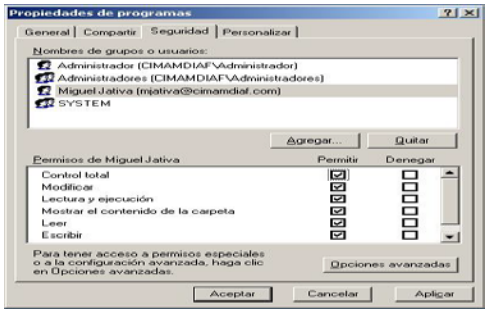
6. A continuación se presenta la ventana del administrador la cual está formada por varias pestañas como se ve en la figura.



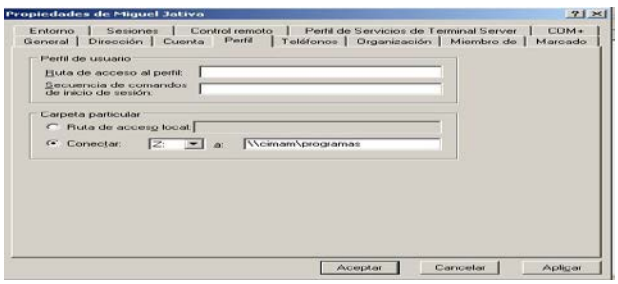
7. En la siguiente ventana se selecciona el Usuario como se ve en la figura.



8. Se visualiza la ventana donde contiene el usuario con sus respectivos permisos como se ve en la figura.



9. Luego nos aparece la ventana propiedades del usuario donde se puede ver que esta compartida en la dirección z: \\cimam\programas como se ve en la figura.



10. Finalmente se visualiza la ventana carpeta compartido como se ve en la figura.

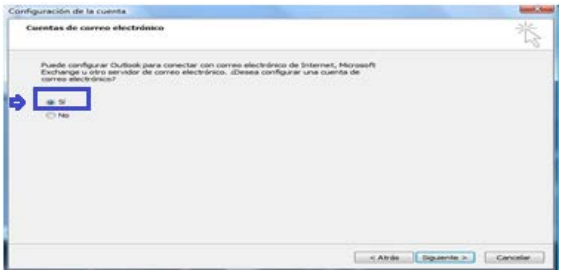
Anexo C:

Configuración del Outlook en Microsoft Office 2007

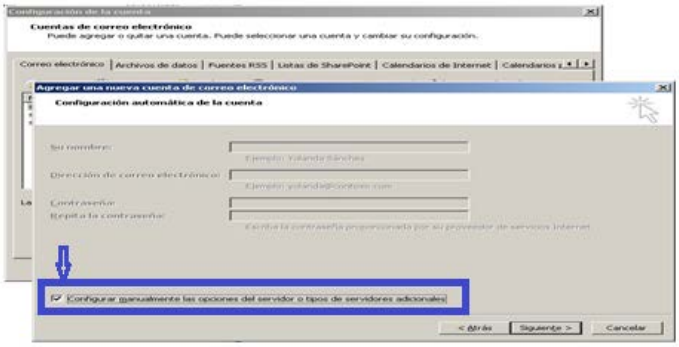
Configuración de Cuenta de Correo en Outlook

1. Una vez creada la cuenta, se ejecuta el programa Microsoft Outlook 2007 y se visualiza la ventana de configuración como se ve en la figura.

2. Se presenta la ventana cuenta de correo electrónico se selecciona la opción si y dar un click en el botón siguiente como se ve en la figura.

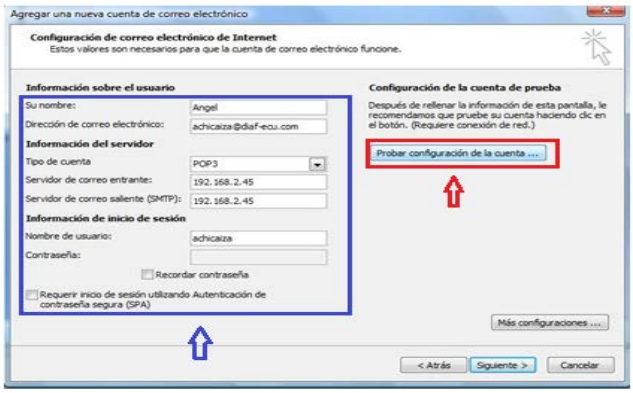


3. Luego se visualiza la venta Configuración y seleccionar la opción Configurar manualmente las opciones del servidor o tipos de servidores adicionales como se ve en la figura.

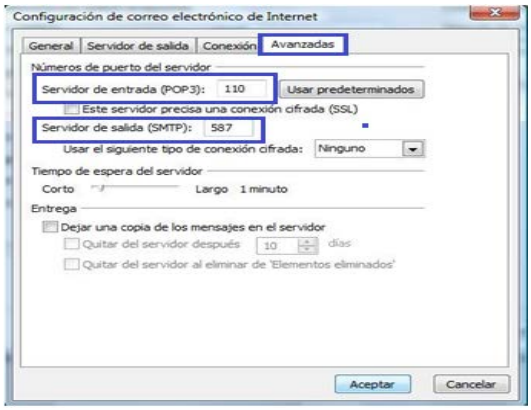


4. Luego se escoge la opción Correo electrónico de Internet como se ve en la figura.

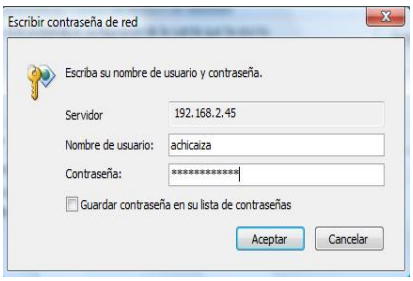
5. Luego se rellena los siguientes campos (recuadro azul) y después se accede a más configuraciones Probar configuración de la cuenta (cuadro rojo) y pulsar en el botón siguiente como se ve en la figura.



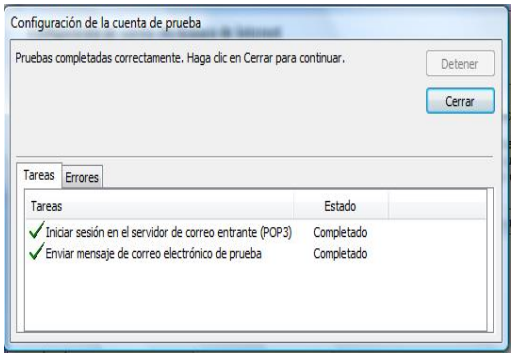
6. Dar un click en la pestaña avanzada e ingresa el número de puerto 110 y 587.A continuación pulsar en el botón aceptar como se ve en la figura.



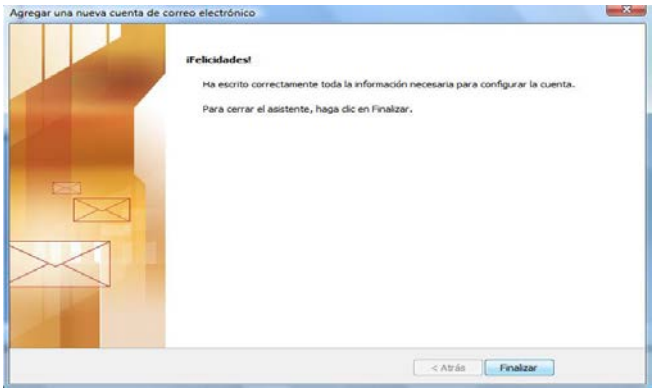
7. Luego nos aparece una venta donde se ingresa la IP del servidor nombre de la cuenta y la contraseña, luego se pulsa el botón aceptar como se ve en la figura.



