

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

TÓPICO DE GRADUACIÓN

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE
ANÁLISIS DE SOPORTE DE MICROCOMPUTADORES**

TEMA

**ADMINISTRACIÓN Y SEGURIDADES DE REDES
TIENDAS INDUSTRIALES ASOCIADAS**

MANUAL DE USUARIO

AUTORES

**MARIUXI GEOVANNA RAMÍREZ AYALA
VICTOR EDUARDO TOLA FRANCO
JONATHAN ENRIQUE BAQUERO LÓPEZ**

DIRECTOR

ANL. FABIÁN BARBOZA

AÑO

2007



AGRADECIMIENTO

Al haber alcanzado una de mis metas, quiero agradecer primeramente a Dios, que con su infinita misericordia ha permitido darme aliento para seguir y alcanzar una de mis metas.

A mis padres, Carmen López Rosado y Galo Baquero Freire, a mi hermana Deybbie Baquero López, por las oraciones que siempre han elevado al Dios maravilloso.

Quiero agradecer al Director Analista Fabián Barboza quien supo guiarme en el transcurso de la elaboración de este manual, brindándome no solo su tiempo, sino también sus conocimientos.

A mis dos grandes amigos Moisés Rodríguez y Bladimir Benítez que de una u otra manera me han respaldado a lo largo de mi vida.

Y a todas aquellas personas que de una u otra forma, colaboraron o participaron en la realización de este proyecto, hago extensivo mi más sincero agradecimiento.

JONATHAN ENRIQUE BAQUERO LÓPEZ



AGRADECIMIENTO

Quiero expresar mi gratitud a mis padres, hermanos, amigos y profesores por ayudarme en el transcurso de mi carrera pero sobre todo a Dios que me ha bendecido para poder alcanzar este propósito.



UNIVERSIDAD DEL LITORAL

BIBLIOTECA

CAMPUS

PEÑAS

MARIUXI GEOVANNA RAMÍREZ AYALA

AGRADECIMIENTO

Quiero agradecer por haber culminado mi carrera, principalmente a Dios por haberme dado salud cada día, a mis padres, por el apoyo incondicional, a mis hermanos quienes siempre han estado conmigo y a mis amigos que de alguna forma ayudaron para que esto sucediera.



VICTOR EDUARDO TOLA FRANCO

DEDICATORIA

Deseo dedicar este trabajo a mis amados padres Sr. Galo Cesar Baquero Freire y Sra. Carmen Cecilia López Rosado quienes me han sabido guiar y cultivar un gran amor hacia Dios y por el mejor camino que sólo unos padres como ellos pueden hacer y no solamente me han brindado su apoyo económico, sino también inculcándome buenos principios y normas para perseverar y alcanzar mis metas.

Dedico también este éxito a mi hermana Deybbie Baquero López, porque ha sido un gran ejemplo en toda mi vida, a tí que haz sabido darme consejos en momentos de angustia y aflicción.



JONATHAN ENRIQUE BAQUERO LÓPEZ
ESPOL
CAMPUS
PENAS

DEDICATORIA

Dedico esta tesis a Dios, quien me ha bendecido con salud y fortaleza en cada uno de mis pasos especialmente en el proceso de esta ilusión que muchas veces me pareció lejana e inalcanzable.

A mis padres y hermanos que me han dado su apoyo incondicional, sobre todo en los momentos más difíciles de mi vida; en especial mi mamá a la que siento más dueña de este mérito que mío por estar siempre conmigo en los momentos de quebranto y por ser siempre mi refugio.

A mis compañeros que en algún momento descuidaron sus obligaciones por ayudarme en mis proyectos, me aconsejaron y fueron verdaderos amigos.

Y finalmente a mi pequeña que es la luz de mi vida y el final propósito de todas mis metas, mi Chapi.



MARIUXI GEOVANNA RAMÍREZ AYALA

BIBLIOTECA
CAMPUS
PEÑAS

DEDICATORIA

Este manual se lo dedico a mis padres, por el apoyo brindado a lo largo de mis años de estudio, pues ustedes han sido las personas que siempre me han ayudado, con sus consejos y su amor desde la primera vez que ingresé a la universidad.

Gracias papá, gracias mamá, por la confianza que me dieron; he cumplido el deseo que siempre tuvieron ser un politécnico, los quiero mucho.



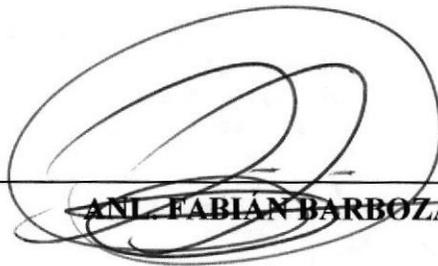
VICTOR EDUARDO TOLA FRANCO

DECLARACIÓN EXPRESA

La responsabilidad por los hechos, ideas y doctrinas expuestas en este Tópico de Graduación nos corresponden exclusivamente. Y el patrimonio intelectual de la misma a EDCOM (**Escuela de Diseño y Comunicación Visual**) de la Escuela Superior Politécnica del Litoral.

(Reglamento de Exámenes y Títulos profesionales de la ESPOL).

FIRMA DEL DIRECTOR DEL TÓPICO DE GRADUACIÓN



FABIAN BARBOZA



FIRMA DE LOS AUTORES DEL TÓPICO DE GRADUACIÓN

Jonathan Enrique Baquero López

JONATHAN ENRIQUE BAQUERO LÓPEZ

Mariuxi Geovanna Ramirez Ayala

MARIUXI GEOVANNA RAMIREZ AYALA

Victor Eduardo Tola Franco

VICTOR EDUARDO TOLA FRANCO



TABLA DE CONTENIDO

CAPÍTULO 1

1 GENERALIDADES.....	1
1.1 INTRODUCCIÓN.....	1
1.2 OBJETIVO DEL MANUAL.....	1
1.3 ¿A QUIEN VA DIRIGIDO ESTE MANUAL?.....	1
1.4 LO QUE SE DEBE CONOCER.....	1
1.5 ORGANIZACIÓN DEL CONTENIDO DEL MANUAL.....	1

CAPÍTULO 2

2 SITUACIÓN ACTUAL.....	1
2.1 ANTECEDENTES DE LA EMPRESA.....	1
2.1.1 MISIÓN.....	1
2.1.2 VISIÓN.....	1
2.2 INFRAESTRUCTURA LAN.....	2
2.2.1 SERVIDORES.....	3
2.2.1.1 MATRIZ GUAYAQUIL.....	3
2.2.1.2 MATRIZ QUITO.....	4
2.2.2 ESTACIONES DE TRABAJO.....	5
2.2.2.1 MATRIZ - GUAYAQUIL.....	5
2.2.2.2 MATRIZ - QUITO.....	14
2.2.3 MEDIOS DE COMUNICACIÓN.....	18
2.2.3.1 MEDIOS ALAMBRICOS - MATRIZ GUAYAQUIL.....	18
2.2.3.2 MEDIOS INALÁMBRICOS - MATRIZ GUAYAQUIL.....	18
2.2.4 DISPOSITIVOS DE CONMUTACIÓN.....	19
2.2.5 CENTRO DE DISTRIBUCION PRINCIPAL MC e IC.....	20
2.2.6 INFRAESTRUCTURA WAN.....	27
2.2.7 ANCHO DE BANDA.....	31
2.2.8 PROBLEMAS ENCONTRADOS.....	32

CAPÍTULO 3

3 SOLUCIÓN PROPUESTA.....	1
3.1 PROBLEMAS, CAUSA Y EFECTO.....	1
3.2 PROBLEMAS, SOLUCIÓN Y ALCANCE.....	2
3.3 ESTUDIO DE FACTIBILIDAD - MATRIZ GUAYAQUIL.....	3
3.3.1 ALTERNATIVA "A".....	3
3.3.1.1 FACTIBILIDAD TÉCNICA.....	4
3.3.1.2 FACTIBILIDAD ECONÓMICA.....	5
3.3.1.3 FACTIBILIDAD OPERATIVA.....	8
3.3.1.4 COSTO TOTAL DE LA ALTERNATIVA "A".....	10
3.3.1.5 VENTAJAS.....	11
3.3.1.6 BENEFICIOS.....	11
3.3.1.7 GARANTIA TÉCNICA DEL CABLEADO DE DATOS.....	12
3.3.1.8 CONDICIONES COMERCIALES ALTERNATIVA "A".....	12
3.3.2 ALTERNATIVA "B".....	13
3.3.2.1 FACTIBILIDAD TÉCNICA.....	14
3.3.2.2 FACTIBILIDAD ECONÓMICA.....	15
3.3.2.3 FACTIBILIDAD OPERATIVA.....	18
3.3.2.4 COSTO TOTAL DE LA ALTERNATIVA "B".....	20
3.3.2.5 VENTAJAS.....	21
3.3.2.6 BENEFICIOS.....	21
3.3.2.7 GARANTIA TÉCNICA DEL CABLEADO DE DATOS.....	22
3.3.2.8 CONDICIONES COMERCIALES ALTERNATIVA "B".....	22

3.3.3 OBSERVACIONES	23
3.3.4 PLAN DE TRABAJO.....	24
3.3.5 DIAGRAMA DE GANT	24

CAPÍTULO 4

4 REGLAS DE CABLEADO ESTRUCTURADO	1
4.1 NORMATIVAS.....	1
4.2 RECOMENDACIONES.....	16

CAPÍTULO 5

5 ANÁLISIS DE CABLEADO ESTRUCTURADO	2
5.1 CABLEADO ESTRUCTURADO DE GUAYAQUIL - SEGUNDO PISO.....	3
5.2 CABLEADO ESTRUCTURADO DE GUAYAQUIL - TERCER PISO.....	8

CAPÍTULO 6

6 ROUTER	1
6.1 FUNCIONES DEL ROUTER	1
6.2 TECNOLOGÍAS SOPORTADAS.	1
6.3 COMPONENTES INTERNOS DEL ROUTER.....	2
6.4 COMPONENTES EXTERNOS DE UN ROUTER	4
6.5 CONEXIÓN AL PUERTO DE CONSOLA.....	5
6.5.1 REQUERIMIENTOS.	5
6.6 CONEXIÓN POR HARDWARE.....	5
6.7 CONEXIÓN POR (HYPER TERMINAL) A LA CONSOLA DE ROUTER.	7
6.8 CONEXIÓN ROUTER A ROUTER.....	16
6.8.1 REQUERIMIENTOS.	16
6.9 CONEXIÓN DE CABLES.....	16
6.10 MODOS DE INTERFAZ DE USUARIO.	18
6.10.1 ASIGNAR NOMBRE AL ROUTER.	18
6.10.2 ASIGNAR CONTRASEÑAS AL ROUTER.	19
6.10.3 COMANDO DE AYUDA MEDIANTE TECLADO.....	21
6.10.4 DEFINICIÓN DE COMANDOS SHOW.....	21
6.10.5 CONFIGURACIÓN DE UNA INTERFAZ SERIAL.	22
6.10.6 CONFIGURACIÓN DE UNA FASTETHERNET.	25
6.10.7 TIPO DE ENRUTAMIENTO.	25
6.10.7.1 ENRUTAMIENTO ESTÁTICO.	25
6.10.7.2 ENRUTAMIENTO POR DEFECTO	26
6.10.7.3 ENRUTAMIENTO DINÁMICO.	26
6.10.8 INTRODUCCIÓN A PROTOCOLOS DE ENRUTAMIENTO.	26
6.10.8 IGRP PROTOCOLO DE ENRUTAMIENTO INTERIOR DE GATEWAY.....	27
6.10.8 PROTOCOLO DE ENRUTAMIENTO POR VECTOR DISTANCIA (RIP).....	27
6.10.8.1 CARACTERÍSTICAS DEL PROTOCOLO RIP.	28
6.10.8.2 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP.....	28
6.10.8.3 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSION 2.....	28
6.10.9 PROTOCOLO DE ENRUTAMIENTO ESTADO ENLACE (OSPF).	29
6.10.9.1 TIPOS DE RED OSPF.	30
6.10.9.2 PROTOCOLO HELLO DE OSPF.....	31
6.10.9.3 MODIFICACIÓN DE LA MÉTRICA DE COSTOS DE OSPF.	32
6.10.9.4 VERIFICACIÓN DE CONFIGURACIÓN OSPF.	33
6.10.10 FIREWALLS.....	34
6.10.10 LISTAS DE CONTROL DE ACCESO (ACL).....	34
6.10.10.1 FUNCIONAMIENTO DE LAS ACL.	35
6.10.10.2 CREACIÓN DE LAS ACL.	35
6.10.10.3 VERIFICACIÓN DE LAS ACL.	36
6.10.10.4 ACL ESTÁNDAR.	36
6.10.10.5 ACL EXTENDIDAS.....	37

6.10.10.4 ACL ESTÁNDAR.....	36
6.10.10.5 ACL EXTENDIDAS.....	37
6.10.10.6 UBICACIÓN DE LAS ACL.....	37
6.10.11 GUARDANDO LA CONFIGURACIÓN.....	38
6.10.12 SWITCH.....	38
6.10.12.1 CARACTERÍSTICAS.....	38
6.10.12.2 NIVELES DE TRANSMISIÓN.....	39
6.10.12.3 TECNOLOGÍA STACK O STACKEABLE.....	40
6.10.12.3.1 TRUNKING PORT.....	40
6.10.12.4 MODOS DE COMANDOS DEL SWITCH.....	40
6.10.12.5 CONFIGURACIÓN DE UN SWITCH.....	40
6.10.12.6 INTRODUCCIÓN A LAS VLANS.....	40
6.10.12.7 FUNCIONAMIENTO DE UNA VLAN.....	40
6.10.12.8 VENTAJAS DE LAS VLANS.....	41
6.10.12.9 CONFIGURACIÓN DE UNA VLAN.....	41
6.10.13 CONFIGURACIÓN DE ROUTERS.....	43
6.10.14 CONFIGURACIÓN DEL ROUTER MATRIZ GUAYAQUIL.....	43
6.10.15 CONFIGURACIÓN DE INTERFACES SERIALES.....	43
6.10.16 CONFIGURACIÓN DEL ROUTER MATRIZ QUITO.....	50
6.10.17 CONFIGURACIÓN PROTOCOLO DE ENRUTAMIENTO RIP VERSIÓN 2.....	52
6.10.18 CONFIGURACIÓN PROTOCOLO DE ENRUTAMIENTO OSPF.....	53
6.10.19 CONFIGURACIÓN DEL ROUTER SUCURSAL GARZOTA.....	58
6.10.19.1 CONFIGURACIÓN DE INTERFACES SERIALES.....	58
6.10.19.1 CONFIGURACIÓN DE FASTETHERNET SUCURSAL GARZOTA.....	59
6.10.19.2 CONFIGURACIÓN DE SUB-INTERFAZ.....	59
6.10.19.3 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSION 2.....	60
6.10.19.4 CONFIGURACIÓN SWITCH SUCURSAL GARZOTA.....	64
6.10.19.5 CREACIÓN DE VLAN.....	64
6.10.19.6 CONFIGURACIÓN DE PUERTOS ASIGNANDO VLAN.....	64
6.10.19.7 SHOW VLAN SWITCH SUCURSAL GARZOTA.....	68
6.10.20 ROUTER SUCURSAL AV. OLMEDO.....	68
6.10.20.1 CONFIGURACIÓN DE FASTETHERNET SUCURSAL AV. OLMEDO.....	69
6.10.20.2 CONFIGURACIÓN DE SUB-INTERFAZ.....	70
6.10.20.3 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSION 2.....	70
6.10.20.4 GUARDANDO LA CONFIGURACIÓN DEL ROUTER.....	71
6.10.20.5 CONFIGURACIÓN SWITCH SUCURSAL AV. OLMEDO.....	74
6.10.20.6 CREACIÓN DE VLAN.....	75
6.10.20.7 CONFIGURACIÓN DE PUERTOS ASIGNANDO VLAN.....	75
6.10.21 CONFIGURACIÓN DEL ROUTER SUCURSAL GRAN COLOMBIA.....	80
6.10.21.1 CONFIGURACIÓN DE INTERFACES SERIALES.....	80
6.10.21.2 CONFIGURACIÓN DE FASTETHERNET SUCURSAL GRAN COLOMBIA.....	81
6.10.21.3 CONFIGURACIÓN DE SUB-INTERFAZ.....	81
6.10.21.4 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSION 2.....	82
6.10.21.5 CONFIGURACIÓN SWITCH SUCURSAL GRAN COLOMBIA.....	86
6.10.21.6 CONFIGURACIÓN DE PUERTOS ASIGNANDO VLAN.....	86
6.10.22 CONFIGURACIÓN DEL ROUTER SUCURSAL MAGDALENA.....	91
6.10.22.1 CONFIGURACIÓN DE INTERFACES SERIALES.....	91
6.10.22.2 CONFIGURACIÓN DE FASTETHERNET SUCURSAL GRAN COLOMBIA.....	92
6.10.22.3 CONFIGURACIÓN DE SUB-INTERFAZ.....	92
6.10.22.4 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSION 2.....	93
6.10.22.5 CONFIGURACIÓN SWITCH SUCURSAL MAGDALENA.....	97
6.10.22.6 CREACIÓN DE VLAN.....	97
6.10.22.7 CONFIGURACIÓN DE PUERTOS ASIGNANDO VLAN.....	98



BIBLIOTECA
CAMPUS
PERAS

CAPÍTULO 7

7 LINUX.....	1
7.1 INTRODUCCIÓN A LINUX.....	1
7.2 REQUERIMIENTO PARA INSTALAR UN SERVIDOR LINUX	2
7.3 CONFIGURACIÓN DEL BIOS	3
7.4 INSTALACIÓN DE LINUX FEDORA CORE 3	5
7.5 POST-CONFIGURACIÓN DE LINUX FEDORA CORE 3	20
7.6 COMANDOS BASICOS DE LINUX FEDORA CORE 3.....	28
7.7 CONFIGURACIONES GENERALES DE LINUX FEDORA	31
7.7.1 CONFIGURACIÓN DE LA TARJETA DE RED MODO TEXTO	31
7.7.2 MODO GRÁFICO.....	33
7.8 CONFIGURACIONES DE LOS SERVIDORES EN LINUX.....	37
7.8.1 CONFIGURACIÓN DEL SERVIDOR SAMBA.....	37
7.8.1.1 CONFIGURACIÓN EN LINUX.....	39
7.8.1.1 CONFIGURACIÓN EN EL CLIENTE WINDOWS	43
7.8.2 CONFIGURACIÓN DEL SERVIDOR DNS.....	49
7.8.2.1 CONFIGURACIÓN DEL BIND.....	52
7.8.2.2 CONFIGURACIÓN EN EL CLIENTE WINDOW	58
7.8.3 CONFIGURACIÓN DEL SERVIDOR WEB.....	62
7.8.3.1 CONFIGURACIÓN EN LINUX.....	64
7.8.3.2 CONFIGURACIÓN EN EL CLIENTE WINDOW	68
7.8.4 CONFIGURACIÓN DEL SERVIDOR PROXY	69
7.8.4.1 CONFIGURACIÓN PARA LEVANTAR EL SQUID	71
7.8.4.1 CONFIGURACIÓN EN EL CLIENTE WINDOWS	76
7.8.5 CONFIGURACIÓN DEL SERVIDOR SENDMAIL	89
7.8.5.1 CONFIGURACIÓN DE SENDMAIL EN SERVIDOR LINUX.....	91
7.8.5.2 CONFIGURACIÓN Y CREACION DE USUARIO EN PC CLIENTE.....	95
7.8.6 CONFIGURACIÓN DEL SERVIDOR DHCP	102
7.8.6.1 CONFIGURACIÓN EN LINUX.....	105
7.8.7 CONFIGURACIÓN DEL SERVIDOR FIREWALL.....	111
7.8.7.1 CONFIGURACIÓN DE FIREWALL EN LINUX	113
7.8.7.1 CONFIGURACIÓN EN EL CLIENTE WINDOWS.....	117

ANEXO A

GLOSARIO



TABLA DE ILUSTRACIONES

CAPÍTULO 2

FIGURA 2-1: GRÁFICO DE LA ESTRUCTURA DEL EDIFICIOMATRIZ GUAYAQUIL	7
FIGURA 2-2: GRÁFICO ANÁLISIS DE PISO APLICATIVO PLANTA BAJA - GUAYAQUIL	8
FIGURA 2-3: GRÁFICO ANÁLISIS DE PISO APLICATIVO PLANTA BAJA - GUAYAQUIL	9
FIGURA 2-4: GRÁFICO ANÁLISIS DE PISO APLICATIVO SEGUNDO PISO - GUAYAQUIL	10
FIGURA 2-5: GRÁFICO ANÁLISIS DE PISO LÓGICO SEGUNDO PISO - GUAYAQUIL.....	11
FIGURA 2-6: GRÁFICO ANÁLISIS DE PISO APLICATIVO TERCER PISO - GUAYAQUIL.....	12
FIGURA 2-7: GRÁFICO ANÁLISIS DE PISO LÓGICO TERCER PISO - GUAYAQUIL.....	13
FIGURA 2-8: GRÁFICO DE LA ESTRUCTURA DEL EDIFICIO QUITO.....	15
FIGURA 2-9: GRÁFICO ANÁLISIS DE PISO APLICATIVO SEGUNDO PISO - QUITO.....	16
FIGURA 2-10: GRÁFICO ANÁLISIS DE PISO LÓGICO SEGUNDO PISO - QUITO	17
FIGURA 2-11: GRÁFICO CUARTO DE COMUNICACIONES GUAYAQUIL	21
FIGURA 2-12: GRÁFICO CENTRO DE DISTRIBUCIÓN PRINCIPAL.....	22
FIGURA 2-13: GRÁFICO CENTRO DE DISTRIBUCIÓN INTERMEDIA.....	23
FIGURA 2-14: GRÁFICO CENTRO DE DISTRIBUCIÓN PRINCIPAL.....	24
FIGURA 2-15: GRÁFICO CENTRO DE DISTRIBUCIÓN INTERMEDIA.....	25
FIGURA 2-16: GRÁFICO CENTRO DE DISTRIBUCIÓN INTERMEDIA.....	26
FIGURA 2-17: GRÁFICO INFRAESTRUCTURA WAN A NIVEL DE DISPOSITIVOS	29
FIGURA 2-18: GRÁFICO INFRAESTRUCTURA WAN A NIVEL DE DISPOSITIVOS	30

CAPÍTULO 4

FIGURA 4-1: NORMATIVA 1.....	1
FIGURA 4-2: NORMATIVA 2.....	1
FIGURA 4-3: NORMATIVA 3.....	1
FIGURA 4-4: NORMATIVA 4.....	2
FIGURA 4-5: NORMATIVA 5.....	2
FIGURA 4-6: NORMATIVA 6.....	2
FIGURA 4-7: NORMATIVA 7.....	2
FIGURA 4-8: NORMATIVA 8.....	3
FIGURA 4-9: NORMATIVA 9.....	3
FIGURA 4-10: NORMATIVA 10.....	3
FIGURA 4-11: NORMATIVA 11.....	4
FIGURA 4-12: NORMATIVA 12.....	4
FIGURA 4-13: NORMATIVA 13.....	4
FIGURA 4-14: NORMATIVA 14.....	4
FIGURA 4-15: NORMATIVA 15.....	5
FIGURA 4-16: NORMATIVA 16.....	5
FIGURA 4-17: NORMATIVA 17.....	5
FIGURA 4-18: NORMATIVA 18.....	6
FIGURA 4-19: NORMATIVA 19.....	6
FIGURA 4-20: NORMATIVA 20.....	6
FIGURA 4-21: NORMATIVA 21.....	7
FIGURA 4-22: NORMATIVA 22.....	7
FIGURA 4-23: NORMATIVA 23.....	7
FIGURA 4-24: NORMATIVA 24.....	8
FIGURA 4-25: NORMATIVA 25.....	8
FIGURA 4-26: NORMATIVA 26.....	8
FIGURA 4-27: NORMATIVA 27.....	8
FIGURA 4-28: NORMATIVA 28.....	9
FIGURA 4-29: NORMATIVA 29.....	9
FIGURA 4-30: NORMATIVA 30.....	9
FIGURA 4-31: NORMATIVA 31.....	9
FIGURA 4-32: NORMATIVA 32.....	10



BIBLIOTECA
CAMPUS
PEÑAS

FIGURA 4-33: NORMATIVA 33.....	10
FIGURA 4-34: NORMATIVA 34.....	10
FIGURA 4-35: NORMATIVA 35.....	10
FIGURA 4-36: NORMATIVA 36.....	11
FIGURA 4-37: NORMATIVA 37.....	11
FIGURA 4-38: NORMATIVA 38.....	11
FIGURA 4-39: NORMATIVA 39.....	11
FIGURA 4-40: NORMATIVA 40.....	12
FIGURA 4-41: NORMATIVA 41.....	12
FIGURA 4-42: NORMATIVA 42.....	12
FIGURA 4-43: NORMATIVA 43.....	13
FIGURA 4-44: NORMATIVA 44.....	13
FIGURA 4-45: NORMATIVA 45.....	13
FIGURA 4-46: NORMATIVA 46.....	13
FIGURA 4-47: NORMATIVA 47.....	14
FIGURA 4-48: NORMATIVA 48.....	14
FIGURA 4-49: NORMATIVA 49.....	14
FIGURA 4-50: NORMATIVA 50.....	14
FIGURA 4-51: NORMATIVA 51.....	15
FIGURA 4-52: NORMATIVA 52.....	15
FIGURA 4-53: NORMATIVA 53.....	15
FIGURA 4-54: RECOMENDACIÓN 1.....	16
FIGURA 4-55: RECOMENDACIÓN 2.....	16
FIGURA 4-56: RECOMENDACIÓN 3.....	16
FIGURA 4-57: RECOMENDACIÓN 4.....	17
FIGURA 4-58: RECOMENDACIÓN 5.....	17
FIGURA 4-59: RECOMENDACIÓN 6.....	17
FIGURA 4-60: RECOMENDACIÓN 7.....	18
FIGURA 4-61: RECOMENDACIÓN 8.....	18
FIGURA 4-62: RECOMENDACIÓN 9.....	18
FIGURA 4-63: RECOMENDACIÓN 10.....	19
FIGURA 4-64: RECOMENDACIÓN 11.....	19
FIGURA 4-65: RECOMENDACIÓN 12.....	19
FIGURA 4-66: RECOMENDACIÓN 13.....	20
FIGURA 4-67: RECOMENDACIÓN 14.....	20

CAPÍTULO 5

FIGURA 5-1: CENTRO DE DISTRIBUCION PRINCIPAL.....	3
FIGURA 5-2: CENTRO DE DISTRIBUCIÓN INTERMEDIA.....	4
FIGURA 5-3: ANÁLISIS DE PISO APLICATIVO SEGUNDA PLANTA.....	5
FIGURA 5-4: ANÁLISIS DE PISO LÓGICO SEGUNDA PLANTA CÁLCULO DEL BACKBONE - SEGUNDO PISO.....	6
FIGURA 5-5: GRÁFICO ANÁLISIS DE PISO APLICATIVO TERCERA PLANTA.....	9
FIGURA 5-6: GRÁFICO ANÁLISIS DE PISO LÓGICO TERCERA PLANTA.....	10

CAPÍTULO 6

FIGURA 6-1: GRÁFICO TECNOLOGÍAS DE ROUTER.....	1
FIGURA 6-2: COMPONENTES INTERNOS DE UN ROUTER.....	2
FIGURA 6-4: COMPONENTES EXTERNOS DE UN ROUTER.....	4
FIGURA 6-5: CONEXIÓN DEL CABLE DE CONSOLA AL ROUTER.....	5
FIGURA 6-7: ESQUEMA DE CONEXIÓN DE UN ROUTER A UNA TERMINAL.....	6
FIGURA 6-8: MENÚ INICIO EN WINDOWS XP.....	7
FIGURA 6-9: MENÚ TODOS LOS PROGRAMAS EN WINDOWS XP.....	8
FIGURA 6-10: MENÚ ACCESORIOS.....	8
FIGURA 6-11: MENÚ COMUNICACIONES.....	9
FIGURA 6-12: APLICACIÓN HYPERTERMINAL.....	9



BIBLIOTECA
CAMPUS
PEÑAS

CAPÍTULO 7

FIGURA 7-1: CONFIGURACIÓN DEL BIOS	3
FIGURA 7-2: BIOS FEATURES SETUP	3
FIGURA 7-3: SELECCION DEL CDROM.....	4
FIGURA 7-4: SELECCIÓN SAVE & EXIT	4
FIGURA 7-5: INSTALACION.....	5
FIGURA 7-6: SKANDISK	5
FIGURA 7-7: BIENVENIDA	6
FIGURA 7-8: SELECCION DE IDIOMA.....	6
FIGURA 7-9: SELECCIÓN DE IDIOMA DEL TECLADO.....	7
FIGURA 7-10: TIPO DE INSTALACIÓN.....	7
FIGURA 7-11: OPCIÓN SERVIDOR.....	8
FIGURA 7-12: OPCIÓN PERSONALIZADA	8
FIGURA 7-13: CONFIGURACIÓN PARTICIONAMIENTO DEL DISCO	8
FIGURA 7-14: CONFIGURACIÓN DEL DISCO.....	9
FIGURA 7-15: AÑADIR PARTICIÓN.....	9
FIGURA 7-16: CREACIÓN SWAP.....	10
FIGURA 7-17: CREACIÓN PARTICIÓN RAIZ	10
FIGURA 7-18: CONFIGURACIÓN DEL DISCO.....	11
FIGURA 7-19: CONFIGURACIÓN DEL GESTOR DE ARRANQUE	11
FIGURA 7-20: CONFIGURACIÓN DE RED.....	12
FIGURA 7-21: CONFIGURACIÓN DE FIREWALL.....	12
FIGURA 7-22: ADVERTENCIA.....	13
FIGURA 7-23: IDIOMA.....	13
FIGURA 7-24: HUSO HORARIO	14
FIGURA 7-25: ASIGNACIÓN DE CLAVE.....	14
FIGURA 7-26: PANTALLA SELECCIÓN DE PAQUETES.....	15
FIGURA 7-27: SERVIDORES DE RED.....	15
FIGURA 7-28: COMIENZO DE INSTALACIÓN	16
FIGURA 7-29: MGEDIO DE INSTALACIÓN REQUERIDO	16
FIGURA 7-30: CREACIÓN Y FORMATEO DE UNIDADES.....	17
FIGURA 7-31: INSTALACIÓN SISTEMA OPERATIVO.....	17
FIGURA 7-32: FINALIZACIÓN DE INSTALACIÓN DE PAQUETES	18
FIGURA 7-33: INSTALACIÓN TERMINADA CON EXITO	18
FIGURA 7-34: GESTOR DE ARRANQUE.....	19
FIGURA 7-35: BIENVENIDA	20
FIGURA 7-36: ACUERDO DE LICENCIA.....	20
FIGURA 7-37: CONFIGURACIÓN FECHA Y HORA.....	21
FIGURA 7-38: RESOLUCIÓN DE PANTALLA.....	21
FIGURA 7-39: CREACIÓN USUARIO DEL SISTEMA.....	22
FIGURA 7-40: CONFIGURACIÓN TARJETA DE SONIDO.....	22
FIGURA 7-41: AGREGAR PAQUETES ADICIONALES.....	23
FIGURA 7-42: FINALIZACIÓN DE LA CONFIGURACIÓN.....	23
FIGURA 7-42: INTRODUCIR NOMBRE DE USUARIO	24
FIGURA 7-43: INTRODUCIR CONTRASEÑA DE USUARIO	24
FIGURA 7-44: SISTEMA OPERATIVO LISTO	25
FIGURA 7-45: ABRIR TERMINAL.....	25
FIGURA 7-46: MODO TEXTO.....	26
FIGURA 7-47: INGRESAR AL ROOT	26
FIGURA 7-48: INGRESAR PASSWORD	27
FIGURA 7-49: VISUALIZACIÓN DEL SISTEMA OPERATIVO	27
FIGURA 7-50: CONFIGURACIÓN TARJETA DE RED MODO TEXTO.....	31
FIGURA 7-51: RUTA PARA VERIFICAR LA TARJETA	31
FIGURA 7-52: VERIFICACIÓN DE LA TARJETA LEVANTADA	32
FIGURA 7-53: INGRESAR AL SETUP	33
FIGURA 7-54: SETUP.....	33
FIGURA 7-55: CONSULTA DE CONFIGURACIÓN DE LA TARJETA.....	34
FIGURA 7-56: ASIGNACIÓN DE IP.....	34
FIGURA 7-57: OPCIÓN OK.....	35



FIGURA 6-13: PANTALLA DE RECOMENDACIÓN DE PROGRAMA PREDETERMINADO PARA TELNET	10
FIGURA 6-14: MENÚ INFORMACIÓN DE UBICACIÓN	10
FIGURA 6-15: PANTALLA DE OPCIONES DE TELÉFONO Y MODEM	11
FIGURA 6-16: PANTALLA DE DESCRIPCIÓN DE LA CONEXIÓN DE LA HYPERTERMINAL ..	11
FIGURA 6-17: PANTALLA DESCRIPCIÓN DE LA CONEXIÓN	12
FIGURA 6-18: PANTALLA CONECTAR A	12
FIGURA 6-19: PANTALLA DEFAULT DE COMI	13
FIGURA 6-20: PANTALLA PROPIEDADES DE COMI	14
FIGURA 6-21: PANTALLA INICIO DE INTERFAZ CON EL ROUTER	15
FIGURA 6-22: DESCRIPCIÓN CABLES SERIALES	16
FIGURA 6-23: CABLES SERIALES LISTOS PARA CONECTARSE A LOS ROUTERS	17
FIGURA	17
FIGURA 6-25: ESQUEMA DE CONEXIÓN ENTRE ROUTER	17
FIGURA 6-26: ASIGNACIÓN DE NOMBRE ROUTER	18
FIGURA 6-27: ASIGNACIÓN DE CONTRASEÑA ROUTER 1	19
FIGURA 6-28: ASIGNACIÓN DE CONTRASEÑA ROUTER 2	19
FIGURA 6-29: ASIGNACIÓN DE CONTRASEÑA ROUTER 2	19
FIGURA 6-30: ASIGNACIÓN DE CONTRASEÑA ENCRIPTADA ROUTER	20
FIGURA 6-31: CONFIGURACIÓN DE CONTRASEÑAS	20
FIGURA 6-32: AYUDA MEDIANTE EL TECLADO	21
FIGURA 6-34: PUERTOS SERIALES	23
FIGURA 6-35: CONECTORES DCE Y DTE	23
FIGURA 6-36: CONECTORES HEMBRA Y MACHO	24
FIGURA 6-37: LEVANTAR EL ESTADO SERIAL	24
FIGURA 6-38: LEVANTAR EL ESTADO DE UNA FASTETHERNET	25
FIGURA 6-39: DETERMINACIÓN DE RUTAS	27
FIGURA 6-40: LEVANTAR PROTOCOLO DE ENRUTAMIENTO RIP	28
FIGURA 6-42: PROTOCOLOS LEVANTADOS CON RIP VERSION 2	29
FIGURA 6-43: RED OSPF CON MULTIACCESO DE BROADCAST	30
FIGURA 6-44: RED OSPF PUNTO A PUNTO	30
FIGURA 6-45: RED OSPF CON MUNLTIACCESO SIN BROADCAST	31
FIGURA 6-46: DAR DIRECCIÓN POR OSPF	32
FIGURA 6-47: FUNCIONAMIENTO DEL FIREWALL	34
FIGURA 6-48: LISTAS DE CONTROL DE ACCESO	35
FIGURA 6-49: PANTALLA DE VERIFICACIÓN DE LA EXISTENCIA DE UNA ACL	36
FIGURA 6-50: UBICACIÓN DE LAS ACL	37
FIGURA 6-51: VISTA FRONTAL DE UN SWITCH NO ADMINISTRABLE	39
FIGURA 6-52: VISTA FRONTAL DE UN SWITCH ADMINISTRABLE	39
FIGURA 6-53: CREACIÓN DEL NOMBRE DE LA VLAN	41
FIGURA 6-54: TRUNCAR PUERTO VLAN	41
FIGURA 6-55: VERIFICACIÓN DE PUERTO ASIGNADO A LA VLAN	42
FIGURA 6-56: SHOW IP ROUTE MATRIZ GUAYAQUIL	49
FIGURA 6-57: SHOW RUN ROUTER MATRIZ QUITO	57
FIGURA 6-58: SHOW RUN ROUTER GARZOTA	63
FIGURA 6-59: SHOW VLAN ROUTER GARZOTA	68
FIGURA 6-60: SHOW IP ROUTE OLMEDO	74
FIGURA 6-61: SHOW VLAN AV OLMEDO	79
FIGURA 6-62: SHOW IP ROUTE GRAN COLOMBIA	85
FIGURA 6-63: SHOW VLAN SWITCH GRAN COLOMBIA	90
FIGURA 6-64: SHOW IP ROUTE SUCUCURSAL MAGDALENA	96
FIGURA 6-65: SHOW VLAN SWITCH MAGDALENA	101



BIBLIOTECA
CAMPUS
PEÑAS

CAPÍTULO 7

FIGURA 7-1: CONFIGURACIÓN DEL BIOS	3
FIGURA 7-2: BIOS FEATURES SETUP	3
FIGURA 7-3: SELECCIÓN DEL CDROM.....	4
FIGURA 7-4: SELECCIÓN SAVE & EXIT	4
FIGURA 7-5: INSTALACIÓN	5
FIGURA 7-6: SKANDISK	5
FIGURA 7-7: BIENVENIDA	6
FIGURA 7-8: SELECCION DE IDIOMA.....	6
FIGURA 7-9: SELECCIÓN DE IDIOMA DEL TECLADO.....	7
FIGURA 7-10: TIPO DE INSTALACIÓN.....	7
FIGURA 7-11: OPCIÓN SERVIDOR.....	8
FIGURA 7-12: OPCIÓN PERSONALIZADA	8
FIGURA 7-13: CONFIGURACIÓN PARTICIONAMIENTO DEL DISCO	8
FIGURA 7-14: CONFIGURACIÓN DEL DISCO.....	9
FIGURA 7-15: AÑADIR PARTICIÓN.....	9
FIGURA 7-16: CREACIÓN SWAP.....	10
FIGURA 7-17: CREACIÓN PARTICIÓN RAIZ	10
FIGURA 7-18: CONFIGURACIÓN DEL DISCO.....	11
FIGURA 7-19: CONFIGURACIÓN DEL GESTOR DE ARRANQUE	11
FIGURA 7-20: CONFIGURACIÓN DE RED.....	12
FIGURA 7-21: CONFIGURACIÓN DE FIREWALL	12
FIGURA 7-22: ADVERTENCIA.....	13
FIGURA 7-23: IDIOMA.....	13
FIGURA 7-24: HUSO HORARIO	14
FIGURA 7-25: ASIGNACIÓN DE CLAVE.....	14
FIGURA 7-26: PANTALLA SELECCIÓN DE PAQUETES.....	15
FIGURA 7-27: SERVIDORES DE RED.....	15
FIGURA 7-28: COMIENZO DE INSTALACIÓN	16
FIGURA 7-29: MGEDIO DE INSTALACIÓN REQUERIDO	16
FIGURA 7-30: CREACIÓN Y FORMATEO DE UNIDADES.....	17
FIGURA 7-31: INSTALACIÓN SISTEMA OPERATIVO.....	17
FIGURA 7-32: FINALIZACIÓN DE INSTALACIÓN DE PAQUETES	18
FIGURA 7-33: INSTALACIÓN TERMINADA CON EXITO	18
FIGURA 7-34: GESTOR DE ARRANQUE.....	19
FIGURA 7-35: BIENVENIDA	20
FIGURA 7-36: ACUERDO DE LICENCIA.....	20
FIGURA 7-37: CONFIGURACIÓN FECHA Y HORA.....	21
FIGURA 7-38: RESOLUCIÓN DE PANTALLA.....	21
FIGURA 7-39: CREACIÓN USUARIO DEL SISTEMA	22
FIGURA 7-40: CONFIGURACIÓN TARJETA DE SONIDO.....	22
FIGURA 7-41: AGREGAR PAQUETES ADICIONALES.....	23
FIGURA 7-42: FINALIZACIÓN DE LA CONFIGURACIÓN.....	23
FIGURA 7-42: INTRODUCIR NOMBRE DE USUARIO	24
FIGURA 7-43: INTRODUCIR CONTRASEÑA DE USUARIO	24
FIGURA 7-44: SISTEMA OPERATIVO LISTO	25
FIGURA 7-45: ABRIR TERMINAL.....	25
FIGURA 7-46: MODO TEXTO.....	26
FIGURA 7-47: INGRESAR AL ROOT	26
FIGURA 7-48: INGRESAR PASSWORD	27
FIGURA 7-49: VISUALIZACIÓN DEL SISTEMA OPERATIVO	27
FIGURA 7-50: CONFIGURACIÓN TARJETA DE RED MODO TEXTO.....	31
FIGURA 7-51: RUTA PARA VERIFICAR LA TARJETA	31
FIGURA 7-52: VERIFICACIÓN DE LA TARJETA LEVANTADA	32
FIGURA 7-53: INGRESAR AL SETUP	33
FIGURA 7-54: SETUP	33
FIGURA 7-55: CONSULTA DE CONFIGURACIÓN DE LA TARJETA.....	34
FIGURA 7-56: ASIGNACIÓN DE IP.....	34
FIGURA 7-57: OPCIÓN OK	35

FIGURA 7-58: CONFIGURACIÓN CON OPCIÓN SALIR	35
FIGURA 7-59: COMANDO NETWORK	36
FIGURA 7-60: ESQUEMA SAMBA	37
FIGURA 7-61: VERIFICACIÓN DEL PAQUETE SAMBA	39
FIGURA 7-62: EDITAR EL ARCHIVO SMB	39
FIGURA 7-64: SECCIÓN SHARE DEFINITION.....	40
FIGURA 7-65: LEVANTAR EL SERVICIO SAMBA	40
FIGURA 7-66: CREAR USUARIO	41
FIGURA 7-67: ASIGNAR PASSWORD	41
FIGURA 7-68: ASIGNAR USUARIO SAMBA	41
FIGURA 7-69: CREAR UNA CARPETA.....	42
FIGURA 7-70: CREAR ARCHIVO.....	42
FIGURA 7-71: DAR PERMISOS	42
FIGURA 7-72: PROPIEDADES DE MIS SITIOS DE RED	43
FIGURA 7-73: PROPIEDADES DE CONEXIONES DE RED	43
FIGURA 7-74: PROPIEDADES DE PROTOCOLO DE INTERNET	44
FIGURA 7-75: ASIGNACIÓN IP.....	44
FIGURA 7-76: BUSCAR EQUIPOS.....	45
FIGURA 7-77: BÚSQUEDA DEL SERVIDOR.....	45
FIGURA 7-78: SERVIDOR.....	46
FIGURA 7-79: CONEXIÓN A LINUX	46
FIGURA 7-80: ARCHIVOS COMPARTIDOS	47
FIGURA 7-81: CREAR USUARIO	47
FIGURA 7-82: AGREGAR MENSAJE	48
FIGURA 7-83: DIRECTORIO DEL ARCHIVO	48
FIGURA 7-84: COMPROBACIÓN	48
FIGURA 7-85: PANTALLA ESQUEMA DNS.....	49
FIGURA 7-86: VERIFICACIÓN DEL PAQUETE BIND	52
FIGURA 7-87: EDITAR ARCHIVO NAMED.....	52
FIGURA 7-88: ARCHIVO PARA EDITAR.....	53
FIGURA 7-89: RUTA PARA ENTRAR AL LOCALHOST.....	53
FIGURA 7-90: COPIAR ARCHIVO.....	53
FIGURA 7-91: RUTA PARA EDITAR EL ARCHIVO.....	54
FIGURA 7-92: ARCHIVO	54
FIGURA 7-93: ARCHIVO EDITADA.....	55
FIGURA 7-94: RUTA DE ARCHIVO RESOLV.CONF	55
FIGURA 7-95: ARCHIVO RESOLV.CONF.....	55
FIGURA 7-96: ARCHIVO RESOLV.CONF EDITADA.....	56
FIGURA 7-97: LEVANTAR EL SERVICIO	56
FIGURA 7-98: PING A TIA .COM	56
FIGURA 7-99: RESULTADO DEL PING	57
FIGURA 7-100: PROPIEDADES DE MIS SITIOS DE RED	58
FIGURA 7-101: PANTALLA PROPIEDADES DE CONEXIÓN	58
FIGURA 7-102: PROPIEDADES DE TCP/IP.....	59
FIGURA 7-103: PANTALLA PARA AGREGAR IP.....	59
FIGURA 7-104: INICIO OPCIÓN EJECUTAR.....	60
FIGURA 7-105: COMANDO PARA ABRIR AMBIENTE TEXTO.....	60
FIGURA 7-106: REALIZAR LA COMPROBACIÓN.....	61
FIGURA 7-107: COMPROBACIÓN	61
FIGURA 7-108: PANTALLA DE ESQUEMA SERVIDOR WEB	62
FIGURA 7-109: PANTALLA VERIFICACIÓN DEL PAQUETE.....	64
FIGURA 7-110: RUTA DEL HTTPD.CONF	64
FIGURA 7-111: TEXTO AGREGADO	64
FIGURA 7-112: RUTA PARA CREAR DIRECTORIO.....	65
FIGURA 7-113: CREACIÓN DE CARPETA SITIO.....	65
FIGURA 7-114: INGRESAR AL SITIO	65
FIGURA 7-115: CREACIÓN DEL ARCHIVO INDEX	66
FIGURA 7-116: EDITAR ARCHIVO.....	66
FIGURA 7-117: AGREGAR TEXTO.....	66
FIGURA 7-118: RESTAURAR EL SERVICIO	67