8. Nos aparece la ventana para confirmar si está configurado correctamente como se ve en la figura.



9. A continuación aparece la venta que fue configurado correctamente la cuenta, se pulsa en el botón finalizar como se ve en la figura.


Agregar una nueva cuenta de correo electrónico
¡Felicidades!
Ha escrito correctamente toda la información necesaria para configurar la cuenta.
Para cerrar el asistente, haga clic en Finalizar.
< Atrás
Finalizar

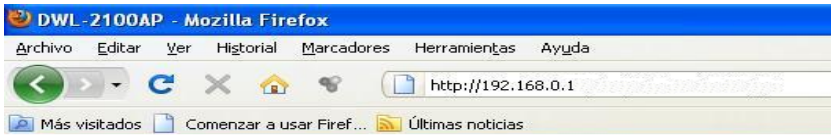
Anexo D:

Configuración del dispositivo Server Printer

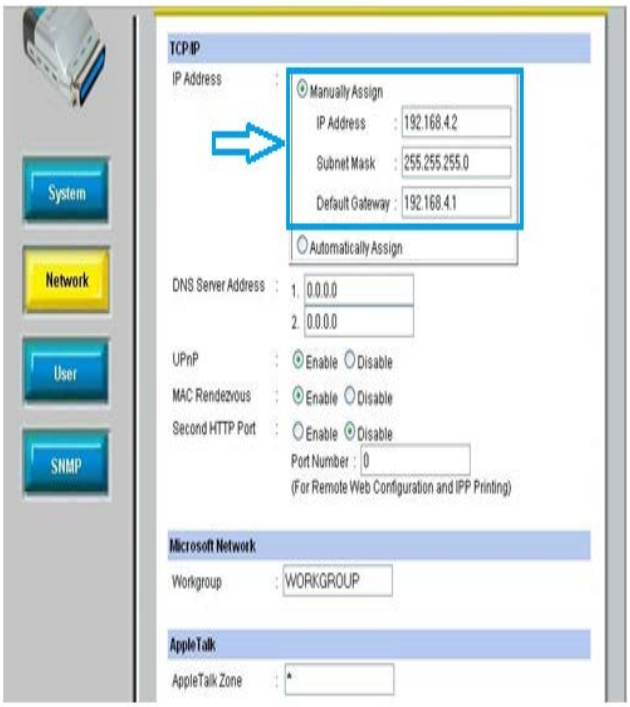
Configuración del Server Printer

Antes de la configuración del Servidor de Impresoras se tiene que cambiar la dirección IP de la red local, por default el dispositivo viene con la siguiente dirección IP: 192.168.0.1, para lo cual se debe configurar la tarjeta de red de un computador con una dirección IP que este en este rango del dispositivo, para poder cambiar la dirección a red local.

1. Conectar el cable de Ethernet al dispositivo DP-310P y el otro extremo a la tarjeta de red del computador previamente configurado.
2. Ejecutar el Internet Explorer o navegador favorito, y en la barra de direcciones digitar la dirección IP 192.168.0.1, que viene por default como se ve en la figura.



3. A continuación, ingresar al menú de configuración, cambiar la dirección IP por una dirección que este dentro del segmento de la red local. El cambio se lo realiza en la opción Network como se ve en la figura.



Ahora la dirección IP del Servidor de Impresoras fue cambiada por la dirección IP 192.168.4.2.

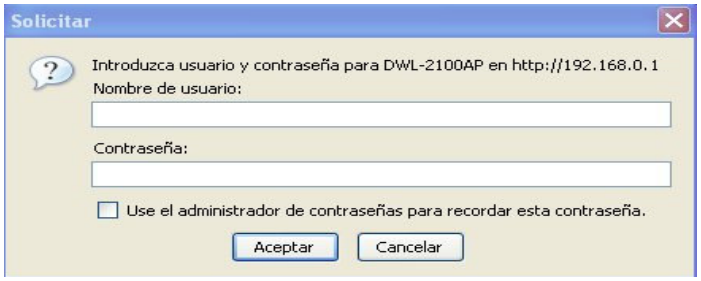
Anexo E:

Configuración del Access Point DWL

Configuración del Access Point

1. Conectar el cable de Ethernet en el Access Point y el otro extremo a la tarjeta de red del computador previamente configurado.
2. Ejecutar el Internet Explorer o navegador favorito, y en la barra de direcciones digitar la dirección IP 192.168.0.1, que viene por default como se ve en la figura.

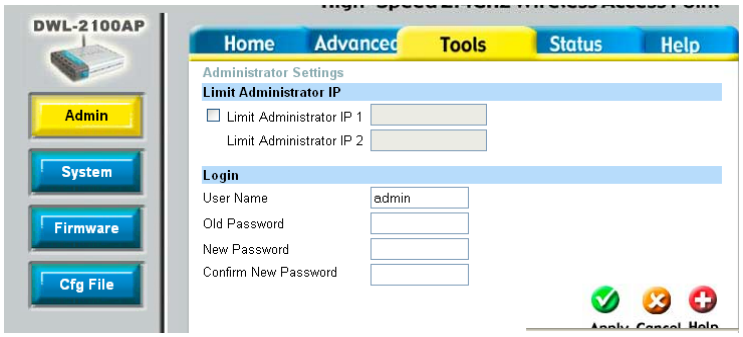
3. Después de digitar la dirección IP en el navegador se deberá ingresar un usuario y una contraseña, en este caso por default el usuario es admin y la contraseña dejar en blanco como se ve en la figura.



4. A continuación, ingresar al menú de configuración, cambiar la dirección IP por una dirección que este dentro del segmento de la red local. El cambio se lo realiza en la opción Home y a continuación LAN como se ve en la figura.

Ahora la dirección IP del Access Point fue cambiada por la 192.168.4.50.

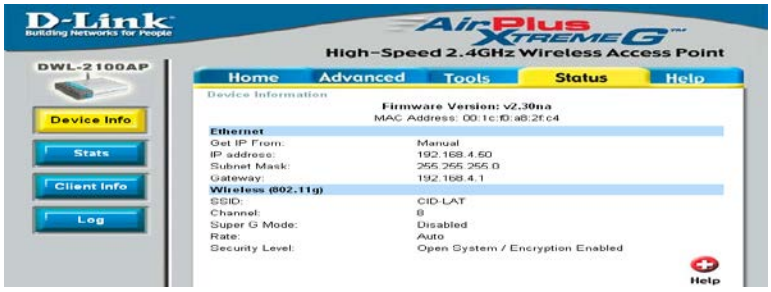
5. Para configurar la clave, ir a la opción Tools y a continuación Admin, se desplegará una pantalla, aquí se puede cambiar el usuario y escribir una contraseña, la cual nos pedirá al ingresar de nuevo para reconfigurar el Access Point como se ve en la figura.