FIGURA 7-119: INTERNET EXPLORER.....	68
FIGURA 7-120: BIENVENIDA	68
FIGURA 7-121: PANTALLA ESQUEMA PROXY	69
FIGURA 7-122: VERIFICACIÓN DEL SQUID	71
FIGURA 7-123: RUTA DEL SQUID.....	71
FIGURA 7-124: SQUID LÍNEA 53	71
FIGURA 7-125: SQUID LÍNEA 52	72
FIGURA 7-126: SQUID LÍNEA 482	72
FIGURA 7-127: SQUID LÍNEA 480	72
FIGURA 7-128: SQUID LÍNEA 695,2	73
FIGURA 7-129: SQUID LÍNEA 695,33.....	73
FIGURA 7-130: SQUID LÍNEA 1818	73
FIGURA 7-131: SQUID LÍNEA 1864	74
FIGURA 7-132: SQUID LÍNEA 1818	74
FIGURA 7-133: ACCESS	75
FIGURA 7-134: RESTAURACIÓN DEL SERVICIO.....	75
FIGURA 7-135: OPCIÓN DE INTERNET	76
FIGURA 7-136: CONFIGURACIÓN LAN.....	76
FIGURA 7-137: CONFIGURACIÓN DE LA RED LAN	77
FIGURA 7-138: DIRECCIÓN WEB.....	77
FIGURA 7-139: RUTA SQUID.CONF.....	78
FIGURA 7-140: SECCIÓN ACL	78
FIGURA 7-141: SECCIÓN HTTP	79
FIGURA 7-142: RESTAURACIÓN SQUID	79
FIGURA 7-143: VERIFICACIÓN	80
FIGURA 7-144: RUTA SQUID	81
FIGURA 7-145: SECCIÓN ACL	81
FIGURA 7-147: SECCIÓN HTTP	82
FIGURA 7-148: CREACIÓN PAGINA	82
FIGURA 7-149: EDITAR PAGINA.....	82
FIGURA 7-150: LISTA DE DIRECCIONES	82
FIGURA 7-151: RESTAURACIÓN DEL SERVICIO.....	83
FIGURA 7-152: INTERNET EXPLORER.....	83
FIGURA 7-153: RUTA DEL SQUID.....	84
FIGURA 7-154: SQUID LÍNEA 1091	84
FIGURA 7-155: SQUID LÍNEA 1093	84
FIGURA 7-156: SQUID LÍNEA 1823	85
FIGURA 7-157: SQUID SECCIÓN HTTP.....	85
FIGURA 7-158: PANTALLA RESTAURACIÓN SQUID	85
FIGURA 7-159: INGRESO SQUID.....	86
FIGURA 7-160: CREACIÓN DEL ARCHIVO	86
FIGURA 7-161: CREACIÓN USUARIO.....	86
FIGURA 7-162: CREACIÓN CONTRASEÑA	87
FIGURA 7-163: CONECTAR	87
FIGURA 7-164: ACCESO A LA PÁGINA	88
FIGURA 7-165: ESQUEMA SENDMAIL	89
FIGURA 7-166: CREACIÓN DEL ARCHIVO	91
FIGURA 7-167: CREACIÓN DEL ARCHIVO	91
FIGURA 7-168: AGREGAR IP	91
FIGURA 7-169: RUTA PARA EDITAR SENDMAIL.CF	91
FIGURA 7-170: CREACIÓN DEL ARCHIVO	92
FIGURA 7-171: SENDMAIL LÍNEA 89	92
FIGURA 7-172: PANTALLA SENDMAIL LÍNEA 266	92
FIGURA 7-173: PANTALLA SENDMAIL LÍNEA 265	92
FIGURA 7-174: SENDMAIL LÍNEA 268	93
FIGURA 7-175: SENDMAIL MODIFICADA	93
FIGURA 7-176: RUTA DOVECOT	93
FIGURA 7-177: DOVECOT LÍNEA 13.....	93
FIGURA 7-178: DOVECOT MODIFICADA.....	94
FIGURA 7-179: RESTAURACIÓN DOVECOT	94

FIGURA 7-180: RESTAURACIÓN SENDMAIL	94
FIGURA 7-181: INICIO OPCIÓN CORREO	95
FIGURA 7-182: OUTLOOK	95
FIGURA 7-182: OUTLOOK OPCIÓN CUENTAS	96
FIGURA 7-183: CUENTA DE INTERNET	96
FIGURA 7-184: CUENTAS DE INTERNET OPCIÓN AGREGAR	97
FIGURA 7-185: ASISTENTE DE CONEXIÓN	97
FIGURA 7-186: CORREO ELECTRONICO	98
FIGURA 7-187: NOMBRE DEL SERVIDOR	98
FIGURA 7-188: INICIO DE SESIÓN	99
FIGURA 7-189: ASISTENTE OPCIÓN FINALIZAR	99
FIGURA 7-190: OUTLOOK EXPRESS	100
FIGURA 7-191: MENSAJE DE PRUEBA	100
FIGURA 7-192: MAIL	101
FIGURA 7-182: LISTA DE MENSAJES	101
FIGURA 7-183: MENSAJE RECIBIDO	101
FIGURA 7-184: ESQUEMA DHCP	102
FIGURA 7-185: RUTA DHCP	105
FIGURA 7-186: EDITAR DHCP	105
FIGURA 7-187: ARCHIVO DHCP	105
FIGURA 7-188: ARCHIVO DHCP MODIFICADO	106
FIGURA 7-189: RESTAURACIÓN DHCP	106
FIGURA 7-190: PROPIEDADES DE MIS SITIOS DE RED	107
FIGURA 7-191: PROPIEDADES DE CONEXIONES DE ÁREA LOCAL	107
FIGURA 7-192: PROPIEDADES DE TCP/IP	108
FIGURA 7-193: PROPIEDADES OPCIÓN ACEPTAR	108
FIGURA 7-194: ESTADO DE CONEXIÓN DE AREA LOCAL	109
FIGURA 7-195: CONEXIÓN OPCIÓN GENERAL	109
FIGURA 7-196: CONEXIÓN DE DHCP	110
FIGURA 7-197: PANTALLA ESQUEMA FIREWALLE	111
FIGURA 7-198: VERIFICACIÓN DEL PING	113
FIGURA 7-199: DENEGAR PING	113
FIGURA 7-200: COMPROBACIÓN DEL PING	114
FIGURA 7-201: PING DENEGADO	114
FIGURA 7-202: INGRESO AL ETC	114
FIGURA 7-203: INGRESO XINETD.D	115
FIGURA 7-204: EDITAR KRB5-TELNET	115
FIGURA 7-205: ARCHIVO KRB5-TELNET	115
FIGURA 7-206: ARCHIVO TELNET EDITADO	115
FIGURA 7-207: CREACIÓN DE USUARIO	116
FIGURA 7-208: ASIGNACIÓN DE CONTRASEÑA	116
FIGURA 7-209: INICIO OPCIÓN EJECUTAR	117
FIGURA 7-210: COMANDO CMD	117
FIGURA 7-211: COMANDO TELNET	118
FIGURA 7-212: AUTENTIFICACIÓN	118
FIGURA 7-213: INGRESO MODO NO PRIVILEGIADO	118
FIGURA 7-214: AUTENTIFICACIÓN MODO PRIVILEGIADO	119
FIGURA 7-215: INGRESO A MODO PRIVILEGIADO	119
FIGURA 7-216: DENEGAR TELNET	120
FIGURA 7-217: VERIFICACIÓN DEL TELNET	120
FIGURA 7-218: VERIFICACIÓN DE TELNET DENEGADO	120

ÍNDICE DE TABLAS

CAPÍTULO 2

TABLA 2-1: SERVIDORES GUAYAQUIL.....	3
TABLA 2-2: SERVIDORES QUITO.....	4
TABLA 2-3: ESTACIONES DE TRABAJO GUAYAQUIL.....	5
TABLA 2-4: DISTRIBUCIÓN COMPUTADORAS SEGUNDO PISO.....	6
TABLA 2-5: DISTRIBUCIÓN COMPUTADORAS TERCER PISO.....	6
TABLA 2-6: ESTACIONES DE TRABAJO QUITO.....	14
TABLA 2-8: DISTRIBUCIÓN COMPUTADORAS QUITO.....	14
TABLA 2-9: DISPOSITIVO DE CONMUTACIÓN.....	19
TABLA 2-10: DISPOSITIVO DE ENRUTAMIENTO.....	27
TABLA 2-11: DESCRIPCIÓN FIREWALLE.....	28
TABLA 2-12: ANCHO DE BANDA GUAYAQUIL.....	31
TABLA 2-13: ANCHO DE BANDA QUITO.....	31

CAPÍTULO 3

TABLA 3-1: PROBLEMA, CAUSA Y EFECTO.....	1
TABLA 3-2: PROBLEMA, SOLUCIÓN, ALCANCE.....	2
TABLA 3-3: FACTIBILIDAD TÉCNICA.....	4
TABLA 3-4: FACTIBILIDAD ECONÓMICA HARDWARE.....	5
TABLA 3-5: FACTIBILIDAD ECONÓMICA MATERIALES.....	6
TABLA 3-6: FACTIBILIDAD ECONÓMICA SOFTWARE.....	7
TABLA 3-7: FACTIBILIDAD OPERATIVA.....	8
TABLA 3-8: COSTOS OPERATIVOS.....	9
TABLA 3-9: FACTIBILIDAD ECONÓMICA HARDWARE.....	10
TABLA 3-10: FACTIBILIDAD TÉCNICA.....	14
TABLA 3-11: FACTIBILIDAD ECONÓMICA HARDWARE.....	15
TABLA 3-12: FACTIBILIDAD ECONÓMICA MATERIALES.....	16
TABLA 3-13: FACTIBILIDAD ECONÓMICA SOFTWARE.....	17
TABLA 3-13: FACTIBILIDAD OPERATIVA.....	18
TABLA 3-14: COSTOS OPERATIVOS.....	19
TABLA 3-15: COSTO TOTAL ALTERNATIVA A.....	20

CAPÍTULO 4

TABLA 4-1: IDENTIFICADOR DE CABLES.....	15
TABLA 4-2: HILOS DE FIBRA.....	19

CAPÍTULO 5

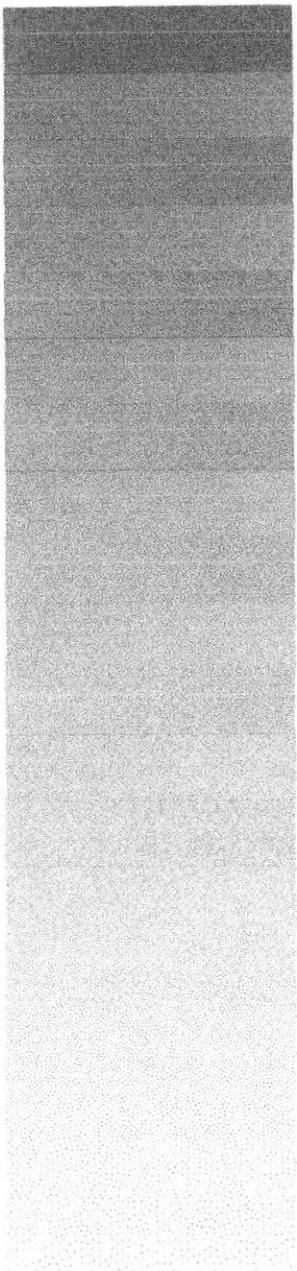
TABLA 5-1: CALCULO DEL BACKBONE SEGUNDO PISO.....	7
TABLA 5-2: CALCULO DEL BACKBONE TERCER PISO.....	14

CAPÍTULO 6

TABLA 6-1: REQUERIMIENTOS PARA CONECTAR UN PC AL ROUTER.....	5
TABLA 6-2: REQUERIMIENTOS PARA CONECTAR DOS ROUTER.....	16

CAPÍTULO 7

TABLA 7-1: REQUERIMIENTO MÍNIMO.....	2
TABLA 7-2: REQUERIMIENTO ÓPTIMO.....	2
TABLA 7-1: COMANDOS BÁSICOS.....	30



BIBLIOTECA
CAMPUS
PEÑAS



CAPÍTULO 1 GENERALIDADES

1 GENERALIDADES

1.1 INTRODUCCIÓN

El presente documento contiene la Situación Actual y Solución Propuesta de acuerdo a la empresa en que se basó el estudio. Configuraciones de Linux Fedora Core 3, Dispositivos de Conmutación y Enrutamiento, para que las personas se involucren en lo que es el campo de las Redes y poder aprender configuraciones sencillas.

1.2 OBJETIVO DEL MANUAL

El objetivo del manual es servir de guía, consulta y ayuda a los Administradores de Red, Jefes Networking, y a todos los relacionados en esta área.

1.3 ¿A QUIEN VA DIRIGIDO ESTE MANUAL?

Este manual esta dirigido al Jefe de Sistemas, autoridades de la empresa Tiendas Industriales Asociadas (TIA). Jefes de Networking, Administradores de Redes y usuarios finales relacionados con el área.

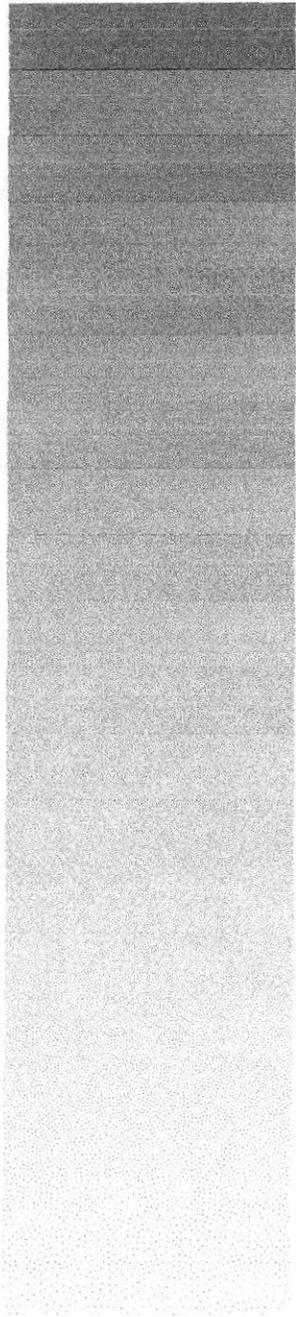
1.4 LO QUE SE DEBE CONOCER

En este manual se ha procurado utilizar un lenguaje flexible, con miras a que tanto usuarios expertos como novatos puedan ayudarse con las configuraciones descritas tanto como para Linux, Dispositivos de Conmutación y Enrutamiento, para interpretarlo de mejor manera se necesita tener conocimientos básicos de redes.

1.5 ORGANIZACIÓN DEL CONTENIDO DEL MANUAL

El manual se divide en siete capítulos, cada uno de los capítulos contiene un propósito específico. El contenido de cada capítulo tiene un propósito diferente. Los mismos que se explican a continuación.





BIBLIOTECA
CAMPUS
PEÑAS

CAPÍTULO 2
SITUACIÓN
ACTUAL

CAPÍTULO 1.- Generalidades

Aquí se indica a quién va dirigido el manual, la organización del manual.

CAPÍTULO 2.- Situación Actual

Este capítulo indica los antecedentes de la empresa, lo que tiene en este momento la empresa, y los problemas encontrados.

CAPÍTULO 3.- Solución Propuesta

Se especifica la solución de los problemas encontrados en el capítulo anterior, la Factibilidad Técnica, Económica y Operativa.

CAPÍTULO 4.- Normativas de Cableado Estructurado

En este capítulo se explican las Normas de Cableado Estructurado.

CAPÍTULO 5.-Implementación de la Solución Propuesta

Aquí se detalla mediante gráficos la implementación de la solución, es decir que va a contener los análisis de piso.

CAPÍTULO 6.- Dispositivos de Enrutamiento y Conmutación

En el capítulo se explica que es un Router y las configuraciones básicas y necesarias para poder armar una red.

CAPÍTULO 7.- Linux Fedora Core 3

Se explican algunas configuraciones, y el por qué de cada una de ellas a detalle.



BIBLIOTECA
CAMPUS
PEÑAS

TIA S.A. TIENDAS INDUSTRIALES ASOCIADAS S.A.

2 SITUACIÓN ACTUAL

2.1 ANTECEDENTES DE LA EMPRESA

Nació en el siglo pasado en los años 20 en Checoslovaquia (Praga), inicio sus operaciones en Colombia (Bogotá) en el año de 1940, expandiéndose posteriormente hacia Argentina, Perú, Uruguay y Ecuador con mucho éxito. Sus fundadores fueron: Sr. Federico Deutsch y el Sr. Kerel Steuer.

Tiendas Industriales Asociadas (TIA) S.A. fue fundada el 29 de noviembre de 1960 en Ecuador, es una cadena de tiendas que ofrece productos de consumo hogareño y personal

Su actividad principal es la venta de productos al Consumidor Final (Cliente que adquiere un producto para uso personal), a través de sus establecimientos. Teniendo así una amplia cobertura nacional.

Tienen 67 locales distribuidos en 42 ciudades y 14 provincias, poseen dos centros de distribución de productos uno en Quito y el otro en Guayaquil.

La matriz está en Guayaquil es un inmueble de tres pisos ubicado en las calles Luque y Chimborazo (centro de Guayaquil).

Constan con sucursales en las provincias de: Guayas, Esmeraldas, Los Ríos, Manabí, El Oro, Imbabura, Pichincha, Cotopaxi, Tungurahua, Chimborazo, Cañar, Azuay, Loja y Pastaza.

2.1.1 MISIÓN

- Generar bienestar en los hogares ecuatorianos
- Promover el crecimiento profesional de los empleados.
- Generar nuevas plazas de trabajo
- Incrementar año a año el valor de la compañía.

2.1.2 VISIÓN

Ser la cadena líder en el abastecimiento de bienes de consumo hogareño, personal y cotidiano.

TIA, será el símbolo nacional de la verdadera economía para el bienestar del hogar Ecuatoriano, sólo se ofrecen cosas prácticas para la familia, con las mejores ofertas y promociones.



2.2 INFRAESTRUCTURA LAN

En la actualidad Tiendas Industriales Asociadas (TIA) Matriz Guayaquil no cuentan con normas de cableado estructurado, la mayor parte del cableado lo tienen tendido sobre el tumbado sin ninguna protección a interferencias, accidentes o factores externos.

El 60% del cableado actual está con cable utp categoría 5e, y el porcentaje restante está con cable utp categoría 5.

Poseen un departamento técnico que se encarga de los problemas que tiene la red de esta Empresa.

En el tercer piso de la matriz de Guayaquil se encuentra el departamento de Sistemas, donde está ubicado el Pop y donde también está su MC (Centro de distribución Principal) con tres IC.(centro de distribución intermedia)



2.2.1 SERVIDORES

2.2.1.1 MATRIZ GUAYAQUIL

Todos Los Servidores Cuentan Con Tarjetas de red 1000 Mbps y con las siguientes características:

CANT	DESCRIPCIÓN	CARACTERÍSTICAS
1	SERVIDOR DE PRODUCCION Sistema operativo UNIX	IBM eServer x236 Procesador: Intel Xeon 3GHz 1 HDD DE 146 Memoria: 1GB
1	SERVIDOR DE INTRANET, DHCP, ANTIVIRUS S.O. Windows 2003 server	IBM Xseries 235 X Procesador: Intel Xeon 2800 MHZ Memoria: 512 MB Disco duro: 109000 MB
1	SERVIDOR DE APLICACION S.O. LINUX RED HAT 9.0	IBM Series 226 Procesador: Pentium IV 3.2 GHZ/800 MHZ Memoria: 512 MB 2 HDD de 146 GB configurados con RAID 1
1	SERVIDOR DE CORREO S.O. WINDOWS 2003 SERVER	IBM Netfinity 3000 Procesador: Pentium III a 500 MHZ Dos discos de 20 GB Memoria: 512 MB
1	SISTEMA DE B/D ORACLE S.O. LINUX RED HAT 9.0	IBM Series 226 Procesador: Pentium IV 3.2 GHZ/800 MHZ Memoria: 512 MB Disco Duro: 72 GB
1	SERVIDOR DE DESAROLLO	COMPAQ PROLIANT ML 350 Memoria: 1 GB 4 HDD de 72 con RAID 1+0
1	SERVIDOR DE CUBO DE INFORMACION S.O. WINDOWS 2003 SERVER	IBM Series 226 Procesador :Pentium IV 3.2 GHZ/800 MHZ Memoria: 1 GB Disco Duro: 72 GB

Tabla 2-1: Servidores Guayaquil



2.2.1.2 MATRIZ QUITO

Todos Los Servidores Cuentan Con Tarjetas 1000 Mbps y con las siguientes características

CANT	DESCRIPCIÓN	CARACTERÍSTICAS
1	SERVIDOR DE INTRANET S.O. LINUX RED HAT 9.0	IBM Series 226 Express (84885AU + 90P1305) Procesador: Intel Xeon 3.20GHz/800MHz Memoria RAM: 1 GB HDD: 2x IBM 73.4GB 15 Krpm Ultra320 SCSI Hot-swap
1	SERVIDOR DE CORREO S.O. WINDOWS 2003 SERVER	IBM Series 226 Express (84885AU + 90P1305) Procesador: Intel Xeon 3.20GHz/800MHz Memoria RAM: 1 GB HDD: 2x IBM 73.4GB 15 Krpm Ultra320 SCSI Hot-swap

Tabla 2-2: Servidores Quito



BIBLIOTECA
CAMPUS
PEÑAS

2.2.2 ESTACIONES DE TRABAJO

Todas las computadoras utilizadas en Tiendas Industriales Asociadas, tienen tarjetas de red de 10/100 Mbps para las estaciones de trabajo.

2.2.2.1 MATRIZ - GUAYAQUIL

Todas las 110 estaciones de trabajo del edificio Matriz de Guayaquil son de marca (HP) y poseen las siguientes características:

MARCA	DESCRIPCIÓN	CARACTERÍSTICAS
HP	Estaciones de trabajo (HP MX2000MT)	Procesador: Pentium IV 2.8 GHZ Memoria: 256 MB Disco Duro: 80 GB

Tabla 2-3: Estaciones de trabajo Guayaquil

- En el primer piso se encuentra la bodega solo de la matriz, cada sucursal posee su propia bodega.



BIBLIOTECA
CAMPUS
PEÑAS

- En el segundo piso se encuentra el UPS general que sirve para todo el edificio, en este piso se encuentran instaladas 30 computadoras distribuidas por departamento de la siguiente manera:

CANTIDAD	UBICACIÓN
12 Computadores	Departamento de Contabilidad
10 Computadores	Departamento de Procesos
8 Computadores	Departamento de Recursos humanos

Tabla 2-4: Distribución computadoras segundopiso

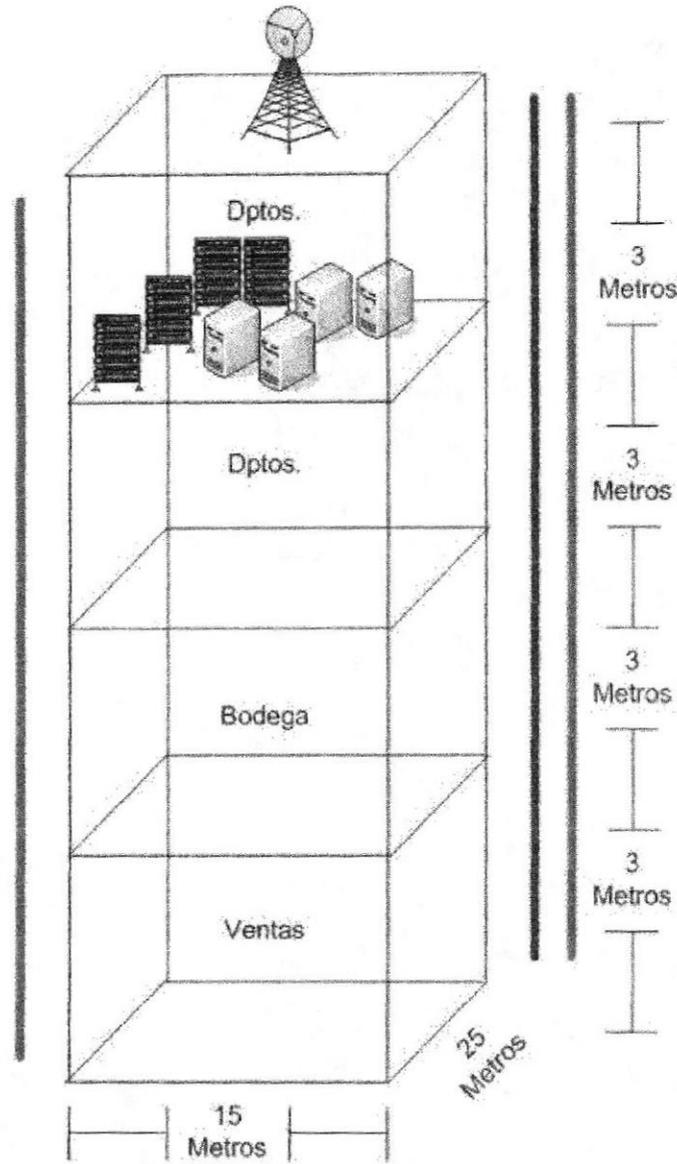
- En el Tercer Piso esta el cuarto de comunicaciones y servidores, aquí se encuentran instaladas 70 computadoras distribuidas por departamento de la siguiente manera:

CANTIDAD	UBICACIÓN
2 Computadores	Departamento de Pagos
2 Computadores	Departamento de Compras
1 Computadores	Presidencia
1 Computadores	Gerencia
5 Computadores 7 Servidores	Sistemas
18 Computadores	Publicidad
4 Computadores	Técnico
30 Computadores	Ventas

Tabla 2-5: Distribución computadoras tercer piso



**GRÁFICO DE LA ESTRUCTURA DEL EDIFICIO
MATRIZ GUAYAQUIL**



Leyenda:

- Cañería de Agua
- Cañería Eléctrica
- Cañería de Red
- Servidor Rack de Piso MC
- Antena Microonda

Autores:

Víctor Tola Franco
Mariuxi Ramírez Ayala
Jonathan Baquero López

Figura 2-1: Gráfico de la Estructura del Edificio Matriz Guayaquil

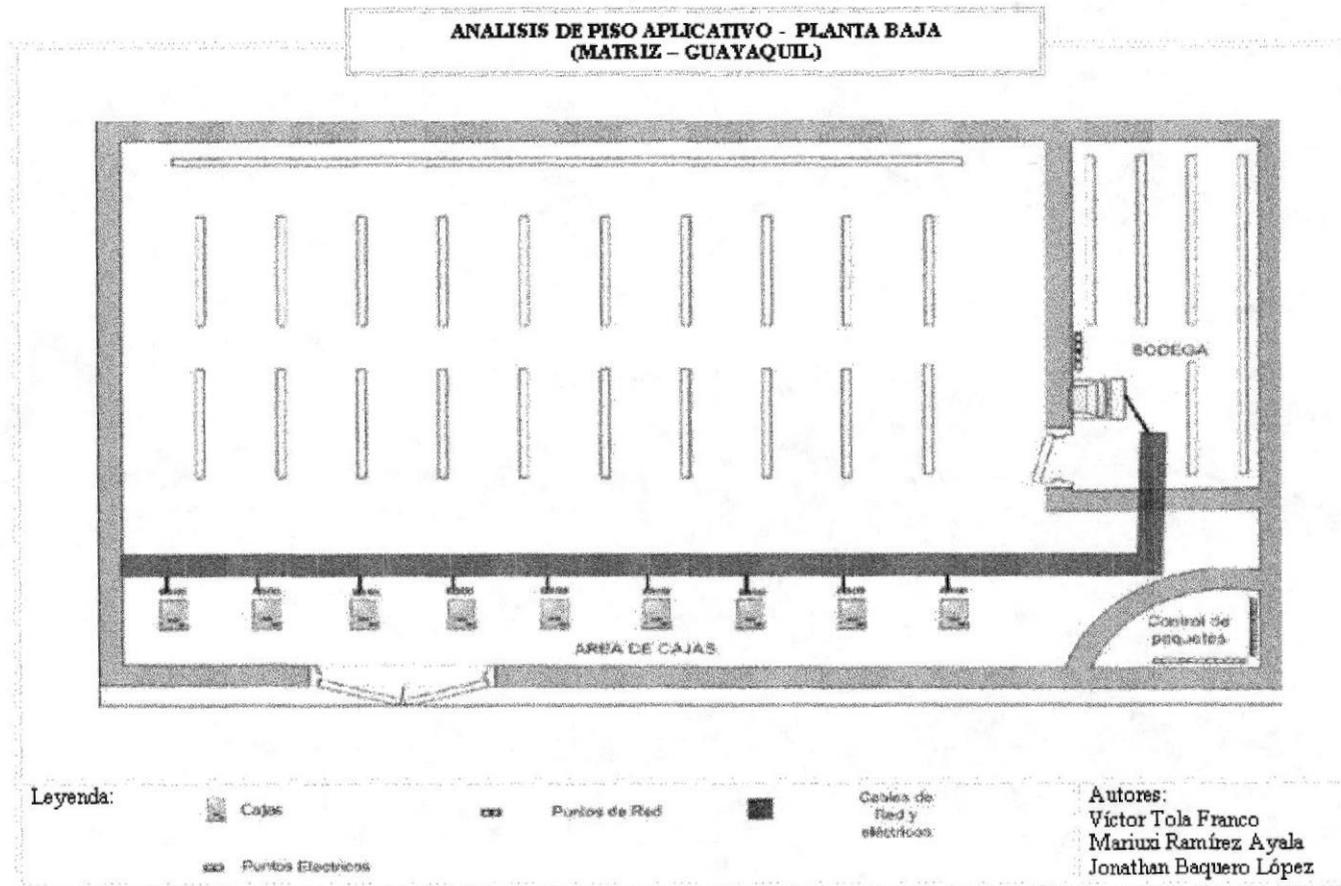


Figura 2-2: Gráfico Análisis de piso Aplicativo Planta Baja - Guayaquil

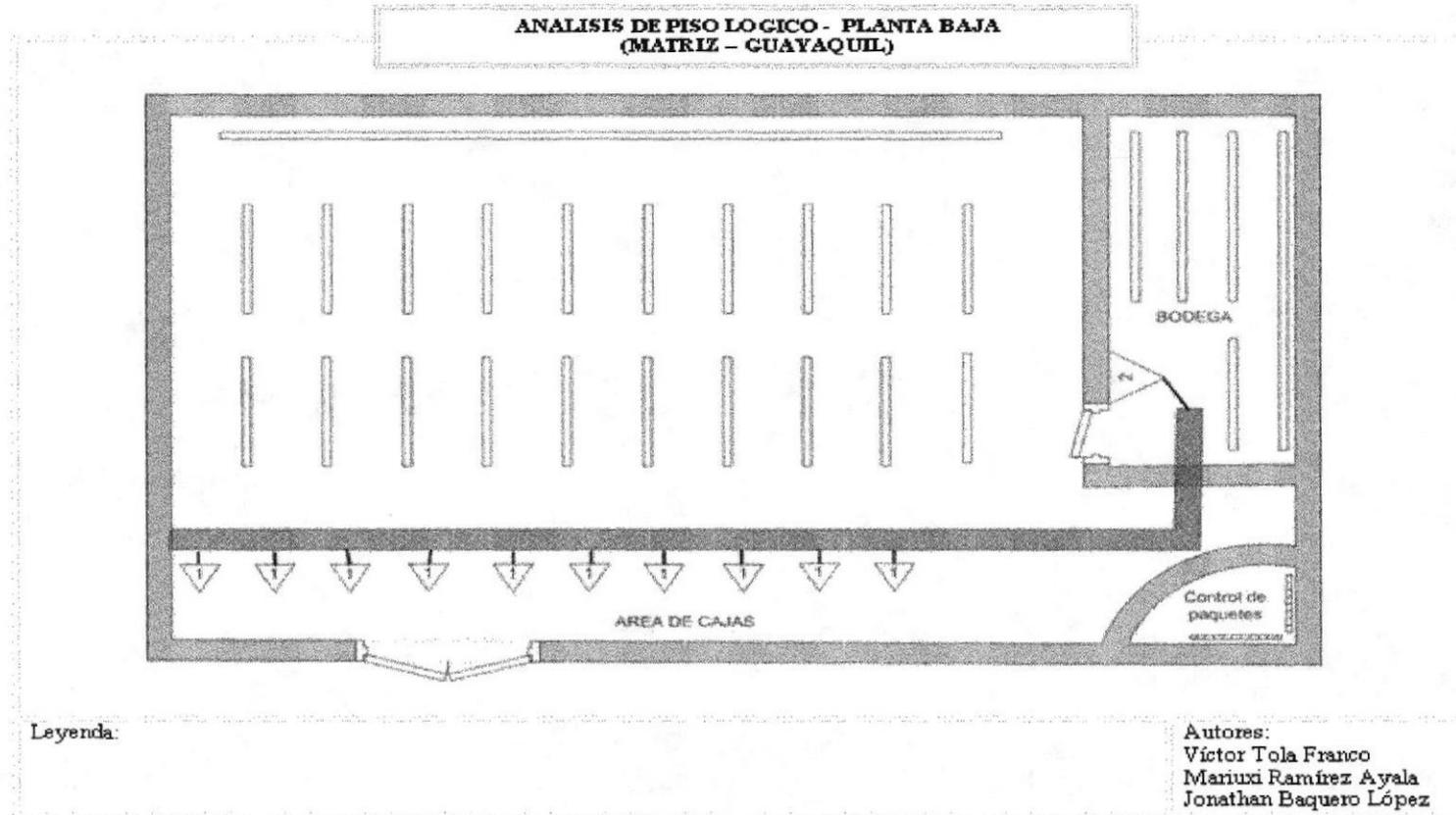


Figura 2-3: Gráfico Análisis de piso Aplicativo Planta Baja - Guayaquil

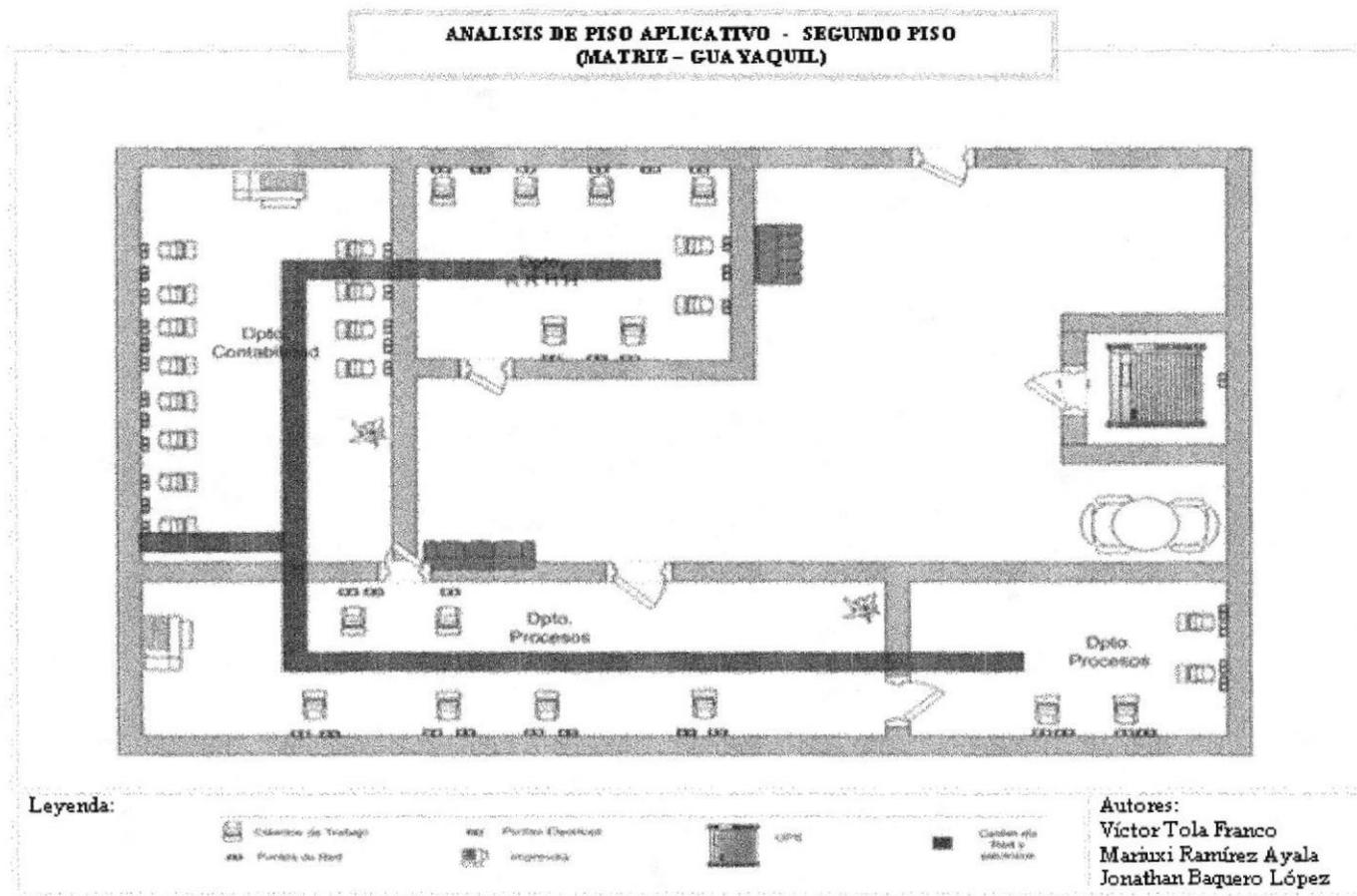


Figura 2-4: Gráfico Análisis de piso Aplicativo Segundo Piso - Guayaquil

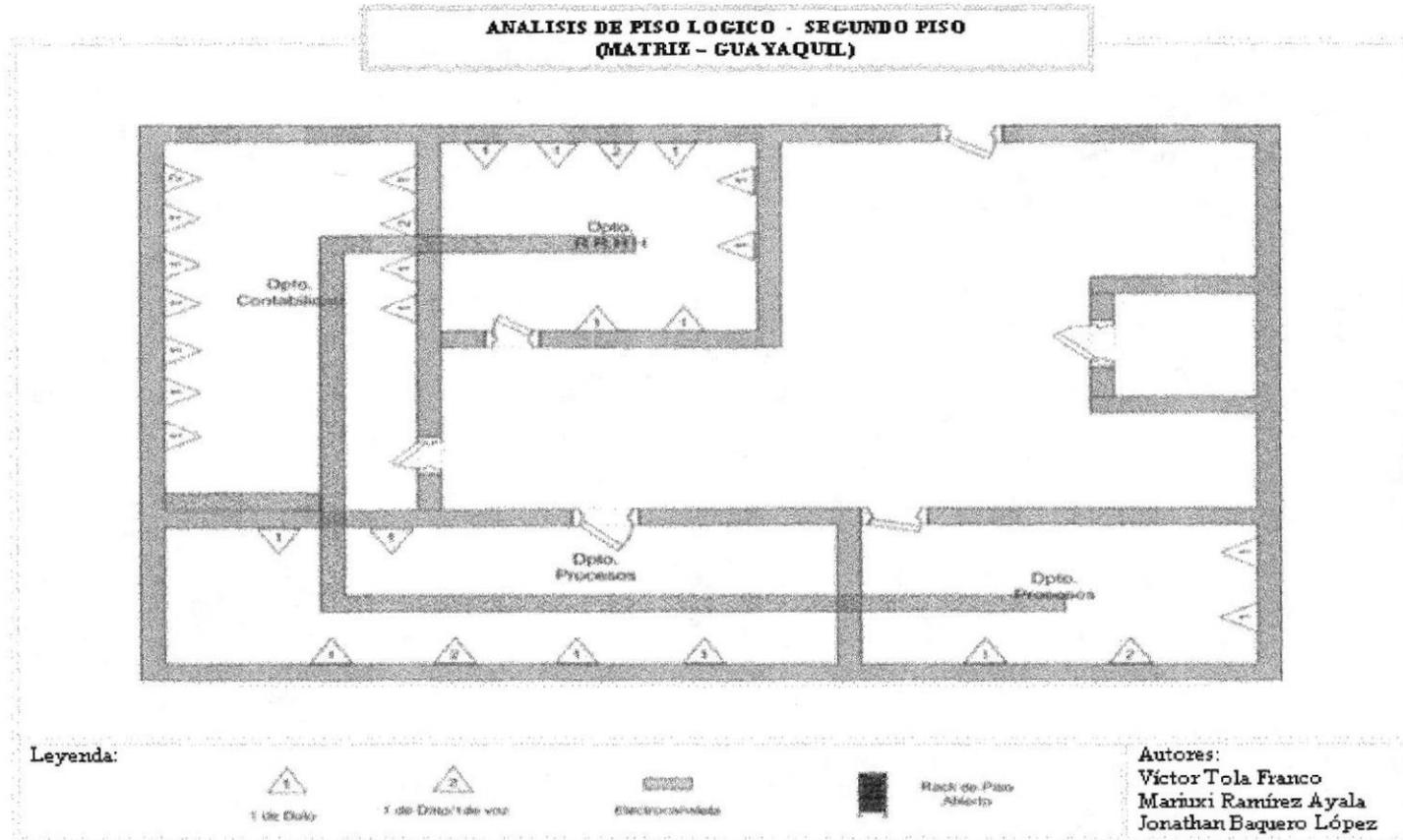


Figura 2-5: Gráfico Análisis de Piso Lógico Segundo Piso - Guayaquil

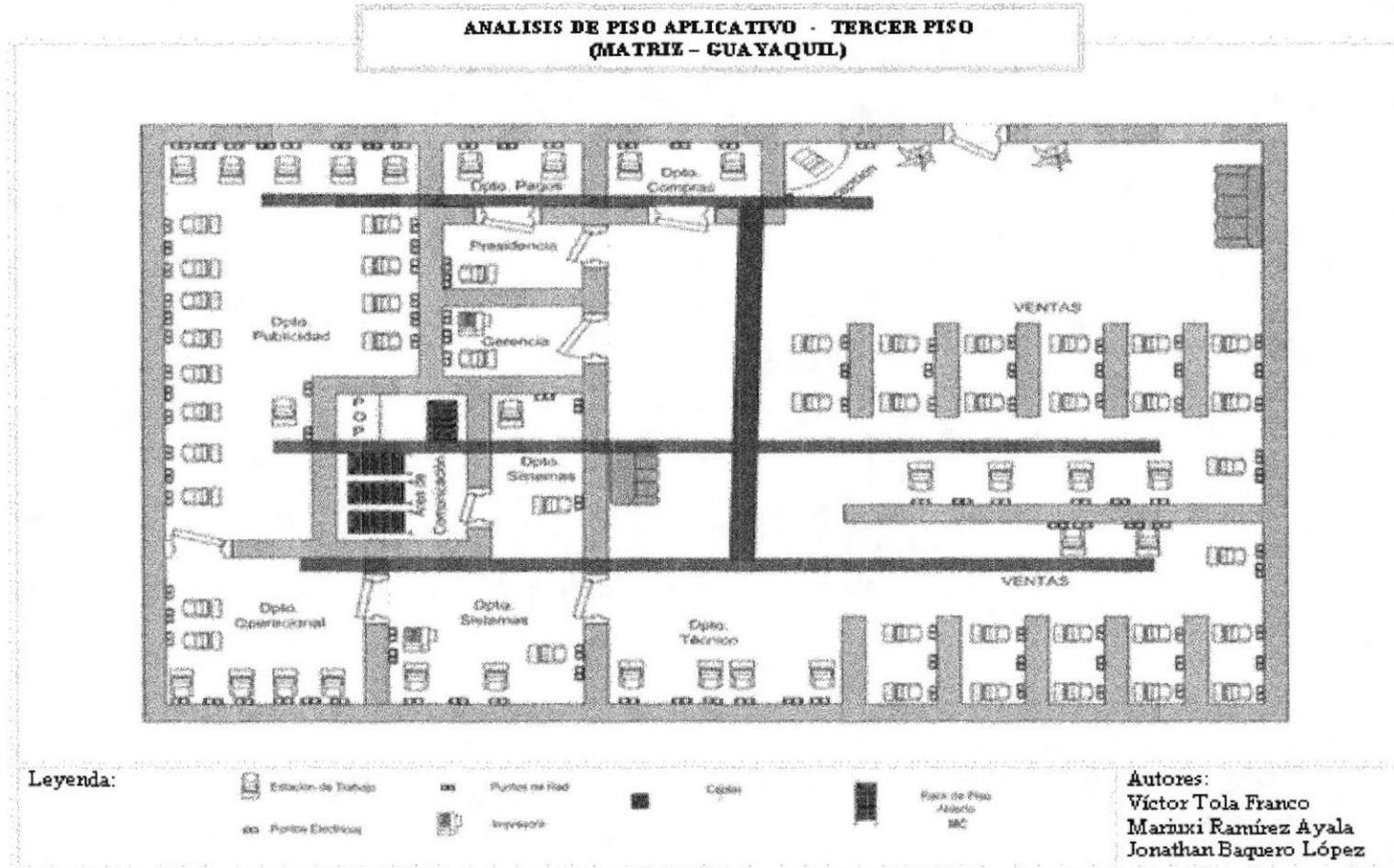


Figura 2-6: Gráfico Análisis de piso Aplicativo Tercer Piso - Guayaquil

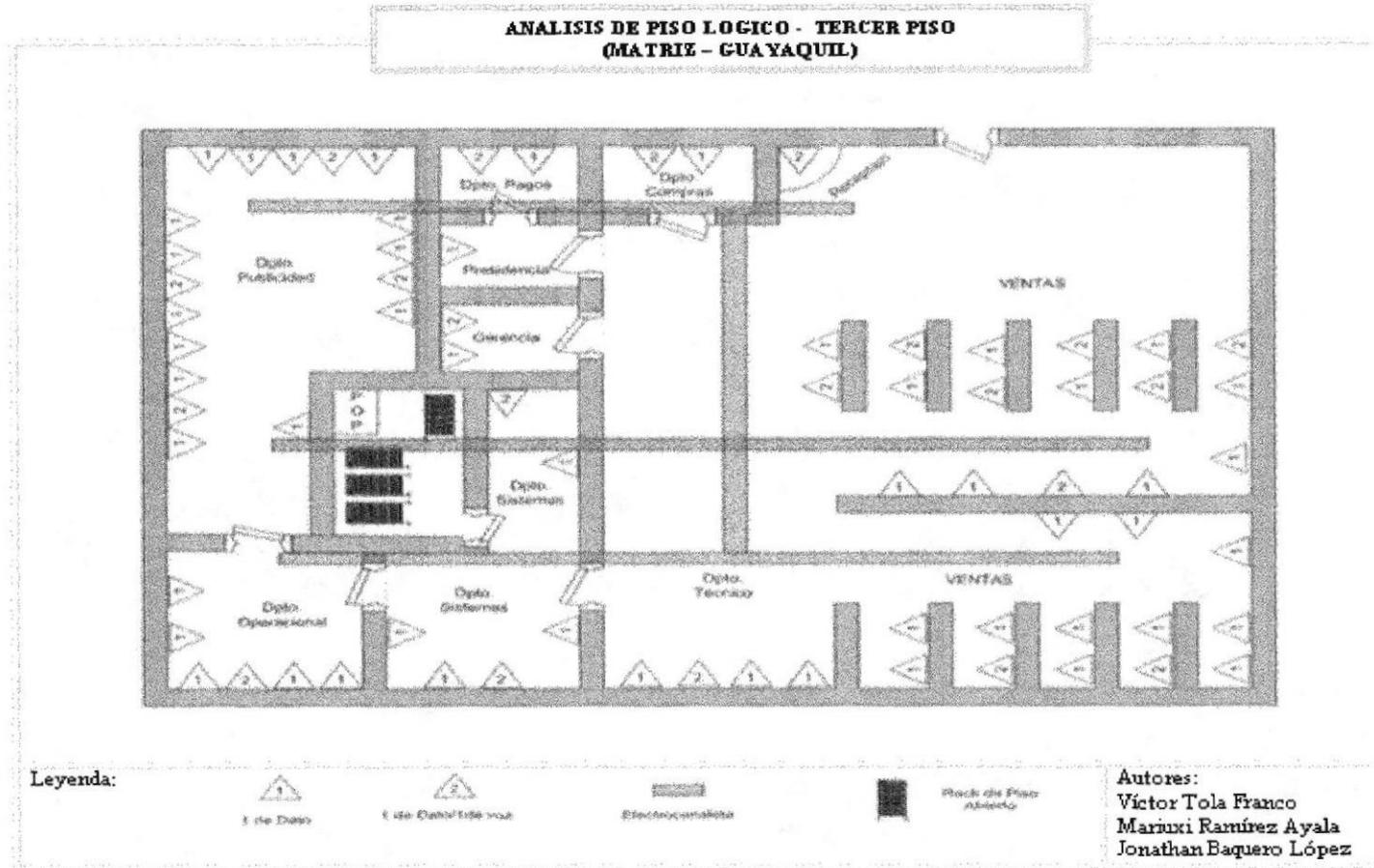


Figura 2-7: Gráfico Análisis de piso Lógico Tercer Piso - Guayaquil

2.2.2.2 MATRIZ - QUITO

Todas las 34 estaciones de trabajo son de marca (HP) poseen las siguientes características:

MARCA	DESCRIPCIÓN	CARACTERÍSTICAS
HP	Estaciones de trabajo (HP MX2000MT)	Procesador: Pentium IV 2.8 GHZ Memoria: 256 MB Disco Duro: 80 GB

Tabla 2-6: Estaciones de trabajo Quito

En el primer piso se encuentra la bodega del local comercial de la matriz.

En el segundo piso se encuentra ubicado el IC, los servidores que hacen de enlace con la Matriz de Guayaquil, tienen un cuarto donde ubican el Rack para distribuir la comunicación, en este piso se encuentran instaladas 20 computadoras distribuidas por departamento de la siguiente manera:

CANTIDAD	UBICACIÓN
5 Maquinas	Compras
1 Maquina	Sistemas
6 Maquinas	RRHH
7 Maquinas	Administración
1 Maquina	Recepción
5 Maquinas	Ventas

Tabla 2-7: Distribución computadoras Quito



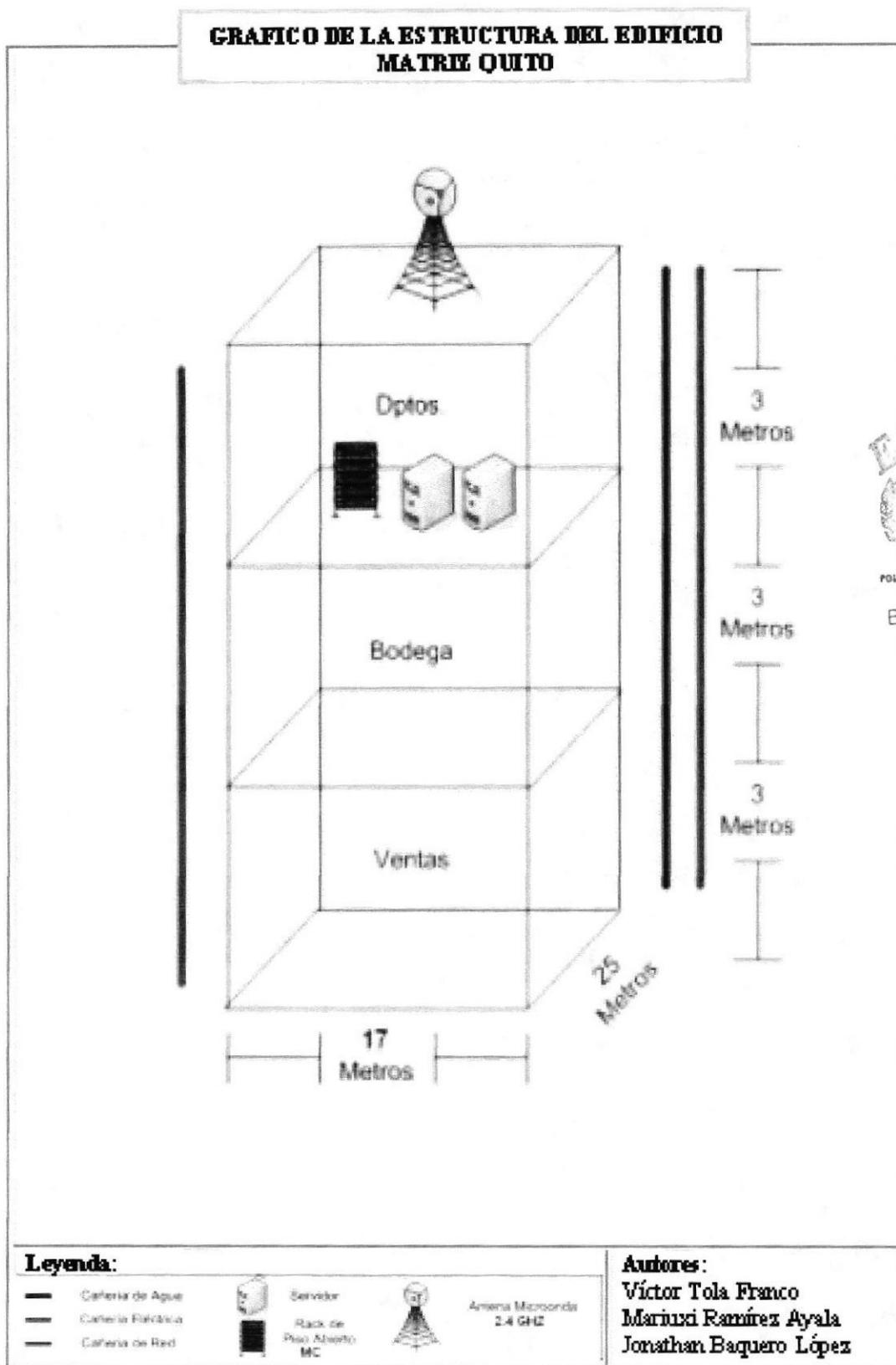
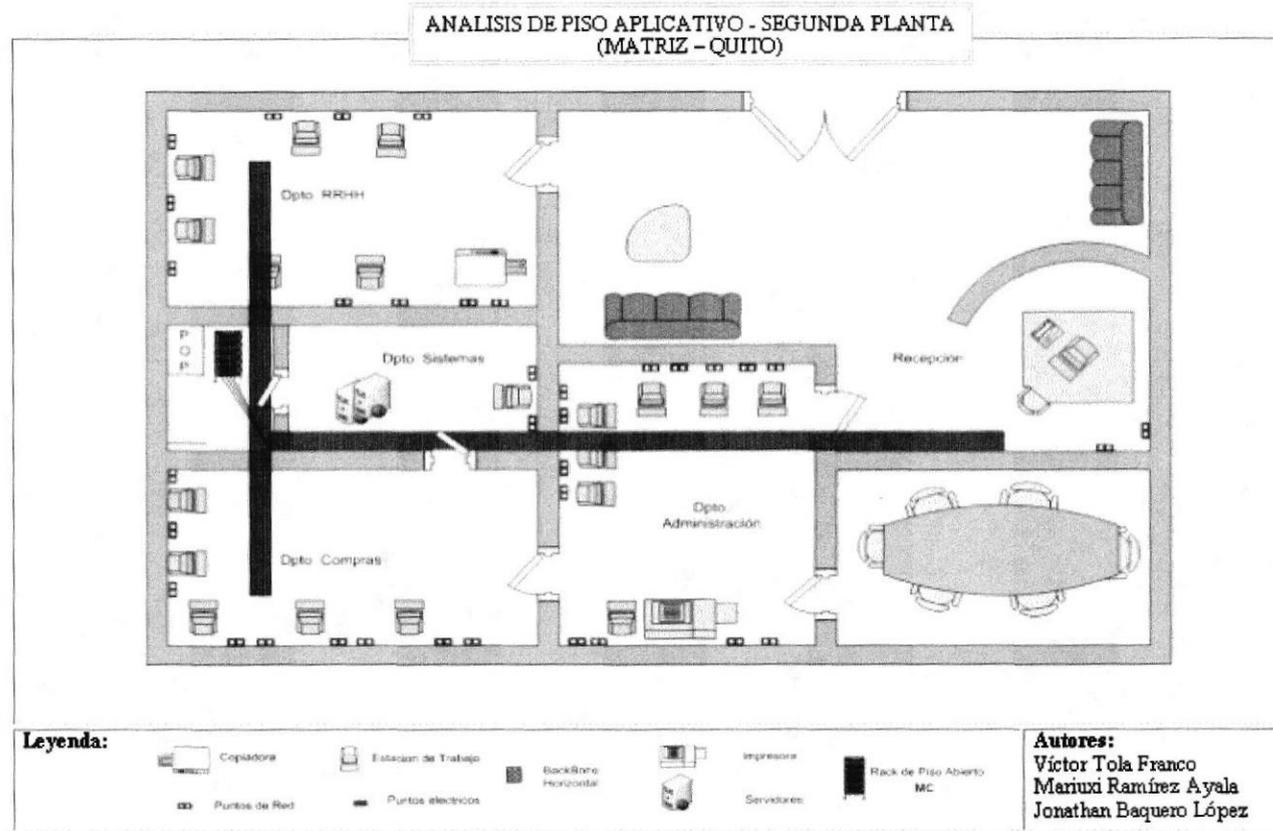


Figura 2-8: Gráfico de la Estructura del Edificio Quito



BIBLIOTECA
CAMPUS
PEÑAS

Figura 2-9: Gráfico Análisis de piso Aplicativo Segundo Piso - Quito

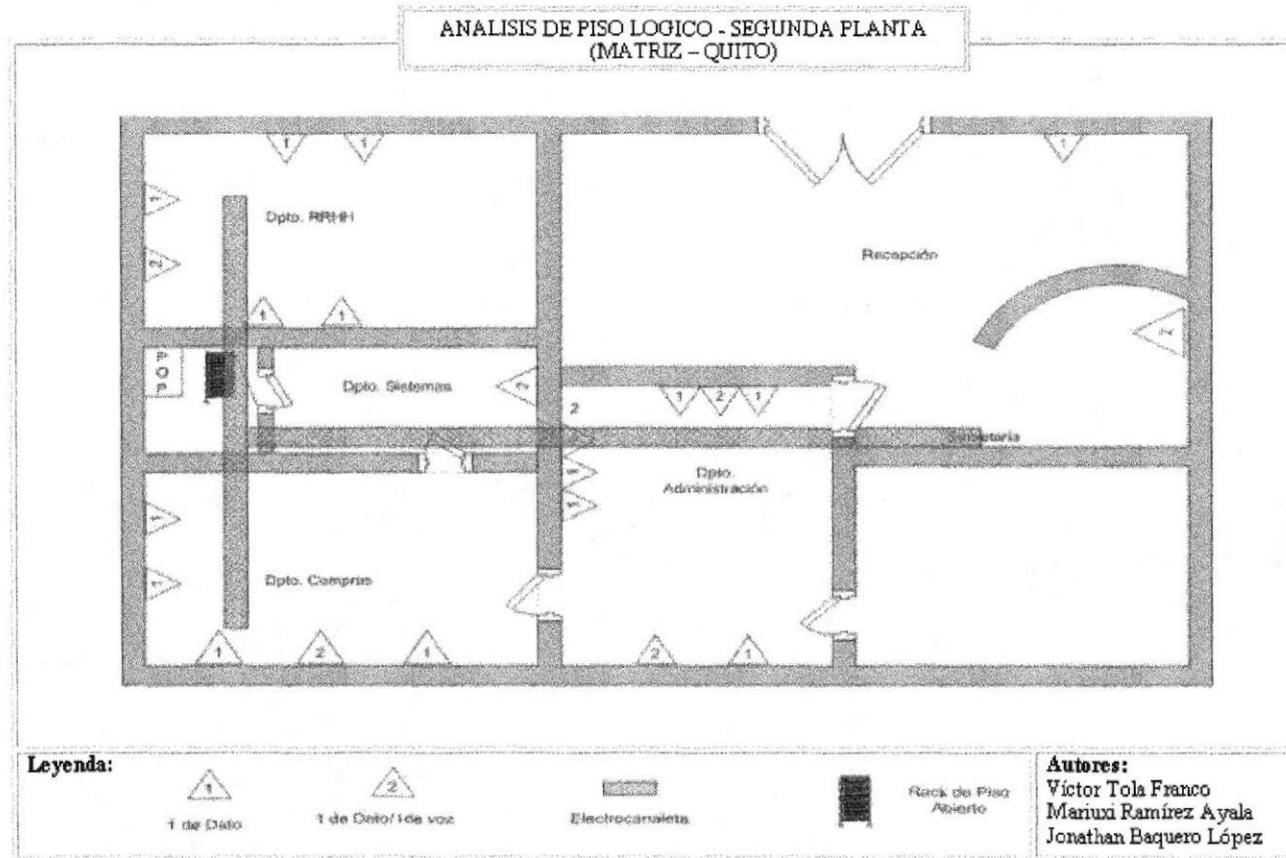


Figura 2-10: Gráfico Análisis de piso Lógico Segundo Piso - Quito



2.2.3 MEDIOS DE COMUNICACIÓN

2.2.3.1 MEDIOS ALAMBRICOS - MATRIZ GUAYAQUIL

Los medios alámbricos utilizados en el edificio matriz de Guayaquil son marca BELDEN distribuidos de la siguiente forma:

- Cable utp categoría 5e para las estaciones de trabajo y servidores a excepción de ciertos puntos antiguos con cable cat 5

2.2.3.2 MEDIOS INALÁMBRICOS - MATRIZ GUAYAQUIL

Los medios inalámbricos utilizados en el edificio matriz Guayaquil son los siguientes:

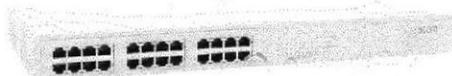
- Una antena de microondas a una frecuencia de 2,4 Ghz

La cual sirve como medio para comunicarse con la matriz Quito, utilizando la empresa porta que les hace de Carrier.



2.2.4 DISPOSITIVOS DE CONMUTACIÓN

MATRIZ GUAYAQUIL Y QUITO



CANT	UBICACIÓN	MARCA	MODELO	DESCRIPCIÓN
6	Tercer piso (Guayaquil)	3COM	4400	<ul style="list-style-type: none"> • Puertos: 24 puertos 10BASE-T/100BASE-TX con auto-detección y auto-configuración.
2	Segundo Piso (Quito)			<ul style="list-style-type: none"> • Interfaces para medios RJ 45 • Funciones de switching Ethernet: Velocidad total

Tabla 2-8: Dispositivo de conmutación

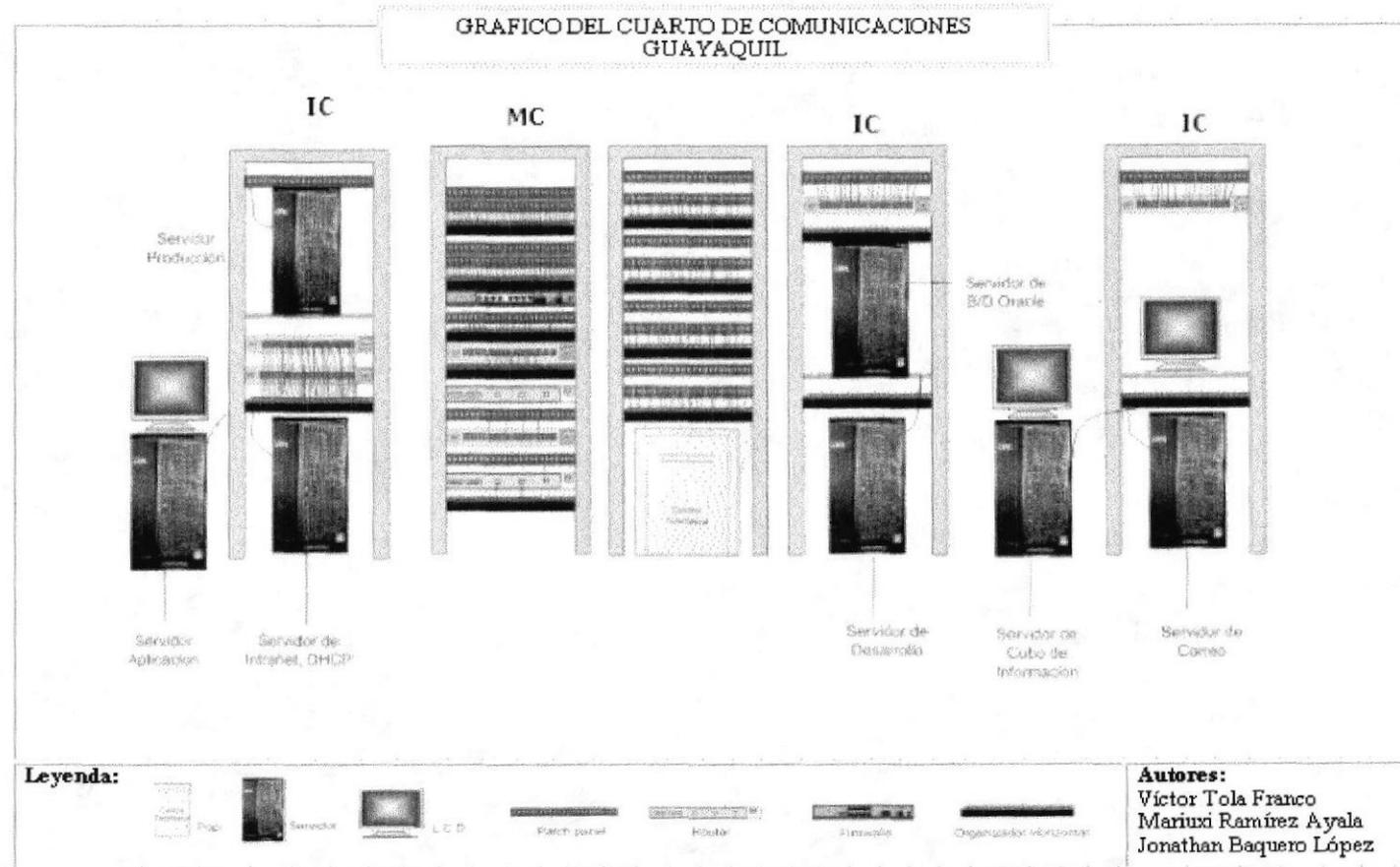


BIBLIOTECA
CAMPUS
PEÑAS

2.2.5 CENTRO DE DISTRIBUCION PRINCIPAL MC e IC

En la matriz de Guayaquil en el tercer piso está su IC y MC para la comunicación de sucursales y matrices (Quito – Guayaquil) además cuentan con sus switches, routers y el pop (ALCATEL), FIREWALL (Físico) y servidores.





ESPOL
POLITECNICO DEL LITORAL
BIBLIOTECA
CAMPUS
PENAS

Figura 2-11: Gráfico Cuarto de Comunicaciones Guayaquil

CENTRO DE DISTRIBUCIÓN PRINCIPAL (MC)

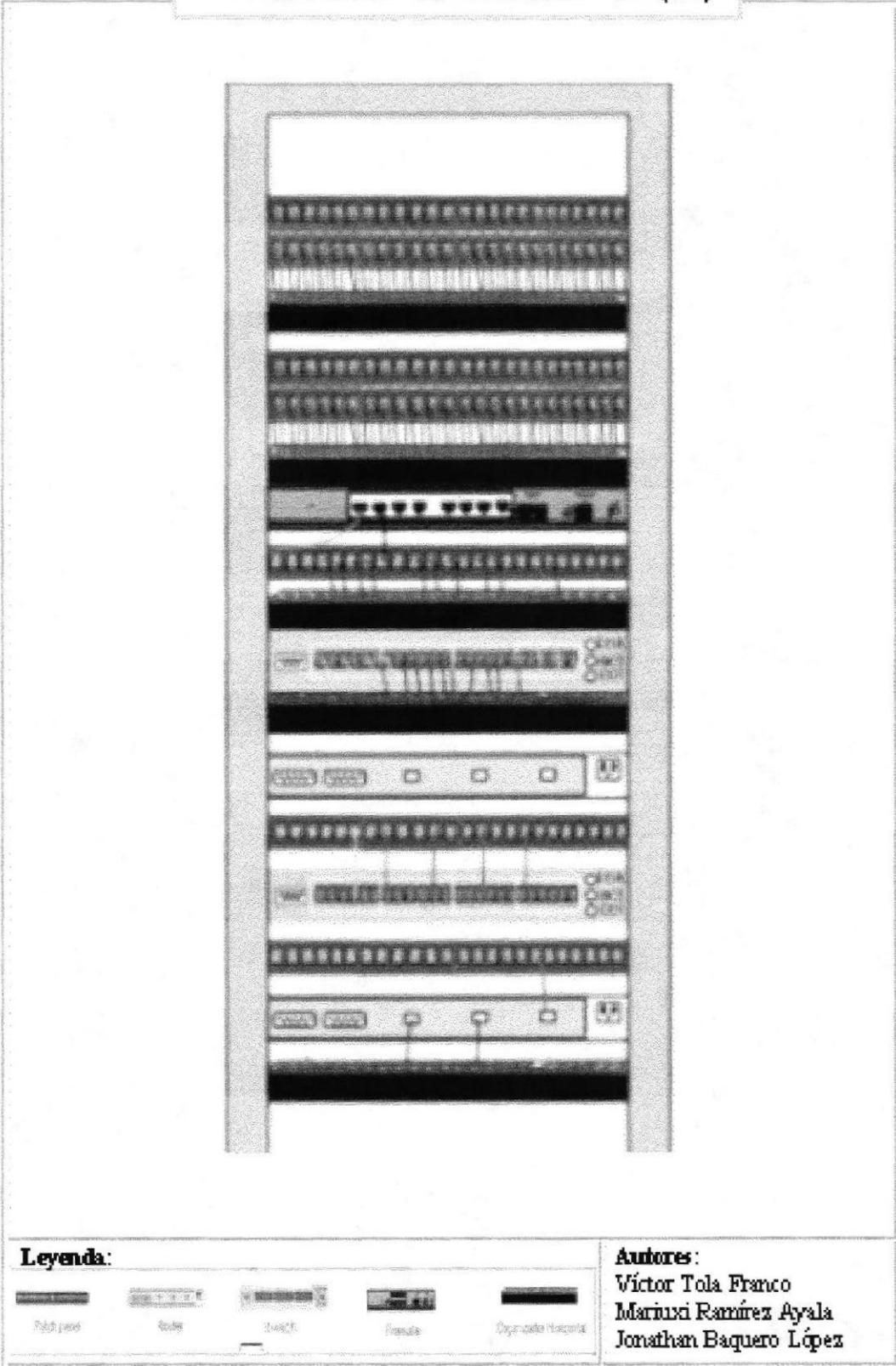


Figura 2-12: Gráfico Centro de Distribución Principal

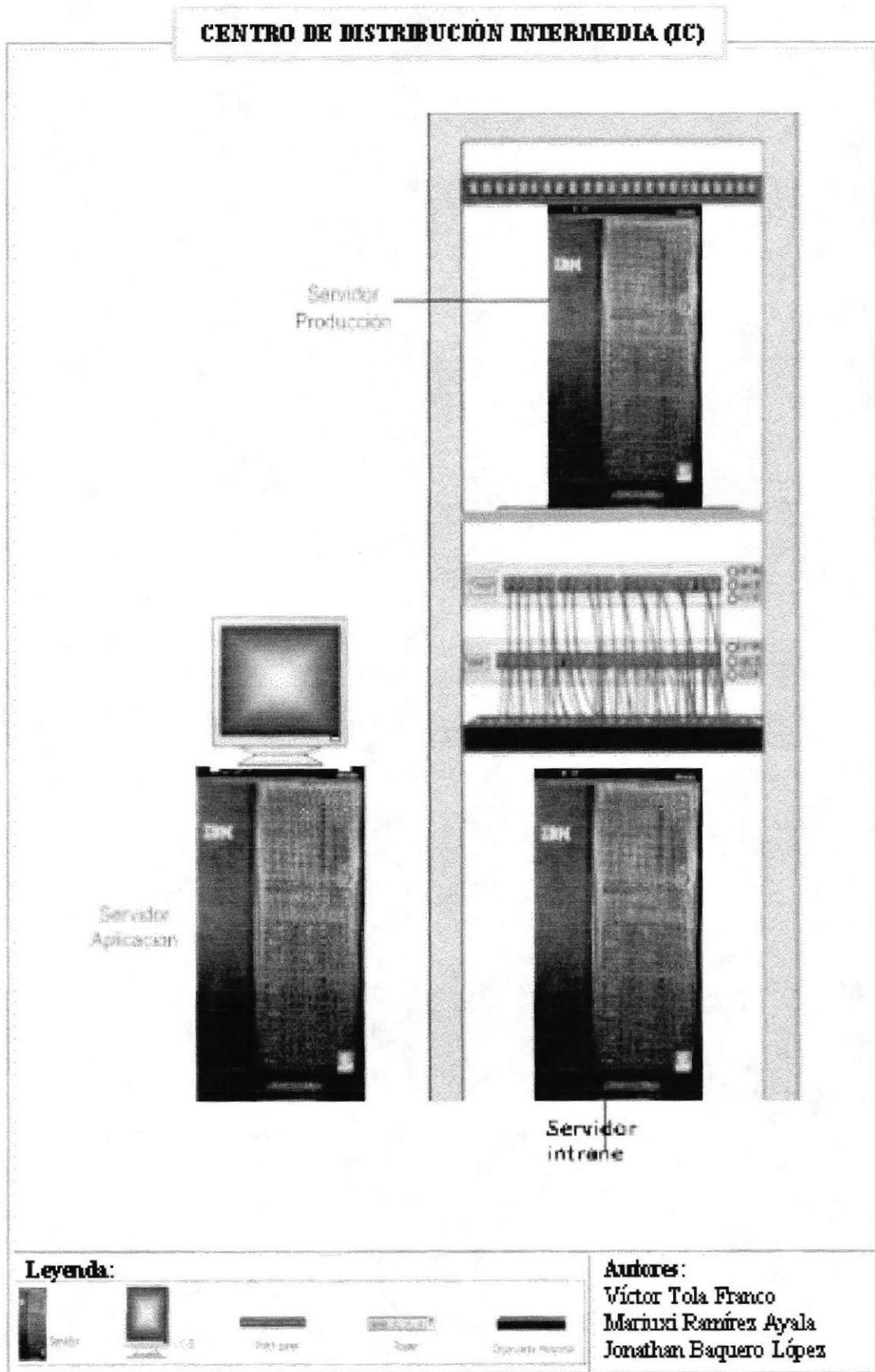


Figura 2-13: Gráfico Centro de Distribución Intermedia

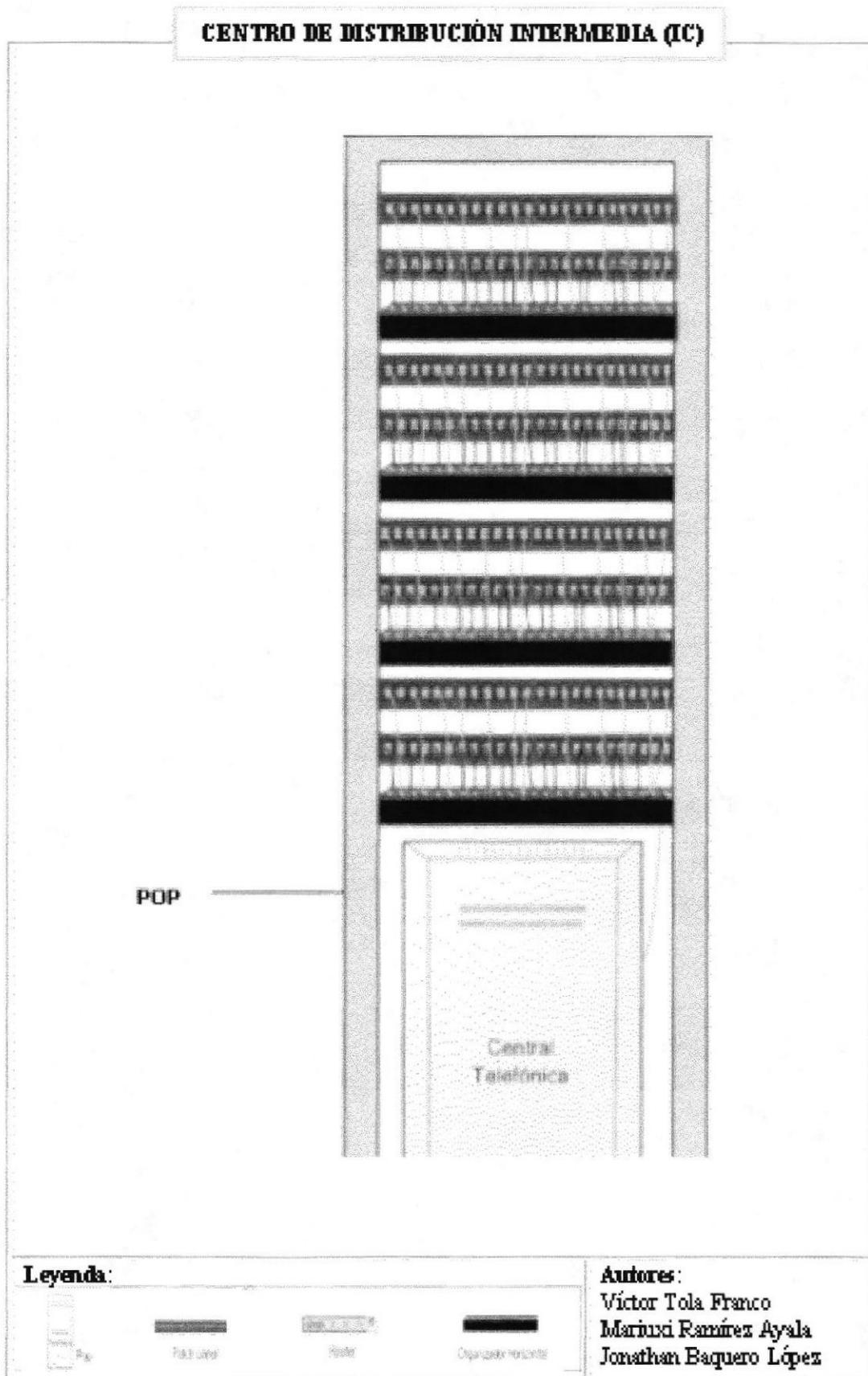


Figura 2-14: Gráfico Centro de Distribución Principal

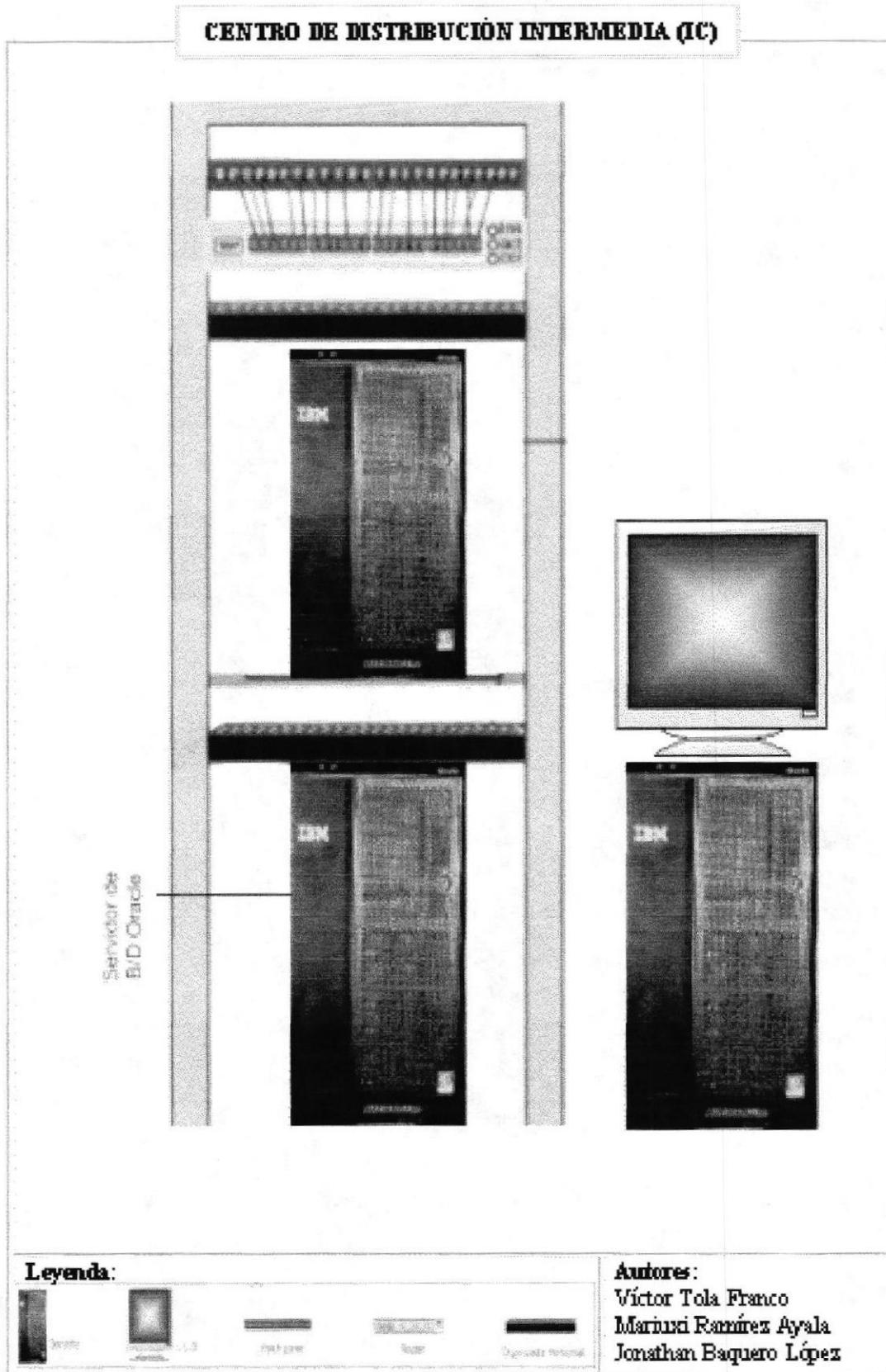
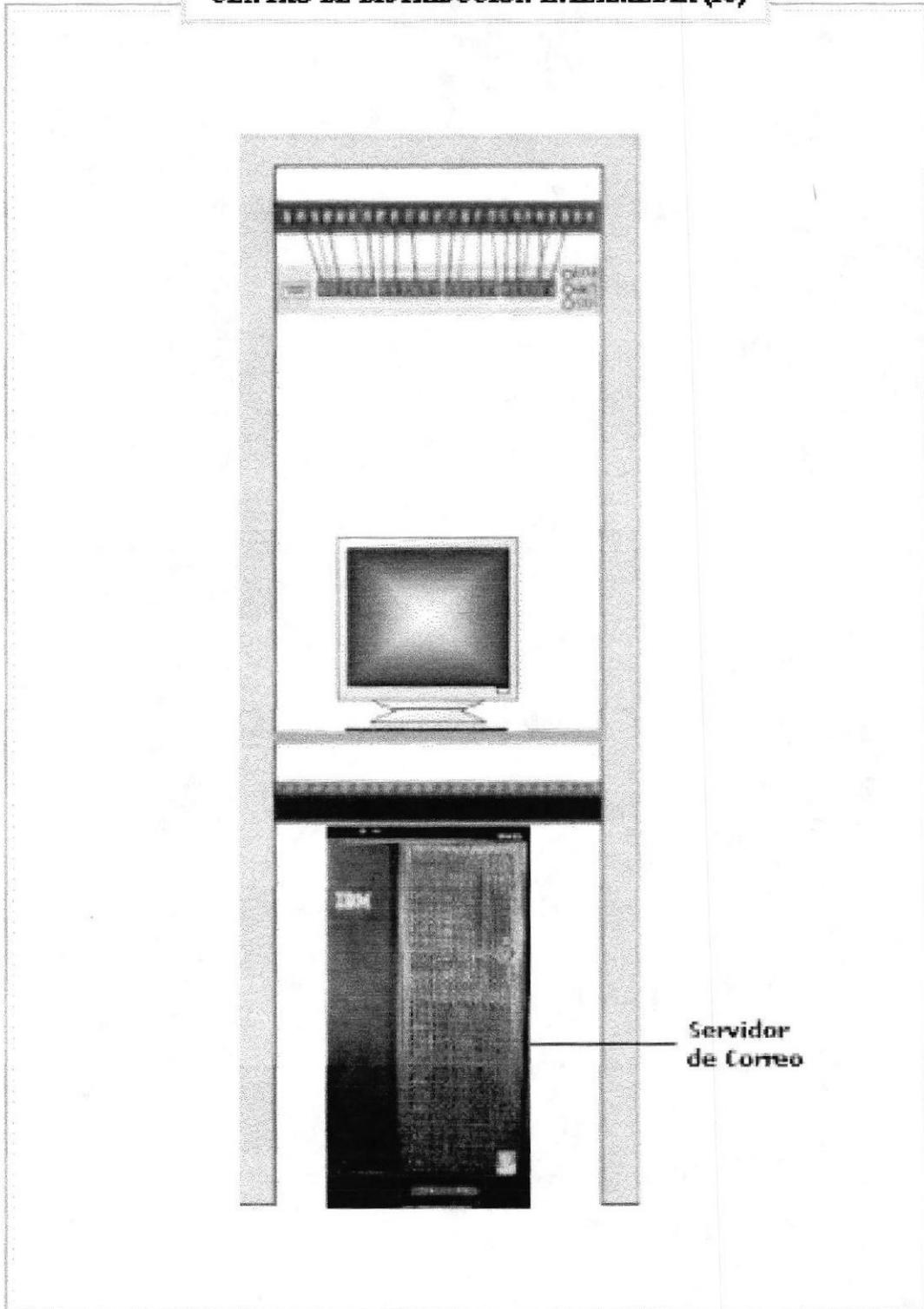


Figura 2-15: Gráfico Centro de Distribución Intermedia

CENTRO DE DISTRIBUCIÓN INTERMEDIA (IC)



Leyenda:



Autores:

Víctor Tola Franco
Mariuxi Ramírez Ayala
Jonathan Baquero López

Figura 2-16: Gráfico Centro de Distribución Intermedia

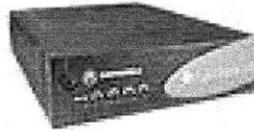
2.2.6 INFRAESTRUCTURA WAN

DISPOSITIVOS DE ENRUTAMIENTOS

Porta, TVCable, Andina datos, Distelcom y Telconet son las empresas que le proveen el servicio de comunicación de datos y enlace de Internet, Telconet es el proveedor de Internet de TIA. Cada una de estas empresas tiene sus propias tecnologías, además de prestar sus propios equipos, de acuerdo a su infraestructura dan el soporte que sea requerido.

Mantiene un ancho de banda entre Guayaquil – Quito de 512 kbps para datos.

ROUTERS



CANT	UBICACIÓN	MARCA	MODELO	DESCRIPCION
1	Tercer piso (Guayaquil)	Motorota Vanguard	320	<ul style="list-style-type: none"> • Puede ser usado para recuperar la conexión de fallo
1	Segundo Piso (Quito)			<ul style="list-style-type: none"> • Integración de voz con tráfico de datos.

Tabla 2-9: Dispositivo de enrutamiento

2.12 SEGURIDADES

En la empresa todas las seguridades las realizan a través de un FIREWALL físico.

- No tienen implementadas políticas para computadores protegidos con contraseñas
- La navegación en Internet es libre sin restricciones.