6. Para configurar el nombre de la red inalámbrica, hacer click en Home y a continuación en la opción Wireless, en esta pantalla se escribe un nombre para identificar la red, se selecciona el canal que no esté utilizando otro AP y para finalizar se le asigna un clave que se pedirá para poder acceder a la red como se ve en la figura.

7. Por último, se configura el servicio de DHCP, hacer click en Advanced y a continuación DHCP SERVER, habilitar esta función y asignar un IP desde donde se obtendrá las direcciones, escribir el rango para el número de computadoras que pueden conectarse, también se debe especificar el Gateway y DNS, para el acceso a Internet. Hacer click en Apply para guardar los cambios realizados del Access Point como se ve en la figura.

8. Para poder ver la información de la configuración del Access Point, hacer click en Status y a continuación en Device Info como se ve en la figura.



Anexo F:

Configuración del Firewall NetCyclón

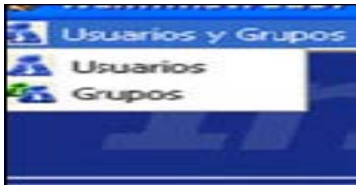
Configuración del Firewall

1. Para ingresar al programa de administración del Firewall, se escribe la dirección IP que fue asignada como se ve en la figura.

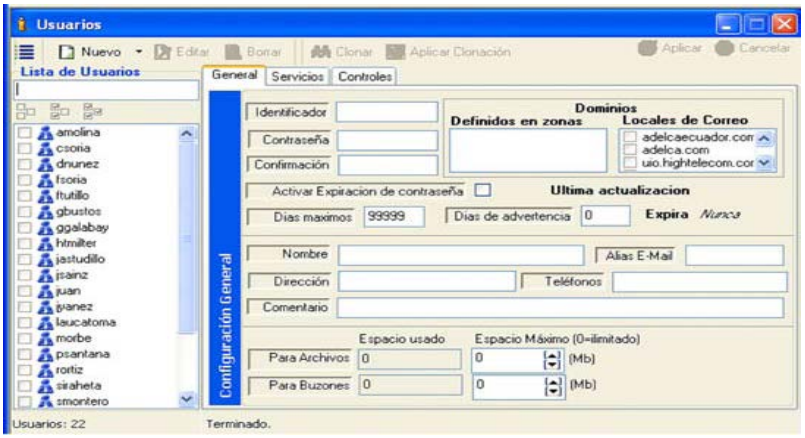
2. El usuario y contraseña por defecto cuando se instala por primera vez el sistema es admin y htserveradmin respectivamente, como se ve en la figura.

3. La interfaz del programa NetCyclón consta de un menú principal de cinco secciones generales como se ve en la figura.

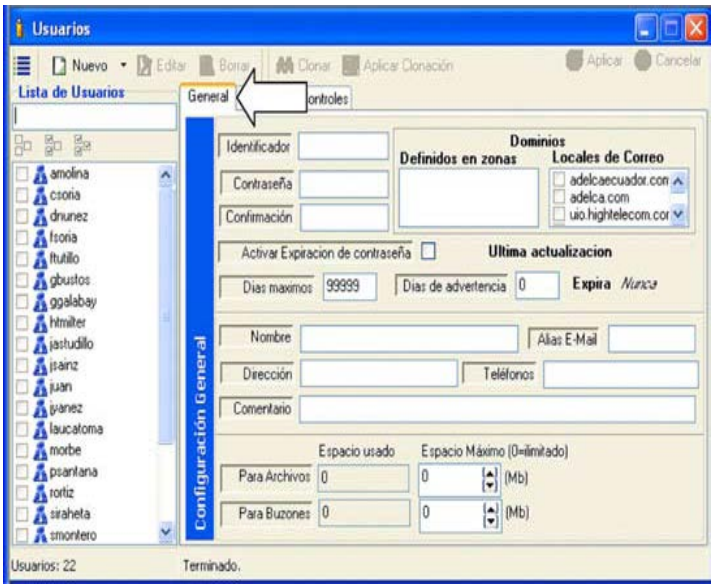
4. Usuarios y Grupos.- contiene la administración completa de usuarios y grupos en dos opciones independientes como se ve en la figura.



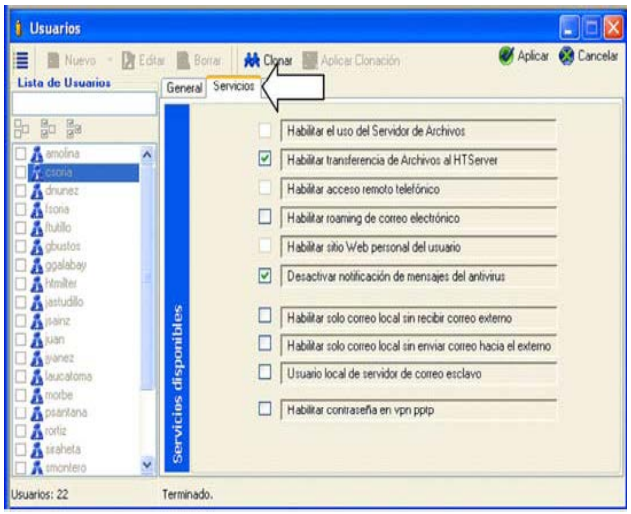
5. Usuarios.- Permite la edición y adición de usuarios. Al acceder al botón de Nuevo, se despliegan dos posibilidades, Usuario y Lista como se ve en la figura.



6. En la pestaña General.- Se ingresarán los datos correspondientes al nuevo usuario como se ve en la figura.



7. La opción Activar Expiración de contraseña.- permite fijar un tiempo durante el cual será válida la contraseña ingresada para el usuario.
8. La sesión de Espacios Máximo.- permite asignar tamaños para los archivos privados de su directorio y para el buzón de mensajería.
9. En la pestaña Servicios.- se indica el perfil que va a tener el usuario en el servidor como se ve en la figura.



A continuación los servicios que puede tener los perfiles de usuario como se muestra en la siguiente tabla:

Servicio	**Descripción**
Habilitar el uso del servidor de archivos	Permite al usuario utilizar el servidor como un servidor de archivos
Habilitar transferencia de archivos al NetCyclón	Permite al usuario utilizar al servidor como un servidor de FTP (File Transfer Protocol)
Habilitar acceso telefónico remoto	Permite al usuario utilizar el servicio de RAS (Remote Access Service)
Habilitar roaming de correo electrónico	Permite al cliente de correo del usuario conectarse al servidor externamente
Habilitar sitio Web personal del usuario	Habilita al usuario a depositar su sitio Web
Desactivar notificación de mensajes del antivirus	El usuario no recibirá mensajes del antivirus

Habilitar solo correo local sin recibir correo externo	El usuario puede enviar correo local y hacia el exterior pero no recibir desde el exterior
Habilitar solo correo local sin enviar correo hacia el exterior	El usuario puede enviar correo local y no hacia el exterior pero si puede recibir desde el exterior
Usuario local de servidor de correo esclavo	El servidor de correo utiliza otro servidor externo, el cual maneja el dominio de Internet donde el usuario es parte de este dominio
Habilitar contraseña en VPNspptp	Se habilita la contraseña del usuario para que éste pueda utilizar la VPN

10. Pestaña de Controles.- Elemento que se encuentra en las interfaces gráficas, que permite cambiar entre distintos documentos o secciones de forma rápida. La sección de Controles está dividida en 4 subsecciones:
    - Navegación
    - Servidor de Archivos
    - Grupos
    - Correo Electrónico

    Navegación.- Establece o deniega permisos por días y en horas hacia sitios específicos para la navegación del usuario, se pueden escoger entre cuatro esquemas: Total, Estricto, Permitir y Denegar.