DESCRIPCION DE FIREWALL

UBICACIÓN	MARCA	MODELO	DESCRIPCION
Guayaquil	Firebox	Firebox V60L	<ul style="list-style-type: none"> • Protección firewall • Soporte de DHCP de NAT, VPN, ARP, LDAP, • soporte VLAN, limitación de tráfico. • filtrado de paquetes, activable. • Capacidad del cortafuegos : 100 Mbps

Tabla 2-10: Descripción Firewalle



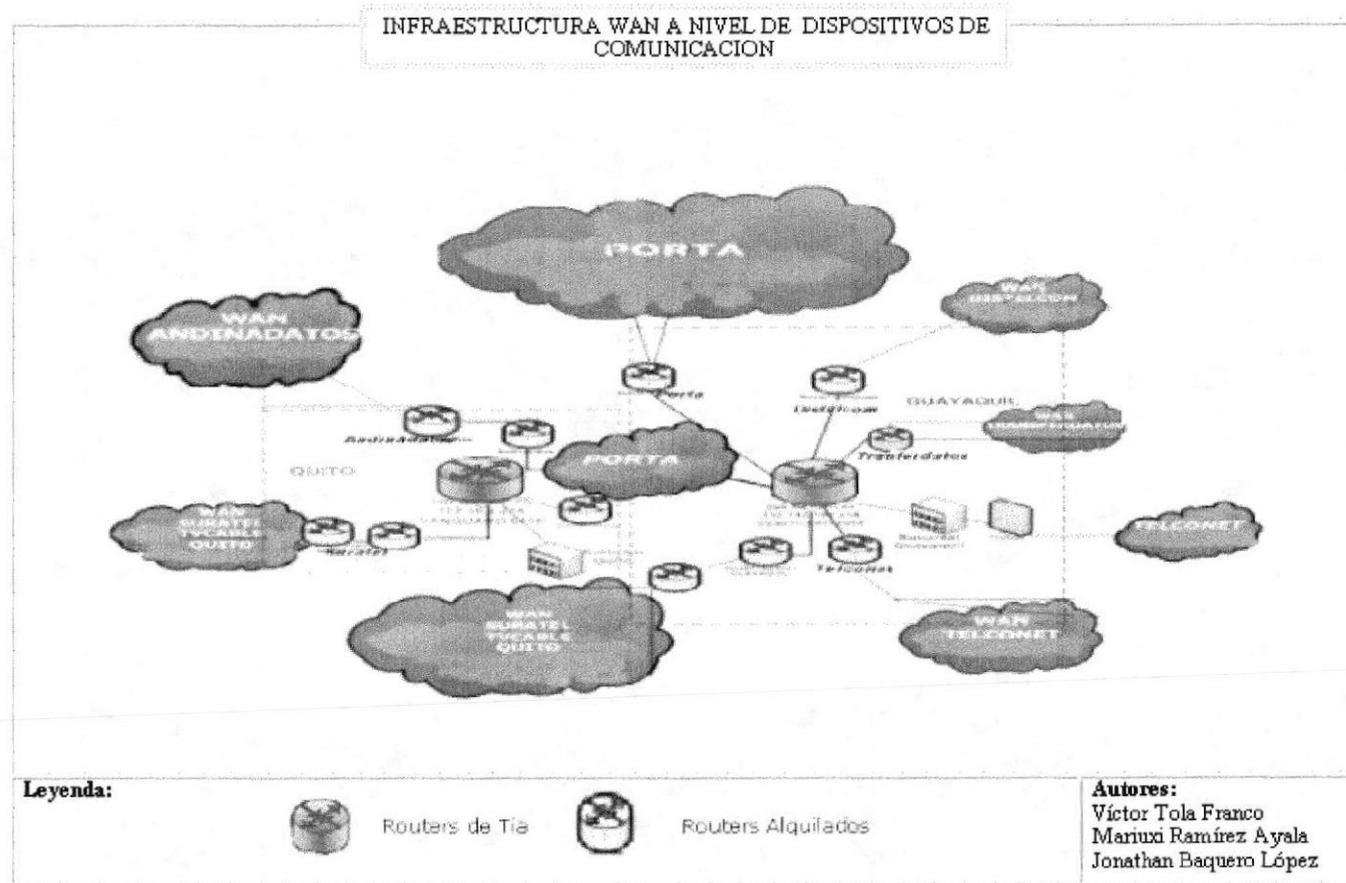


Figura 2-17: Gráfico Infraestructura Wan a Nivel de Dispositivos

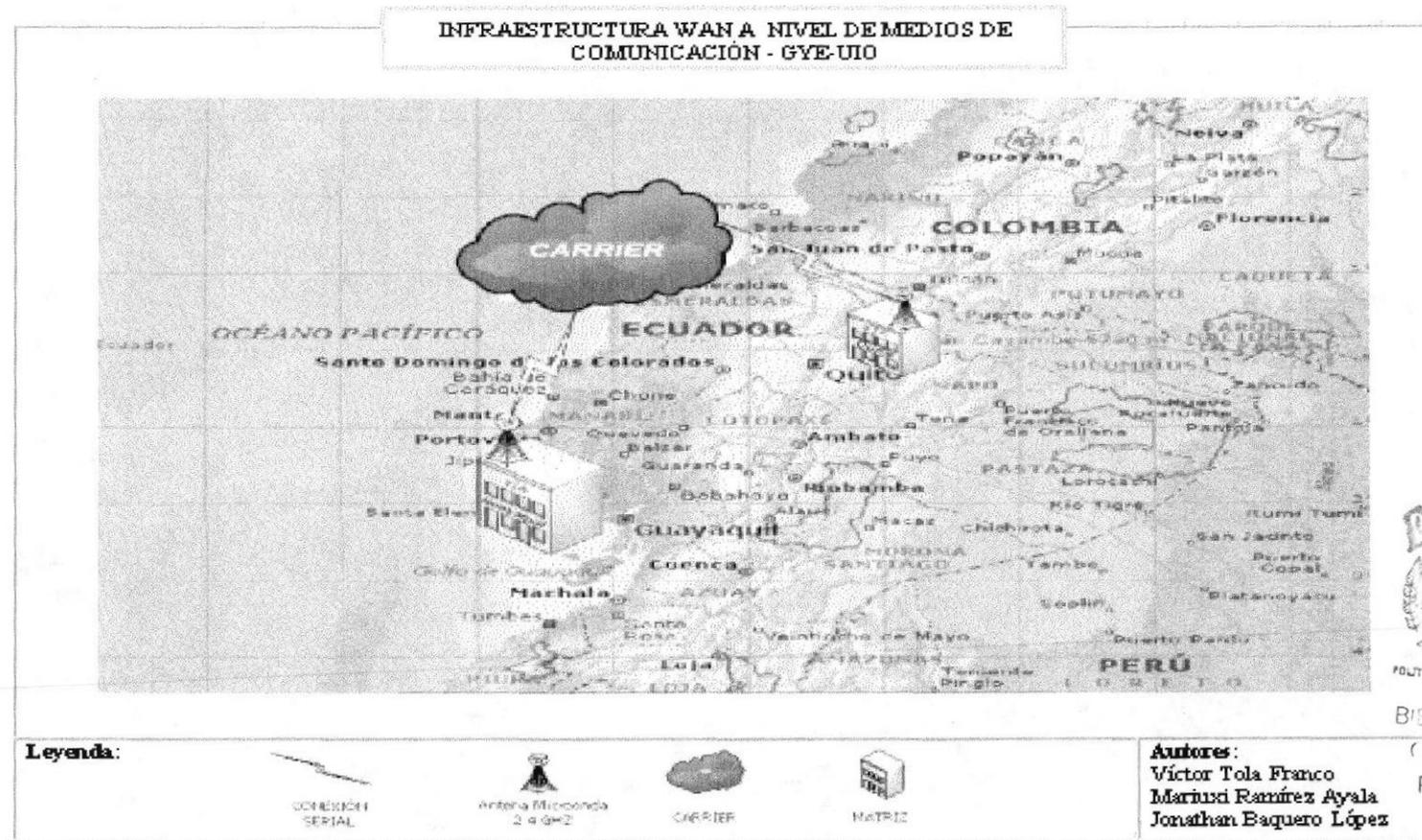


Figura 2-18: Gráfico Infraestructura Wan a Nivel de Dispositivos

2.2.7 ANCHO DE BANDA

GUAYAQUIL EDIFICIO MATRIZ

ANCHO DE BANDA	MEDIO
1 Mbps	Línea dedicada

Tabla 2-11: Ancho de Banda Guayaquil

QUITO EDIFICIO MATRIZ

ANCHO DE BANDA	MEDIO
128 Kbps.	Línea dedicada

Tabla 2-12: Ancho de Banda Quito



BIBLIOTECA
CAMPUS
PEÑAS

2.2.8 PROBLEMAS ENCONTRADOS

- **No poseen normas de cableado estructurado en la red Lan**
- **Saturación en su red LAN**
- **No cuentan con un servidor Proxy**





CAPÍTULO 3
SOLUCIÓN
PROPUESTA



BIBLIOTECA
CAMPUS
PEÑAS

3 SOLUCIÓN PROPUESTA

3.1 PROBLEMAS, CAUSA Y EFECTO

Los problemas encontrados después del análisis realizado serán descritos y detallados a continuación:

PROBLEMA	CAUSA	EFECTO
No poseen normas de cableado estructurado en la red Lan	<ul style="list-style-type: none"> ▪ Falta de conocimiento por parte del departamento técnico. ▪ Descuido por parte de la empresa.(Directivos). 	<ul style="list-style-type: none"> ▪ Dificultad al momento de solucionar un problema en la red.(cables) ▪ No cuentan con protección ante siniestros.
Saturación en su red LAN	<ul style="list-style-type: none"> ▪ No hay redes segmentadas. ▪ Mala administración por parte del encargado de la red 	<ul style="list-style-type: none"> ▪ Colisión al momento de acceder a los recursos de la red, forzando el reenvío de paquetes.
No cuentan con un servidor Proxy	<ul style="list-style-type: none"> ▪ El Internet es administrado por un firewall físico 	<ul style="list-style-type: none"> ▪ Libre navegación en Internet. ▪ No existe control sobre los sitios visitados, ni restricción sobre ellos.

Tabla 3-1: Problema, Causa y efecto



3.2 PROBLEMAS, SOLUCIÓN Y ALCANCE

PROBLEMA	SOLUCIÓN	ALCANCE
No poseen normas de cableado estructurado en la red Lan	<ul style="list-style-type: none"> • Realizar un nuevo cableado estructurado conforme a las normas para categoría 6. 	<ul style="list-style-type: none"> ▪ Garantizar un alto desempeño de los recursos de la red LAN (equipos de comunicación y computadores). ▪ Prever el futuro crecimiento de equipos en la red LAN. ▪ Facilidad de mantenimiento, detección y corrección de errores.
Saturación en su red LAN	<ul style="list-style-type: none"> ▪ Segmentar las redes por área de trabajo. ▪ Verificar las cascadas de los switches e implementar políticas de administración de la red. 	<ul style="list-style-type: none"> ▪ Mejorar los tiempos de respuestas. ▪ Control de colisiones al tener una administración sobre cada equipo.
No cuentan con un servidor Proxy	<ul style="list-style-type: none"> ▪ Adquirir y Configurar un equipo para las funciones de Proxy 	<ul style="list-style-type: none"> ▪ Las páginas visitadas serán guardadas en el registro del servidor. ▪ Restricciones en la navegación

Tabla 3-2: Problema, Solución, Alcance



3.3 ESTUDIO DE FACTIBILIDAD - MATRIZ GUAYAQUIL

3.3.1 ALTERNATIVA "A"

Se realizará la implementación del cableado estructurado, esto abarca el cambio de categorías de cables en toda la empresa, la que actualmente consta con la categoría 5 y 5e, estos pasarán a ser de categoría 6 operando con los actuales computadores a 1000 Mbps y con los actuales equipos de comunicación operando a las mismas velocidades. Previo a la instalación de tarjetas de red y equipos de comunicación que operen a 1000 Mbps, manteniendo una velocidad integral en toda la red lan.

Otro punto que abarca la implementación del cableado estructurado es el rotulado de los cables, estos tendrán identificaciones y numeraciones para identificar los cables de cada departamento. También se implementarán los respectivos electros canaletas en los pisos de la matriz de Guayaquil, para proteger los cables de agentes varios y perturbaciones que afectan al medio de comunicación.

Se adquirirá un computador de Marca que hará las funciones de servidor Proxy que encargará de compartir el Internet y se pondrá las debidas políticas para navegación, el cual trabajara con el sistema Operativo Linux.



BIBLIOTECA
CAMPUS
PEÑAS

3.3.1.1 FACTIBILIDAD TÉCNICA

ALTERNATIVA "A"

CANT	DESCRIPCIÓN	UBICACIÓN
1	EQUIPO PROXY (Marca) Procesador de doble núcleo *INTEL 1 GB Ram, 2 Disco 160 GB 2 Tarjetas de red Gigabit	Departamento de sistema
18 Bobinas	Cable utp cat 6 Signamax 105 puntos de red y 105 de voz	Edificio matriz (Guayaquil)
210	Patch Cord cat 6 de 1m	Edificio matriz (Guayaquil)
105	Patch Cord cat 6 de 3m	Edificio matriz (Guayaquil)
18	Patch panel cat 6	Edificio matriz (Guayaquil)
210	Jacks cat 6 Signamax	Edificio matriz (Guayaquil)
105	Face Plate de 2puertos servicios Signamax	Edificio matriz (Guayaquil)
105	Cajas sobre puestas	Edificio matriz (Guayaquil)
75	Electro canales metálicos con tapa de 25x15 cm	Edificio matriz (Guayaquil)
2	Paquetes de amarras plásticas de 15 y 30cm	Edificio matriz (Guayaquil)
3	Paquetes de etiquetas	Edificio matriz (Guayaquil)
100 m	Tubería EMT 1"	Edificio matriz (Guayaquil)
50	Grapas EMT 1"	Edificio matriz (Guayaquil)
1	Materiales Varios Tornillos, Tacos Fisher, conectores EMT 1"	Edificio matriz (Guayaquil)
45	Canaletas 40x25 Decorativas de 2m	Edificio matriz (Guayaquil)
30	Canaletas 24x12 Decorativas de 2m	Edificio matriz (Guayaquil)

Tabla 3-3: Factibilidad técnica



3.3.1.2 FACTIBILIDAD ECONÓMICA

COSTOS DE HARDWARE

CANT	DESCRIPCIÓN	COSTO TOTAL
1	EQUIPO PROXY (Marca) Que soporte RAID 0 y 1 Procesador de doble núcleo de preferencia INTEL 1 GB Ram 2 Disco 160 GB 2 Tarjetas de red Gigabit	\$ 1300.00
6	Switch AT-GS950/24 Allied Telesis	2553.60
93	Tarjetas de red 10/100/1000 Mbps	\$ 1395.00
		\$ 5248,60

Tabla 3-4: Factibilidad Económica Hardware



BIBLIOTECA
CAMPUS
PEÑAS

MATERIALES PARA CABLEADO ESTRUCTURADO		
CANT.	DESCRIPCIÓN	TOTAL
18 Bobinas	Cable utp cat 6 Signamax 105 puntos de red	3443.40
210	Patch Cord 1m	1528.80
105	Patch Cord 3m	963.90
105	Jacks cat 6 Signamax	648,90
18	Patch Panel Sólido Cat 6 Marca Signamax 24 puertos	3322.26
6	Organizadores Horizontales 2UR	0
105	Face Plate de 2 puertos de servicios Signamax	164,64
105	Cajas sobre puestas	176,16
1	Gabinete de Pared Panorámico 10 UR	200.00
75	Electro canales metálicos con tapa de 25x15 cm	1125.00
50	Tubería EMT 1"	353.00
50	Grapas EMT 1"	5.00
2	Materiales Varios Tornillos, Tacos Fisher, conectores EMT 1" Paquetes de amarras plásticas de 15 y 30cm, Paquetes de etiquetas, ángulos interno externo y plano	300.00
45	Canaletas 40x25 Decorativas de 2m	196.65
30	Canaletas 24x12 Decorativas de 2m	33.60
TOTAL MATERIALES PARA CABLEADO ESTRUCTURADO		12,461.10

Tabla 3-5: Factibilidad Económica Materiales



COSTOS DE SOFTWARE

CANT.	DESCRIPCIÓN	COSTOS UNITARIOS	COSTO TOTAL
1	PAQUETE DE LINUX RED HAT 9.0 Licencia	70.00	70.00
TOTAL COSTO DE SOFTWARE			\$ 70.00

Tabla 3-6: Factibilidad Económica Software



BIBLIOTECA
CAMPUS
PEÑAS

3.3.1.3 FACTIBILIDAD OPERATIVA

FASES	SEMANAS
ANÁLISIS DE CABLEADO ESTRUCTURADO *Grupo de trabajo 1 Técnico de redes	2.5
DISEÑO DE LA RED LAN Grupo de trabajo	1.5
IMPLEMENTACIÓN DEL CABLEADO ESTRUCTURADO * Grupo de trabajo 1 Técnicos en Redes 4 Ayudantes	3.5
PRUEBA DE LA RED LAN *Grupo de trabajo 3 Técnicos en redes	2.5
DOCUMENTACIÓN Y CERTIFICACION DE LA RED LAN *Grupo de trabajo Empresa certificadora	1

Tabla 3-7: Factibilidad Operativa

* **EL GRUPO DE TRABAJO**_ Son los estudiantes que elaboran la propuesta para la empresa "TIA"



COSTOS OPERATIVOS

FASES	SEMANAS	COSTO SEMANA	COSTO TOTAL	COSTO FASE
DISEÑO DE LA RED LAN				
Grupo de trabajo	1.5	200.00		
TOTAL DE LA FASE DE DISEÑO				300.00
IMPLEMENTACIÓN DE LA RED LAN (Construcción)				
Grupo de trabajo		300.00		1050.00
1 Técnicos de Redes	3.5	150.00		525.00
4 Ayudantes		75.00		262.50
TOTAL DE LA FASE DE IMPLEMENTACION				1837.50
PRUEBA DE LA RED LAN				
Grupo de trabajo	2.5	300.00		750.00
1 Técnico de Redes		150.00		375.00
TOTAL DE LA FASE DE PRUEBA DE LA RED				1125.00
DOCUMENTACION DE LA RED LAN				
Grupo de trabajo	1	200.00		200.00
TOTAL DE LA FASE DE DOCUMENTACION				200.00
TOTAL DE COSTOS OPERATIVOS				\$ 3462.50

Tabla 3-8: Costos operativos

3.3.1.4 COSTO TOTAL DE LA ALTERNATIVA "A"

En el costo total de la propuesta están incluidos los siguientes valores:

DESCRIPCIÓN	COSTO
Costo De Materiales	\$17709.70
Costo Software	\$ 70.00
Costos de Mano de Obra	\$3462.50
COSTO TOTAL DE LA PROPUESTA	\$ 21242,20

I.V.A.	12 %	\$ 2549.06
--------	------	------------

Tabla 3-9: Factibilidad Económica Hardware

COSTO TOTAL DE LA ALTERNATIVA "A" \$ 23,791.20



3.3.1.5 VENTAJAS

Cableado Estructurado:

- Flexibilidad de Mantenimiento, crecimiento y migración de puestos de trabajos.
- Fácil administración de la red LAN.
- Alta disponibilidad de los recursos en red debido a la alta velocidad de operación de la misma (1Gbps)
- Certificación de la Red incluida con el cableado estructurado, conforme a todas las normas para certificación de medios y equipos
- Control de colisiones (al segmentar la red)

Servidor Proxy

- En la adquisición del servidor Proxy al ser de marca, se contará con una confiabilidad mayor debido a la garantía y soporte que ofrece el proveedor del equipo y se garantiza el mayor desempeño posible sobre él.
- Al tener un arreglo de discos RAID 1, se tiene una protección ante fallos mecánicos de los discos duros y se baja el tiempo de inactividad del servidor PROXY.
- Control de navegación y restricción de accesos no permitidos.
- Bloqueo de puertos. Ejemplo (Restringir Messenger)
- Almacenamiento de páginas visitadas en cache (Agilidad para navegación)

3.3.1.6 BENEFICIOS

- Competitividad con otras empresas al tener una tecnología de punta
- Tener un mejor control de la empresa al manejarse de manera estructurada.
- Ser reconocida por sus avances tecnológicos.



BIBLIOTECA
CAMPUS
PEÑAS

3.3.1.7 GARANTIA TÉCNICA DEL CABLEADO DE DATOS

- Se garantiza la calidad de los materiales utilizados, por lo menos 10 años, esto implica que cualquier daño de su funcionamiento dentro de este páginas, atendido sin ningún costo.
- La empresa contará con la mano de obra sin costo, de por lo menos 1 año, esto incluye cualquier anomalía con el cableado en ese lapso de tiempo.
- Garantía en el cableado estructurado de 10 años y 20 años en elementos pasivos.

3.3.1.8 CONDICIONES COMERCIALES ALTERNATIVA "A"

A continuación se detallara la forma de pago:

- Se entregará el 50% del valor total en la aceptación formal de la propuesta.
- El 50% restante contra entrega.
- Los Precios Incluyen IVA.
- Validez de la oferta 15 días.



ESTUDIO DE FACTIBILIDAD MATRIZ GUAYAQUIL

3.3.2 ALTERNATIVA “B”

Se realizará la implementación del cableado estructurado, esto abarca el cambio de categorías de cables en toda la empresa, la que actualmente consta con la categoría 5 y 5e, estos pasarán a ser de categoría 6 en su totalidad, operando con los actuales computadores a 100 Mbps y con los actuales equipos de comunicación.

Se reutilizarán switches existentes 3com 4400, y los Rack de Piso.

Otro punto que abarca la implementación del cableado estructurado es el rotulado de los cables, estos tendrán identificaciones y numeraciones para identificar los cables de cada departamento. También se implementarán los respectivos electros canaletas en los pisos de la matriz de Guayaquil, para proteger los cables de agentes varios y perturbaciones que afectan al medio de comunicación.

Se adquirirá un computador de Marca que hará las funciones de servidor Proxy que se encargará de compartir el Internet y se pondrá las debidas políticas para navegación, el cual trabajará con el sistema Operativo Linux..



3.3.2.1 FACTIBILIDAD TÉCNICA

ALTERNATIVA "B"

CANT.	DESCRIPCIÓN	UBICACIÓN
1	EQUIPO PROXY (Marca) Procesador de doble núcleo * INTEL 1 GB Ram, 2 Disco 160 GB 2 Tarjetas de red Gigabit	Departamento de sistema
18 Bobinas	Cable utp cat 6 Signamax 105 puntos de red y 105 de voz	Edificio matriz (Guayaquil)
210	Patch Cord cat 6 1m	Edificio matriz
105	Patch Cord cat 6 3m	Edificio matriz
18	Patch panel cat 6	Edificio matriz (Guayaquil)
210	Jacks cat 6 Signamax	Edificio matriz (Guayaquil)
105	Face Plate de 2 puertos servicios Signamax	Edificio matriz (Guayaquil)
105	Cajas sobre puestas	Edificio matriz (Guayaquil)
75	Electro canales metálicos con tapa de 25x15 cm	Edificio matriz (Guayaquil)
2	Paquetes de amarras plásticas de 15 y 30cm	Edificio matriz (Guayaquil)
3	Paquetes de etiquetas	Edificio matriz (Guayaquil)
100 m	Tubería EMT 1"	Edificio matriz (Guayaquil)
50	Grapas EMT 1"	Edificio matriz (Guayaquil)
1	Materiales Varios Tornillos, Tacos Fisher, conectores EMT 1"	Edificio matriz (Guayaquil)
45	Canaletas 40x25 Decorativas de 2m	Edificio matriz (Guayaquil)
30	Canaletas 24x12 Decorativas de 2m	Edificio matriz (Guayaquil)

Tabla 3-10: Factibilidad Técnica

3.3.2.2 FACTIBILIDAD ECONÓMICA

COSTOS DE HARDWARE

CANT	DESCRIPCIÓN	COSTO TOTAL
1	EQUIPO PROXY (Marca) Que soporte RAID 0 y 1 Procesador de doble núcleo de preferencia INTEL 1 GB Ram 2 Disco 160 GB 2 Tarjetas de red Gigabit	\$ 1300.00
6	Switch 3com 4400 Capa 3 24Ptos	0
TOTAL COSTO DE HARDWARE		\$ 1300.00

Tabla 3-11: Factibilidad Económica Hardware

MATERIALES PARA CABLEADO ESTRUCTURADO		
CANT.	DESCRIPCIÓN	TOTAL
18 Bobinas	Cable utp cat 6 Signamax 105 puntos de red	3443.40
210	Patch Cord 1m	1528.80
105	Patch Cord 3m	963.90
105	Jacks cat 6 Signamax	648,90
18	Patch Panel Sólido Cat 6 Marca Signamax 24 puertos	3322.26
6	Organizadores Horizontales 2UR	0
105	Face Plate de 2 puertos de servicios Signamax	164,64
105	Cajas sobre puestas	176,16
1	Gabinete de Pared Panorámico 10 UR	200.00
75	Electro canales metálicos con tapa de 25x15 cm	1125.00
50	Tubería EMT 1"	353.00
50	Grapas EMT 1"	5.00
2	Materiales Varios Tornillos, Tacos Fisher, conectores EMT 1" Paquetes de amarras plásticas de 15 y 30cm, Paquetes de etiquetas, ángulos interno externo y plano	300.00
45	Canaletas 40x25 Decorativas de 2m	196.65
30	Canaletas 24x12 Decorativas de 2m	33.60
TOTAL MATERIALES PARA CABLEADO ESTRUCTURADO		12.461,10

Tabla 3-12: Factibilidad Económica Materiales



COSTOS DE SOFTWARE

CANT	DESCRIPCIÓN	COSTOS UNITARIOS	COSTO TOTAL
1	PAQUETE DE LINUX RED HAT 9.0	70.00	70.00
TOTAL COSTO DE SOFTWARE			\$ 70.00

Tabla 3-13: Factibilidad Económica Software

3.3.2.3 FACTIBILIDAD OPERATIVA

FASES	SEMANAS
ANÁLISIS DE CABLEADO ESTRUCTURADO *Grupo de trabajo 1 Técnico de redes	2.5
DISEÑO DE LA RED LAN Grupo de trabajo	1.5
IMPLEMENTACIÓN DEL CABLEADO ESTRUCTURADO * Grupo de trabajo 1 Técnicos en Redes 4 Ayudantes	3.5
PRUEBA DE LA RED LAN *Grupo de trabajo 3 Técnicos en redes	2.5
DOCUMENTACIÓN Y CERTIFICACION DE LA RED LAN *Grupo de trabajo Empresa certificadora	1

Tabla 3-13: Factibilidad operativa

* **EL GRUPO DE TRABAJO** Son los estudiantes que elaboran la propuesta para la empresa "TIA"

COSTOS OPERATIVOS

FASES	SEMANAS	COSTO SEMANA	COSTO TOTAL	COSTO FASE
DISEÑO DE LA RED LAN				
Grupo de trabajo	1.5	200.00		
TOTAL DE LA FASE DE DISEÑO				300.00
IMPLEMENTACIÓN DE LA RED LAN (Construcción)				
Grupo de trabajo		300.00		1050.00
1 Técnicos de Redes	3.5	150.00		525.00
4 Ayudantes		75.00		262.50
TOTAL DE LA FASE DE IMPLEMENTACION				1837.50
PRUEBA DE LA RED LAN				
Grupo de trabajo	2.5	300.00		750.00
1 Técnico de Redes		150.00		375.00
TOTAL DE LA FASE DE PRUEBA DE LA RED				1125.00
DOCUMENTACION DE LA RED LAN				
Grupo de trabajo	1	200.00		200.00
TOTAL DE LA FASE DE DOCUMENTACION				200.00
TOTAL DE COSTOS OPERATIVOS				\$ 3462.50

Tabla 3-14: Costos operativos

3.3.2.4 COSTO TOTAL DE LA ALTERNATIVA "B"

En el costo total de la propuesta están incluidos los siguientes valores:

DESCRIPCIÓN	COSTO
Costo de Materiales	\$ 13761.10
Costo Software	\$ 70.00
Costos de Mano de Obra	\$ 3462.50
COSTO TOTAL DE LA PROPUESTA	\$ 17,293,60

I.V.A. 12 %	\$ 2,075.23
COSTO TOTAL DE LA PROPUESTA	\$ 19,368.80

Tabla 3-15: Costo Total Alternativa A

3.3.2.5 VENTAJAS

Cableado Estructurado:

- Velocidad de operación de la red 100Mbps con los equipos activos actuales, velocidad de transmisión soportada por el medio físico 1000 Mbps
- Flexibilidad de Mantenimiento, crecimiento y migración de puestos de trabajos.
- Certificación de la Red incluida con el cableado estructurado, conforme a todas las normas para certificación de medios y equipos

Servidor Proxy

- En la adquisición del servidor Proxy al ser de marca, se contará con una confiabilidad mayor debido a la garantía y soporte que ofrece el proveedor del equipo y se garantiza el mayor desempeño posible sobre él.
- Al tener un Arreglo de discos RAID 1, se tiene una protección ante fallos mecánicos de los discos duros y se baja el tiempo de inactividad del servidor PROXY.
- Control de navegación y restricción de accesos no permitidos.
- Bloqueo de puertos. Ejemplo (Restringir Messenger)
- Almacenamiento de páginas visitadas en cache (Agilidad para navegación)

3.3.2.6 BENEFICIOS

- Tener un mejor control de la empresa al manejarse de manera estructurada.



3.3.2.7 GARANTIA TÉCNICA DEL CABLEADO DE DATOS

- Se garantiza la calidad de los materiales utilizados, por lo menos 10 años, esto implica que cualquier daño de su funcionamiento dentro de este páginas, atendido sin ningún costo.
- La empresa contara con la mano de obra sin costo, de por lo menos 1 año, esto incluye cualquier anomalía con el cableado en ese lapso de tiempo.
- Garantía en el cableado estructurado de 10 años y 20 años en elementos pasivos.

3.3.2.8 CONDICIONES COMERCIALES ALTERNATIVA “B”

A continuación se detallará la forma de pago:

- Se entregará el 50% del valor total en la aceptación formal de la propuesta.
- El 50% restante contra entrega.
- Los Precios Incluyen IVA.
- Validez de la oferta 15 días.

3.3.3 OBSERVACIONES

La Alternativa A es la recomendada debido a la instalación de una nueva infraestructura de comunicaciones acorde a las necesidades actuales y futuras conforme a los estándares de comunicación para cableado estructurado basados en Categoría 6.

Esta infraestructura involucra un cambio en los equipos de comunicación y una actualización de las tarjetas de red de los computadores para operar a las velocidades de 1Gbps de manera integral, justificando el alto desempeño de la red y la inversión económica en este documento Planteado

La Alternativa B, incluye una implementación nueva también de un cableado estructurado categoría 6, pero con un rendimiento de 100Mbps, debido a la reutilización de ciertos componentes activos que incluyen a sus switches administrables y ninguna actualización de hardware en sus computadores.

En ambas alternativas, se entregará un cableado debidamente garantizado, certificado y documentado, con garantía técnica de 10 años sobre el mismo y en sus componentes pasivos.

Incluyen también la instalación de un servidor para las funciones de Proxy con su debida configuración y sus soportes necesarios para continuar con su administración.

Configuración de Switches administrables.



3.3.4 PLAN DE TRABAJO

3.3.5 DIAGRAMA DE GANT

EL DIAGRAMA SE APLICA A LAS DOS PROPUESTAS

Alternativa "A" y Alternativa "B"

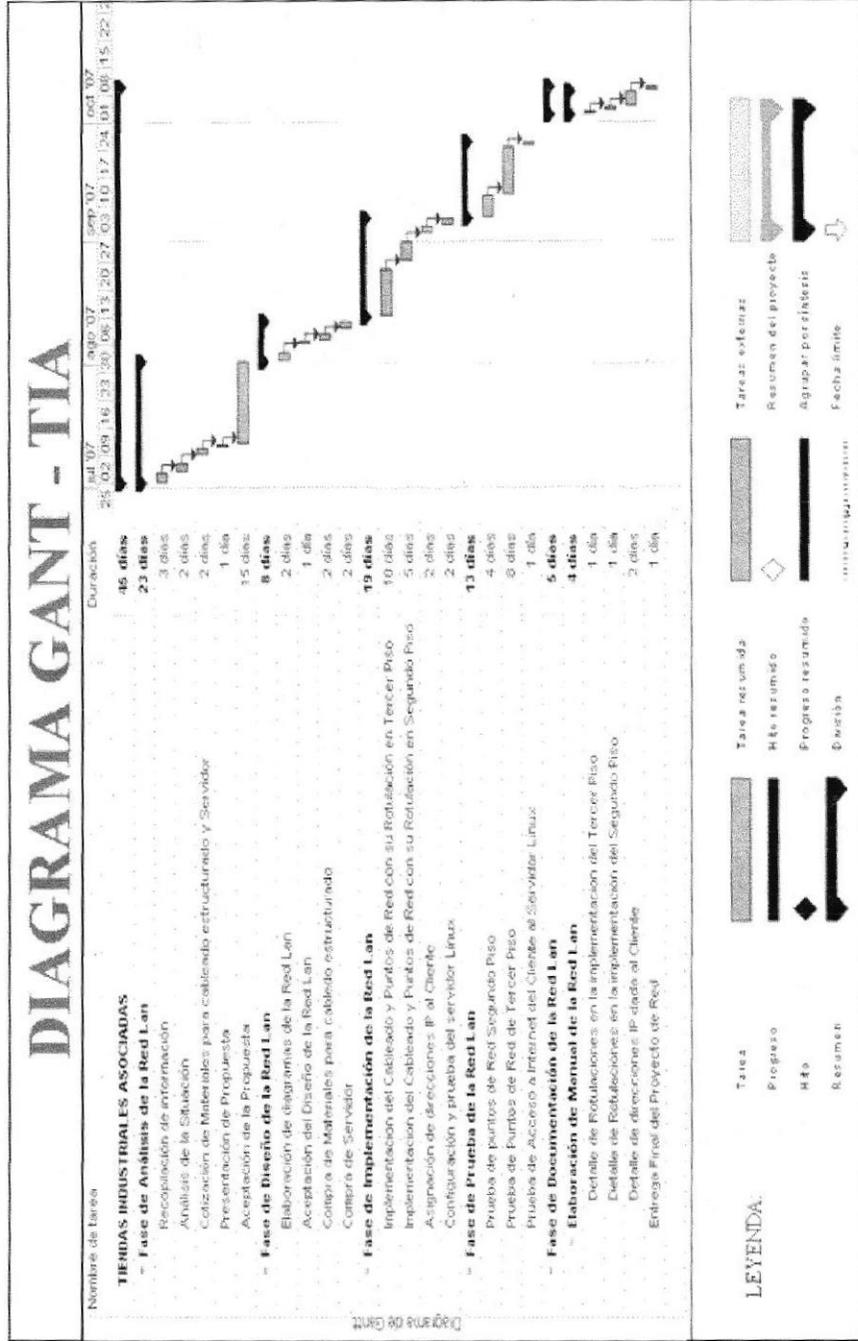
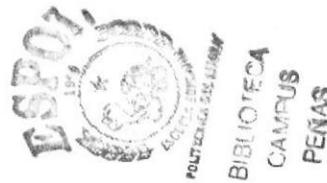


Figura 3-1: Gráfico Diagrama de Gant





CAPÍTULO 4
NORMATIVAS DE
CABLEADO
ESTRUCTURADO

4 REGLAS DE CABLEADO ESTRUCTURADO

4.1 NORMATIVAS

▲ Normativa 1:

Para considerar problemas cuando por emisión electromagnética provenientes de cables de potencia y otros equipos se cubrirán.

Requisitos tales como:

- 1.- Todo sistema deberán estar puesto y unidos a tierra
- 2.- Deberán mantenerse una separación mínima de 50 mm (2 pulgadas) entre el cableado de telecomunicación de par trenzado sin blindaje (UTP) y los circuitos derivados menores a 3 KBA



Figura 4-1: Normativa 1

▲ Normativa 2:

El cableado horizontal deberá estar configurado como estrella con cada salida de telecomunicaciones conectadas con su HC o conector de piso.



Figura 4-2: Normativa 2

▲ Normativa 3:

Se emplearán conexiones cruzadas para conexiones de cableado horizontales y backbone.

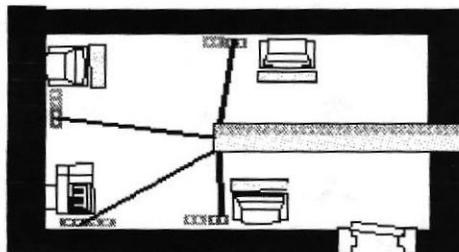


Figura 4-3: Normativa 3



▲ **Normativa 4:**

Cada área de trabajo será atendida por un HC localizado en un mismo piso o a un piso adyacente.

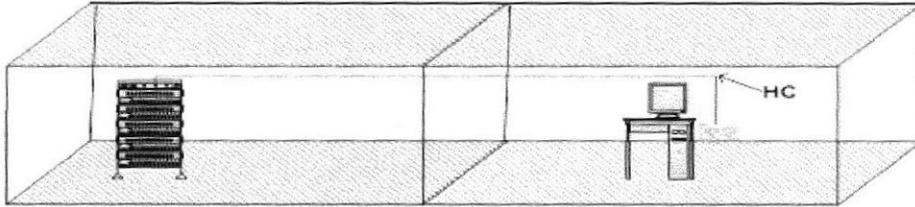


Figura 4-4: Normativa 4

▲ **Normativa 5:**

No se permitirá el uso de derivaciones puenteadas en cableado horizontal.

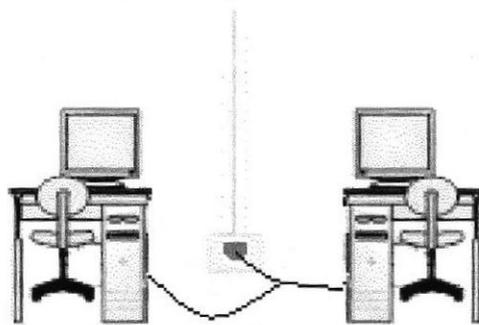


Figura 4-5: Normativa 5

▲ **Normativa 6:**

La longitud del cable entre la salida de telecomunicaciones hasta el HC no excederá de los 90 metros independiente del tipo de medio.

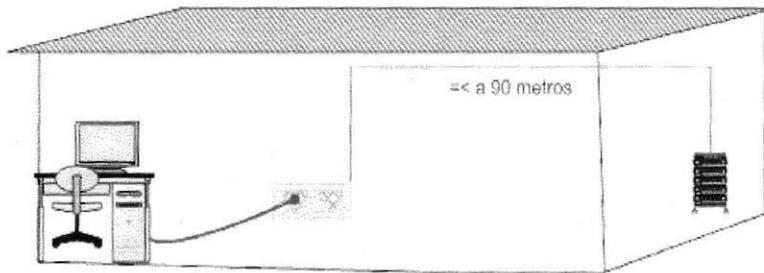


Figura 4-6: Normativa 6

▲ **Normativa 7:**

La longitud individual o combinada del patch cord de par trenzado balanceado de 24 awg (calibre americano de alambre) o fibra óptica utilizado en el HC no excederá los 5 metros.

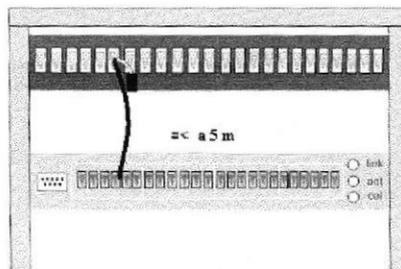


Figura 4-7: Normativa 7



▲ **Normativa 8:**

No se permitirá más de un punto de consolidación dentro de un mismo tendido de cableado horizontal.

Punto de consolidación.- Es un hardware de conexiones que proporciona interconexión entre el cableado de oficina abierto y el cableado horizontal.

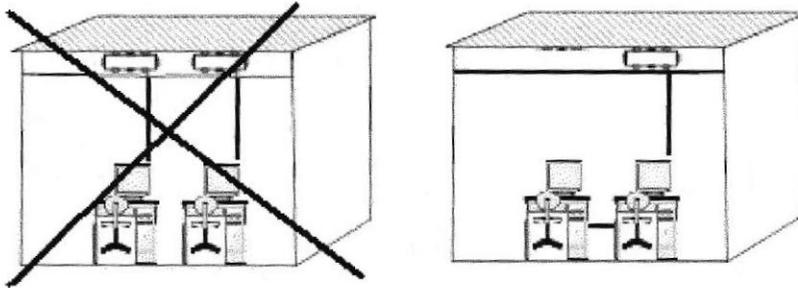


Figura 4-8: Normativa 8

▲ **Normativa 9:**

La distancia máxima entre el HC y la salida de telecomunicaciones será de 90 metros.

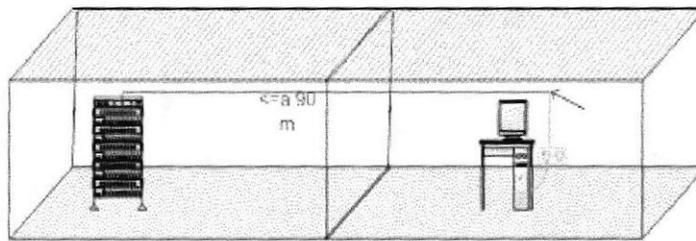


Figura 4-9: Normativa 9

▲ **Normativa 10:**

La distancia mínima entre el HC y el punto de consolidación será de 15 metros.

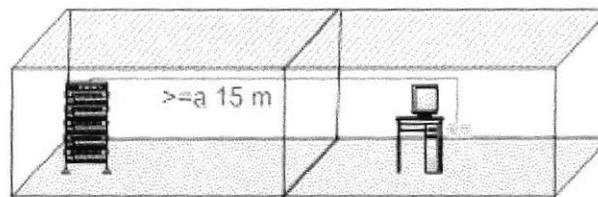


Figura 4-10: Normativa 10



▲ Normativa 11:

La distancia mínima entre el punto de consolidación y la salida de telecomunicaciones será de 5 metros.

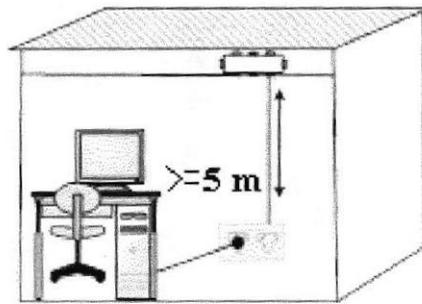


Figura 4-11: Normativa 11

▲ Normativa 12:

La distancia del canal del cableado horizontal incluyendo patch cord y salida de telecomunicaciones no excederá los 100 metros.

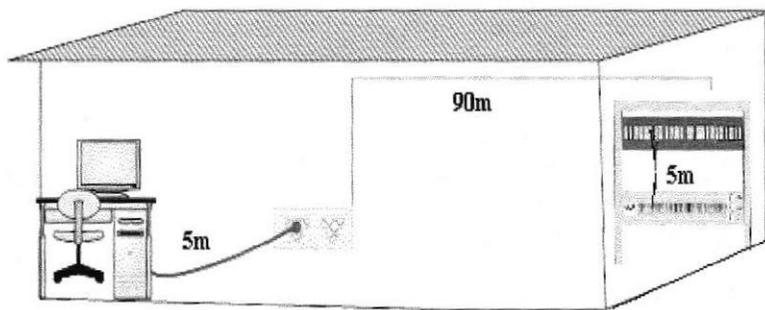


Figura 4-12: Normativa 12

▲ Normativa 13:

Todos los pares de cables estarán totalmente terminados en ambos extremos.



Figura 4-13: Normativa 13

▲ Normativa 14:

La longitud del canal del cableado de fibra óptica multimodo no excederá los 300 metros.



Figura 4-14: Normativa 14

▲ **Normativa 15:**

La longitud del cableado de fibra óptica multimodo entre HC y salida de telecomunicaciones no excederá los 90 metros.

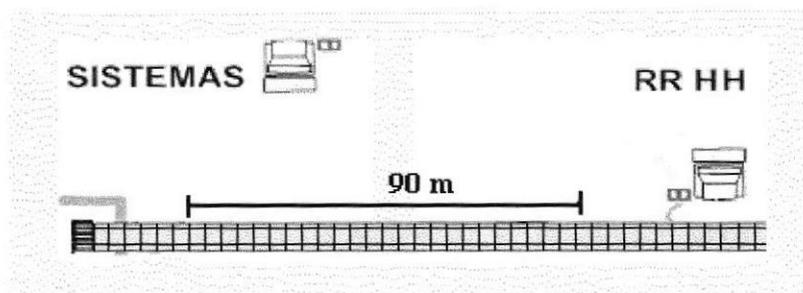


Figura 4-15: Normativa 15

▲ **Normativa 16:**

Las canalizaciones horizontales se diseñarán e instalarán para cumplir los reglamentos eléctricos y de construcción, locales y nacionales y normas aplicables.

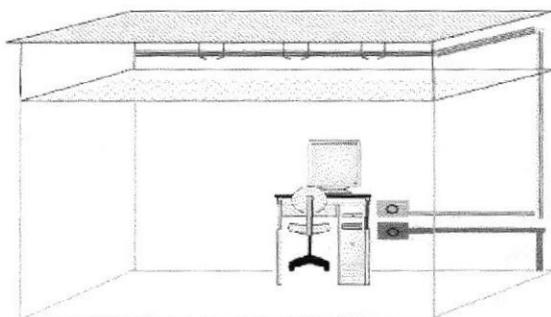


Figura 4-16: Normativa 16



▲ **Normativa 17:**

Las canalizaciones horizontales serán apropiadas para el ambiente en cual se instalarán y no obstaculizarán conductos de calefacción, ventilación y aire acondicionado, distribución de energía eléctrica o estructura del edificio.

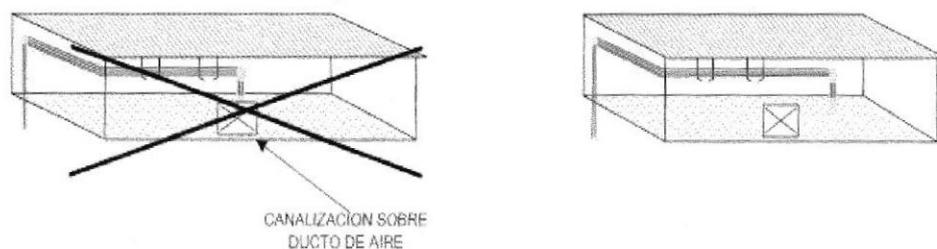


Figura 4-17: Normativa 17

▲ Normativa 18:

Las canalizaciones horizontales se instalarán o seleccionarán de manera que el radio mínimo de curvatura de los cables horizontales se mantenga dentro de las especificaciones del fabricante durante y después de la instalación.



Figura 4-18: Normativa 18

▲ Normativa19:

Todas las canalizaciones instaladas serán accesibles con el fin de efectuar cambios retiros de cable. Las canalizaciones cerradas tendrán punto de accesos cada 30 metros.

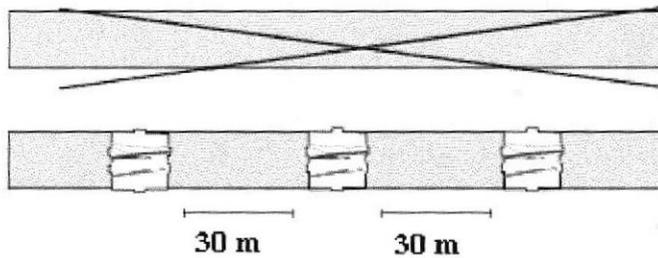


Figura 4-19: Normativa 19

▲ Normativa 20:

El backbone vertical usar una topología jerárquica desde el HC hasta cada IC.

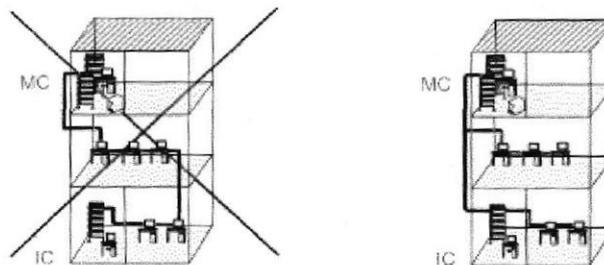


Figura 4-20: Normativa 20

▲ Normativa 21:

Para cada tendido de backbone de Edificio que sea mayor a 90 metros debe proveerse de cable de fibra óptica.