    • Total.- No realiza ningún tipo de control en la navegación de un usuario en particular.

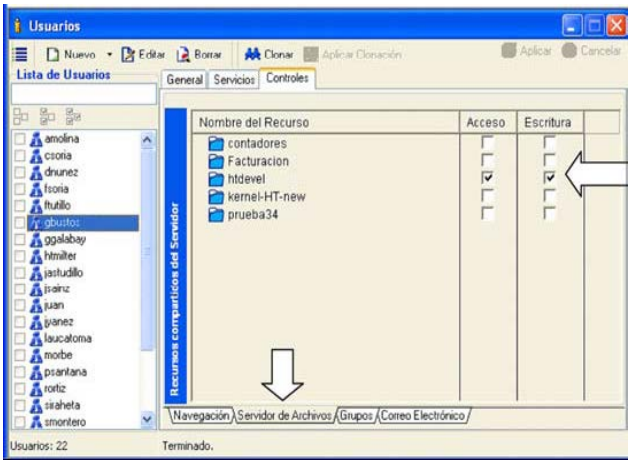
    • Estricto.- Se autoriza solamente la navegación a los sitios que se han introducido en la lista durante el horario configurado, fuera de este lapso se niega toda navegación.

• Permitir.- Se autoriza la navegación a los sitios que se han introducido en la lista durante el horario configurado, fuera de este lapso se permite toda la navegación.

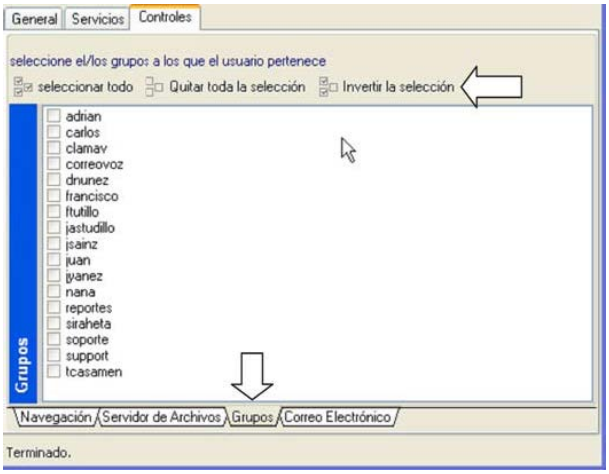
Bien, es importante hacer notar la diferencia entre estas dos opciones Estricto y Permitir, e indicar que es necesario para que entren en operación que se configure un horario, es decir que el periodo de tiempo no puede estar Desde 00:00 hasta 23:00 todos los días.

• Denegar.- Se deniega el acceso a los sitios de la lista, como se ve en la figura.

Servidor de Archivos.- Permite establecer permisos de lectura y/o escritura para los directorios privados que se hayan creado en el módulo servidor de archivos como se ve en la figura.



Grupos.- Establece a que grupos pertenece el usuario como se ve en la figura.

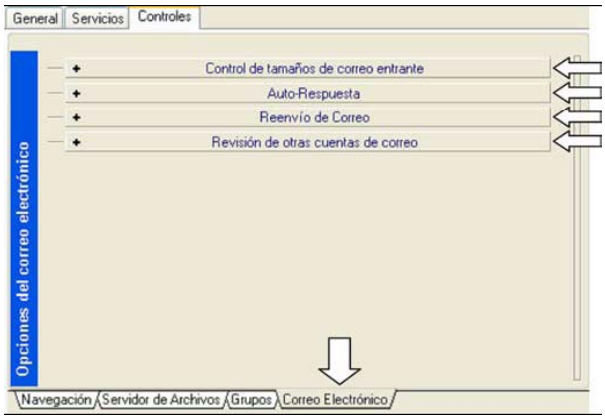


Nota: en esta ventana solo se puede realizar operaciones de selección y eliminación de los grupos existentes por usuario.

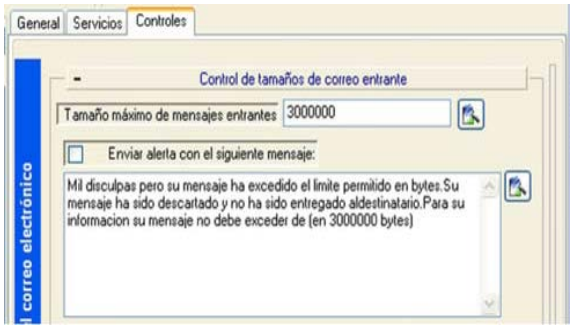
Correo Electrónico.- Posee 4 subsecciones:

- Control de tamaños de correo entrante
- Auto-Respuesta
- Reenvío de Correo
- Revisión de otras cuentas de correo

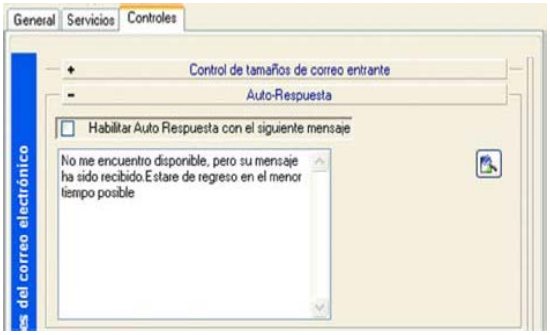
Se puede ver en la figura.



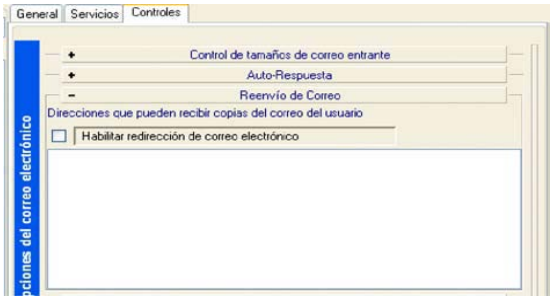
Control de tamaño de correo entrante.- Establece el tamaño máximo permitido para el mensaje entrante y define una alerta a enviar al remitente cuando el mensaje excede la longitud especificada, este mensaje puede ser personalizado según las necesidades del usuario como se ve en la figura.



Auto-Respuesta.- Permite activar el contestador automático de mensajes cuando el usuario se ausenta, o no puede responder su correo por un tiempo prolongado. También el mensaje puede personalizarse como se ve en la figura.



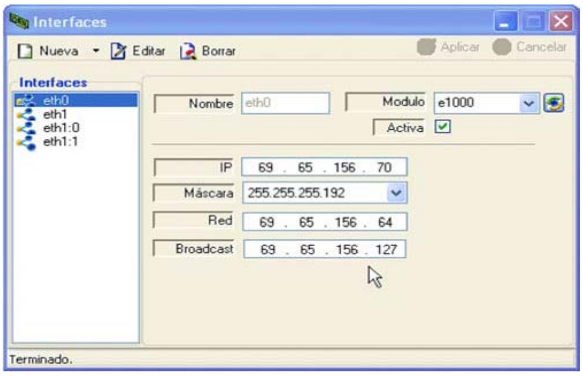
Reenvío de Correo.- Permite establecer una lista de direcciones electrónicas a las cuales se enviará una copia de los mensajes recibidos como se ve en la figura.



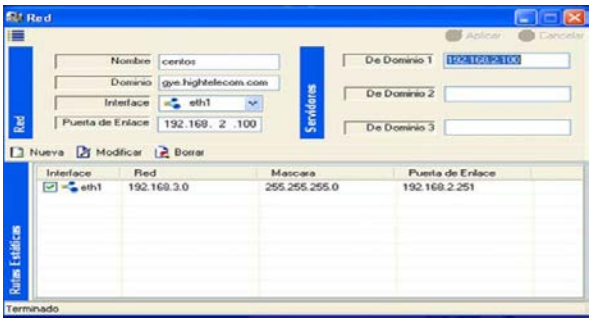
Configuraciones

Dentro de esta opción se configura las direcciones IP.

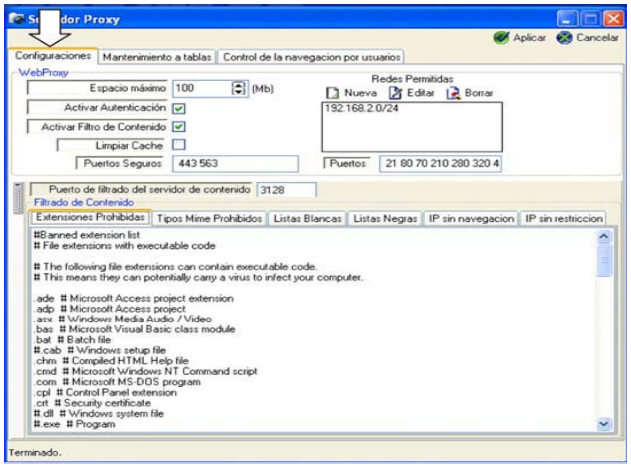
Interfaces.- Define las interfaces de conexión internas y externas como se ve en la figura



Red.- En éste módulo se pueden especificar: el nombre, el dominio, la puerta de enlace, los servidores que realizarán la resolución de nombres y las rutas estáticas, como se ve en la figura.



Servidor Proxy.- Se define como una computadora, o dispositivo que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas, hacia otros servicios de red, como se ve en la figura.



Web Proxy.- Es un intermediario entre el usuario y una determinada web de destino, y permite al que lo utiliza acceder a determinados sitios web no desde su propia dirección de IP sino que a través de la dirección de IP y datos de conexión del Proxy, por motivos de seguridad, anonimato, rendimiento.

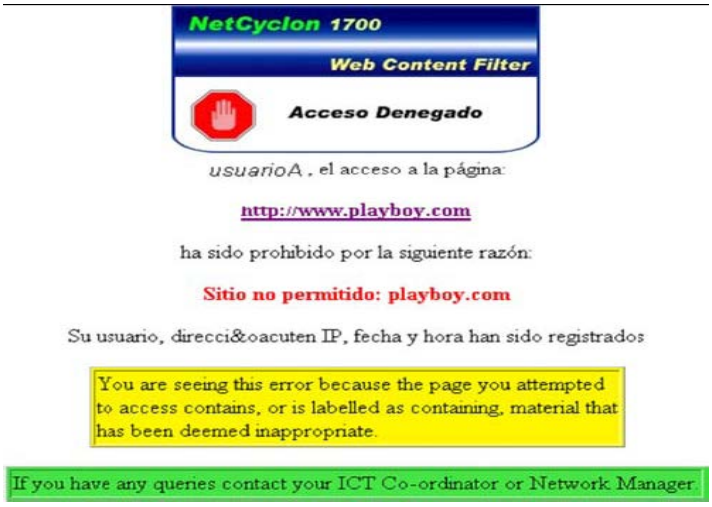
Está formado por:

- **Espacio Máximo.-** 

Se utiliza para establecer que tamaño se desea que tenga el caché en el disco duro.
- **Activar Autenticación.-** 

Es muy útil para poder acceder hacia Internet, pues esto permite controlar quienes sí y quienes no accederán a Internet, sin importar desde que máquina de la red local lo hagan.
- **Activar Filtro de Contenido.-** 

Permite restringir páginas no deseadas.



- **Limpiar Cache.-** 

Al chequear la opción de Limpiar el cache y dar aplicar, se borra todo el cache del servidor y se reinicia el Proxy.
- **Redes Permitidas**

En este apartado se deben establecer todas las redes que se van a apoyar en el servidor proxy, si una red no se halla enlistada simplemente no se va permitir la navegación.

- **Puertos**

Es una interfaz para comunicarse con un programa a través de una red.

Estos son los puertos a los que se hace la translación desde el puerto definido para el filtrado, se enumeran bajo dos criterios, los seguros que son aquellos usados para aplicaciones tipo https; los demás son los comúnmente usados.

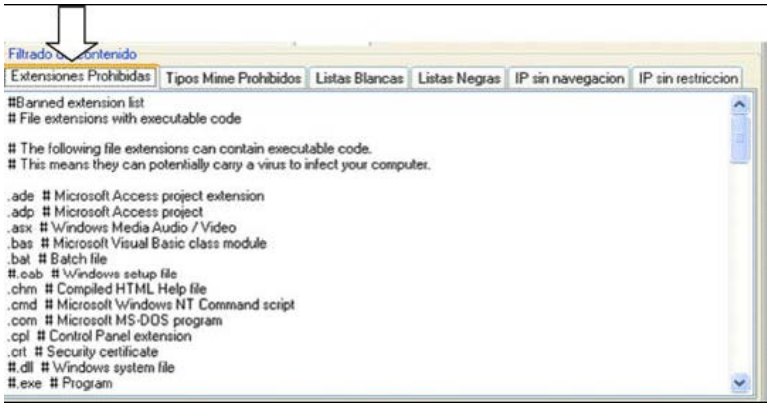
- **Puerto de filtrado del servidor de contenidos**

De acuerdo a las asignaciones hechas por IANA los Puertos Registrados (rango desde 1024 hasta 49151) recomendados para Servidores Intermediarios (Proxies) pueden ser el 3128 y 8080 a través de TCP.