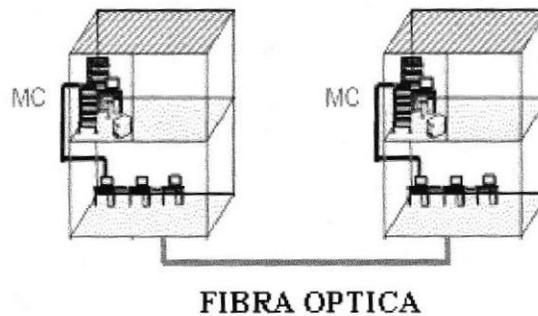


Figura 4-21: Normativa 21

▲ Normativa 22:

La longitud total del canal del cable entre el MC y cualquier HC no excederá los siguientes límites:

- ♣ 3000 metros para fibra óptica monomodo.
- ♣ 2000 para fibra óptica multimodo.
- ♣ 2000 para par trenzado para aplicaciones PBX.
- ♣

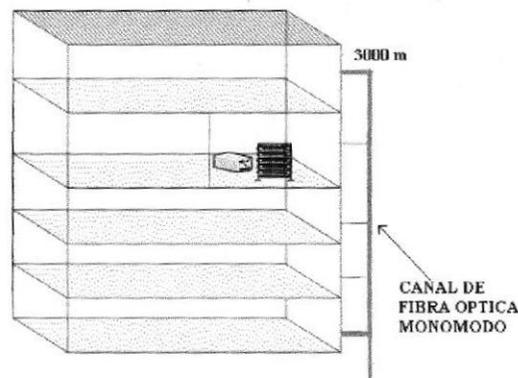


Figura 4-22: Normativa 22

▲ Normativa 23:

Las canalizaciones de edificios proveerán accesos de cuartos telecomunicaciones, cuarto de equipos y o acometidas localizadas en el mismo edificio.

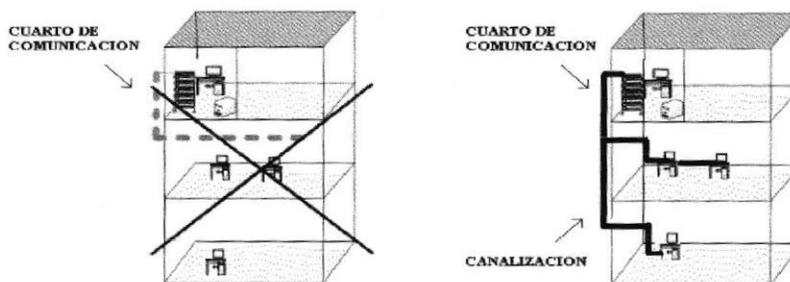


Figura 4-23: Normativa 23

▲ **Normativa 24:**

Las canalizaciones no se ubicarán en ductos de ascensores.

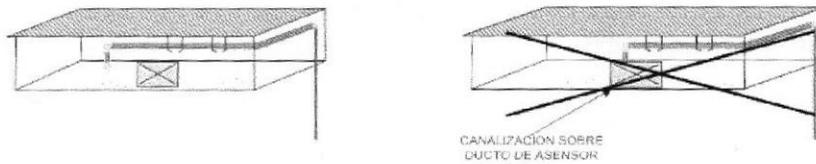


Figura 4-24: Gráfico Normativa 24

▲ **Normativa 25:**

El cable que corre entre el cuarto de telecomunicaciones y la salida de telecomunicaciones no estará expuesto en el área de trabajo u otros espacios con accesos públicos.

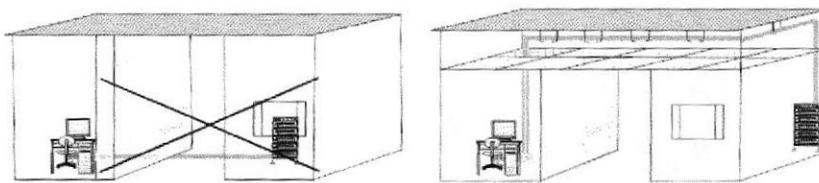


Figura 4-25: Normativa 25

▲ **Normativa 26:**

El cuarto de telecomunicaciones se diseñará y equipará para contener equipos de telecomunicaciones, terminaciones de cables y asociados.

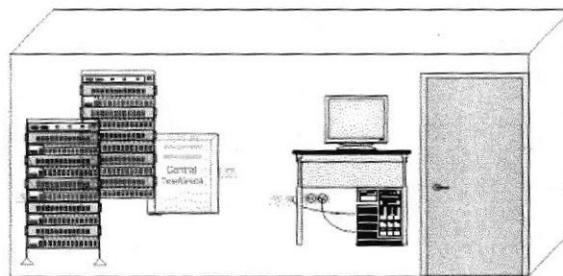


Figura 4-26: Normativa 26



▲ **Normativa 27:**

El acceso al cuarto de telecomunicaciones se restringe al acceso de servicio autorizado y no será compartido por el personal del edificio que puedan interferir con los sistemas de telecomunicaciones.

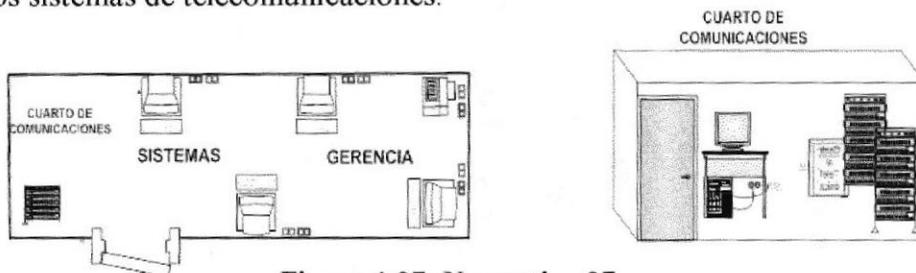


Figura 4-27: Normativa 27

▲ Normativa 28:

Las instalaciones unidad o puestas tierras cumplirán las normas aplicables.

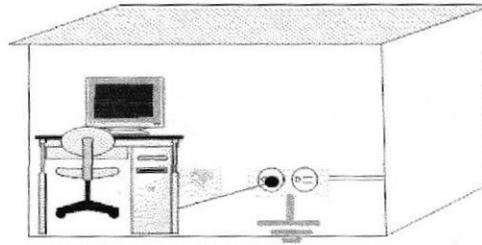


Figura 4-28: Normativa 28

▲ Normativa 29:

Los gabinetes usados como espacios alternativos cumplirán los requisitos de alteración y tendrán una puerta provista con cerradura y se mostrará en una ubicación fija.



Figura 4-29: Normativa 29

▲ Normativa 30:

El cuarto de equipos no será compartido por servicios del edificio que puede interferir con los sistemas de telecomunicaciones o se utilicen para el servicio de mantenimiento del edificio.

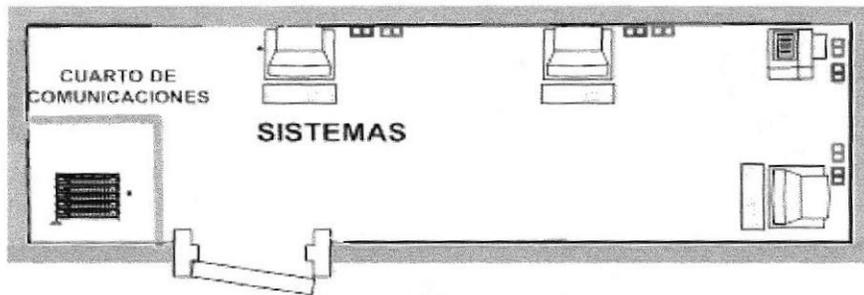


Figura 4-30: Normativa 30

▲ Normativa 31:

El cableado se instalará para facilitar el rotulado y la documentación y para permitir el código de colores en forma consistente de acuerdo a los requisitos.

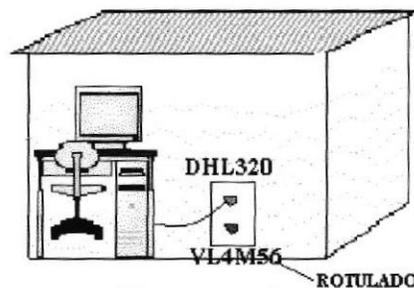


Figura 4-31: Normativa 31

▲ Normativa 32:

La instalación de gabinetes del rack deberá proporcionar las separaciones estipuladas en los reglamentos y normas aplicadas.

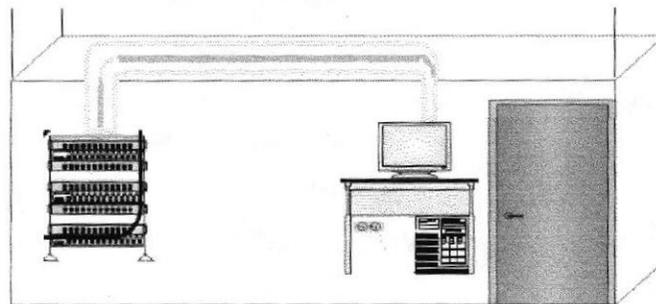


Figura 4-32: Normativa 32

▲ Normativa 33:

Los cables de telecomunicaciones se soportarán con dispositivos diseñados para este fin y en forma independiente para cualquier otra estructura.

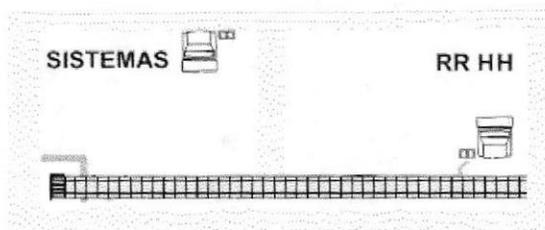


Figura 4-33: Normativa 33

▲ Normativa 34:

Los cables entrucado verticalmente, como en el caso de cables de backbone horizontal enrutados en el piso se soportarán con abrazaderas u otros mecanismos. Se requieren un mínimo por dos pisos.

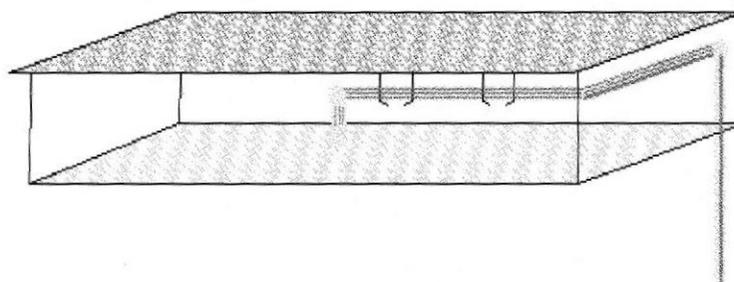


Figura 4-34: Normativa 34

▲ Normativa 35:

El número de cables horizontales de par trenzado balanceado (cable de fibra óptica) colocados en un soporte de canalización se limitará a una cantidad que altere de forma genética el cable.



Figura 4-35: Normativa 35



▲ Normativa 36:

Las canalizaciones tipo bandeja o canal no excederá a una capacidad máxima del 50 % de llenado y una altura máxima de interior de 6 pulgadas.



Figura 4-36: Normativa 36

▲ Normativa 37:

Para canalizaciones en espacios de techos falsos los sistemas de soporte de cable se diseñaran e instalarán con un mínimo de 3 pulgadas por encima de la rejilla del techo soportado.

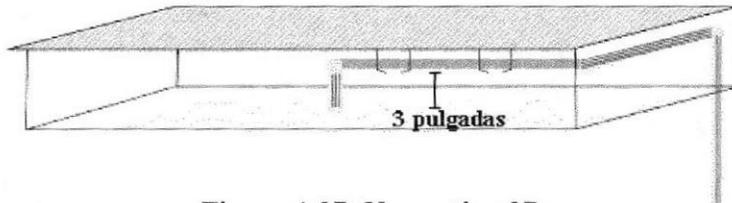


Figura 4-37: Normativa 37

▲ Normativa 38:

Las tensionas máximas del jalado del cable por radio mínimos de curvatura no sobrepasarán las especificaciones del fabricante

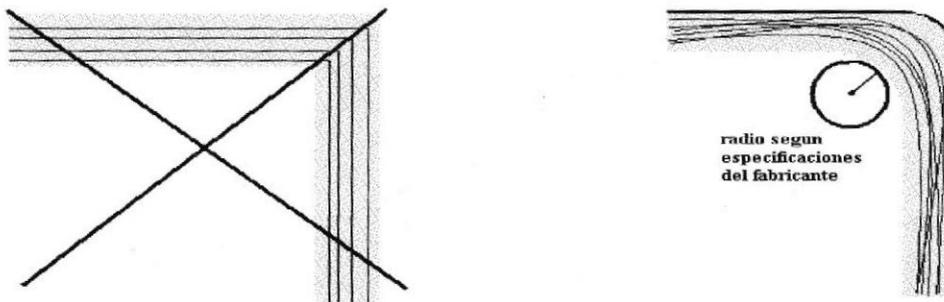


Figura 4-38: Normativa 38

▲ Normativa 39:

No se permitirá el engrapado de ningún tipo de cable reconocido.

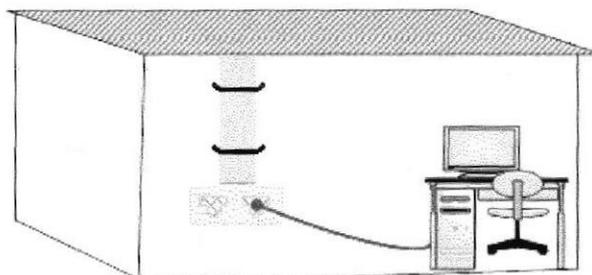


Figura 4-39: Normativa 39

▲ Normativa 40:

Los cables se instalarán en canalizaciones y espacios que brinden protección adecuada contra la intemperie y demás riesgos del entorno.

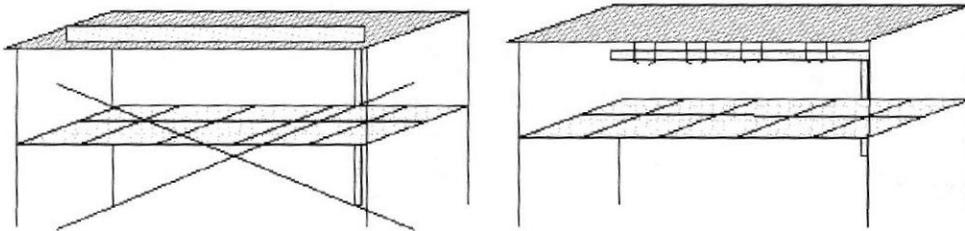


Figura 4-40: Normativa 40

▲ Normativa 41:

El radio mínimo de curvatura en condiciones de no tensión (cuando el cable es solo colocado y no jalado); será de una pulgada para STCP o SFTP de diámetro menor a 6 milímetros. 2 Pulgadas SCTP o SFTP de diámetro mayor a 6 milímetros (0.25 pulgadas)

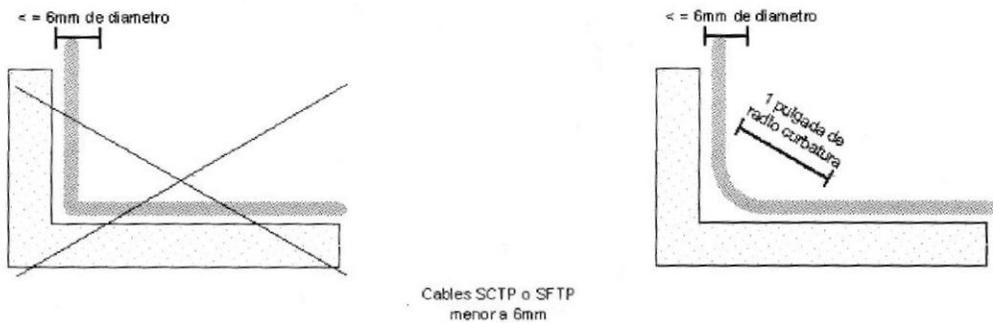


Figura 4-41: Normativa 41

▲ Normativa 42:

El radio mínimo de curvatura para cable horizontal de 2 y 4 fibras será de 1 pulgada bajo condiciones de tensión; en donde la tensión máxima de jalado permitida será de 222 N (libre de fuerza).

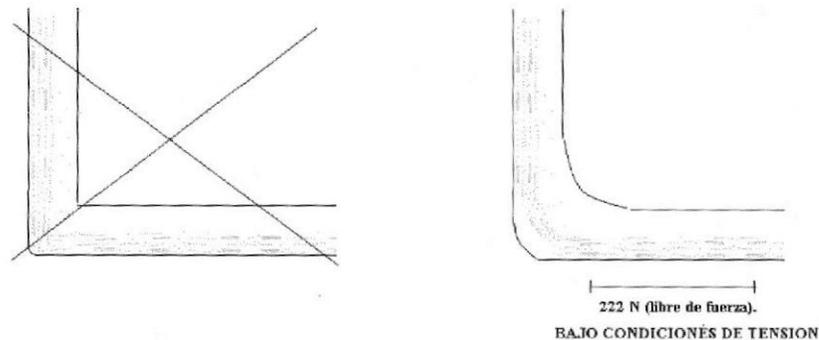


Figura 4-42: Normativa 42



▲ **Normativa 43:**

El radio de curvatura para cable backbone de fibra óptica bajo condiciones de no tensión no será menor a 10 veces el diámetro externo del cable y no menor a 15 veces bajo condiciones de tensión.

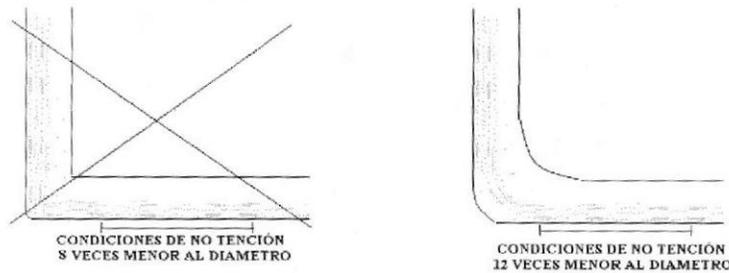


Figura 4-43: Normativa 43

▲ **Normativa 44:**

El cable que corra entre el cuarto de telecomunicaciones y salida de telecomunicaciones, no estará expuesto en el área de trabajo u otro espacio acceso al público

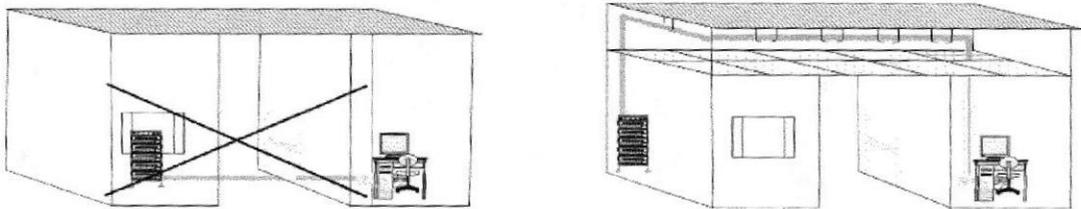


Figura 4-44: Normativa 44

▲ **Normativa 45:**

El hardware de conexión se instalara de una manera que evite un control de cables ordenados y bien organizados.

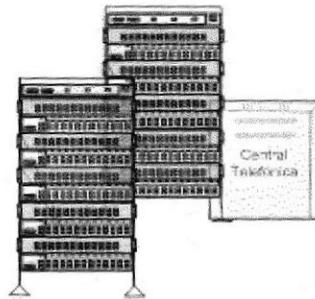


Figura 4-45: Gráfico Normativa 45

▲ **Normativa 46:**

Con el fin de reducir el desentrenado de par trenzado instalador debe de pelar cantidad de forros que se requiera para determinar el hardware de comunicación.



Figura 4-46: Normativa 46

▲ Normativa 47:

La cantidad máx. del desentrezado de cada par, resultante de la terminación del hardware de conexión, será de 13 milímetro, para cable de categoría 5e o mayor y de 75 milímetro para cables de categoría 3



Figura 4-47: Normativa 47

▲ Normativa 48:

No se deberá terminar cables de diferente categoría de desempeño en el mismo hardware de conexión.

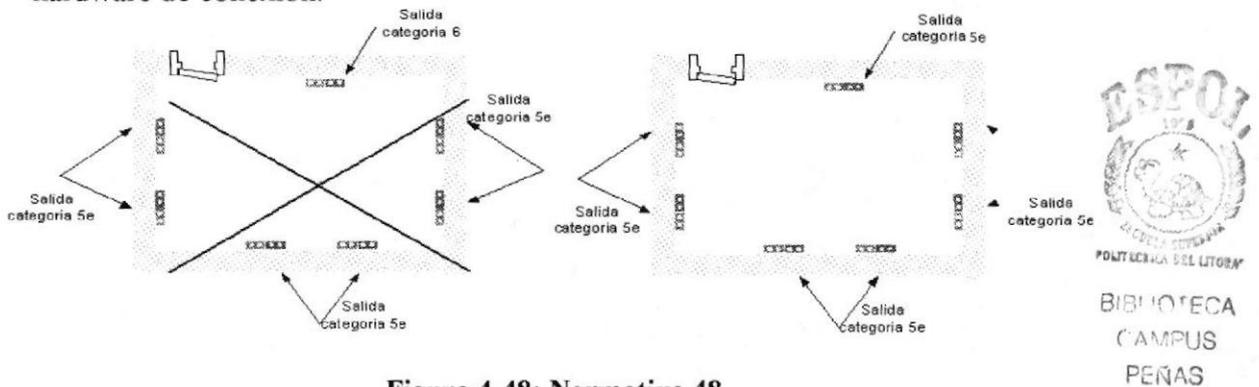


Figura 4-48: Normativa 48

▲ Normativa 49:

Los identificadores que se utilizan para acceder a grupos de registro deben ser únicos

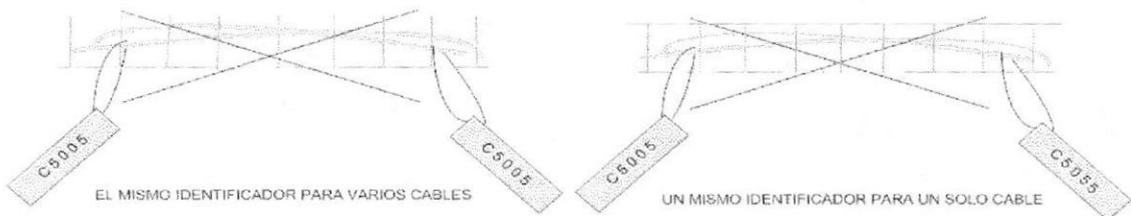


Figura 4-49: Normativa 49

▲ Normativa 50:

El rotulado se deberá realizar ya sea pegando o colocando firmemente una etiqueta independiente al elemento que se va a registrar o marcando el elemento directamente.



Figura 4-50: Normativa 50

▲ Normativa 51:

El rotulado deberá ser legible y permanecer firmemente unido al elemento durante el páginas de garantía (depende de la marca del cable para establecer la garantía lo normal es de 5 años)



Figura 4-51: Normativa 51

▲ Normativa 52:

A cada cable se le asignará un identificador único que sirva de referencia de un registro respectivo Ejemplos:

Descripción	Identificación
Cable n°9 Multimodo	FOM009
Cable N°5 de UTP cat. 5E	C5005

Tabla 4-1: Identificador de cables

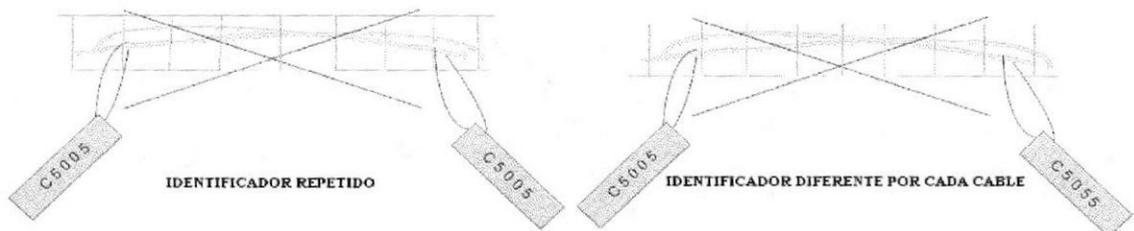


Figura 4-52: Normativa 52

▲ Normativa 53:

Los cables de Backbone deberán rotularse en cada extremo la etiqueta puede ser colocada a 30 centímetro del extremo del cable está marca deberá permanecer en el cable después de terminar la instalación.

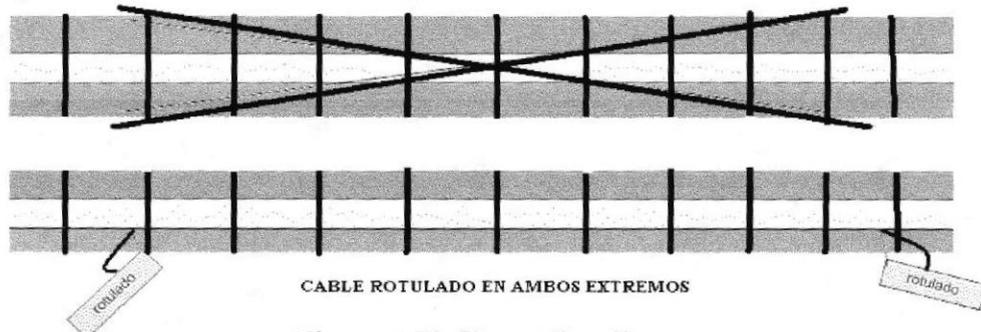


Figura 4-53: Normativa 53

4.2 RECOMENDACIONES

Δ Recomendación 1:

Se pueden emplear interconexiones para conexiones de cableado horizontal y equipos con puertos individuales.

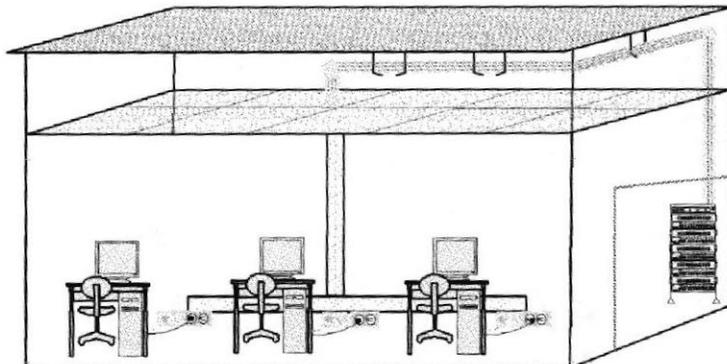


Figura 4-54: Recomendación 1

Δ Recomendación 2:

Con el fin de poseer una infraestructura capaz de acomodar un ambiente de oficinas dinámico se recomienda un mínimo de un cuarto de telecomunicaciones por cada piso.

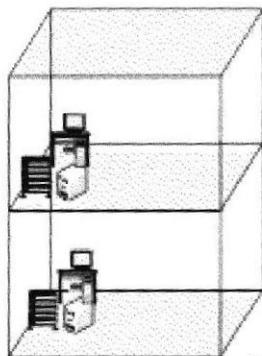


Figura 4-55: Recomendación 2

Δ Recomendación 3:

El área que puede atenderse efectivamente por un cuarto de telecomunicaciones abarca un área máxima de 60 metros.

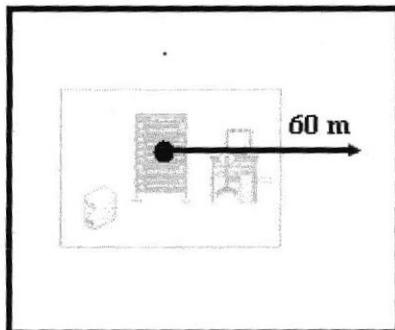


Figura 4-56: Recomendación 3



Δ Recomendación 4:

Se recomienda un mínimo de 15 metros entre el HC y la salida de telecomunicaciones.

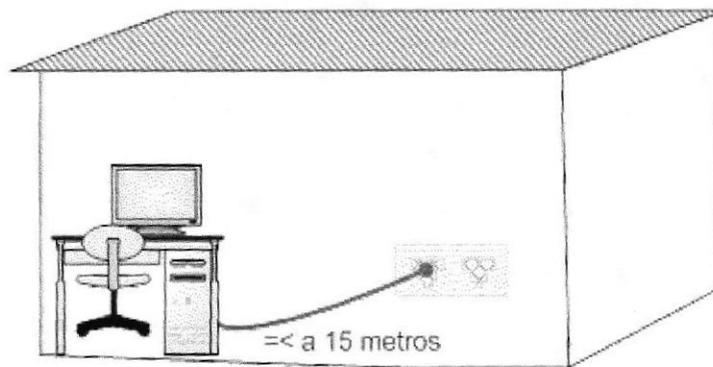


Figura 4-57: Recomendación 4

Δ Recomendación 5:

Se recomienda un mínimo de 2 salidas de categoría 6 por cada área de trabajo individual con el fin de soportar numerosas aplicaciones.

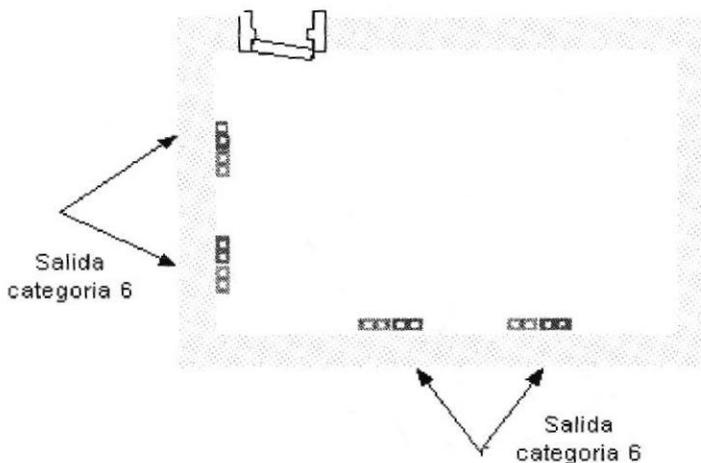


Figura 4-58: Recomendación 5

Δ Recomendación 6:

El punto de consolidación debe estar localizado a la altura conveniente de trabajo con el fin de facilitar la instalación y los cambios

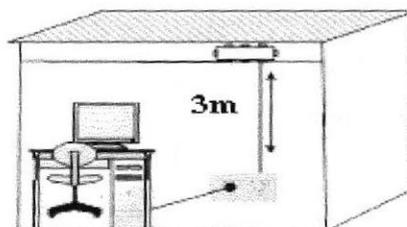
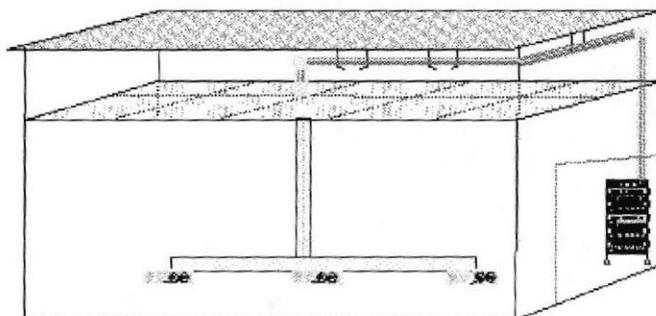


Figura 4-59: Recomendación 6

Δ Recomendación 7:

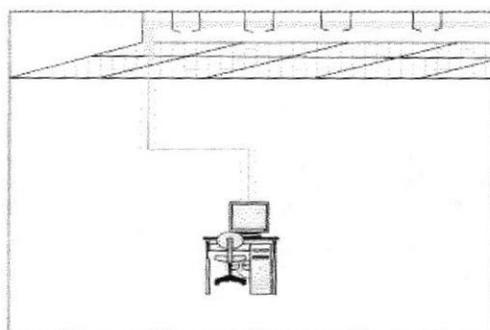
El cableado de backbone del edificio debe diseñarse con la capacidad de reserva suficiente para tener salidas adicionales de telecomunicaciones desde el cuarto de telecomunicaciones.

**Figura 4-60: Recomendación 7****Δ Recomendación 8:**

El radio de curvatura interior mínimo de las canalizaciones horizontales no debe ser inferior a diez veces al mayor diámetro a los cables a instalarse.

**Figura 4-61: Recomendación 8****Δ Recomendación 9:**

Ningún segmento de canal contendrá más de 2 curvas de 90° entre puntos de acceso.

**Figura 4-62: Recomendación 9**

Δ Recomendación 10:

Se recomienda que se provean como mínimos 2 hilos de fibra óptica por cada aplicación conocida durante su período de planificación. Debe preverse los factores de crecimiento de 100 %.

Aplicación	Números de hilos de fibra
Voz	2
Video	2
Lan	2
Crecimiento	6
Total	12

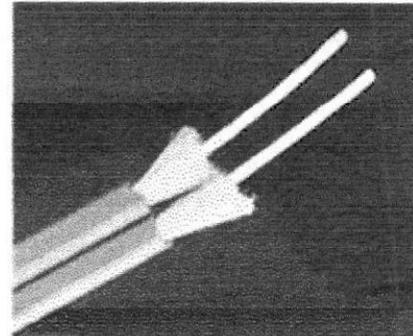


Tabla 4-2: Hilos de fibra

Figura 4-63: Recomendación 10

Δ Recomendación 11:

Para cables de backbone se recomienda un mínimo de 3 metros de reserva para cada cable.

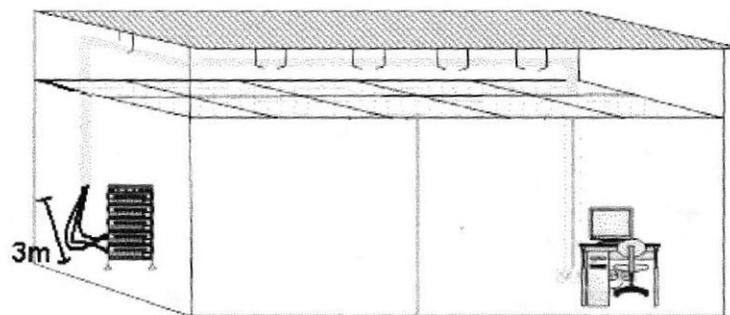


Figura 4-64: Recomendación 11



Δ Recomendación 12:

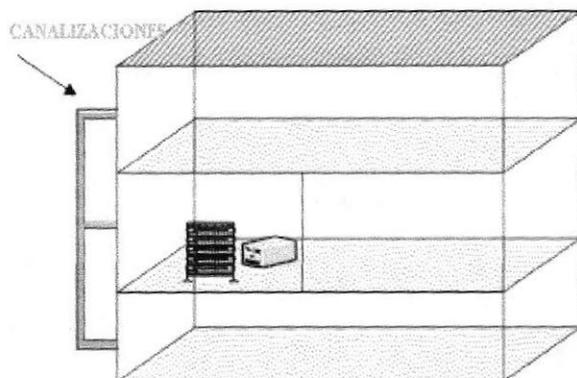
El acabado en el cuarto de telecomunicaciones deben ser colores claros para mejorar la iluminación del mismo.



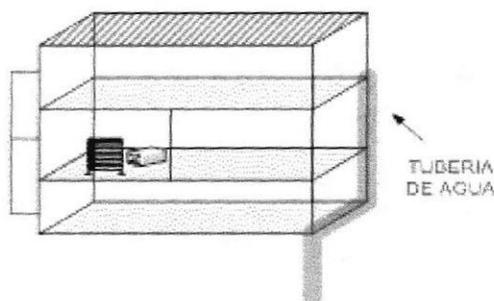
Figura 4-65: Recomendación 12

Δ Recomendación 13:

Cuando sea factible, en un edificio de varios pisos, se recomienda que el cuarto de telecomunicaciones se localice en el piso medio y en una ubicación que facilite el acceso a canalizaciones de los cuartos de telecomunicaciones de otros pisos.

**Figura 4-66: Recomendación 13****Δ Recomendación 14:**

Se recomienda que el cuarto de equipos se ubique por encima del nivel de inundación y este protegido contra infiltraciones de tuberías de agua y drenaje.

**Figura 4-67: Recomendación 14**



BIBLIOTECA
CAMPUS
PEÑAS

CAPÍTULO 5
IMPLEMENTACIÓN
DE LA
SOLUCIÓN PROPUESTA

5 ANÁLISIS DE CABLEADO ESTRUCTURADO

TIENDAS INDUSTRIALES ASOCIADAS ha contemplado la implementación de un sistema de cableado estructurado UTP categoría 6 con el afán de establecer una base tecnológica de última línea que se verá modificada con nuevos switch y demás equipos activos que logren la optimización de recursos y servicios al interior de la Empresa.

En esta implementación se detallara las siguientes especificaciones técnicas:

- Se modificará el cableado horizontal desarrollando una red en estrella.
- La red Horizontal y Vertical de datos cumplira principalmente con los estándares ANSI/ EIA/ TIA para categoría 6.
- Se ubicará un Gabinete (IC) encargado de enlazar la sala de equipos principal (MC) con las estaciones de trabajo en la distribución de voz y de datos.
- Los cables estarán con su respectiva identificación para mejorar la organización.
- En las electro canaletas cada 30 m se harán puntos de accesos espaciados para facilitar las posibles reparaciones.
- Se deberá mantener los cuartos de comunicaciones del tercer y segundo piso cerrados, aislados y con la temperatura adecuada que exige el fabricante.
- Para evitar sobre calentamientos, se evitara la instalación de equipos cercanos que dirijan el aire caliente hacia los switches.
- Las canalizaciones no estarán cerca de ductos de ascensores.
- El cuarto de comunicaciones no será compartido por el personal del edificio que puedan interferir con los sistemas de telecomunicaciones.
- Las canalizaciones horizontales serán apropiadas para el ambiente el cual no obstaculizarán conductos de aire acondicionado, estructura del edificio, distribución de energía eléctrica o terminales de salida de agua para evitar las condensaciones.
- Para canalizaciones en espacios de techos falsos los sistemas de soporte de cable se diseñarán e instalarán con un mínimo de 3 pulgadas por encima de la rejilla del techo soportado.

5.1 CABLEADO ESTRUCTURADO DE GUAYAQUIL - SEGUNDO PISO

En el segundo piso de Guayaquil, el cableado a realizarse será sobrepuesto debido a que el edificio ya está construido, como se demuestra en el gráfico del cableado, se procederá a ubicar los puntos de red respetando los estándares de las normativas de cableado estructurado, ubicando las estaciones de trabajo e impresoras de tal manera que estén cerca de los puntos de red para que el sobrante de cable no sea considerable y este acorde al espacio físico del piso.

Además en este piso se ubicará un Gabinete IC con el propósito de evitar la atenuación (perdida total de señal de extremo a extremo) con respecto a los cables que bajan desde el tercer piso este alimentará al piso contiguo.

CENTRO DE DISTRIBUCION PRINCIPAL

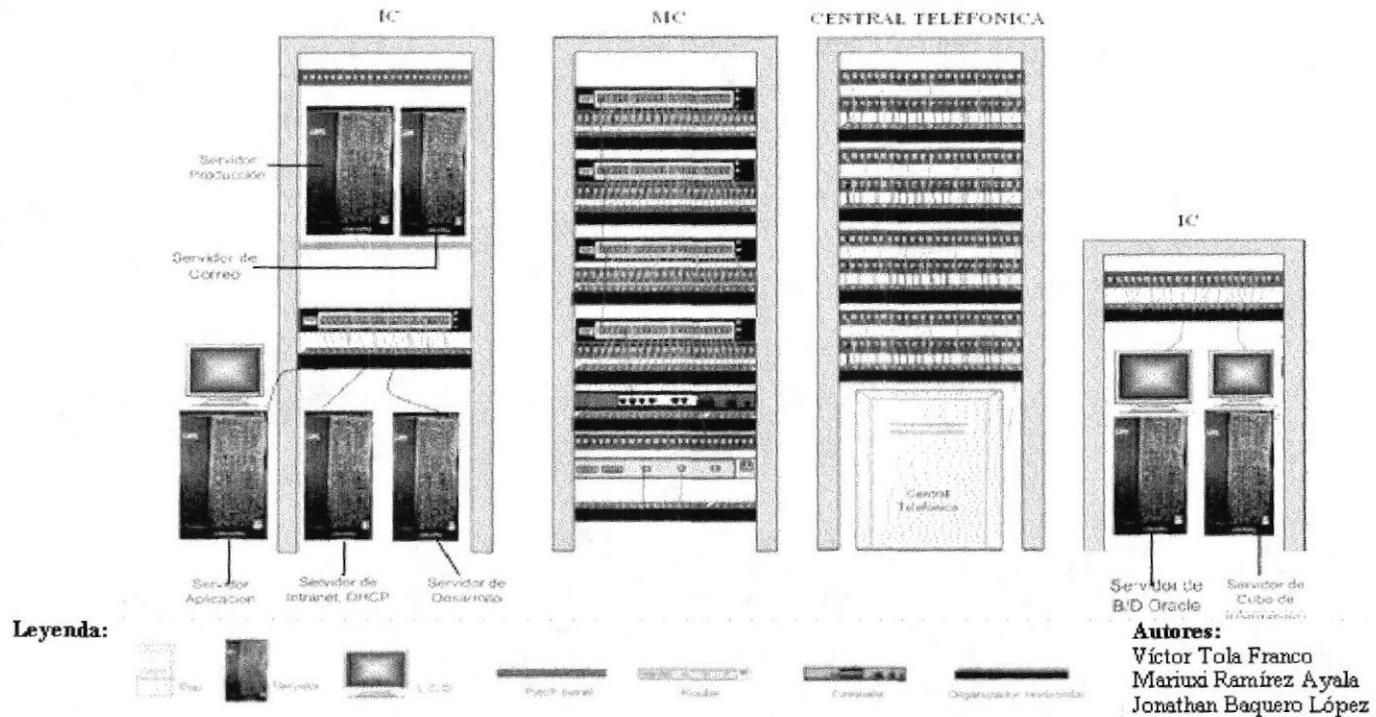


Figura 5-1: Centro de Distribución Principal

CENTRO DE DISTRIBUCION INTERMEDIA



BIBLIOTECA
CAMPUS
PEÑAS

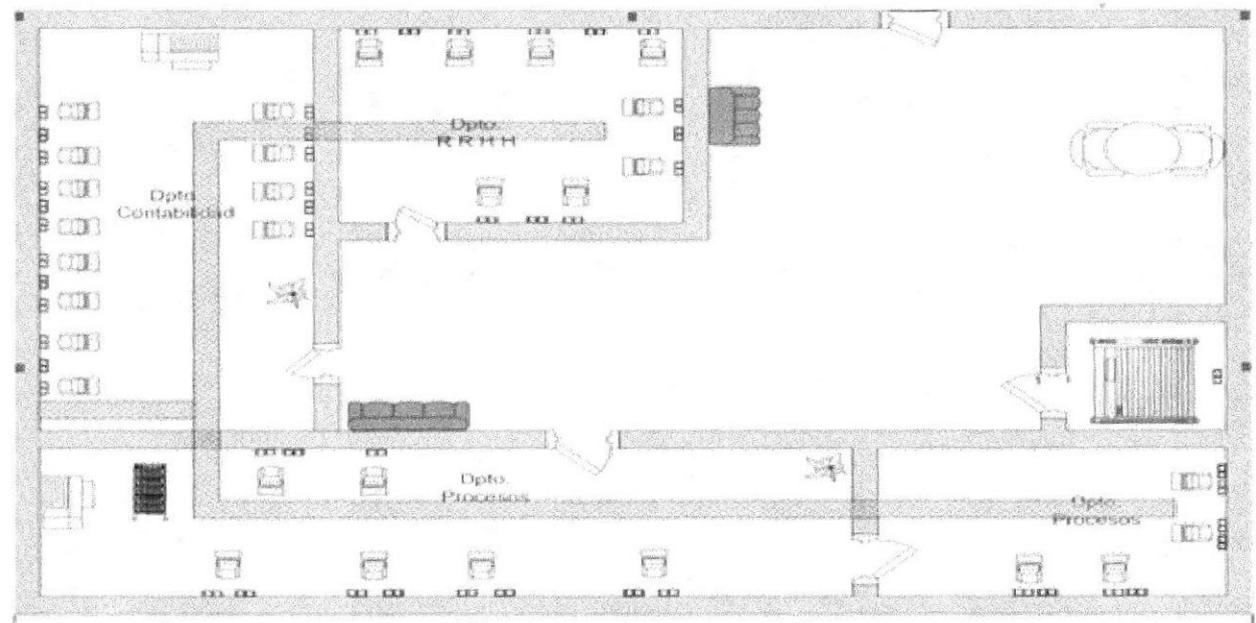
Leyenda:



Autores:
Víctor Tola Franco
Mariuxi Ramírez Ayala
Jonathan Baquero López

Figura 5-2: Centro de Distribución Intermedia

ANÁLISIS DE PISO APLICATIVO
SEGUNDA PLANTA GUAYAQUIL



Leyenda:

- Estación de Trabajo
- Puntos de Red
- Impresora
- UPS
- Rack de Piso Abierto
- Backbone Horizontal

Autores:
Víctor Tola Franco
Mariuxi Ramírez Ayala
Jonathan Baquero López

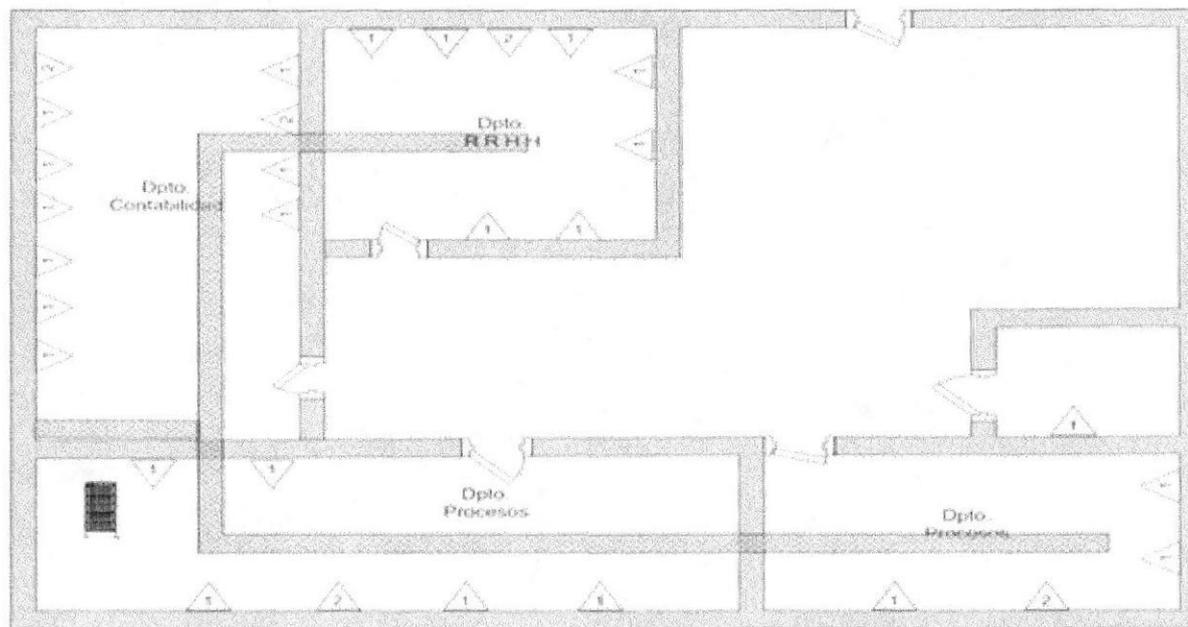
Figura 5-3: Análisis de Piso Aplicativo Segunda Planta



POLITECNICA DEL LITORAL

BIBLIOTECA
CAMPUS
PEÑAS

ANÁLISIS DE PISO LÓGICO
SEGUNDA PLANTA GUAYAQUIL



Leyenda:



1 de Dato



1 de Dato/1 de voz



Electroconduleta



Rack de Piso Abierto

Autores:

Víctor Tola Franco
Maruxi Ramírez Ayala
Jonathan Baquero López

Figura 5-4: Análisis de Piso Lógico Segunda Planta

CÁLCULO DEL BACKBONE - SEGUNDO PISO

Medida salida comunicaciones al rack en cm	Conversión de cm a m	Resultado En Metros	Subida y bajada del cable de cada extremo	Resultado En Metros	Total de # de Servicios	Total En Metros
8	1,92	15,36	9	24,36	2	48,72
5,9	1,92	11,328	9	20,328	2	40,656
9,9	1,92	19,008	9	28,008	2	56,016
10,9	1,92	20,928	9	29,928	2	59,856
12,9	1,92	24,768	9	33,768	2	67,536
13,9	1,92	26,688	9	35,688	2	71,376
11	1,92	21,12	9	30,12	2	60,24
12	1,92	23,04	9	32,04	2	64,08
11	1,92	21,12	9	30,12	2	60,24
12,1	1,92	23,232	9	32,232	2	64,464
12,9	1,92	24,768	9	33,768	2	67,536
13,9	1,92	26,688	9	35,688	2	71,376
14,93	1,92	28,6656	9	37,6656	2	75,3312
17,3	1,92	33,216	9	42,216	2	84,432
17,5	1,92	33,6	9	42,6	2	85,2
17	1,92	32,64	9	41,64	2	83,28
16,5	1,92	31,68	9	40,68	2	81,36
14,6	1,92	28,032	9	37,032	2	74,064
Suma en Metros						1279,459

Tabla 5-1: Calculo del Backbone Segundo piso



5.2 CABLEADO ESTRUCTURADO DE GUAYAQUIL - TERCER PISO

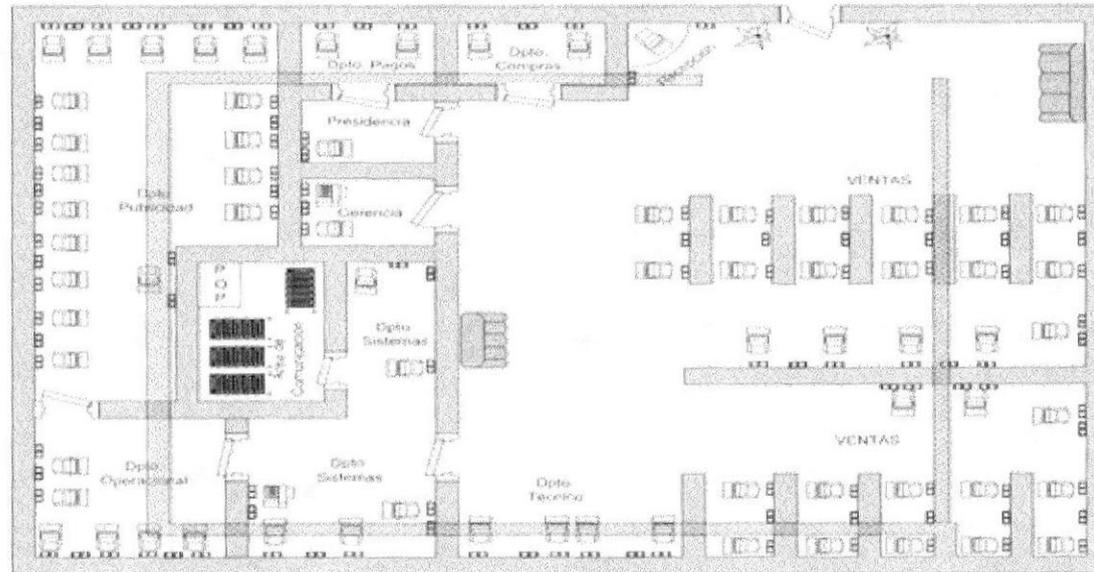
En el tercer piso de Guayaquil, se encuentran los equipos principales, el cuarto de comunicaciones desde el cual se alimentan el gabinete de red.