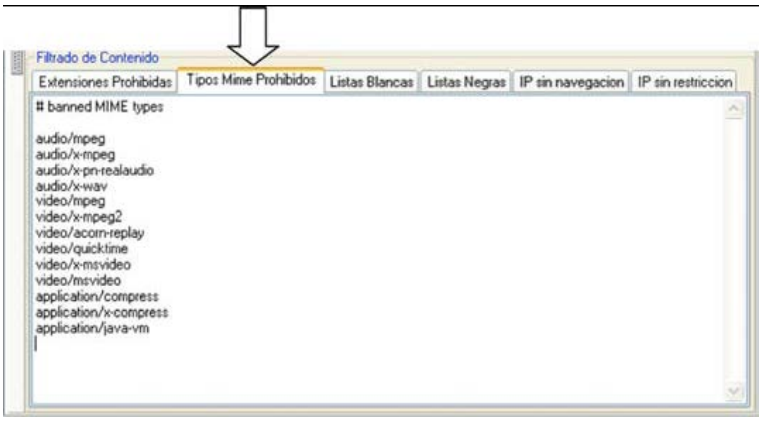
De modo predefinido Squid utilizará el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto disponible.

Filtrado de Contenido.- Esta opción incluye las siguientes secciones: Extensiones Prohibidas, Tipos MIME Prohibidos, Listas Negras, Listas Blancas, IP sin navegación e IP sin restricción.

Extensiones Prohibidas.- Se listan todas las extensiones que no son permitidas para descargarse cuando se está navegando. Se pueden añadir fácilmente cualquier extensión, y en el caso de que se liste una y se quiere permitir luego basta con colocar un signo # para que se inhabilite esa línea y se permita la descarga de archivos con esa extensión, como se ve en la figura.



Tipos Mime Prohibidos.- Especifican los tipos de datos, como por ejemplo texto, imagen, audio, etc. Los tipos MIME prohibidos son aquellos contenidos especiales de las páginas que no son permitidos en la navegación como se ve en la figura.



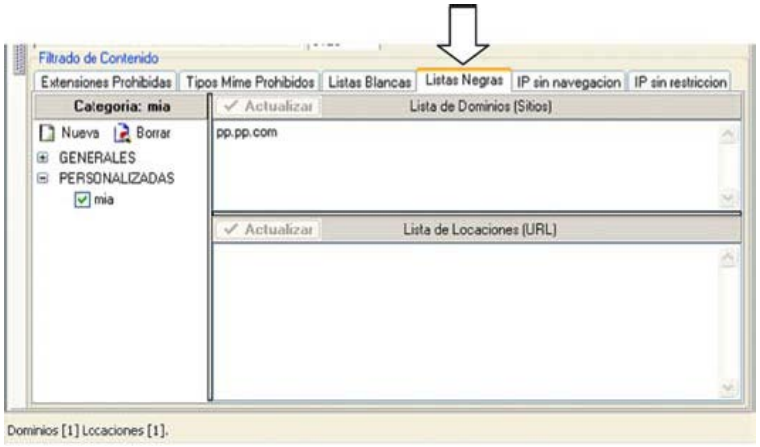
Listas Negras y Listas Blancas

El filtro de Internet se basa en una “lista negra”, lo que significa que el acceso a todos los sitios está permitido.

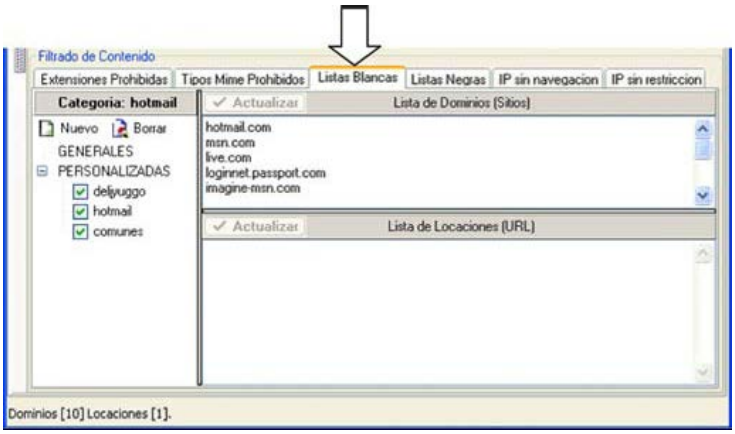
Una “lista blanca” trabaja de manera opuesta, el acceso a todos los sitios está bloqueado.

Las listas negras se dividen en dos categorías: las Generales y las Personalizadas.

- **Generales.-** Son listas cuyo contenido no es modificable, ya que las mismas se actualizan automáticamente de los sitios oficiales, éstas solo se activan o se desactivan manejando su Check correspondiente.
- **Personalizadas.-** Son aquellas listas que crea el usuario donde se especifican dominios o URL’s que estarán prohibidos, ejemplo de url: pp.pp.com.



En las listas blancas se tienen los dominios o URL que tienen permitido su acceso, y se manejan de manera similar a las listas negras: Generales y Personalizadas.

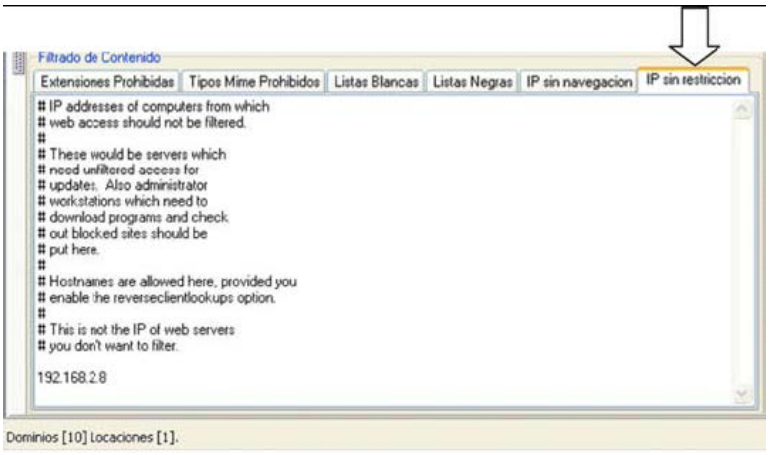


Cuando se coloque un sitio tanto en listas blancas como en negras, debe notarse que basta con escribir el dominio.

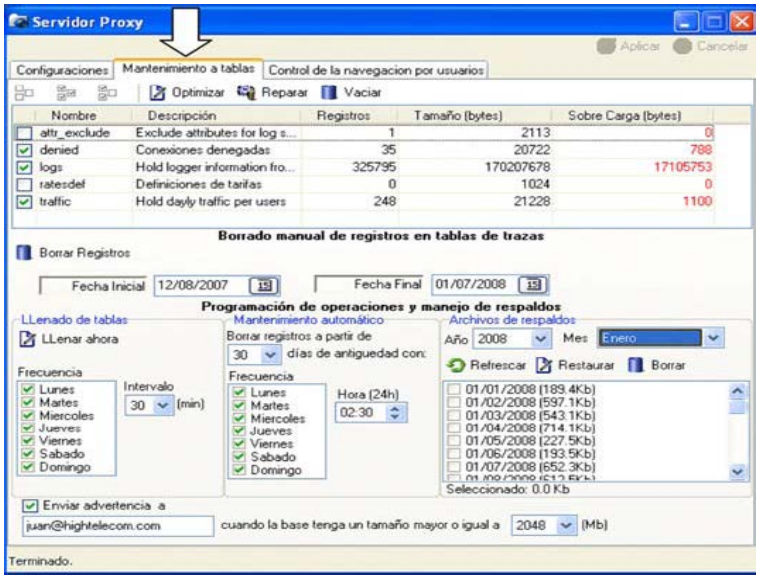
Ejemplo: si se quiere colocar en un lista blanca al sitio web del SRI, primero se crea una Nueva Categoría (o se añade a una existente), luego en la lista de dominios se escoge Nuevo y se escribe: sri.gov.ec, no se debe escribir http: //www.sri.gov.ec, si se desea especificar de esta manera se lo hace en Lista de Locaciones (URL), pero en ese caso restringe la localidad de esa página y no todo el contenido del dominio.