Los puntos de red y datos serán instalados como lo indican las normas de cableado, se ha realizado una reestructuración en este piso reubicando los puntos de red y datos, se ha tratado de aprovechar el espacio entre los puntos de red y las estaciones de trabajo de tal manera que se pueda obtener uniformidad, ahorro de espacio y cable.

Como se puede observar aquí se aplica la norma que indica que el cuarto de comunicaciones deberá estar un lugar fresco y restringido de tal manera que no sea compartido con demás departamentos, el cableado para los servidores también se realizará con cable utp categoría 6 para un mejor rendimiento en la red y mejor tiempo de respuesta.



**ANÁLISIS DE PISO APLICATIVO
TERCERA PLANTA DE GUAYAQUIL**



Leyenda:

- | | | | |
|---------------------|---------------|---------------------|----------------------|
| Estacion de Trabajo | Puntos de Red | BackBone Horizontal | Rack de Piso Abierto |
| Puntos Electricos | Impresora | | |

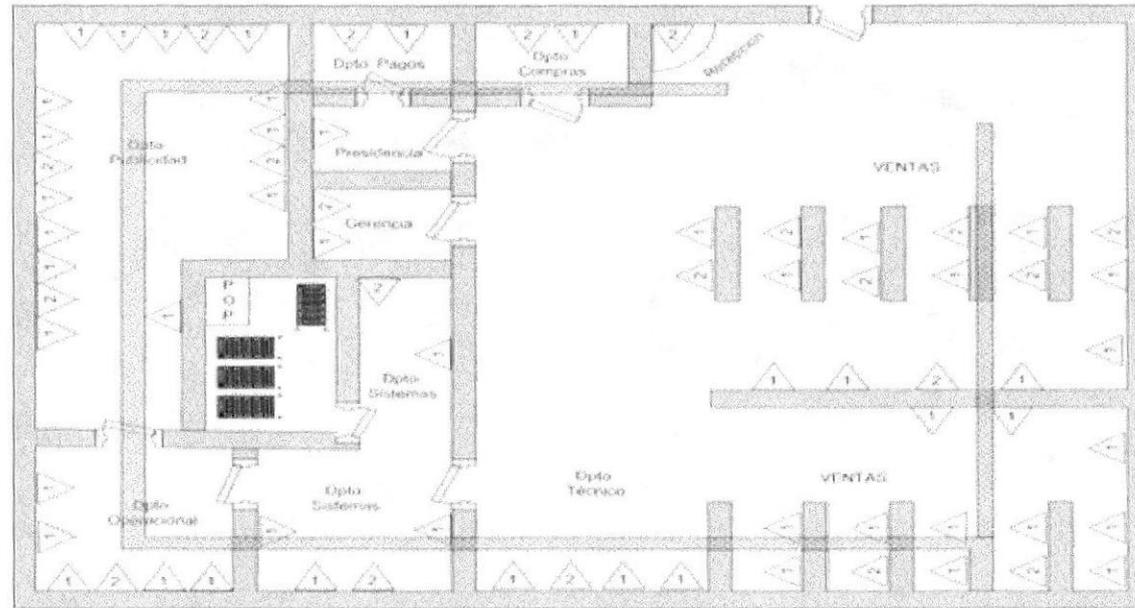
Autores:

Victor Tola Franco
Maruxi Ramirez Ayala
Jonathan Baquero López

Figura 5-5: Gráfico Análisis de Piso Aplicativo Tercera Planta



**ANÁLISIS DE PISO LÓGICO
TERCERA PLANTA DE GUAYAQUIL**



Leyenda:

- 1 de Dato
- 1 de Dato/1 de voz
- Electrocañaleta
- Rack de Piso Abierto

Autores:

- Victor Tola Franco
- Maruxi Ramírez Ayala
- Jonathan Baquero López

Figura 5-6: Gráfico Análisis de Piso Lógico Tercera Planta

CÁLCULO DEL BACKBONE - TERCER PISO

Salida de comunicaciones al rack en cm	Conversión de cm a m	Resultado En Metros	Subida y bajada del cable de cada extremo	Resultado En Metros	Total de # de Servicios	Total en Metros
5	1,92	9,6	9	18,6	2	37,2
5,3	1,92	10,176	9	19,176	2	38,352
5,3	1,92	10,176	9	19,176	2	38,352
4	1,92	7,68	9	16,68	2	33,36
5,5	1,92	10,56	9	19,56	2	39,12
6,3	1,92	12,096	9	21,096	2	42,192
6,6	1,92	12,672	9	21,672	2	43,344
7	1,92	13,44	9	22,44	2	44,88
7,5	1,92	14,4	9	23,4	2	46,8
10	1,92	19,2	9	28,2	2	56,4
9,6	1,92	18,432	9	27,432	2	54,864
9,6	1,92	18,432	9	27,432	2	54,864
9,7	1,92	18,624	9	27,624	2	55,248
9	1,92	17,28	9	26,28	2	52,56
9,7	1,92	18,624	9	27,624	2	55,248



5,3	1,92	10,176	9	19,176	2	38,352
6,5	1,92	12,48	9	21,48	2	42,96
7	1,92	13,44	9	22,44	2	44,88
9	1,92	17,28	9	26,28	2	52,56
9,5	1,92	18,24	9	27,24	2	54,48
9,5	1,92	18,24	9	27,24	2	54,48
11	1,92	21,12	9	30,12	2	60,24
3	1,92	5,76	9	14,76	2	29,52
9	1,92	17,28	9	26,28	2	52,56
8,5	1,92	16,32	9	25,32	2	50,64
12	1,92	23,04	9	32,04	2	64,08
12	1,92	23,04	9	32,04	2	64,08
13	1,92	24,96	9	33,96	2	67,92
14	1,92	26,88	9	35,88	2	71,76
11,5	1,92	22,08	9	31,08	2	62,16
15	1,92	28,8	9	37,8	2	75,6
15,5	1,92	29,76	9	38,76	2	77,52
15	1,92	28,8	9	37,8	2	75,6
16	1,92	30,72	9	39,72	2	79,44

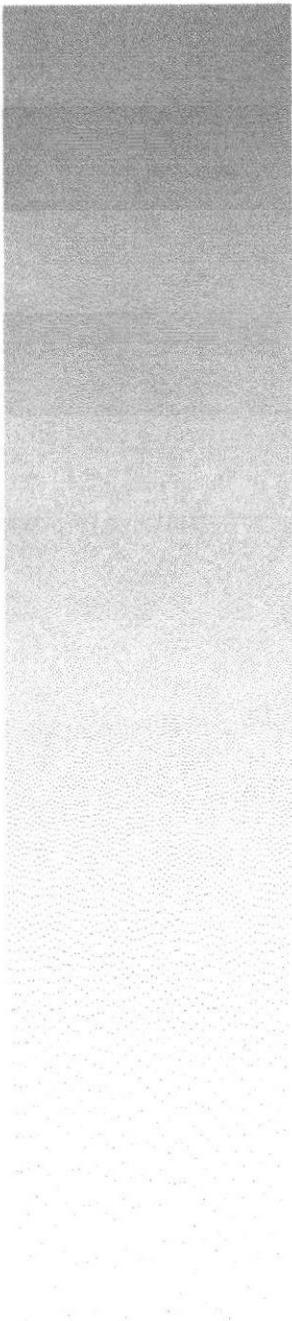


17,5	1,92	33,6	9	42,6	2	85,2
17	1,92	32,64	9	41,64	2	83,28
16	1,92	30,72	9	39,72	2	79,44
12	1,92	23,04	9	32,04	2	64,08
9	1,92	17,28	9	26,28	2	52,56
17	1,92	32,64	9	41,64	2	83,28
17	1,92	32,64	9	41,64	2	83,28
17	1,92	32,64	9	41,64	2	83,28
18	1,92	34,56	9	43,56	2	87,12
15,5	1,92	29,76	9	38,76	2	77,52
15	1,92	28,8	9	37,8	2	75,6
13	1,92	24,96	9	33,96	2	67,92
12	1,92	23,04	9	32,04	2	64,08
11	1,92	21,12	9	30,12	2	60,24
15	1,92	28,8	9	37,8	2	75,6
14	1,92	26,88	9	35,88	2	71,76
11	1,92	21,12	9	30,12	2	60,24
9	1,92	17,28	9	26,28	2	52,56
10	1,92	19,2	9	28,2	2	56,4



11	1,92	21,12	9	30,12	2	60,24
9	1,92	17,28	9	26,28	2	52,56
7,5	1,92	14,4	9	23,4	2	46,8
7,5	1,92	14,4	9	23,4	2	46,8
3,5	1,92	6,72	9	15,72	2	31,44
5	1,92	9,6	9	18,6	2	37,2
5	1,92	9,6	9	18,6	2	37,2
5,5	1,92	10,56	9	19,56	2	39,12
4	1,92	7,68	9	16,68	2	33,36
6	1,92	11,52	9	20,52	2	41,04
5,5	1,92	10,56	9	19,56	2	39,12
7,5	1,92	14,4	9	23,4	2	46,8
7	1,92	13,44	9	22,44	2	44,88
7,5	1,92	14,4	9	23,4	2	46,8
Suma en Metros						3819,456
Total de los dos pisos en Metros						5098,915
Total de bobinas						17.2

Tabla 5-2: Calculo del Backbone Tercer piso



BIBLIOTECA
CAMPUS
PEÑAS



CAPÍTULO 6
DISPOSITIVOS DE
ENRUTAMIENTO Y
CONMUTACIÓN

6 ROUTER

Un router es un tipo especial de computador. Cuenta con los mismos componentes básicos que un PC estándar de escritorio. Es decir, posee una CPU, memoria, bus de sistema y distintas interfaces de entrada/salida.

6.1 FUNCIONES DEL ROUTER

- La función principal de un router es enrutar.
- Un router es un dispositivo LAN y WAN.
- Proporciona conexiones con y entre los diversos estándares de enlace de datos y físico WAN.

6.2 TECNOLOGÍAS SOPORTADAS.

- Control de enlace de datos de alto nivel (HDLC).
- Frame Relay.
- Protocolo punto a punto (PPP).
- Control de enlace de datos síncrono (SDLC).
- Protocolo Internet de enlace serial (SLIP).
- X.25.
- ATM.

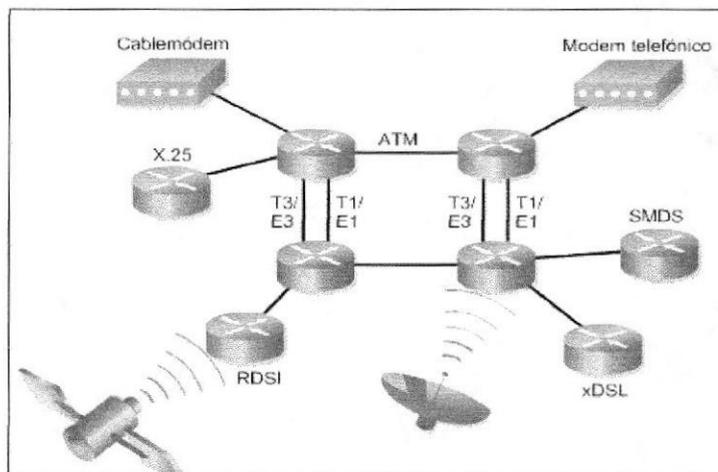


Figura 6-1: Gráfico Tecnologías de Router



6.3 COMPONENTES INTERNOS DEL ROUTER

Los principales componentes internos del router son:

- La memoria de acceso aleatorio (RAM).
- La memoria de acceso aleatorio no volátil (NVRAM).
- La memoria flash.
- La memoria de sólo lectura (ROM).

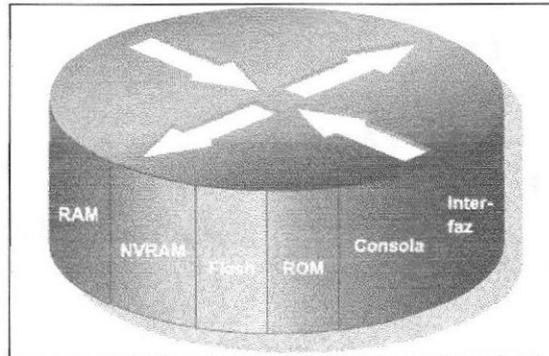


Figura 6-2: Componentes internos de un router.



CPU: La unidad central de procesamiento (CPU) ejecuta las instrucciones del sistema operativo. Estas funciones incluyen la inicialización del sistema, las funciones de enrutamiento y el control de la interfaz de red. La CPU es un microprocesador. Los grandes routers pueden tener varias CPU.

RAM: La memoria de acceso aleatorio (RAM) se usa para la información de las tablas de enrutamiento, el caché de conmutación rápida, la configuración actual y las colas de paquetes. En la mayoría de los routers, la RAM proporciona espacio de tiempo de ejecución para el software IOS de Cisco y sus subsistemas. Por lo general, la RAM se divide de forma lógica en memoria del procesador principal y memoria compartida de entrada/salida (I/O). Las interfaces de almacenamiento temporal de los paquetes comparten la memoria de I/O compartida. El contenido de la RAM se pierde cuando se apaga la unidad. En general, la RAM es una memoria de acceso aleatorio dinámica (DRAM) y puede actualizarse agregando más módulos de memoria en línea doble (DIMM).

Memoria flash: Se utiliza para almacenar una imagen completa del software IOS. Normalmente el router adquiere el IOS por defecto de la memoria flash. Estas imágenes pueden actualizarse cargando una nueva imagen en la memoria flash. En la mayoría de los routers, una copia ejecutable del IOS se transfiere a la RAM durante el proceso de arranque. En otros routers, el IOS puede ejecutarse directamente desde la memoria flash, agregando o reemplazando los módulos de memoria en línea simples flash (SIMMs) o las tarjetas PCMCIA se puede actualizar la cantidad de memoria flash.

NVRAM: La memoria de acceso aleatorio no volátil (NVRAM) se utiliza para guardar la configuración de inicio. En algunos dispositivos, la NVRAM se implementa utilizando distintas memorias de solo lectura programables, que se pueden borrar electrónicamente (EEPROM).

Buses: La mayoría de los routers contienen un bus de sistema y un bus de CPU. El bus de sistema se usa para la comunicación entre la CPU y las interfaces y/o ranuras de expansión. Este bus transfiere los paquetes hacia y desde las interfaces.

La CPU usa el bus para tener acceso a los componentes desde el almacenamiento del router. Este bus transfiere las instrucciones y los datos hacia o desde las direcciones de memoria especificadas.

ROM: La memoria de solo lectura (ROM) se utiliza para almacenar de forma permanente el código de diagnóstico de inicio (Monitor de ROM). Las tareas principales de la ROM son el diagnóstico del hardware durante el arranque del router y la carga del software IOS, desde la memoria flash a la RAM. Algunos routers también tienen una versión más básica del IOS que puede usarse como fuente alternativa de arranque. Las memorias ROM no se pueden borrar. Sólo pueden actualizarse reemplazando los chips de ROM en los tomas.

Fuente de alimentación: La fuente de alimentación brinda la energía necesaria para operar los componentes internos. Los routers de mayor tamaño pueden contar con varias fuentes de alimentación o fuentes modulares. En algunos de los routers de menor tamaño, la fuente de alimentación puede ser externa al router.

Los routers conectan y permiten la comunicación entre dos redes y determinan la mejor ruta para la transmisión de datos a través de las redes conectadas.

Los routers necesitan el software denominado Sistema Operativo de Internetworking (IOS) para ejecutar los archivos de configuración.

Son dispositivos electrónicos complejos que permiten manejar comunicaciones entre redes que se encuentran a gran distancia, utilizando vínculos provistos por las empresas prestatarias del servicio telefónico (líneas punto a punto), líneas de datos (Arpac), enlaces vía satélite, etc.

Poseen avanzadas funciones de negociación del enlace y conversión de protocolos de transmisión. Se utilizan por lo general en empresas que manejan muchas sucursales, tales como Bancos, etc. Están relacionados con sistemas bajo Unix y TCP-IP.

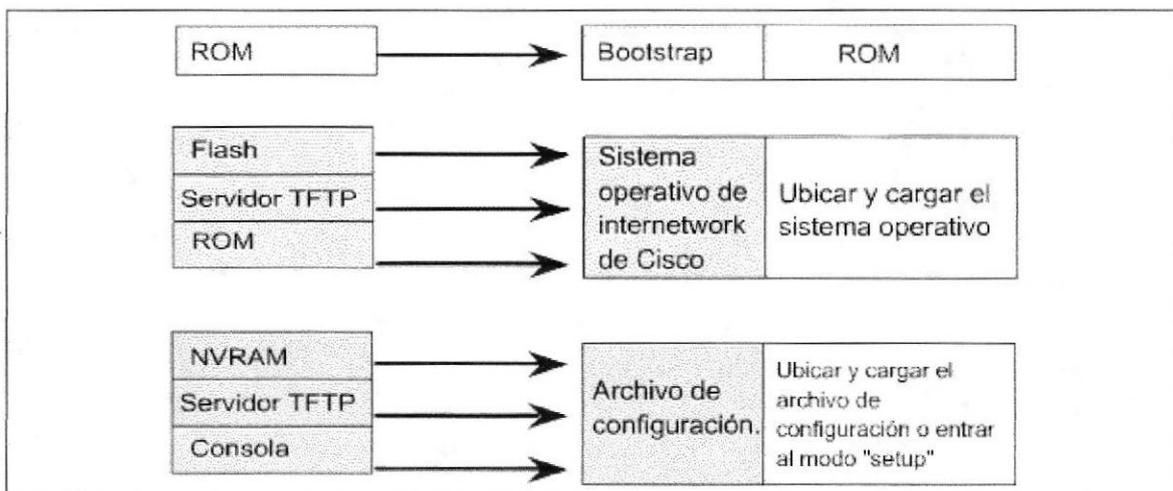


Figura 6-3: Secuencia de arranque.

6.4 COMPONENTES EXTERNOS DE UN ROUTER

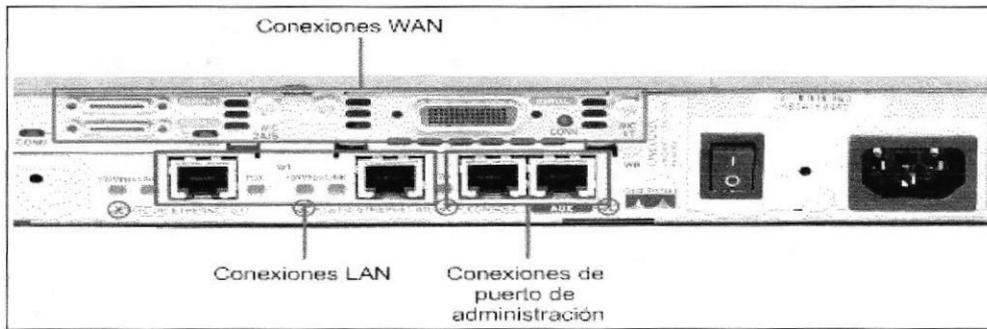


Figura 6-4: Componentes externos de un router.

Las interfaces son las conexiones de los routers con el exterior. Los tres tipos de interfaces son la red de área local (LAN), la red de área amplia (WAN) y la Consola/AUX. Las interfaces LAN generalmente constan de uno de los distintos tipos de Ethernet o Token Ring.

Las interfaces WAN incluyen la Unidad de servicio de canal (CSU) integrada, la RDSI y la serial. Al igual que las interfaces LAN, las interfaces WAN también cuentan con chips controladores para las interfaces. Las interfaces WAN pueden ser de configuraciones fijas o modulares.

Los puertos de Consola/AUX son puertos seriales que se utilizan principalmente para la configuración inicial del router. Estos puertos no son puertos de networking. Se usan para realizar sesiones terminales desde los puertos de comunicación del computador o a través de un módem.



6.5 CONEXIÓN AL PUERTO DE CONSOLA.

6.5.1 REQUERIMIENTOS.

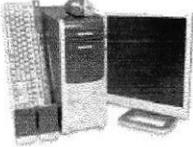
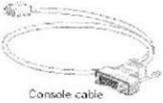
IMAGEN	EQUIPO
	Computador Tarjeta 10/100 Mbps Puerto Com disponible.
	Cable de consola
	Router

Tabla 6-1: Requerimientos para conectar un pc al router.

6.6 CONEXIÓN POR HARDWARE.

Para conectar un PC al Puerto de consola, se debe usar un cable Rollover RJ-45 a RJ-45, y cualquier adaptador DTE RJ-45 a DB-25 o RJ-45 a DB-9 hembra.

- Se debe conectar el extremo RJ-45 del cable de la consola al puerto **consola** del panel posterior del router, tal como se muestra en la figura a continuación.

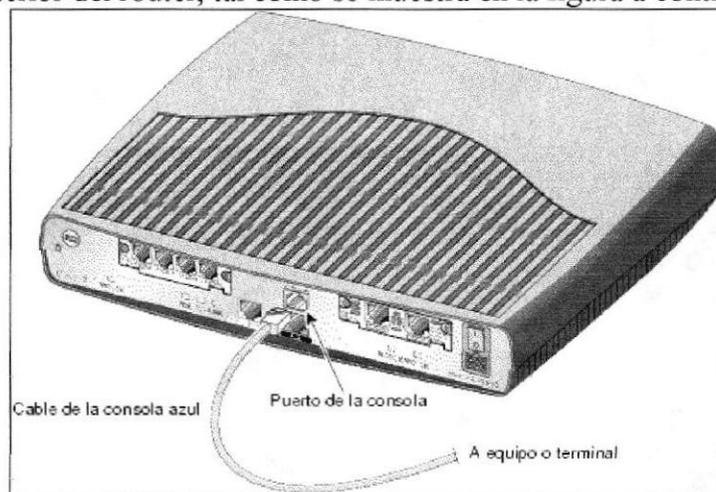


Figura 6-5: Conexión del cable de consola al router.



- Identifique el puerto serial, ubicado el parte posterior del computador.

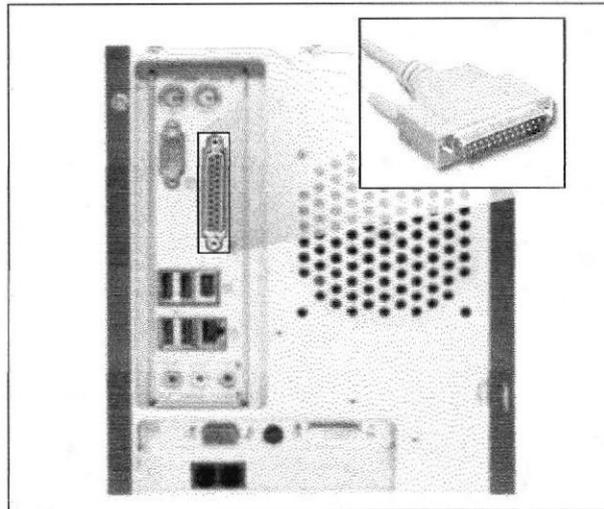


Figura 6-6: Puerto Serial del Computador.

- Conecte el extremo DB-9 del cable de la consola al puerto de la consola (también denominado *puerto serie*) del equipo. Si este adaptador no encaja, necesitará uno adecuado.

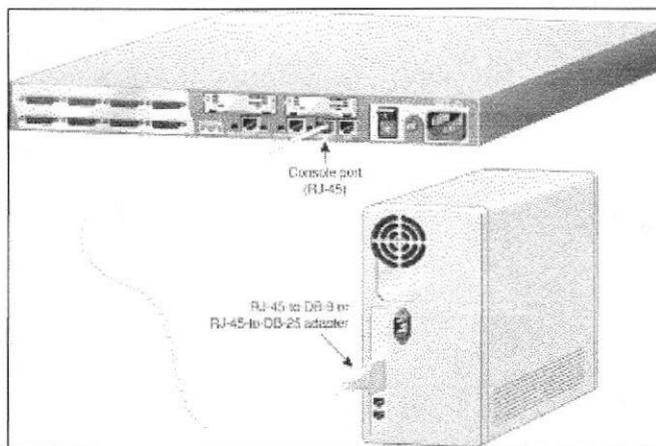


Figura 6-7: Esquema de conexión de un Router a una terminal.

6.7 CONEXIÓN POR (HYPER TERMINAL) A LA CONSOLA DE ROUTER.

Antes de empezar, hay que tener claro que la conexión se realizará a través de la Aplicación HyperTerminal de Windows.

HyperTerminal es un programa que se puede utilizar para conectar con otros equipos, sitios Telnet, sistemas de boletines electrónicos (BBS, Bulletin Board Systems), servicios en línea y equipos host, mediante un módem, un cable de módem nulo o una conexión (Winsock) TCP/IP.

Pasos a seguir:

1. Con un cable transpuesto **RJ-45 a RJ-45** y un adaptador **RJ-45 a DB-9** o **RJ-45 a DB-25** conectar de una Terminal (PC – Personal Computer) al puerto de consola del Router.
2. Abrir la aplicación HyperTerminal siguiendo los siguientes pasos.
 - En el Escritorio de Windows clic con el botón izquierdo en el menú “Inicio”

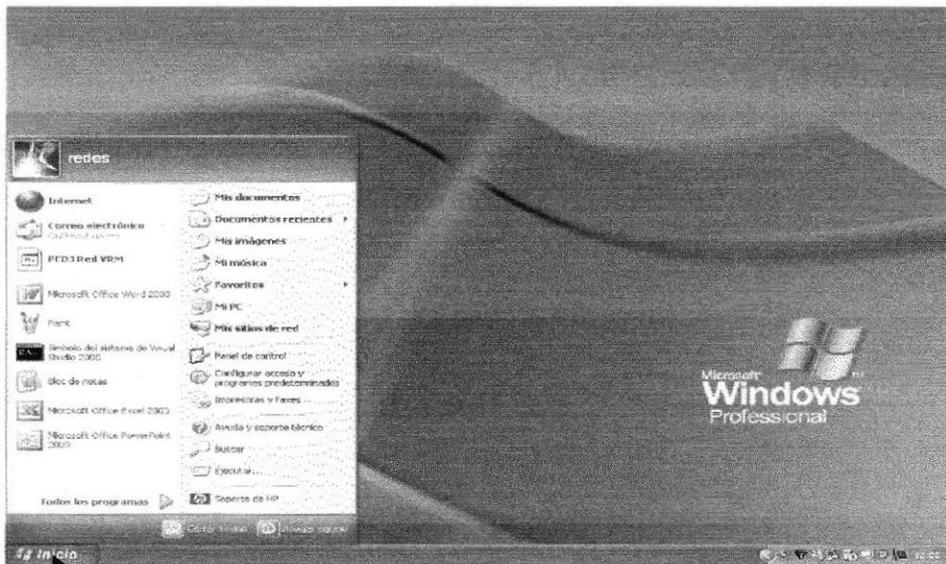


Figura 6-8: Menú Inicio en Windows XP

- En el menú desplegable buscar la opción **“Todos los Programas”** o **“Programas”** según la versión y dar un clic con el botón izquierdo la cual desplegará otro pequeño submenú.

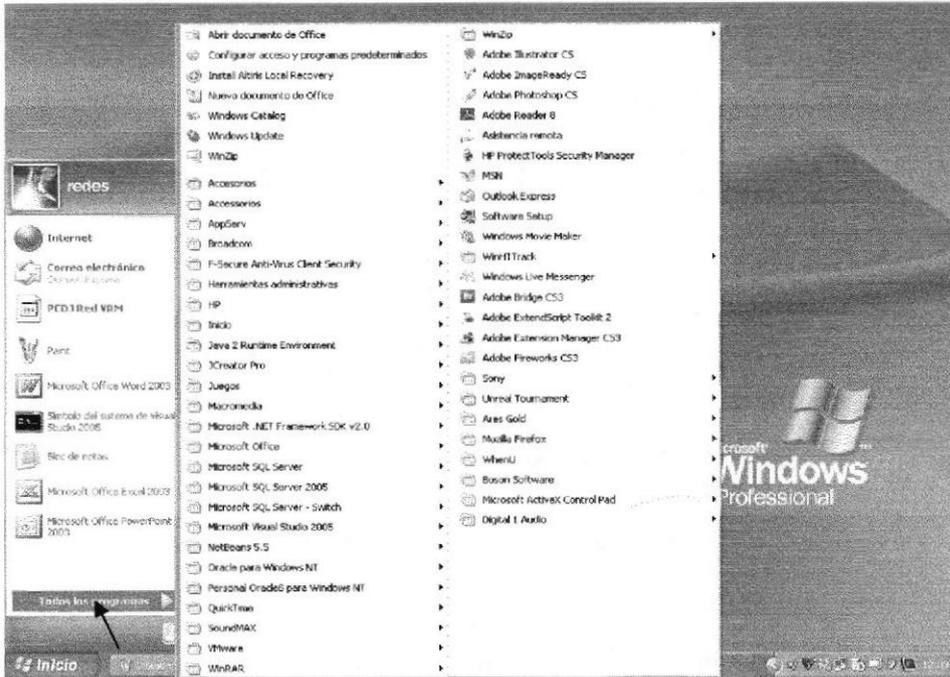


Figura 6-9: Menú Todos los Programas en Windows XP

- En el submenú buscar la opción **“Accesorios”** y dar un clic izquierdo, la cual hará acceder a un nuevo nivel de submenú.

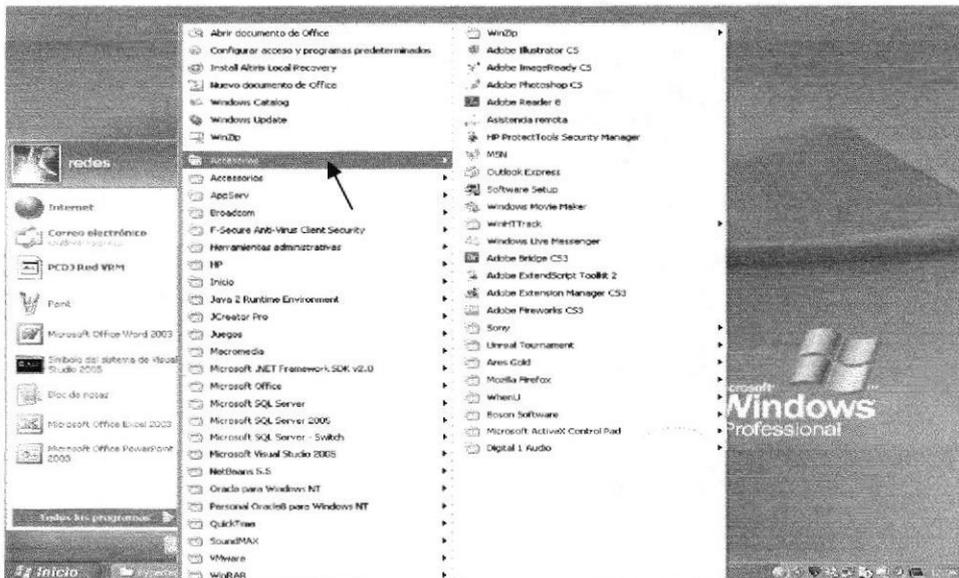


Figura 6-10: Menú Accesorios

- En este submenú aparecerá algunas de las herramientas que proporciona Windows, y la que interesa es la de Comunicaciones, dar clic izquierdo.

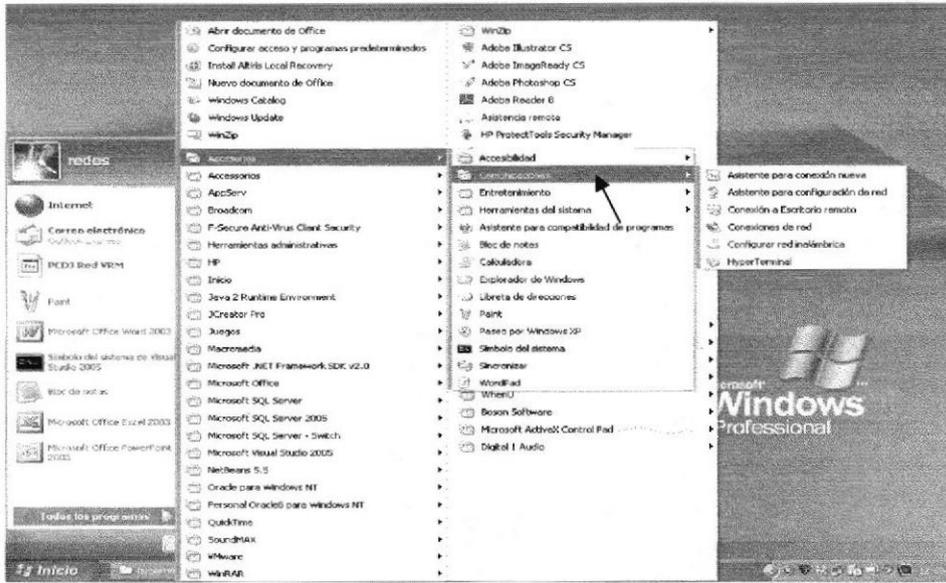


Figura 6-11: Menú Comunicaciones

- Buscar la aplicación de HyperTerminal en el submenú que se desplegó y dar clic izquierdo.

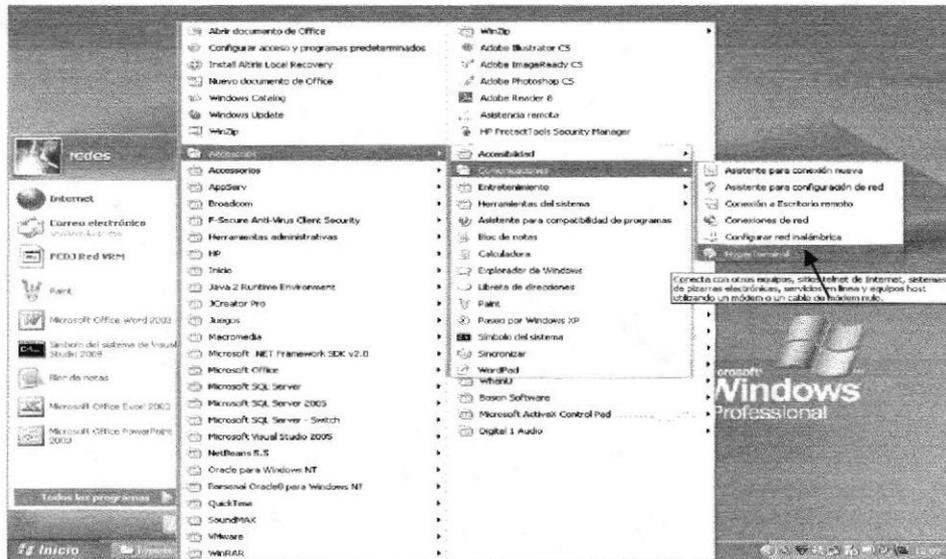


Figura 6-12: Aplicación HyperTerminal

- 3. Una vez que se ha encontrado dar clic izquierdo en el menú de HyperTerminal, si es la primera vez que se accede a esta aplicación, aparecerá una ventana de Advertencia, donde se recomienda establecer la Aplicación HyperTerminal como programa predeterminado de Telnet.

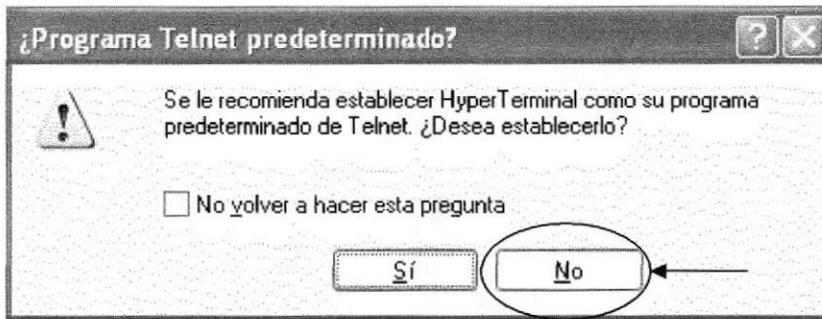


Figura 6-13: Pantalla de recomendación de programa predeterminado para Telnet

- La primera opción es si se desea volver a ver esta pregunta la próxima vez que se acceda al HyperTerminal. Esta opción no afectará en lo más mínimo a la conexión.
- Ahora presenta dos opciones de respuesta referente a la recomendación que hace Windows, si se acepta "Sí" automáticamente aparecerá una ventana, la cual solicita cierta información para una conexión mediante un MODEM; pero como este no es el caso simplemente "cancelar", y automáticamente aparecerá la ventana de "Descripción de conexión" de la HyperTerminal.
- Especifique el país en el que se encuentra, especifique el código de área, el número telefónico de acceso, dar clic en **Aceptar**.

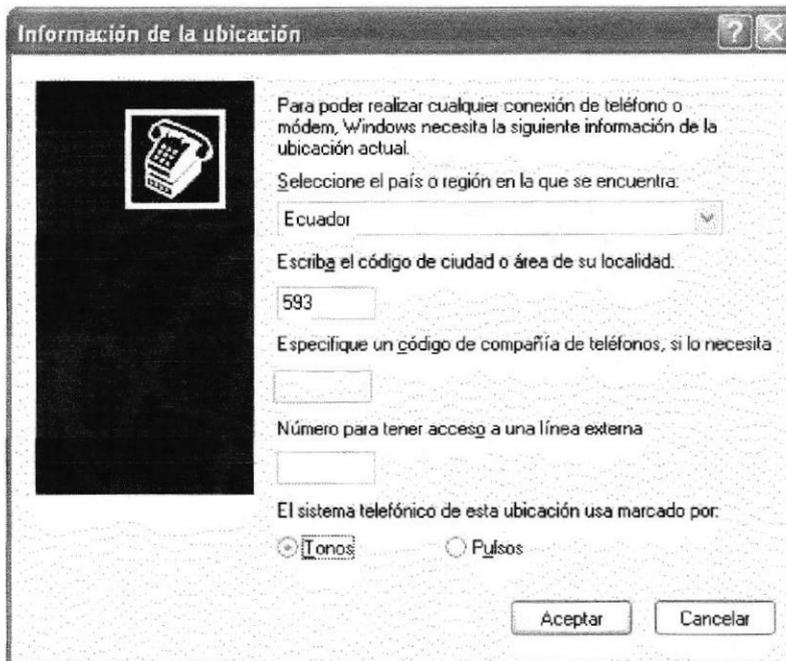


Figura 6-14: Menú Información de Ubicación



- Al terminar la configuración del modem aparecerá una pantalla que muestra los datos anteriormente suministrados, dar clic en **Aceptar**.

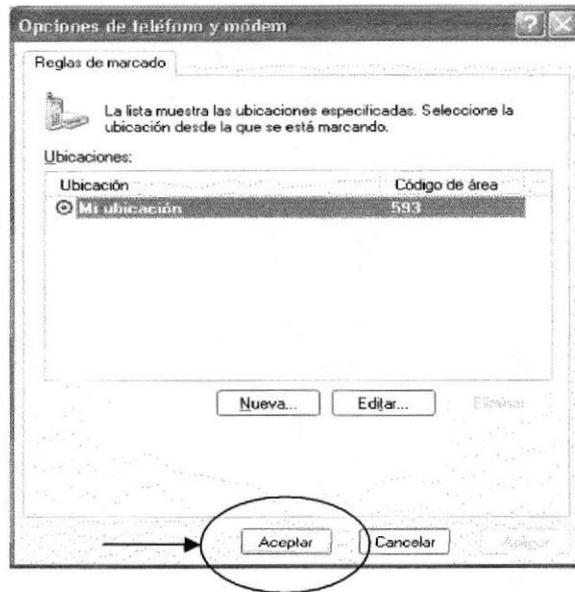


Figura 6-15: Pantalla de opciones de teléfono y modem.