IP Sin Navegación.- Las computadoras locales sin navegación, son las que no tienen ningún permiso de salida, no navegan a ningún sitio.

IP Sin Restricción.- Las computadoras locales sin restricción, son aquellas que no se le aplican ninguna regla de prohibición en la navegación.



Mantenimiento de Tablas

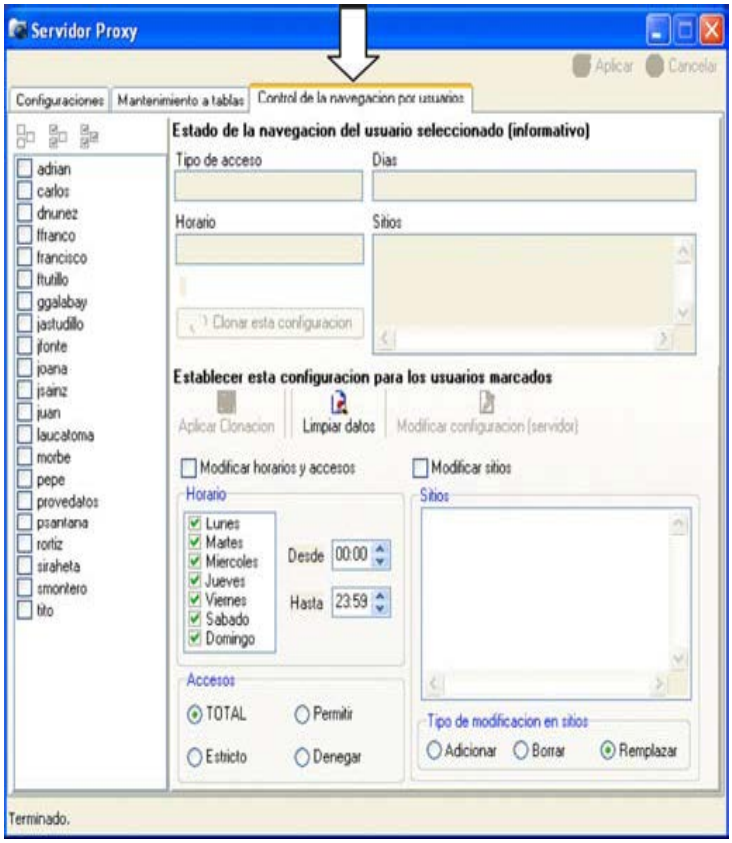


Con la opción de mantenimiento de tablas se mejora el uso y desempeño de los archivos de registro que servirán para generar los reportes de navegación. En el caso de proxy se manejan 5 log files, encargados de almacenar información referida a:

- attr_exclude: Atributos excluidos
- denied: Conexiones denegadas
- logs: Trazas de conexión

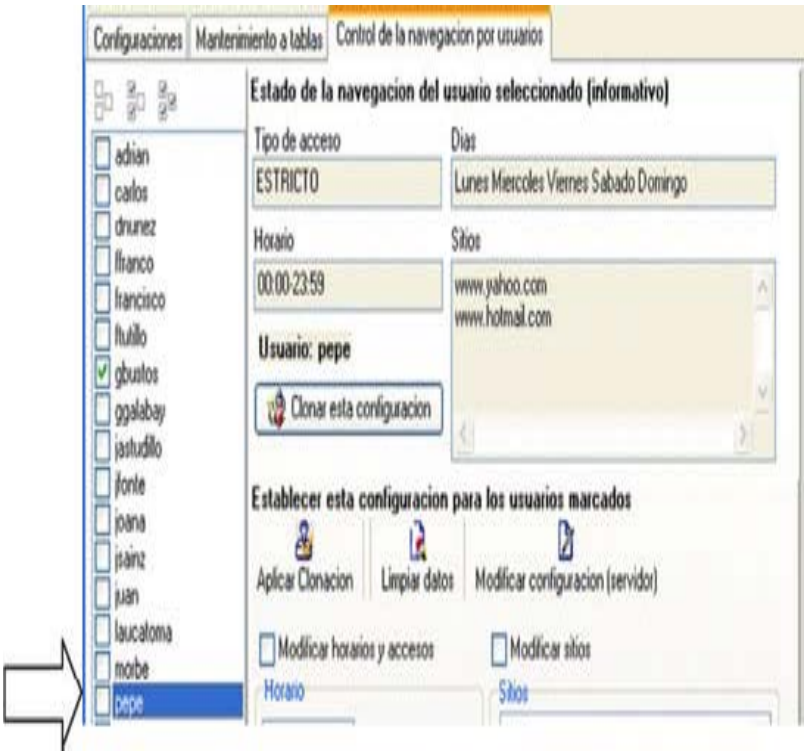
- ratesdef: Definiciones de tarifas
- traffic: Resumen de tráfico por usuarios

Control de navegación por usuarios



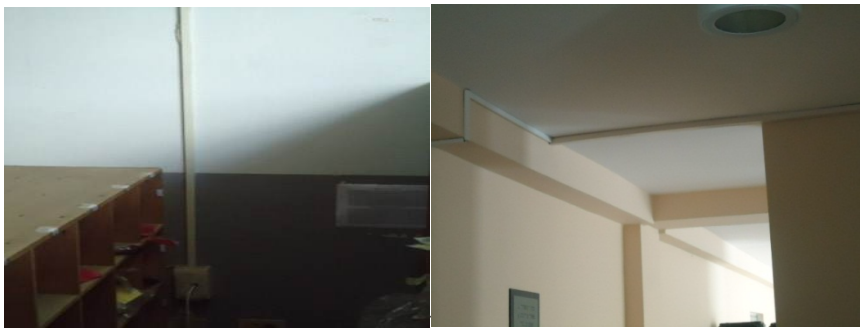
El control de navegación por usuarios permite definir el esquema de navegación y establecer o denegar permisos por días, horas y sitios específicos para la navegación del usuario.

Al seleccionar un usuario con un click sobre éste, en Estado de la navegación del usuario seleccionado (informativo) se presentan los datos del perfil de navegación definido para el usuario (tipo de acceso, días, horario y sitios).