- Si en un caso en la ventana que Windows recomienda establecer a la aplicación HyperTerminal como predeterminada para Telnet, se la cancela, automáticamente aparecerá la ventana de **“Descripción de la conexión”** de la HyperTerminal.

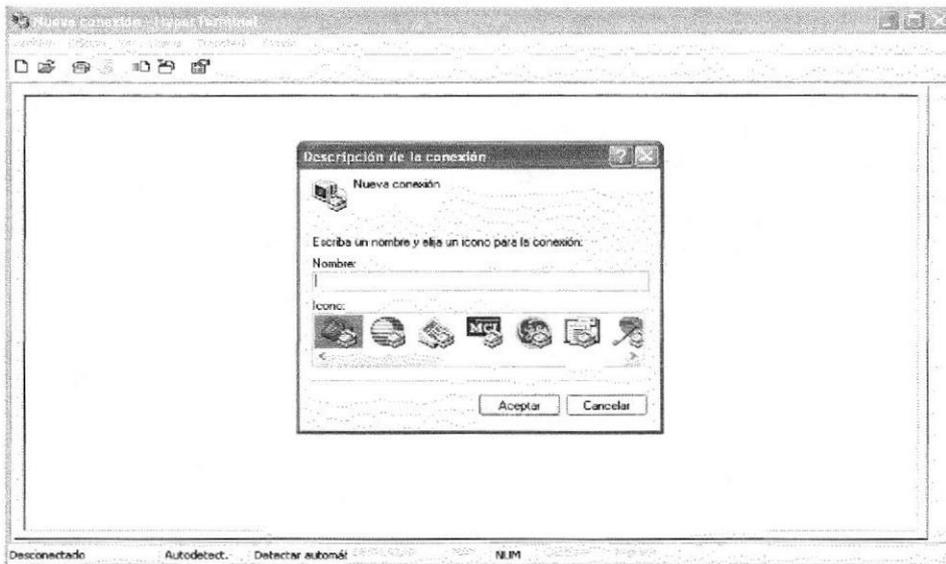


Figura 6-16: Pantalla de Descripción de la conexión de la HyperTerminal



4. En la ventana de **“Descripción de la conexión”** de la HyperTerminal pedirá un nombre y un icono para la conexión.
 - El nombre puede ser cualquiera, en este caso se llamará Grupo_Tia.
 - Cada icono es un tipo de conexión diferente, para este caso utilizar el primero, el que viene marcado por default.
 - Si se llena los datos que pide la ventana de **“Descripción de conexión”** y da clic en aceptar, automáticamente aparecerá la venta de **“Conectar a”**

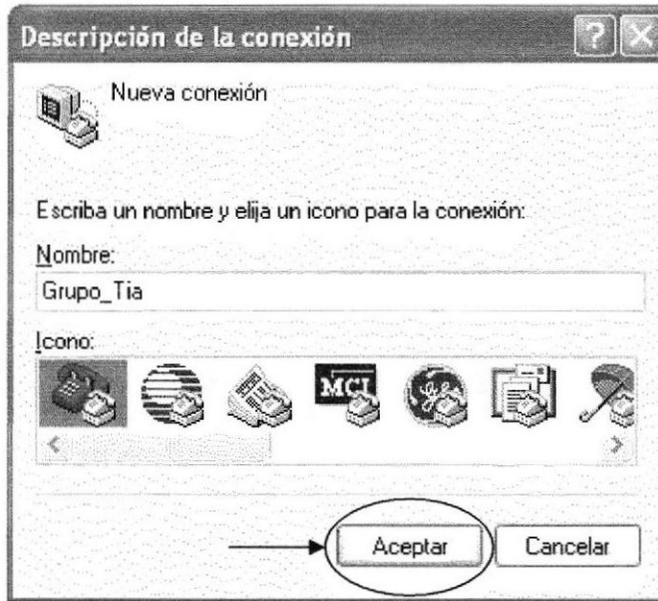


Figura 6-17: Pantalla Descripción de la conexión



Figura 6-18: Pantalla Conectar a



5. En la ventana de “**Conectar a**” aparte de la opción “**Conectar usando**” las demás vendrán deshabilitadas, y en la opción habilitada escoger por medio de que puerto del computador y conectarse al router, por lo general es el puerto COM1, y viene por default. Al desplegar la caja de texto se podrá ver los diferentes puertos disponibles del PC.
 - Si se acepta, aparecerá una ventana de “**Propiedades del COM1**”, estas son la propiedades del puerto que deberá escoger para conectarse con el Router.

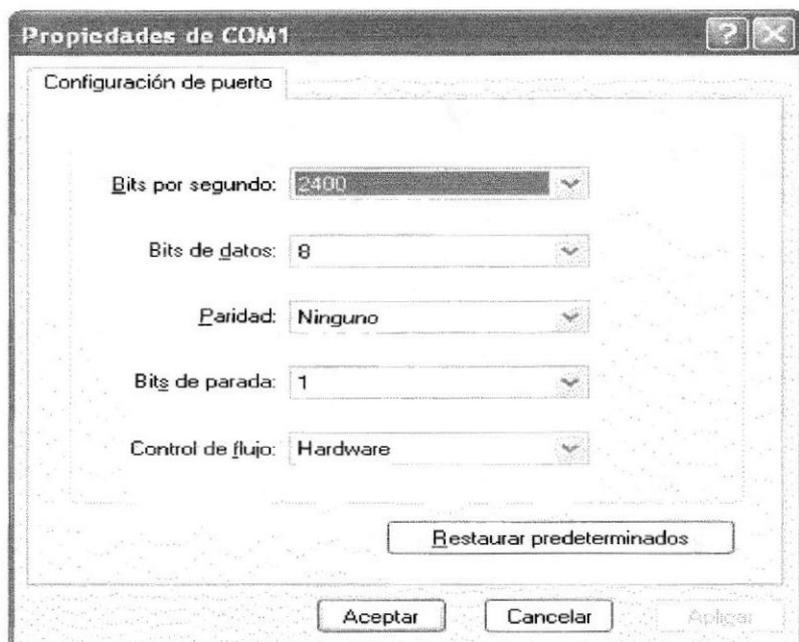


Figura 6-19: Pantalla Default de COM1

6. En la ventana de “**Propiedades de COM1**”, se debe configurar según las especificaciones dadas a continuación.
 - 9600 bps
 - 8 bits de datos
 - Ninguno (paridad)
 - 1 (Bit de parada)
 - Ninguno (Control de flujo)

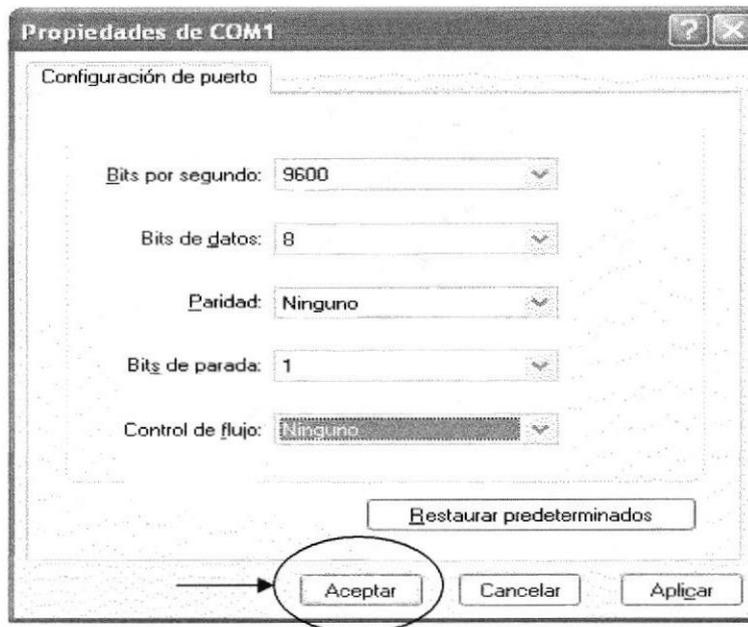


Figura 6-20: Pantalla Propiedades de COM1

- a. La pantalla de “**Propiedades de COM1**” proporciona 3 diferentes opciones: Restaurar Predeterminados, Aceptar, Cancelar y Aplicar. Cada una tiene una función diferente. Si se da clic izquierdo en el botón **Restaurar Predeterminados**, las propiedades del COM1 regresarán a las que estaban cuando recién se abrió la ventana.
- b. La segunda opción es “**Aplicar**”, esta opción establecerá las opciones que se están configurando, pero aun no los hará surtir efecto.
- c. La otra opción es la ventana de “**Propiedades de COM1**” es la de “**Aceptar**”, esta opción surtirá efecto las opciones configuradas, inclusive se podrá obviar el paso de primero “**Aplicar**” y luego “**Aceptar**”. Una vez dado clic en “**Aceptar**” conectarse inmediatamente al Router.



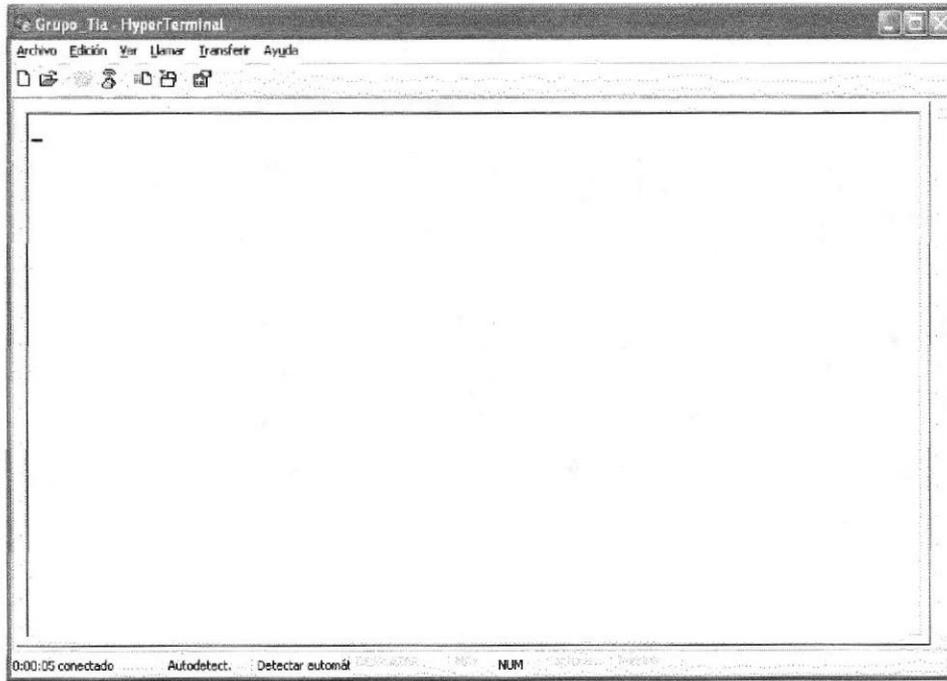


Figura 6-21: Pantalla Inicio de Interfaz con el Router

- d. La tercera y ultima opción es la de **“Cancelar”**, si se da clic aquí automáticamente la ventana se cerrará y se activará la ventana de **“Nueva Conexión - HyperTerminal”**, luego se la cierra según lo requerido y ya aprendido.



BIBLIOTECA
CAMPUS
PEÑAS

6.8 CONEXIÓN ROUTER A ROUTER.

6.8.1 REQUERIMIENTOS.

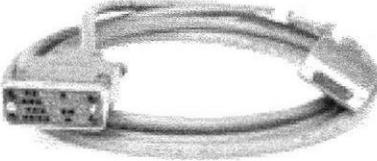
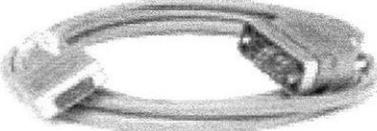
IMAGEN	EQUIPO
	<p>Dos Router</p>
	<p>Cable DCE</p>
	<p>Cable DTE</p>

Tabla 6-2: Requerimientos para conectar dos router.

6.9 CONEXIÓN DE CABLES.

Siga estos pasos para conectar dos router entre sí:

- Identifique el conector DCE y DTE de cada cable serial.

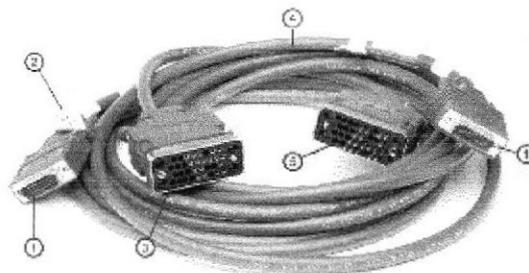


Figura 6-22: Descripción cables seriales.

- | | |
|------------------------------|--|
| 1 Conector serial del Router | Conectado al Puerto serial del router. |
| 2 Etiqueta | Información Provista acerca del cable. |
| 3 Conector DCE DB-60 | Es provisto con una interfaz para conectar el DTE. |
| 5 Conector DTE DB-60 | Conector que se une al del DCE. |



BIBLIOTECA
CAMPUS
PEÑAS

- Conectar el extremo de los cables seriales DCE con DTE de manera que se forme un solo cable.

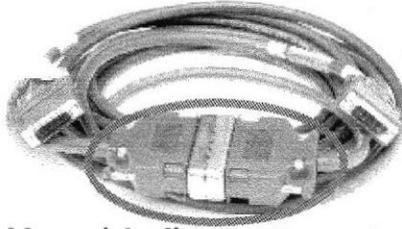


Figura 6-23: Cables seriales listos para conectarse a los routers.

- Identificar las interfaces seriales de cada router, por lo general se encuentran en la parte delantera del router.

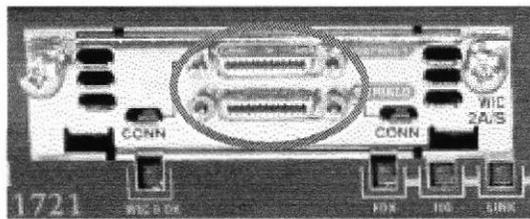


Figura 6-24: Vista frontal del router.

- Conectar los extremos de los cables a una de las interfaces seriales de cada router, de modo que quede un extremo conectado a un router y el otro extremo en el otro router.



Figura 6-25: Esquema de conexión entre router.



6.10 MODOS DE INTERFAZ DE USUARIO.

La interfaz de línea de comando (CLI) de Cisco usa una estructura jerárquica, la misma que requiere el ingreso a distintos modos para realizar tareas particulares. Por ejemplo, para configurar una interfaz del router, el usuario debe ingresar al modo de configuración de interfaces. Desde el modo de configuración de interfaces, todo cambio de configuración que se realice, tendrá efecto únicamente en esa interfaz en particular.

Como característica de seguridad, el software Cisco IOS divide las sesiones EXEC en dos niveles de acceso, que son el modo EXEC usuario y el modo EXEC privilegiado, denominado también modo enable.

6.10.1 ASIGNAR NOMBRE AL ROUTER.

Antes de empezar la configuración de un router se debe establecer un nombre para el mismo, esta tarea se la realizará desde el modo de configuración global.

```
Router(config)#hostname Jonathan  
Jonathan(config)#
```

```
Press Enter to Start  
  
Router>  
Router>enable  
Router#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#hostname Jonathan  
Jonathan(config)#
```

Figura 6-26: Asignación de nombre router.

Una vez presionada la tecla **Enter**, la petición de entrada ya no mostrará el nombre de host por defecto ('Router'), sino el nombre de host que se acaba de asignar.



6.10.2 ASIGNAR CONTRASEÑAS AL ROUTER.

Las contraseñas sirven para restringir el acceso a los routers, estas deben configurarse para las líneas de terminales virtuales (line vty), para habilitar el acceso remoto de usuarios al router mediante Telnet. Normalmente y para la línea de consola (line console).

Aunque es opcional, se recomienda configurar una contraseña para la línea de comando.

```
Router(config)#line console 0
Router(config-line)#password cisco(cualquier contraseña)
Router(config-line)#login
```

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#|
```

Figura 6-27: Asignación de contraseña router 1.

Los routers Cisco permiten cinco líneas de VTY identificadas del 0 al 4, aunque según el hardware particular, puede haber modalidades diferentes para las conexiones de VTY.

Se suele usar la misma contraseña para todas las líneas, pero a veces se reserva una línea mediante una contraseña exclusiva, para que sea posible el acceso al router aunque haya demanda de más de cuatro conexiones.

```
Router(config)#line vty 0 4
Router(config-line)#password cisco(cualquier contraseña)
Router(config-line)#login
```

```
Router>ena
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#|
```

Figura 6-28: Asignación de contraseña router 2.

Los comandos `enable password` y `enable secret` (contraseña encriptada) se utilizan para restringir el acceso al modo EXEC privilegiado. El comando `enable password` se utiliza sólo si no se ha configurado previamente `enable secret`.

```
Router(config)#enable password cisco
Router(config)#enable secret cisco
```

```
Router(config)#enable password cisco
Router(config)#enable secret cisco
Router(config)#|
```

Figura 6-29: Asignación de contraseña router 2.



En ocasiones es deseable evitar que las contraseñas se muestren en texto sin cifrar al ejecutar los comandos `show running-config` o `show startup-config`. Por tal razón se usa el comando `service password-encryption` para cifrar las contraseñas al mostrar los datos de configuración.

```
Router(config)#service password-encryption
```

```
Router(config)#service password encryption
```

Figura 6-30: Asignación de contraseña encriptada router.

El comando `service password-encryption` aplica un cifrado débil a todas las contraseñas sin cifrar. El comando `enable secret <password>` usa un fuerte algoritmo MD5 para cifrar.

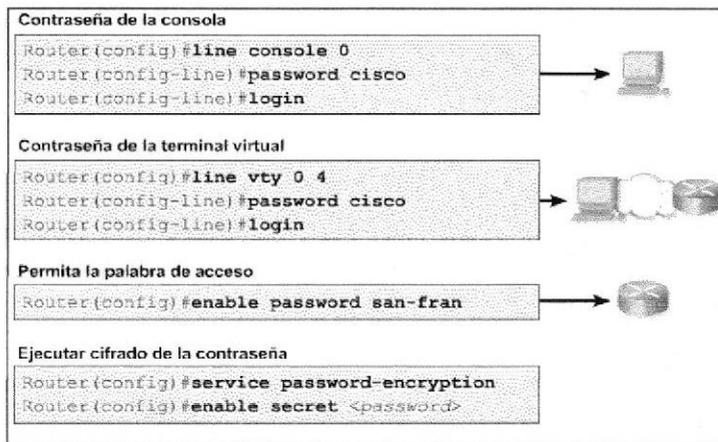
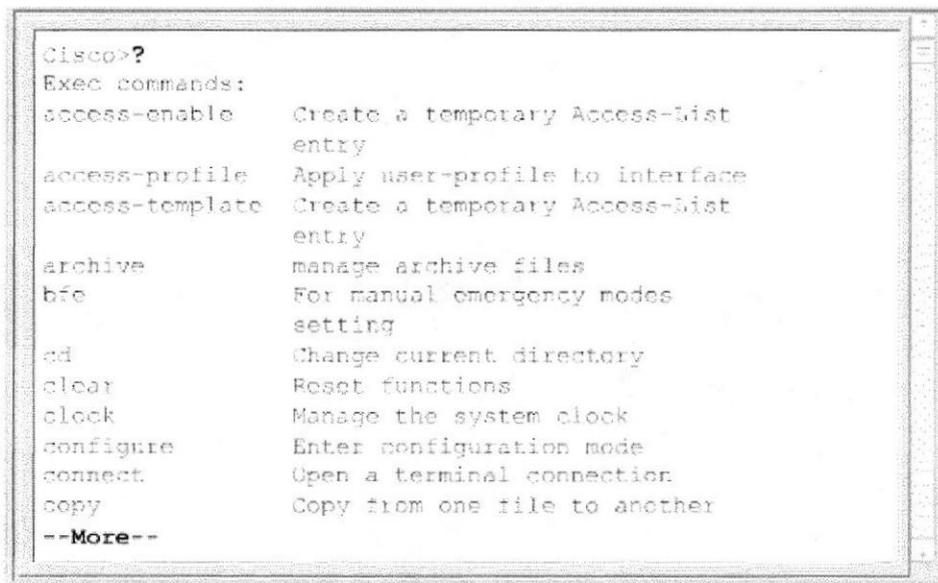


Figura 6-31: Configuración de contraseñas.



6.10.3 COMANDO DE AYUDA MEDIANTE TECLADO.

Al escribir un signo de interrogación (?) en la petición de entrada del modo usuario o del modo privilegiado, aparece una útil lista de los comandos disponibles.



```

Cisco>?
Exec commands:
access-enable      Create a temporary Access-list
                   entry
access-profile     Apply user-profile to interface
access-template    Create a temporary Access-list
                   entry
archive            manage archive files
bfe                For manual emergency modes
                   setting
cd                 Change current directory
clear              Reset functions
clock              Manage the system clock
configure          Enter configuration mode
connect            Open a terminal connection
copy               Copy from one file to another
--More--
  
```

Figura 6-32: Ayuda mediante el teclado.

Es decir, que cuando no se conoce el comando adecuado a utilizar se puede usar el signo? para listar por pantalla los comandos con su respectiva sintaxis que el modo en uso contiene.

6.10.4 DEFINICIÓN DE COMANDOS SHOW.

Los numerosos comandos **show** se pueden utilizar para examinar el contenido de los archivos en el router y para diagnosticar fallas. Tanto en el modo privilegiado como en el modo de usuario.

- **show interfaces:** Muestra las estadísticas completas de todas las interfaces del router. Para ver las estadísticas de una interfaz específica, ejecute el comando `show interfaces` seguido de la interfaz específica y el número de puerto.
- **show controllers serial:** muestra información específica de la interface de hardware. El comando debe incluir el número de puerto y/o de ranura de la interfaz.
- **show clock:** Muestra la hora fijada en el router.
- **show hosts:** Muestra la lista en caché de los nombres de host y sus direcciones.
- **show users:** Muestra todos los usuarios conectados al router.
- **show history:** Muestra un historial de los comandos ingresados.



- **show flash:** Muestra información acerca de la memoria flash y cuáles archivos IOS se encuentran almacenados allí.
- **show version:** Despliega la información acerca del router y de la imagen de IOS que esté corriendo en al RAM. Este comando también muestra el valor del registro de configuración del router.
- **show ARP:** Muestra la tabla ARP del router.
- **show protocols:** Muestra el estado global y por interface de cualquier protocolo de capa 3 que haya sido configurado.
- **show startup-configuration:** Muestra el archivo de configuración almacenado en la NVRAM.
- **show running-configuration:** Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.

6.10.5 CONFIGURACIÓN DE UNA INTERFAZ SERIAL.

Es posible configurar una interfaz serial desde la consola o a través de una línea de terminal virtual.

- Ingrese al modo de configuración global.
- Ingrese al modo de configuración de interfaz.
- Especifique la dirección de la interfaz y la máscara de subred.
- Si el cable de conexión es DCE, fije la velocidad de sincronización. Omita este paso si el cable es DTE.
- Active la interfaz.

A cada interfaz serial activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP. Configure la dirección de IP mediante los siguientes comandos:

```
Router(config)#interface serial 0
Router(config-if)#ip address 192.168.7.1 255.255.255.252
```

```
Router(config)#interface serial 0
Router(config-if)#ip address 192.168.7.1 255.255.255.252
Router(config-if)#|
```

Figura 6-33: Dar dirección a una interfaz serial.



BIBLIOTECA
CAMPUS
PEÑAS

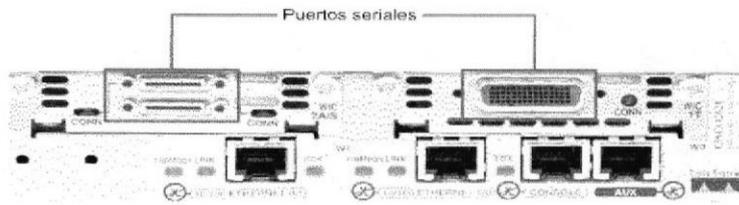


Figura 6-34: Puertos seriales.

- El DTE y el DCE son dos tipos de interfaces seriales que los dispositivos usan para comunicarse. La diferencia clave entre los dos es que el dispositivo DCE proporciona la señal reloj para las comunicaciones en el bus. La documentación del dispositivo debe especificar si es DTE o DCE.

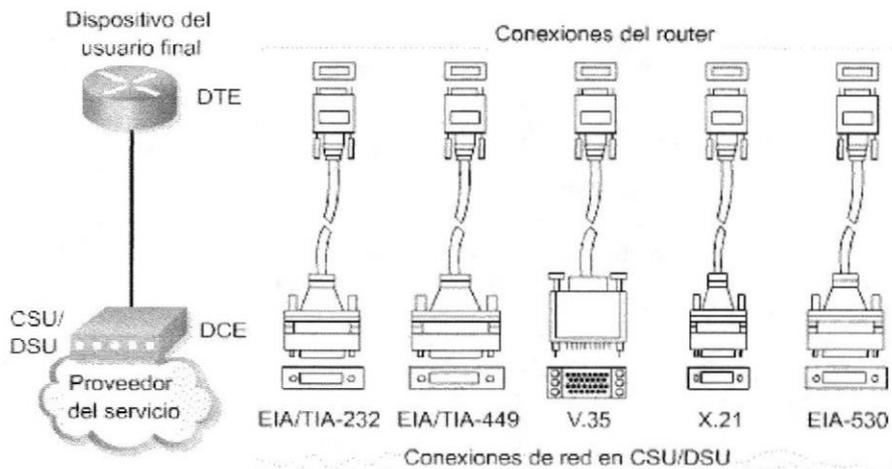


Figura 6-35: Conectores DCE y DTE.

- Cada dispositivo podrá requerir un estándar serial diferente. Cada estándar define las señales del cable y especifica el conector del extremo del cable. Siempre se debe consultar la documentación del dispositivo para obtener información sobre el estándar de señalización.



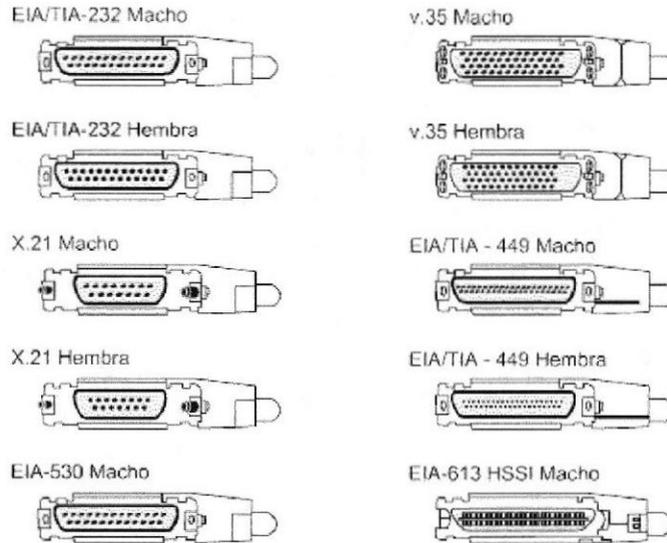


Figura 6-36: Conectores hembra y macho.

- Si el conector tiene ping salientes visibles, es macho. Si el conector tiene tomas para los ping salientes, es hembra.

En los enlaces seriales interconectados directamente, un extremo debe considerarse como un DCE y debe proporcionar la señal de sincronización. Se activa la sincronización y se fija la velocidad mediante el comando `clock rate`. Las velocidades de sincronización disponibles (en bits por segundo) son: 56000, 64000, 72000, etc... No obstante, es posible que algunas de estas velocidades no estén disponibles en algunas interfaces seriales, según su capacidad.

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ingresa el comando `no shutdown`. Cuando resulte necesario inhabilitar administrativamente una interfaz a efectos de mantenimiento o de diagnóstico de fallas, se utiliza el comando `shutdown` para desactivarla.

```
Router(config)#interface serial 0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

```
Router(config)#interface serial 0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
Router(config-if)#
```

Figura 6-37: Levantar el estado serial.



6.10.6 CONFIGURACIÓN DE UNA FASTETHERNET.

Se puede configurar una interfaz Ethernet desde la consola o a través de una línea de terminal virtual.

- Ingrese al modo de configuración global.
- Ingrese al modo de configuración de interfaz.
- Especifique la dirección de la interfaz y la máscara de subred.
- Active la interfaz.

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ejecuta el comando `no shutdown`. Cuando resulte necesario inhabilitar administrativamente una interfaz a efectos de mantenimiento o diagnóstico de fallas, se utiliza el comando `shutdown` para desactivarla.

```
Router#configure terminal
Router(config)#interface fasthethernet 0/0
Router(config-if)#ip address 192.168.7.33 255.255.255.248
Router(config-if)#no shutdown
```

```
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip add 192.168.7.33 255.255.255.248
Router(config-if)#no shutdown
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
Router(config-if)#
```

Figura 6-38: Levantar el estado de una fastethernet.

6.10.7 TIPO DE ENRUTAMIENTO.

- Enrutamiento estático.
- Enrutamiento por defecto.
- Enrutamiento dinámico.

6.10.7.1 ENRUTAMIENTO ESTÁTICO.

Las operaciones con rutas estáticas pueden dividirse en tres partes:

- El administrador de red configura la ruta.
- El router instala la ruta en la tabla de enrutamiento.
- Los paquetes se enrutan de acuerdo a la ruta estática.

Como las rutas estáticas se configuran manualmente, el administrador debe configurarla en el router, mediante el comando `ip route`, seguido de la dirección de red, máscara respectiva e interfaz saliente.

```
Router(config)#ip route 192.168.12.0 255.255.255.0 s0
```



La distancia administrativa es un parámetro opcional que da una medida del nivel de confiabilidad de la ruta. Un valor menor de distancia administrativa indica una ruta más confiable. La distancia administrativa por defecto cuando se usa una ruta estática es 1.

6.10.7.2 ENRUTAMIENTO POR DEFECTO.

Las rutas por defecto se usan para enviar paquetes a destinos que no coinciden con los de ninguna de las otras rutas en la tabla de enrutamiento. Generalmente, se las usa para el tráfico que se dirige a la Internet, ya que a menudo resulta poco práctico e innecesario mantener rutas hacia todas las redes de la Internet.

```
Router#configure terminal
Router(config)# ip route 0.0.0.0 0.0.0.0 s0
Router(config)# exit
Router# copy running-config startup-config
```

6.10.7.3 ENRUTAMIENTO DINÁMICO.

El enrutamiento dinámico significa que el router va averiguando las rutas para llegar al destino por medio de actualizaciones periódicas enviadas desde otros routers.

6.10.8 INTRODUCCIÓN A PROTOCOLOS DE ENRUTAMIENTO.

Los protocolos de enrutamiento son diferentes a los protocolos enrutados tanto en su función como en su tarea.

Un protocolo de enrutamiento es el esquema de comunicación entre routers. Un protocolo de enrutamiento permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers. La información que un router obtiene de otro, mediante el protocolo de enrutamiento, es usada para crear y mantener las tablas de enrutamiento.

Ejemplos de protocolos de enrutamiento:

- Protocolo de información de enrutamiento (RIP).
- Protocolo de enrutamiento de gateway interior (IGRP).
- Protocolo "Primero la ruta más corta" (OSPF).

Un protocolo enrutado se usa para dirigir el tráfico generado por los usuarios. Un protocolo enrutado proporciona información suficiente en su dirección de la capa de red, para permitir que un paquete pueda ser enviado desde un host a otro, basado en el esquema de direcciones.

Ejemplos de protocolos enrutados:

- Protocolo Internet (IP)
- Intercambio de paquetes de internetwork (IPX)



BIBLIOTECA
CAMPUS
PEÑAS

Los protocolos de enrutamiento aprenden todas las rutas disponibles, incluyen las mejores rutas en las tablas de enrutamiento y descartan las rutas que ya no son válidas. El router utiliza la información en la tabla de enrutamiento para enviar los paquetes de datos. Cuando todos los routers de una red se encuentran operando con la misma información, se dice que la red ha hecho convergencia.

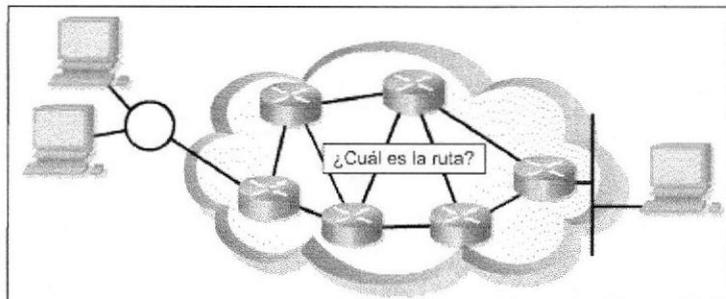


Figura 6-39: Determinación de rutas.

6.10.8 IGRP PROTOCOLO DE ENRUTAMIENTO INTERIOR DE GATEWAY.

Características:

- Es un protocolo de enrutamiento por vector-distancia.
- Se considera el ancho de banda, la carga, el retardo y la confiabilidad para crear una métrica compuesta.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 90 segundos.

6.10.8 PROTOCOLO DE ENRUTAMIENTO POR VECTOR DISTANCIA (RIP).

Los protocolos de enrutamiento por vector-distancia envían copias periódicas de las tablas de enrutamiento de un router a otro. Estas actualizaciones periódicas entre routers informan de los cambios de topología. Los algoritmos de vector-distancia no permiten que un router conozca la topología exacta de una red, ya que cada router solo ve a sus routers vecinos.

Las actualizaciones de las tablas de enrutamiento se producen al haber cambios en la topología. Las tablas de enrutamiento incluyen información acerca del costo total de la ruta (definido por su métrica) y la dirección lógica del primer router en la ruta hacia cada una de las redes indicadas en la tabla.

La habilitación del enrutamiento de paquetes de IP, requiere fijar parámetros tanto globales como de enrutamiento. Las tareas globales incluyen la selección de un protocolo de enrutamiento, por ejemplo: RIP, IGRP, EIGRP o OSPF. La tarea principal del modo configuración de enrutamiento es indicar los números IP de la red. El enrutamiento dinámico utiliza comunicaciones broadcast y multicast con los otros routers. La métrica de enrutamiento ayuda a los routers a encontrar la mejor ruta hacia cada red o subred.



6.10.8.1 CARACTERÍSTICAS DEL PROTOCOLO RIP.

- Es un protocolo de enrutamiento por vector-distancia.
- Utiliza el número de saltos como métrica para la selección de rutas.
- Si el número de saltos es superior a 15, el paquete es desechado.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 30 segundos.

6.10.8.2 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP.

El Protocolo de información de enrutamiento (RIP) es un protocolo de enrutamiento por vector-distancia, este protocolo se base en estándares abiertos y que sea de fácil implementación. Aunque RIP carece de la capacidad y de las características de los protocolos de enrutamiento más avanzados.

RIP ha evolucionado desde el Protocolo de enrutamiento con definición de clases, RIP Versión 1 (RIP v1), hasta el Protocolo de enrutamiento sin clase, RIP Version 2 (RIP v2).

El comando **router** inicia el proceso de enrutamiento.

El comando **network** es necesario, ya que permite que el proceso de enrutamiento determine cuáles son las interfaces que participan en el envío y la recepción de las actualizaciones de enrutamiento.

```
router(config)#router rip
router(config-router)#network 192.168.7.0
```

```
Router(config-if)#router rip
Router(config-router)#network 192.168.7.0
Router(config-router)#
```

Figura 6-40: Levantar protocolo de enrutamiento rip.

6.10.8.3 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSION 2.

Capacidad para transportar mayor información relativa al enrutamiento de paquetes. Mecanismo de autenticación para la seguridad de origen al hacer actualizaciones de las tablas. Soporta enmáscaramiento de subredes de longitud variable (VLSM).

```
router#configure terminal
router(config)#router rip
router(config-router)#version 2
router(config-router)#network 192.168.7.0
```

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.7.0
Router(config-router)#|
```

Figura 6-41: Levantar protocolo de enrutamiento rip version 2.



Entre las tareas opcionales se encuentran:

- Aplicar compensaciones a la métrica de enrutamiento.
- Ajustar los temporizadores.
- Especificar una versión de RIP.
- Habilitar la autenticación de RIP.
- Configurar el resumen de las rutas en una interfaz.
- Verificar el resumen de las rutas IP.
- Inhabilitar el resumen automático de rutas.

El comando `show ip route` se puede utilizar para verificar que las rutas recibidas por los routers RIP vecinos estén instaladas en la tabla de enrutamiento. Examine el resultado del comando y busque las rutas RIP que señaladas con "R". Recuerde que la red tardará algún tiempo en converger, de modo que puede que no aparezcan las rutas de forma inmediata.

`router#show ip route`

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

Gateway of last resort is not set

    192.168.7.0/0 is variably subnetted, 3 subnets
C       192.168.7.32/30 is directly connected, FastEthernet0/0
C       192.168.7.0/30 is directly connected, Serial0
R       192.168.7.40/29 [120/1] via 192.168.7.2, 00:02:40, Serial0

Router#
```

Figura 6-42: Protocolos levantados con rip version 2.

6.10.9 PROTOCOLO DE ENRUTAMIENTO ESTADO ENLACE (OSPF).

Los protocolos de enrutamiento de estado del enlace mantienen una base de datos compleja, con la información de la topología de la red. El algoritmo de enrutamiento de estado del enlace mantiene información completa sobre routers lejanos y su interconexión.

OSPF es un protocolo de enrutamiento del estado de enlace basado en estándares abiertos. Se describe en diversos estándares de la Fuerza de Tareas de Ingeniería de Internet (IETF). El término "libre" en "Primero la ruta libre más corta" significa que está abierto al público y no es propiedad de ninguna empresa.

OSPF se puede usar y configurar en una sola área en las redes pequeñas. También se puede utilizar en las redes grandes. Varias áreas se conectan a un área de distribución o a un área 0 que también se denomina backbone. El enfoque del diseño permite el control extenso de las actualizaciones de enrutamiento. La definición de área reduce el gasto de procesamiento, acelera la convergencia, limita la inestabilidad de la red a un área y mejora el rendimiento.

OSPF ofrece soluciones a los siguientes problemas:

- Velocidad de convergencia.
- Admite Máscara de subred de longitud variable (VLSM).
- Tamaño de la red.
- Selección de ruta.
- Agrupación de miembros

CARACTERÍSTICAS DE OSPF.

- Es un protocolo público conocido como "PRIMERO LA RUTA MÁS CORTA"
- Es un protocolo de enrutamiento de estado del enlace.
- Es un protocolo de enrutamiento público (open Standard).
- Usa el algoritmo SPF para calcular el costo más bajo hasta un destino.
- Las actualizaciones de enrutamiento producen un gran volumen de tráfico al ocurrir cambios en la topología.

6.10.9.1 TIPOS DE RED OSPF.

Las interfaces OSPF reconocen tres tipos de redes:

- Multiacceso de broadcast como por ejemplo Ethernet.

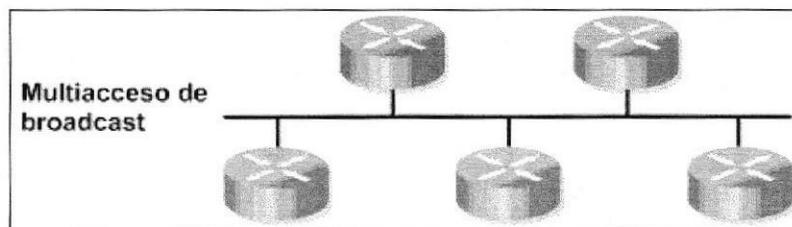


Figura 6-43: Red Ospf con multiacceso de broadcast.

- Redes punto a punto.

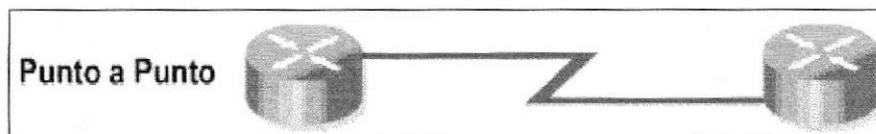


Figura 6-44: Red Ospf punto a punto.

- Multiacceso sin broadcast (NBMA), como por ejemplo Frame Relay.

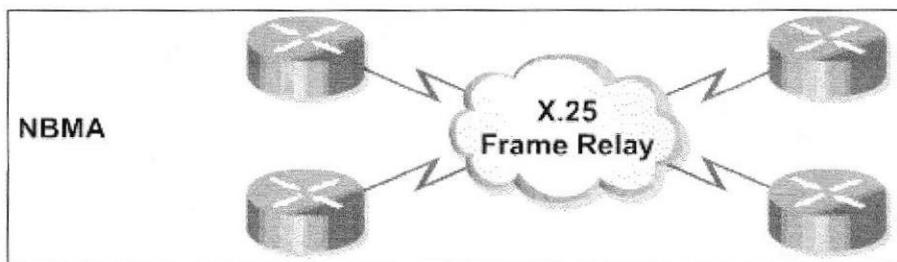


Figura 6-45: Red Ospf con multiacceso sin broadcast.

6.10.9.2 PROTOCOLO HELLO DE OSPF.

Cuando un router inicia un proceso de enrutamiento OSPF en una interfaz, envía un paquete hello y sigue enviando hellos a intervalos regulares. Las reglas de intercambio de paquetes hello de OSPF se denominan protocolo Hello.

En la capa 3 del modelo OSI, los paquetes hello se direccionan hacia la dirección multicast 224.0.0.5. Esta dirección equivale a "todos los routers OSPF". Los routers OSPF utilizan los paquetes hello para iniciar nuevas adyacencias y asegurarse de que los routers vecinos sigan funcionando. Los Hellos se envían cada 10 segundos por defecto en las redes multiacceso de broadcast y punto a punto. En las interfaces que se conectan a las redes NBMA, como por ejemplo Frame Relay, el tiempo por defecto es de 30 segundos.

En las redes multiacceso el protocolo Hello elige un router designado (DR) y un router designado de respaldo (BDR). El paquete hello transmite información para la cual todos los vecinos deben estar de acuerdo antes de que se forme una adyacencia y que se pueda intercambiar información del estado de enlace.

La configuración de OSPF requiere que el proceso de enrutamiento OSPF esté activo en el router con las direcciones de red y la información de área especificadas.

```
Router(config)#router ospf process-id
```

El ID de proceso es un número que se utiliza para identificar un proceso de enrutamiento OSPF en el router. Se pueden iniciar varios procesos OSPF en el mismo router. El número puede tener cualquier valor entre 1 y 65.535.

Se puede habilitar más de un proceso de ejecución de ospf al mismo tiempo en el mismo router si se requiere, este número puede ser el mismo en todos los router sobre la red, o puede ser diferente, esto no importa.

Las redes IP se publican de la siguiente manera en OSPF:

```
Router(config-router)#network address wildcard-mask area area-id
```



```
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.7.0 0.0.0.3 area 0
Router(config-router)#|
```

Figura 6-46: Dar dirección por ospf.

- **Dirección.**-Esta puede ser la dirección de red, subred o de la interfaz. Indica a los routers cuales son los enlaces en los que se deben escuchar publicaciones y que enlaces y redes se deben publicar.
- **Máscara de wildcard.**- Esta es una máscara inversa que se utiliza para determinar como se lee una dirección. La máscara tiene bits wildcard donde 0 representa coincidencia y 1 no es importante.
- **Id de área.**- Este valor indica el área que se debe asociar con una dirección. Puede ser un número o puede ser similar a una dirección ip. Para un área backbone, la id deber ser igual a 0.

Ejemplo: **area 0**

Contienen la misma información de red, todos los routers de una misma área se llaman internos, especifica el grupo de nodos o redes contiguos, **base de datos topológica por área**, invisible fuera del área, **reducción del tráfico de ruteo**.

6.10.9.3 MODIFICACIÓN DE LA MÉTRICA DE COSTOS DE OSPF.

OSPF utiliza el costo como métrica para determinar la mejor ruta. Un costo se asocia con el lado de salida de cada interfaz de router. Los costos también se asocian con datos de enrutamiento derivados en forma externa. Por lo general, el costo de ruta se calcula mediante la fórmula $10^8/\text{ancho de banda}$, donde el ancho de banda se expresa en bps. El ancho de banda por defecto para las interfaces seriales Cisco es 1,544 Mbps o 1544 kbps.

```
router(config)#interface serial 0
router(config-if)#bandwidth 5000
```

6.10.9.4 VERIFICACIÓN DE CONFIGURACIÓN OSPF.

Para verificar la configuración de OSPF existe una serie de comandos show.

Show ip protocol.-Esto muestra parámetros para temporizadores, filtros, métricas, redes y otra información acerca de todo el router.

Show ip route.- Ésta es una de las mejores maneras para determinar la conectividad entre el router local y el resto de la red.

Show ip ospf interface.- Esto verifica que las interfaces se hayan configurado en la áreas planificadas. Si no se especifica una dirección loopback, la interfaz con la dirección más alta se considera como el ID del router. Además proporciona los intervalos de temporización como el intervalo hello y muestra las adyacencias del router.

Show ip ospf.- Muestra la cantidad de veces en que se ha usado el algoritmo SPF. También muestra el intervalo de actualización de estado de enlace si no se han producido cambios topológicos.

Show ip ospf neighbor detail. - Este muestra un listado detallado de vecinos, sus prioridades y estados.