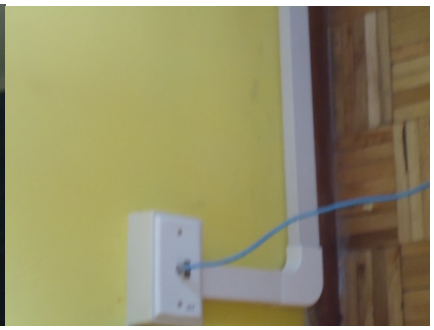

Configuraciones
Mantenimiento a tablas
Control de la navegacion por usuarios
Estado de la navegacion del usuario seleccionado (informativo)
adrian
carlos
dnunez
ftranco
francisco
ftuillo
gbuatos
ggalabay
jastudillo
jfonte
joana
jsainz
juan
laucatoma
maibe
pepe
Tipo de acceso
ESTRICTO
Dias
Lunes Miercoles Viernes Sabado Domingo
Horario
00:00-23:59
Sitios
www.yahoo.com
www.hotmail.com
Usuario: pepe
Clonar esta configuracion
Establecer esta configuracion para los usuarios marcados
Aplicar Clonacion
Limpiar datos
Modificar configuracion (servidor)
Modificar horarios y accesos
Modificar sitios
Horario
Sitios

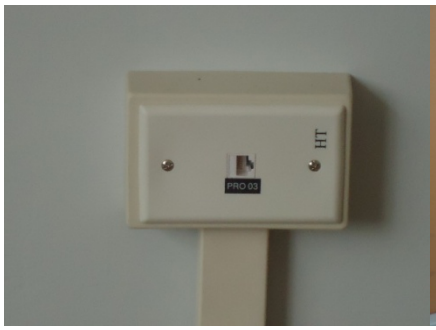
Anexo G:

Imágenes del Cableado Estructurado




110 V




HT
PRO 03


HT
PRO 03

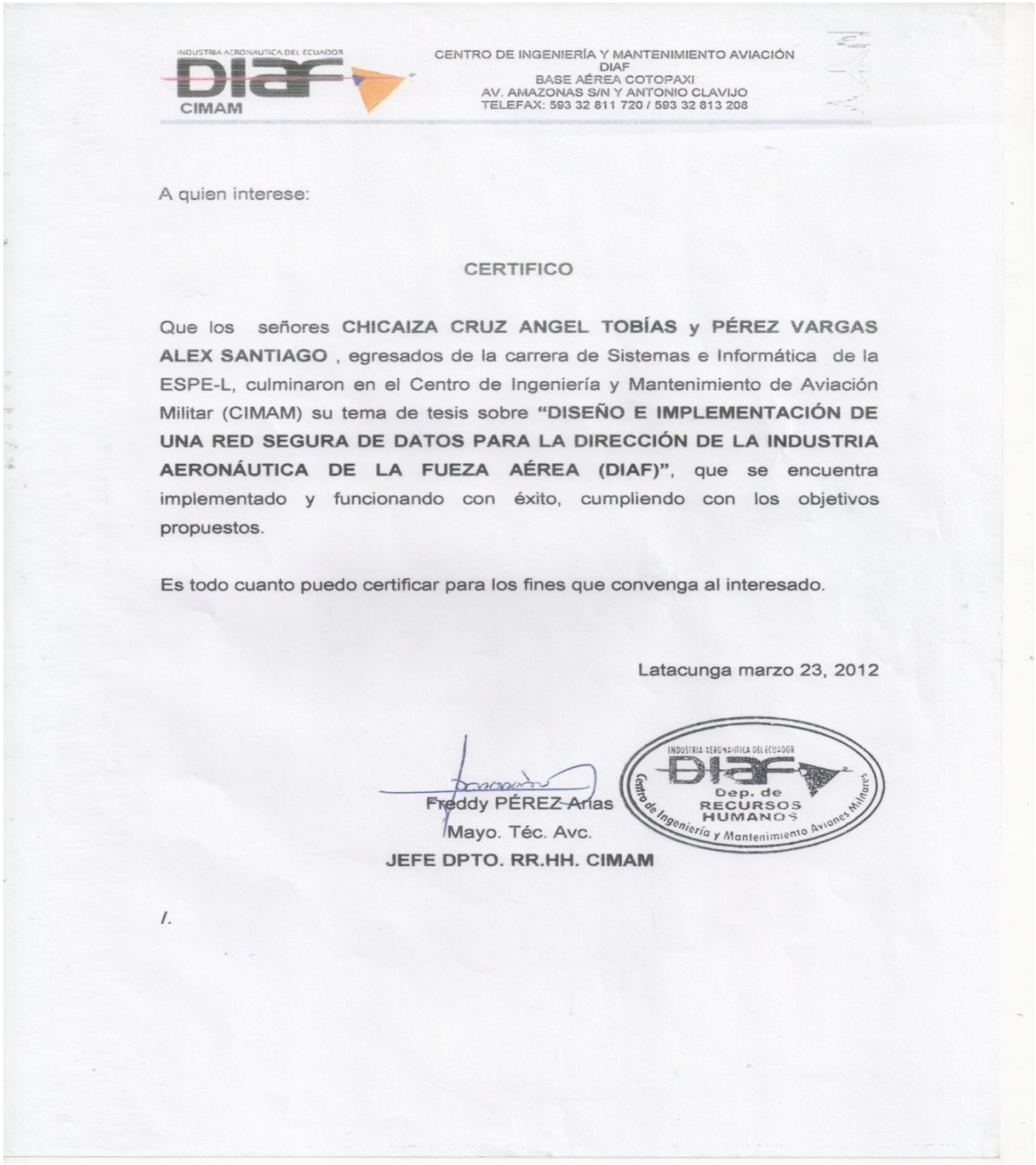
Anexo: H

Imágenes del Hangar CIMAM


FAE812

Anexo: I

Certificado de Finalización y Aceptación del Proyecto



INDUSTRIA AERONAUTICA DEL ECUADOR
DIAF
CIMAM

CENTRO DE INGENIERÍA Y MANTENIMIENTO AVIACIÓN
DIAF
BASE AÉREA COTOPAXI
AV. AMAZONAS S/N Y ANTONIO CLAVIJO
TELEFAX: 593 32 811 720 / 593 32 813 208

A quien interese:

CERTIFICO

Que los señores **CHICAIZA CRUZ ANGEL TOBÍAS y PÉREZ VARGAS ALEX SANTIAGO** , egresados de la carrera de Sistemas e Informática de la ESPE-L, culminaron en el Centro de Ingeniería y Mantenimiento de Aviación Militar (CIMAM) su tema de tesis sobre **"DISEÑO E IMPLEMENTACIÓN DE UNA RED SEGURA DE DATOS PARA LA DIRECCIÓN DE LA INDUSTRIA AERONÁUTICA DE LA FUEZA AÉREA (DIAF)"**, que se encuentra implementado y funcionando con éxito, cumpliendo con los objetivos propuestos.

Es todo cuanto puedo certificar para los fines que convenga al interesado.

Latacunga marzo 23, 2012

INDUSTRIA AERONAUTICA DEL ECUADOR
DIAF
Dep. de
RECURSOS
HUMANOS
Centro de Ingeniería y Mantenimiento Aviones Militares

Freddy PÉREZ Arias
Mayo. Téc. Avc.
JEFE DPTO. RR.HH. CIMAM

/.

Latacunga, Agosto del 2012

_____

Ángel Tobías Chicaiza Cruz

CI. 1803303609

_____

Alex Santiago Pérez Vargas

CI. 1803880416

_____

Ing. Santiago Jácome

COORDINADOR DE LA CARRERA DE SISTEMAS E INFORMATICA

_____

Dr. Rodrigo Vaca

SECRETARIO ACADEMICO