Show ip ospf database.- Esto muestra el contenido de la base de datos topológica que mantiene el router y el ID del proceso OSPF.



6.10.10 FIREWALLS.

Un firewall es una estructura arquitectónica que existe entre el usuario y el mundo exterior para proteger la red interna de los intrusos. En la mayoría de los casos, los intrusos provienen de la Internet mundial y de las miles de redes remotas que interconecta. Normalmente, un firewall de red se compone de varias máquinas diferentes que funcionan al mismo tiempo para impedir el acceso no deseado e ilegal.

Se deben utilizar ACL en los routers firewall, que a menudo se sitúan entre la red interna y una red externa, como Internet. Esto permite el control del tráfico entrante o saliente de alguna parte específica de la red interna. El router firewall proporciona aislamiento, de manera que el resto de la estructura interna de la red no se vea afectada.

Se necesita configurar las ACL en routers fronterizos, para brindar mayor seguridad.

Esto proporciona protección básica contra la red externa u otra parte menos controlada de la red, en un área más privada de la red. En estos routers fronterizos, es posible crear ACLs para cada protocolo de red configurado en las interfaces del router.

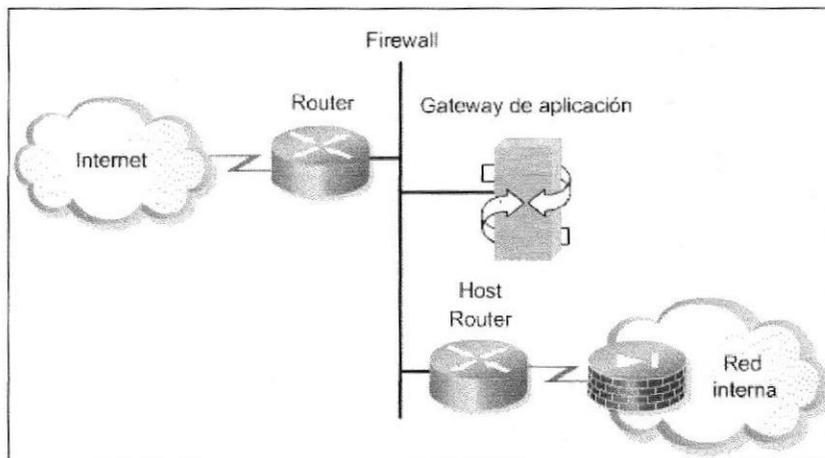


Figura 6-47: Funcionamiento del firewall.

6.10.10 LISTAS DE CONTROL DE ACCESO (ACL).

Los administradores de red deben buscar maneras de impedir el acceso no autorizado a la red, permitiendo al mismo tiempo el acceso de los usuarios internos a los servicios requeridos.

Los routers ofrecen funciones del filtrado básico de tráfico, como el bloqueo del tráfico de Internet, mediante el uso de las listas de control de acceso (ACLs).

Una ACL es una lista secuencial de sentencias de permiso o rechazo, que se aplican a direcciones o protocolos de capa superior.

Las ACL pueden ser tan simples como una sola línea destinada a permitir paquetes desde un host específico o pueden ser un conjunto de reglas y condiciones



extremadamente complejas que definan el tráfico de forma precisa y modelen el funcionamiento de los procesos de los routers.

Es posible crear ACL en todos los protocolos de red enrutados, por ejemplo: el Protocolo de Internet (IP) y el Intercambio de paquetes de internetwork (IPX). Las ACL se pueden configurar en el router para controlar el acceso a una red o subred.

Las ACL filtran el tráfico de red, controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router. El router examina cada paquete y lo enviará o lo descartará, según las condiciones especificadas en la ACL. Algunos de los puntos de decisión de ACL son direcciones origen y destino, protocolos y números de puerto de capa superior.

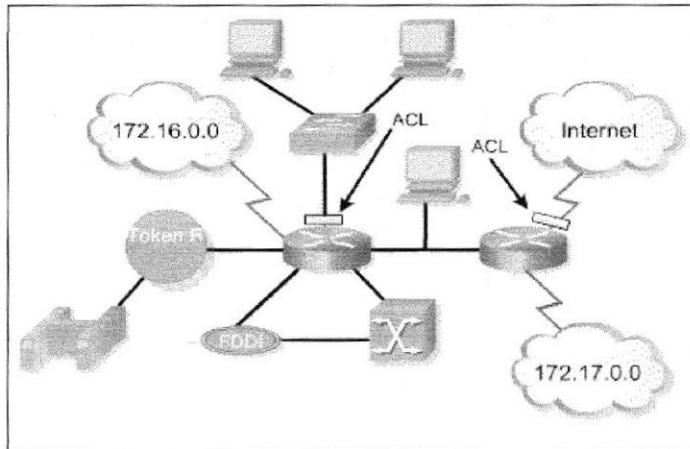


Figura 6-48: Listas de control de acceso.



6.10.10.1 FUNCIONAMIENTO DE LAS ACL.

El orden en el que se ubican las sentencias de la ACL es importante. Una vez que se encuentra una coincidencia, se lleva a cabo la acción de aceptar o rechazar y no se verifican otras sentencias ACL. Si una sentencia de condición que permite todo el tráfico está ubicada en la parte superior de la lista, no se verifica ninguna sentencia que esté por debajo. Si se requieren más cantidad de sentencias de condición en una lista de acceso, se debe borrar y volver a crear toda la ACL con las nuevas sentencias de condición.

6.10.10.2 CREACIÓN DE LAS ACL.

Las ACL se crean en el modo de configuración global. Existen varias clases diferentes de ACLs: estándar, extendidas, IPX, AppleTalk, entre otras.

Cuando configure las ACL en el router, cada ACL debe identificarse de forma única, asignándole un número. Este número identifica el tipo de lista de acceso creado y debe ubicarse dentro de un rango específico de números que es válido para ese tipo de lista.

La configuración de una ACL se realiza con el comando **access-list**. En TCP/IP, las ACL se asignan a una o más interfaces y pueden filtrar el tráfico entrante o saliente, usando el comando **ip access-group** en el modo de configuración de interfaz. Al

asignar una ACL a una interfaz, se debe especificar la ubicación entrante o saliente. Después de crear una ACL numerada, se la debe asignar a una interfaz.

```
router#configure terminal
router(config)#access-list 1 deny 172.20.12.1
router(config)#access-list 1 permit 172.20.12.0 0.0.0.255
router(config)#access-list 1 deny 172.20.0.0 0.0.255.255
router(config)#access-list 1 permit 172.0.0.0
router(config)#interface eth0
router(config-if)#ip access-group 2 in
```

Una ACL que contiene sentencias ACL numeradas no puede ser alterada. Se debe borrar utilizando el comando `no access-list` seguido del número de la acl.

```
router(config)#no access-list 1
```

6.10.10.3 VERIFICACIÓN DE LAS ACL.

El comando `show ip interface` muestra información de la interfaz IP e indica si se ha establecido alguna ACL. El comando `show access-lists` muestra el contenido de todas las ACL en el router. Para ver una lista específica, agregue el nombre o número ACL como opción a este comando. El comando `show running-config` también revela las listas de acceso en el router y la información de asignación de interfaz.

```
Router#show access-lists
Standard IP access list 2
deny 172.16.1.1
permit 172.16.1.0, wildcard bits 0.0.0.255
deny 172.16.0.0, wildcard bits 0.0.255.255
permit 172.0.0.0, wildcard bits 0.255.255.255
Extended IP access list 101
permit tcp 192.168.8.0 0.0.0.255 any eq telnet
permit tcp 192.168.8.0 0.0.0.255 any eq ftp
permit tcp 192.168.0.0 0.0.0.255 any eq ftp-data
Router#
```

Figura 6-49: Pantalla de verificación de la existencia de una acl.

6.10.10.4 ACL ESTÁNDAR.

Las ACL estándar se colocan cerca del destino del tráfico. Esto se debe a sus limitaciones: no se puede distinguir el destino. Usan los números de lista de acceso desde 1 - 99 y de la 1300 - 1999, su sintaxis es:

```
router(config)# access-list access-list-number {deny | permit |
remark} source [source-wildcard] [log]
```

El uso de `remark` facilita el entendimiento de la lista de acceso. Cada `remark` está limitado a 100 caracteres. Por ejemplo, no es suficientemente claro cual es el propósito del siguiente comando: `access-list 1 permit 192.1.89.15.15`. Es mucho más fácil leer un comentario acerca de un comando para entender sus efectos, así como sigue:

```
access-list 1 remark Permit only karix workstation through
access-list 1 permit 192.168.15.1
```

La forma `no` de este comando se utiliza para eliminar una ACL estándar.

```
Router(config)#no access-list access-list-number
```

El comando `ip access-group` relaciona una ACL existente a una interface:

```
Router(config)#ip access-group {access-list-number | access-list-name}
{in | out}
```

6.10.10.5 ACL EXTENDIDAS.

Las ACL extendidas se colocan cerca del origen del tráfico, por eficiencia - es decir, para evitar tráfico innecesario en el resto de la red. Utilizan el número de lista de acceso desde la 100 a la 199 y desde la 2000 a la 2699.

El comando `ip access-group` enlaza una ACL extendida existente a una interfaz. Recuerde que sólo se permite una ACL por interfaz por protocolo por dirección.

El formato del comando es:

```
router(config)#interface eth1
router(config-if)#ip access-group 110 in
router(config-if)#exit
router(config)#
```

6.10.10.6 UBICACIÓN DE LAS ACL.

Las ACL se utilizan para controlar el tráfico, filtrando paquetes y eliminando el tráfico no deseado de la red. Otra consideración importante a tener en cuenta al implementar la ACL es dónde se ubica la lista de acceso. Si las ACL se colocan en el lugar correcto, no sólo es posible filtrar el tráfico sino también toda la red se hace más eficiente. Si se tiene que filtrar el tráfico, la ACL se debe colocar en un lugar donde mejore la eficiencia de forma significativa.

La regla es colocar las ACL extendidas lo más cerca posible del origen del tráfico denegado. Las ACL estándar no especifican las direcciones destino, de modo que se deben colocar lo más cerca posible del destino. Por ejemplo, una ACL estándar se debe colocar en Fa0/0 del Router D para evitar el tráfico desde el Router A.

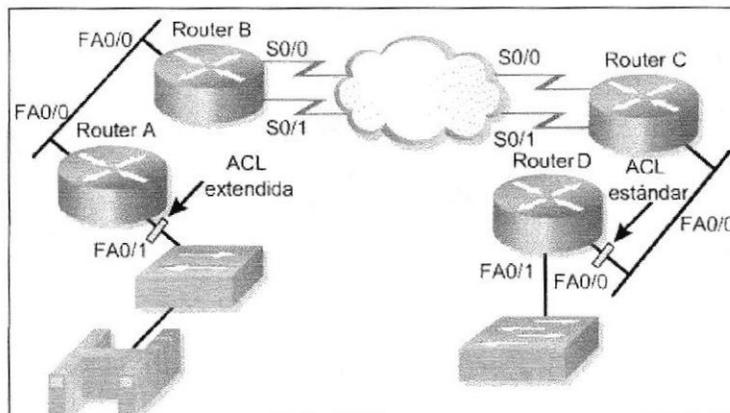


Figura 6-50: Ubicación de las ACL



6.10.11 GUARDANDO LA CONFIGURACIÓN.

Los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán. Para guardar los cambios que vaya realizando en el router utilice el siguiente comando **copy running-config startup-config** o abreviado **wr**.

Guayaquil (config-if)# copy running-config startup-config

Lo que se le indica al router con esta instrucción es que el contenido del archivo **running-config** se copie en el **startup-config**. El archivo **running-config** se encuentra en memoria RAM y el **startup-config** se almacena en memoria **NVRAM**, así, si se pierde el fluido eléctrico la configuración que se tenía se recuperará de la memoria **NVRAM (startup-config)**.

6.10.12 SWITCH.

Un switch es un dispositivo de red de Capa 2 que actúa como punto de concentración para la conexión de estaciones de trabajo, servidores, routers, hubs y otros switches.

Los switches se pueden configurar y administrar desde una interfaz de línea de comando (CLI). Además contienen una unidad de procesamiento central (CPU), memoria de acceso aleatorio (RAM), y un sistema operativo.

Una vez que se conecta el cable de energía eléctrica, el switch inicia una serie de pruebas denominadas Autocomprobación de Encendido (POST).

POST se ejecuta automáticamente para verificar que el switch funcione correctamente.

El LED del sistema indica el éxito o falla de la POST. Si el LED del sistema está apagado pero el switch está enchufado, entonces POST está funcionando.

Si el LED del sistema está verde, entonces la POST fue exitosa, pero si el LED del sistema está ámbar, entonces la POST falló. La falla de la POST se considera como un error fatal. No se puede esperar que el switch funcione de forma confiable si la POST falla.

6.10.12.1 CARACTERÍSTICAS.

- Existen administrables y no administrables
- No comparten velocidad de transmisión.
- El switch no administrable reemplazo al hub.
- Comunicación punto a punto.
- No existen colisiones.
- Los switches de capa 2 centran su administración en direcciones mac y los de capa 3 en direcciones ip.
- El ancho de banda no es compartido.
- Permite reducir el dominio de broadcast
- Controlan broadcast.

- No se puede hacer cascada en más de 8 switch.
- Existen switch con puerto de fibra.
- 10/100/1000 mbps.
- Existen switch:

ethernet	10
fast ethernet	100
gigabit ethernet	1000

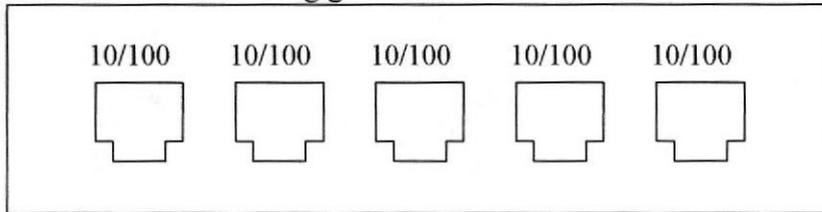


Figura 6-51: Vista frontal de un switch no administrable.

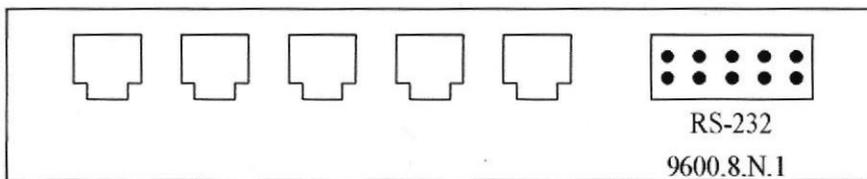


Figura 6-52: Vista frontal de un switch administrable.

6.10.12.2 NIVELES DE TRANSMISIÓN.

- Store and forward
- Fragment free
- Cut through

Por método de almacenamiento y envío (store-and-forward):

- Se recibe la trama entera antes de reenviarla.
- Latencia mayor.
- Se aplican filtros.
- Detección de errores.

Libre de fragmentos (fragment-free):

- Filtra los fragmentos de colisión.
- Después de 64 bytes, se considera válido.

Por método de corte (cut-through):

- Sólo se lee la dirección de destino de la trama.
- Latencia menor.
- Sin detección de errores.



POLITÉCNICA DEL LITORAL

BIBLIOTECA
CAMPUS
PEÑAS

6.10.12.3 TECNOLOGÍA STACK O STACKEABLE.

Permite administrar diferentes dispositivos físicos con un solo dispositivo lógico. Tecnología con fines administrables.

6.10.12.3.1 TRUNKING PORT.

Permite disminuir el nivel de congestión entre 2 dispositivos de comunicación.

Requerimientos: Es necesario que todos los switches sean truncados.

Fuente redundante: Si la fuente principal cae se activa la secundaria.

6.10.12.4 MODOS DE COMANDOS DEL SWITCH.

EXEC de usuario:

- Indicador: >
- Cambia parámetros de terminal.
- Pruebas básicas.
- Mostrar información de sistema.

EXEC privilegiado:

- Indicador: #
- Entrar a él con >enable.
- #configure nos lleva a otros modos de configuración.



BIBLIOTECA
CAMPUS
PEÑAS

6.10.12.5 CONFIGURACIÓN DE UN SWITCH.

6.10.12.6 INTRODUCCIÓN A LAS VLANS.

- Son grupos de servicios de red restringidos según puertos de switch o segmento.
- Se configuran por software, para evitar movimientos físicos. Segmentan redes conmutadas lógicamente.

6.10.12.7 FUNCIONAMIENTO DE UNA VLAN.

Cuando un host se conecta a un puerto de una VLAN, se añade a esa VLAN. Se deben reasignar los puertos de la VLAN debido a que por defecto, están en la VLAN1.

La administración de una VLAN de puerto central sólo está sujeta a la configuración de los puertos, con lo que no hay que montar ni vigilar complejas bases de datos de VLAN. Tanto si la VLAN es dinámica como estática, el administrador debe configurarla.

6.10.12.8 VENTAJAS DE LAS VLANS.

- Trasladar fácilmente las estaciones de trabajo en la LAN
- Agregar fácilmente estaciones de trabajo a la LAN
- Cambiar fácilmente la configuración de la LAN
- Controlar fácilmente el tráfico de red
- Mejorar la seguridad.

6.10.12.9 CONFIGURACIÓN DE UNA VLAN.

Creación:

```
#vlan database
(vlan)#vlan número_de_VLAN
```

```
Switch#vlan database
Switch(vlan)#vlan 10 name Sistemas
VLAN 10 added:
  Name: Sistemas
APPLY completed.
Exiting....
Switch#
```

Figura 6-53: Creación del nombre de la vlan.

Añadir un puerto a una VLAN:

```
interface número_de_interfaz
(config-if)#switchport access VLAN número_de_VLAN.
```

```
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 10
Switch(config-if)#
```

Figura 6-54: Truncar puerto vlan.



Verificación: show vlan: muestra características de todas las VLAN

```
Switch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12
10	Sistemas	active	Fa0/1
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ihm	-	0	0

Switch#

Figura 6-55: Verificación de puerto asignado a la vlan.



6.10.13 CONFIGURACIÓN DE ROUTERS.

6.10.14 CONFIGURACIÓN DEL ROUTER MATRIZ GUAYAQUIL.



ASIGNAR NOMBRE.

Router>**enable**

- A nivel del modo usuario normal, se debe digitar el comando anterior para pasar a modo de usuario privilegiado.

Router#**configure terminal**

- Digitar éste comando en el modo de usuario privilegiado para pasar al modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.

- Aparecerá un mensaje que le indica al usuario que debe ingresar los comandos de configuración, línea por línea.

Router(config)#**hostname Matriz_Gye**

- En el modo de configuración general, digitar el comando anterior y a continuación un nombre para el dispositivo.

6.10.15 CONFIGURACIÓN DE INTERFACES SERIALES.

Para poder configurar una interfaz serial, se debe entrar primeramente al modo de usuario privilegiado.

Matriz_Gye(config)#**interface serial 0/0 conexión Sucursal Garzota**

- Digitar el comando anterior para entrar al modo de configuración de la interfaz serial 0/0.

Matriz_Gye(config-if)#**ip address 192.168.7.5 255.255.255.252**

- Éste comando permite asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

Matriz_Gye(config-if)#**clock rate 64000**

- Digitar el comando anterior para indicar la velocidad del puerto en bps. Se necesita incluir éste comando ya que está definido como DCE. Según el gráfico de la implementación.

Matriz_Gye(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente el puerto. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up
```

Matriz_Gye(config-if)#**interface serial 0/1 Sucursal Av. Olmedo**

- Digitar el comando anterior para ingresar al modo de configuración de la interfaz serial 0/1.

Matriz_Gye(config-if)#**ip address 192.168.7.9 255.255.255.252**

- Éste comando permite asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

Matriz_Gye(config-if)#**clock rate 64000**

- Digitar el comando anterior para indicar la velocidad del puerto en bps. Se necesitará incluir éste comando ya que está definido como DCE. Según el gráfico de la implementación.

Matriz_Gye(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente el puerto. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface serial0/1, changed state to up
%LINK -3-UPDOWN: Interface serial0/1, changed state to up
```

Matriz_Gye(config-if)#**interface serial 0/2 Matriz Quito**

- Digitar el comando anterior para configurar la interfaz serial 0/2.

Matriz_Gye(config-if)#**ip address 192.168.7.1 255.255.255.252**

- Éste comando permite asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

Matriz_Gye(config-if)#**clock rate 64000**

- Digitar el comando anterior para indicar la velocidad del puerto en bps. Se necesitará incluir éste comando ya que está definido como DCE. Según el gráfico de la implementación.

Matriz_Gye(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente el puerto. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

```
%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/2, changed state to up
%LINK -3-UPDOWN: Interface serial0/2, changed state to up
```

CONFIGURACIÓN PROTOCOLO DE ENRUTAMIENTO RIP VERSIÓN 2.

Para poder configurar un protocolo de enrutamiento, se debe entrar primeramente al modo de usuario privilegiado.

Matriz_Gye(config)#**router rip**

- Con éste comando se habilita el protocolo de enrutamiento rip.

Matriz_Gye(config -router)#**version 2**

- Se deberá especificar la versión del protocolo de enrutamiento rip.

Matriz_Gye(config -router)#**network 192.168.7.0**

Matriz_Gye(config -router)#**network 192.168.8.0**

- Una vez activado el protocolo de enrutamiento es preciso indicar qué redes va ha enrutar.
- Se deberá asignar las redes que seguirá el protocolo.

Matriz_Gye(config -router)#**redistribute ospf 1**

- Éste comando permite redistribuir paquetes ospf por la red rip.

CONFIGURACIÓN PROTOCOLO DE ENRUTAMIENTO OSPF.

Para poder configurar un protocolo de enrutamiento, se deberá ingresar al modo de usuario privilegiado.

Matriz_Gye(config)#**router ospf 1**



- Con éste comando se habilitará el protocolo de enrutamiento ospf.

```
Matriz_Gye(config -router)# network 192.168.7.0 0.0.0.3 area 0
network 192.168.7.4 0.0.0.3 area 0
network 192.168.7.8 0.0.0.3 area 0
network 192.168.7.32 0.0.0.7 area 0
```

- Al activar el protocolo de enrutamiento se deberá especificar la red con su respectiva wildcard y el área en la que va a trabajar.

```
Matriz_Gye(config -router)#redistribute rip
```

- El comando anterior permite redistribuir paquetes rip v2, por la red.

GUARDAR LAS CONFIGURACIONES.

Para poder guardar las configuraciones hechas en el router, se deberá entrar primeramente al modo de usuario privilegiado.

```
Matriz_Gye# wr
```

- Con éste comando se guarda la configuración actual a la configuración de inicio.

```
Building configuration...
```

- Éste mensaje aparecerá cuando se está guardando la configuración.

```
[OK]
```

- Luego aparece un mensaje de aprobación.

SHOW RUN ROUTER MATRIZ GUAYAQUIL.

```
Matriz_Gye#show run
Building configuration...
```

```
!
Version 12.1
```

- Indica la versión del IOS.

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

- Indica que el servicio de encriptación de contraseña se encuentra activo.

```
!
hostname Matriz_Gye
!
```

- Refleja el nombre asignado al router.

```
ip subnet-zero
!
interface Serial0/0
```

- Especifica la interfaz serial 0 slot 0.

```
ip address 192.168.7.5 255.255.255.252
```

- Dirección ip y máscara de de sub-red de la interfaz.

```
no ip directed-broadcast
clock rate 64000
```

- Muestra la velocidad del puerto en bps.

```
bandwidth 1544
!
```

- Valor del ancho de banda del enlace.

```
!
interface Serial0/1
```

- Especifica la interfaz serial 1 slot 0.

```
ip address 192.168.7.9 255.255.255.252
```

- Dirección ip y máscara de sub-red de la interfaz.

```
no ip directed-broadcast
clock rate 64000
```

- Muestra la velocidad del puerto en bps.

```
!
interface Serial0/2
```

- Especifica la interfaz serial 2 slot 0.

```
ip address 192.168.7.1 255.255.255.252
```

- Dirección ip y máscara de sub-red de la interfaz.

```
no ip directed-broadcast
clock rate 64000
```



- Muestra la velocidad del puerto en bps.

```
!
interface FastEthernet1/0
```

- Especifica la interfaz fastethernet 1 slot 0.

```
ip address 192.168.7.33 255.255.255.248
no ip directed-broadcast
bandwidth 100000
!
```

- Dirección ip y máscara de sub-red.

```
!
router rip
```

- Indica que se ha configurado el protocolo de enrutamiento rip.

```
version 2
```

- Versión del protocolo de enrutamiento.

```
redistribute OSPF 1
```

- Se ha permitido redistribuir por la red rip paquetes ospf.

```
network 192.168.7.0
network 192.168.8.0
!
```

- Muestra las redes asignadas al protocolo de enrutamiento.

```
!
router ospf 1
```

- Indica que se ha configurado el protocolo de enrutamiento ospf.

```
redistribute RIP
```

- Permite redistribuir a la red ospf paquetes rip.

```
network 192.168.7.0 0.0.0.3 area 0
network 192.168.7.4 0.0.0.3 area 0
network 192.168.7.8 0.0.0.3 area 0
network 192.168.7.32 0.0.0.7 area 0
!
```

- Especifica la red con su respectiva wildcard y el área en la cual se desea trabajar trabajar.

```
!
ip classless
```

- Indica el acceso a las redes no remotas con máscara de sub-red diferente.

```
no ip http server
!
```

- Especifica que no existe un servidor http.

```
line con 0
transport input none
```

- Configuración Puerto de consola.

```
line aux 0
line vty 0 4
!
```

- Configuración Puerto auxiliar y remota de telnet.



SHOW IP ROUTE MATRIZ GUAYAQUIL.

```
Matriz_Gye#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

Gateway of last resort is not set

192.168.7.0/0 is variably subnetted, 11 subnets
O   192.168.7.12/30 [110/64] via 192.168.7.13, 01:27:51, FastEthernet1/0
O   192.168.7.16/30 [110/64] via 192.168.7.17, 01:27:51, FastEthernet1/0
O   192.168.7.88/29 [110/64] via 192.168.7.89, 01:27:51, FastEthernet1/0
C   192.168.7.4/30 is directly connected, Serial0/0
C   192.168.7.8/30 is directly connected, Serial0/1
C   192.168.7.0/30 is directly connected, Serial0/2
C   192.168.7.32/29 is directly connected, FastEthernet1/0
R   192.168.7.120/29 [120/1] via 192.168.7.10, 00:03:42, Serial0/1
R   192.168.7.112/29 [120/1] via 192.168.7.6, 00:01:15, Serial0/0
R   192.168.7.128/29 [120/2] via 192.168.7.2, 00:07:14, Serial0/2
    is directly connected, 192.168.8.0/29 is subnetted, 4 subnets
R   192.168.8.32 [120/1] via 192.168.7.10, 00:01:14, Serial0/1
R   192.168.8.24 [120/1] via 192.168.7.6, 00:09:22, Serial0/0
R   192.168.8.40 [120/2] via 192.168.7.2, 00:02:30, Serial0/2
R   192.168.8.48 [120/2] via 192.168.7.2, 00:02:25, Serial0/2

Matriz_Gye#
```

Figura 6-56: Show ip route matriz guayaquil.

- **O:** Especifica el protocolo de enrutamiento usado para conectarse a la red destino (**OSPF**), **192.168.x.x:** la dirección de la sub-red, **[110/64]:** La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente para comunicarse con la sub-red, **hh:mm:ss:** la hora de la última actualización y **FastEthernet 1/0:** la interfaz de salida.
- **C:** Especifica que la interfaz está conectada directamente, **192.168.x.x:** la dirección de la sub-red a la cual está conectado y **Serial 0/x:** la interfaz de salida por la cual se accede a la red de destino.

- **R:** Especifica el protocolo de enrutamiento usado para conectarse a la red destino (RIP), **192.168.x.x:** la dirección ip de la sub-red, **[120/1]:** La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente para comunicarse con la sub-red, **hh:mm:ss:** la hora de la última actualización y **Serial 0/x:** la interfaz de salida.

6.10.16 CONFIGURACIÓN DEL ROUTER MATRIZ QUITO.

ASIGNAR NOMBRE.

Router>**enable**

- A nivel del modo usuario normal, se deberá digitar el comando anterior para pasar a modo de usuario privilegiado.

Router#**configure terminal**

- Digitar éste comando en el modo de usuario privilegiado para pasar al modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.

- Aparecerá un mensaje que le indica al usuario que deberá ingresar los comandos de configuración, línea por línea.

Router(config)#**hostname Matriz_Uio**

- En el modo de configuración general, digitar el comando anterior y a continuación un nombre para el dispositivo.

CONFIGURACIÓN DE INTERFACES SERIALES.

Para poder configurar una interfaz serial, se deberá entrar primeramente al modo de usuario privilegiado.

Matriz_Uio(config)#**interface serial 0/0 conexión Matriz guayaquil**

- Digitar el comando anterior para entrar al modo de configuración de la interfaz serial 0/0.

Matriz_Uio(config-if)#**ip address 192.168.7.2 255.255.255.252**

- Éste comando permitirá asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

Matriz_Uio(config-if)#**clock rate 64000**



- Digitar el comando anterior para indicar la velocidad del puerto en bps. Se necesitará incluir éste comando ya que está definido como DCE. Según el gráfico de la implementación.

Matriz_Uio(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente el puerto. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up
```

Matriz_Uio(config-if)#**interface serial 0/1 conexión sucursal Gran Colombia**

- Digitar el comando anterior para ingresar al modo de configuración de la interfaz serial 0/1.

Matriz_Uio(config-if)#**ip address 192.168.7.13 255.255.255.252**

- Éste comando permitirá asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

Matriz_Uio(config-if)#**clock rate 64000**

- Digitar el comando anterior para indicar la velocidad del puerto en bps. Se necesitará incluir éste comando ya que está definido como DCE. Según el gráfico de la implementación.

Matriz_Uio(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente el puerto. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface serial0/1, changed state to up
%LINK -3-UPDOWN: Interface serial0/1, changed state to up
```

Matriz_Uio(config-if)#**interface serial 0/2 conexión sucursal Magdalena**

- Digitar el comando anterior para configurar la interfaz serial 0/2.

Matriz_Uio(config-if)#**ip address 192.168.7.17 255.255.255.252**



- Éste comando permitirá asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

Matriz_Uio(config-if)#**clock rate 64000**

- Digitar el comando anterior para indicar la velocidad del puerto en bps. Se necesita incluir éste comando ya que está definido como DCE. Según el gráfico de la implementación.

Matriz_Uio(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente el puerto. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

```
%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/2, changed state to up
%LINK -3-UPDOWN: Interface serial0/2, changed state to up
```

6.10.17 CONFIGURACIÓN PROTOCOLO DE ENRUTAMIENTO RIP VERSIÓN 2.

Para poder configurar un protocolo de enrutamiento, se debe entrar primeramente al modo de usuario privilegiado.

Matriz_Uio(config)#**router rip**

- Con éste comando habilitará el protocolo de enrutamiento rip.

Matriz_Uio(config-router)#**version 2**

- Se deberá especificar la versión del protocolo de enrutamiento rip.

Matriz_Uio(config-router)#**network 192.168.7.0**

Matriz_Uio(config-router)#**network 192.168.8.0**

- Una vez activado el protocolo de enrutamiento es preciso indicar qué redes va ha enrutar.
- Se deberá asignar las redes que seguirá el protocolo.

Matriz_Uio(config-router)#**redistribute ospf 1**

- Éste comando permitirá redistribuir paquetes ospf por la red rip.



6.10.18 CONFIGURACIÓN PROTOCOLO DE ENRUTAMIENTO OSPF.

Para poder configurar un protocolo de enrutamiento, se debe entrar primeramente al modo de usuario privilegiado.

Matriz_Uio(config)#**router ospf 1**

- Con éste comando habilitará el protocolo de enrutamiento ospf.

Matriz_Uio(config -router)# **network** 192.168.7.0 0.0.0.3 area 0
network 192.168.7.12 0.0.0.3 area 0
network 192.168.7.16 0.0.0.3 area 0
network 192.168.7.88 0.0.0.7 area 0

- Al activar el protocolo de enrutamiento se especificará la red con su respectiva wildcard y el área en la que va a trabajar.

Matriz_Uio(config -router)#**redistribute rip**

- El comando anterior permitirá redistribuir paquetes rip v2, por la red.

GUARDAR LAS CONFIGURACIONES.

Para poder guardar las configuraciones hechas en el router, se deberá entrar primeramente al modo de usuario privilegiado.

Matriz_Uio# **wr**

- Con éste comando guardará desde la configuración actual a la configuración de inicio.

Building configuration...

- Éste mensaje aparecerá cuando se está guardando la configuración.

[OK]

- Luego aparecerá un mensaje de aprobación.



BIBLIOTECA
CAMPUS
PEÑAS

SHOW RUN ROUTER MATRIZ QUITO.

```

Matriz_Uio#show run
Building configuration...

!
Version 12.1

```

- Indica la versión del IOS.

```

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!

```

- Indica que el servicio de encriptación de contraseña se encuentra activo.

```

!
hostname Matriz_Uio
!

```

- Refleja el nombre asignado al router.

```

ip subnet-zero
!
interface Serial0/0

```

- Especifica la interfaz serial 0 slot 0.

```

ip address 192.168.7.2 255.255.255.252

```

- Dirección ip y máscara de de sub-red de la interfaz.

```

no ip directed-broadcast
clock rate 64000

```

- Muestra la velocidad del puerto en bps.

```

bandwidth 1544
!

```

- Valor del ancho de banda del enlace.

```

!
interface Serial0/1

```

- Especifica la interfaz serial 1 slot 0.

```

ip address 192.168.7.13 255.255.255.252

```

- Dirección ip y máscara de sub-red de la interfaz.



```
no ip directed-broadcast
clock rate 64000
```

- Muestra la velocidad del puerto en bps.

```
!
interface Serial0/2
```

- Especifica la interfaz serial 2 slot 0.

```
ip address 192.168.7.17 255.255.255.252
```

- Dirección ip y máscara de sub-red de la interfaz.

```
no ip directed-broadcast
clock rate 64000
```

- Muestra la velocidad del puerto en bps.

```
!
interface FastEthernet1/0
```

- Especifica la interfaz fastethernet 1 slot 0.

```
ip address 192.168.7.89 255.255.255.248
```

- Dirección ip y máscara de sub-red.

```
!
router rip
```

- Indica que se ha configurado el protocolo de enrutamiento rip.

```
version 2
```

- Versión del protocolo de enrutamiento.

```
redistribute OSPF 1
```

- Se ha permitido redistribuir por la red rip paquetes ospf.

```
network 192.168.7.0
network 192.168.8.0
```

```
!
```

- Muestra las redes asignadas al protocolo de enrutamiento rip.



BIBLIOTECA
CAMPUS
PEÑAS

```
!
router ospf 1
```

- Indica que se ha configurado el protocolo de enrutamiento ospf.

```
redistribute RIP
```

- Permite redistribuir por la red ospf paquetes rip.

```
network 192.168.7.0 0.0.0.3 area 0
network 192.168.7.12 0.0.0.3 area 0
network 192.168.7.16 0.0.0.3 area 0
network 192.168.7.88 0.0.0.7 area 0
!
```

- Especifica la red con su respectiva wildcard y el área en la cual se desea trabajar.

```
!
ip classless
```

- Indica el acceso a las redes no remotas con máscara de sub-red diferente.

```
no ip http server
!
```

- Especifica que no existe un servidor http.

```
line con 0
transport input none
```

- Configuración Puerto de consola.

```
line aux 0
line vty 0 4
!
```

- Configuración Puerto auxiliar y remota de telnet.



BIBLIOTECA
CAMPUS
PEÑAS

SHOW IP ROUTE MATRIZ QUITO.

```

Matriz_Uio#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route

Gateway of last resort is not set

    192.168.7.0/0 is variably subnetted, 11 subnets
O       192.168.7.4/30 [110/64] via 192.168.7.1, 00:34:43, FastEthernet1/0
O       192.168.7.8/30 [110/64] via 192.168.7.1, 00:34:43, FastEthernet1/0
O       192.168.7.32/29 [110/64] via 192.168.7.33, 00:34:43, FastEthernet1/0
C       192.168.7.0/30 is directly connected, Serial0/0
C       192.168.7.12/30 is directly connected, Serial0/1
C       192.168.7.16/30 is directly connected, Serial0/2
C       192.168.7.88/29 is directly connected, FastEthernet1/0
R       192.168.7.136/29 [120/1] via 192.168.7.18, 00:04:34, Serial0/2
R       192.168.7.128/29 [120/1] via 192.168.7.14, 00:07:17, Serial0/1
R       192.168.7.112/29 [120/2] via 192.168.7.1, 00:08:28, Serial0/0
        is directly connected,      192.168.8.0/29 is subnetted, 4 subnets
R       192.168.8.40 [120/1] via 192.168.7.14, 00:01:41, Serial0/1
R       192.168.8.48 [120/1] via 192.168.7.18, 00:04:27, Serial0/2
R       192.168.8.24 [120/2] via 192.168.7.1, 00:07:30, Serial0/0
R       192.168.8.32 [120/2] via 192.168.7.1, 00:02:32, Serial0/0

Matriz_Uio#
Matriz_Uio#

```

Figura 6-57: Show run router matriz Quito.

- **O:** Especifica el protocolo de enrutamiento usado para conectarse a la red destino (OSPF), **192.168.x.x:** la dirección de la sub-red, **[110/64]:** La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente para comunicarse con la sub-red, **hh:mm:ss:** la hora de la última actualización y **FastEthernet 1/0:** la interfaz de salida.
- **C:** Especifica que la interfaz está conectada directamente, **192.168.x.x:** la dirección de la sub-red a la cual está conectado y **Serial 0/x:** la interfaz de salida por la cual se accede a la red de destino.
- **R:** Especifica el protocolo de enrutamiento usado para conectarse a la red destino (RIP), **192.168.x.x:** la dirección ip de la sub-red, **[120/1]:** La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente para comunicarse con la sub-red, **hh:mm:ss:** la hora de la última actualización y **Serial 0/x:** la interfaz de salida.



6.10.19 CONFIGURACIÓN DEL ROUTER SUCURSAL GARZOTA.

Router>**enable**

- A nivel del modo usuario normal se debe digitar el comando anterior para pasar a modo de usuario privilegiado.

Router#**configure terminal**

- Digitar éste comando en el modo de usuario privilegiado para pasar al modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.

- Aparecerá un mensaje que le indica al usuario que debe ingresar los comandos de configuración, línea por línea.

Router(config)#**hostname Suc_Garzota**

- En el modo de configuración general digitar el comando anterior y a continuación un nombre para el dispositivo.

6.10.19.1 CONFIGURACIÓN DE INTERFACES SERIALES.

Suc_Garzota(config)#**interface serial 1**

- Digitar el comando anterior para entrar al modo de configuración de la interfaz serial 1.

Suc_Garzota(config-if)#**ip address 192.168.7.6 255.255.255.252**

- Este comando permite asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

Suc_Garzota(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente la interfaz. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

```
%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up
```



BIBLIOTECA
CAMPUS
PEÑAS

6.10.19.1 CONFIGURACIÓN DE FASTETHERNET SUCURSAL GARZOTA

Suc_Garzota(config)#**interface fastethernet 0/0**

- Digitar el comando anterior para entrar al modo de configuración de la interfaz fastethernet 0/0.

Suc_Garzota(config-if)#**ip address 192.168.7.113 255.255.255.248**

- Este comando permitirá asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz.

Suc_Garzota(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente la interfaz. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

%LINK -3-UPDOWN: Interface Fastethernet 0/0, changed state to up

6.10.19.2 CONFIGURACIÓN DE SUB-INTERFAZ.

Para poder configurar una sub-interfaz, se deberá entrar al modo de usuario privilegiado.

Suc_Garzota (config)#**interface fastethernet 0.1**

- Digitar el comando anterior para entrar al modo de configuración de la sub-interfaz FastEthernet 0.1.

Suc_Garzota(config-subif)#**encapsulation dot1q 10**

- Se deberá digitar el comando encapsulation dot1q para definir el tipo de encapsulamiento.

Suc_Garzota(config-subif)#**ip address 192.168.8.25 255.255.255.248**

- Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz.

Suc_Garzota(config-subif)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente la interfaz.



6.10.19.3 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSION 2.

Suc_Garzota# **configure Terminal**

- A nivel de modo usuario privilegiado se deberá digitar el comando anterior para pasar a modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.

- Aparecerá un mensaje que indica al usuario que ingrese los comandos de configuración, línea por línea.

Suc_Garzota(config-if)#**router rip**

- Se deberá habilitar el protocolo de enrutamiento con el comando anterior.

Suc_Garzota(config-router)#**version 2**

- Se deberá especificar la versión del protocolo de enrutamiento.

Suc_Garzota(config-router)#**network 192.168.7.0**

Suc_Garzota(config-router)#**network 192.168.8.0**

- Una vez activado el protocolo de enrutamiento es preciso indicar qué redes se van a enrutar.
- Asignando las redes que seguirán el protocolo.

GUARDANDO LA CONFIGURACIÓN DEL ROUTER.

Suc_Garzota#**wr**

- Con el comando anterior se guardará la configuración actual a la configuración de inicio.

Building configuration...

- El siguiente mensaje indica que se está guardando la configuración.

[OK]

- Ahora aparecerá un mensaje de aprobación



POLITÉCNICA DEL LITORAL

BIBLIOTECA
CAMPUS
PEÑAS

SHOW RUN ROUTER SUCURSAL GARZOTA.

```

Suc_Garzota#show run
Building configuration...

```

```

!
Version 12.1

```

- Indica la versión del IOS.

```

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!

```

- Indica que el servicio de encriptación de contraseña está activo.

```

!
hostname Suc_Garzota
!

```

- Refleja el nombre que el administrador le ha asignado al router

```

!
ip subnet-zero
!
!
interface Serial1
!

```

- Especifica interfaz serial 1

```

ip address 192.168.7.6 255.255.255.252

```

- Dirección ip y máscara de de sub-red de la interfaz.

```

no ip directed-broadcast

```

- Indica la velocidad de la interfaz en bits por segundo. Se lo encuentra en interfaces DCE.

```

bandwidth 1544
!

```

- Valor del ancho de banda del enlace en la interfaz.

```

!
interface FastEthernet0/0

```

- Especifica interfaz fastethernet 0 slot 0



```
ip address 192.168.7.113 255.255.255.248
```

- Dirección ip y máscara de de sub-red de la Fastethernet.

```
no ip directed-broadcast
bandwidth 100000
!
```

- Valor del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/0.1
```

- Especifica sub-interfaz fastetehrnet 0.1 slot 0.

```
encapsulation dot1q 10
```

- Define el tipo de encapsulamiento asignado a la VLAN 10.

```
ip address 192.168.8.25 255.255.255.248
!
```

- Dirección ip y máscara de de sub-red de la sub-interfaz.

```
!
router rip
```

- Indica que se ha configurado el protocolo de enrutamiento rip.

```
version 2
```

- Define la versión 2 del protocolo de enrutamiento.

```
network 192.168.7.0
network 192.168.8.0
!
```

- Indica qué redes enruta el protocolo de enrutamiento.

```
!
ip classless
```

- Indica acceso a las redes no remotas con máscara de sub-red diferente.

```
no ip http server
!
!
```

- Especifica que no existe un servidor http.



BIBLIOTECA
CAMPUS
PEÑAS

```
!
line con 0
transport input none
```

- Configuración Puerto de consola.
- Ningún transporte impuesto.

```
line aux 0
line vty 0 4
!
```

- Configuración Puerto auxiliar.
- Configuración remota por telnet.

```
!
no scheduler allocate
end
```

- Fin del reporte de la configuración actual.

SHOW IP ROUTE SUCURSAL GARZOTA.

```
Suc_Garzota#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

Gateway of last resort is not set

192.168.8.0/29 is subnetted, 4 subnets
C    192.168.8.24 is directly connected, 192.168.8.25
R    192.168.8.32 [120/2] via 192.168.7.5, 00:03:15, Serial1
R    192.168.8.40 [120/3] via 192.168.7.5, 00:07:22, Serial1
R    192.168.8.48 [120/3] via 192.168.7.5, 00:05:33, Serial1
192.168.7.0/0 is variably subnetted, 8 subnets
C    192.168.7.4/30 is directly connected, Serial1
C    192.168.7.112/29 is directly connected, FastEthernet0/0
R    192.168.7.8/30 [120/1] via 192.168.7.5, 00:09:26, Serial1
R    192.168.7.0/30 [120/1] via 192.168.7.5, 00:09:31, Serial1
R    192.168.7.32/29 [120/1] via 192.168.7.5, 00:05:12, Serial1
R    192.168.7.120/29 [120/2] via 192.168.7.5, 00:05:13, Serial1
R    192.168.7.136/29 [120/3] via 192.168.7.5, 00:03:42, Serial1
R    192.168.7.128/29 [120/3] via 192.168.7.5, 00:04:18, Serial1

Suc_Garzota#
Suc_Garzota#
```

Figura 6-58: Show run router Garzota.

- **C:** Especifica que la interfaz está conectada directamente, **192.168.x.x:** la dirección de la sub-red a la cual está conectado y **Serial 0/x:** la interfaz de salida por la cual se accede a la red de destino.
- **R:** Especifica el protocolo de enrutamiento usado para conectarse a la red destino (RIP), **192.168.x.x:** la dirección ip de la sub-red, **[120/1]:** La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente.



BIBLIOTECA
CAMPUS
PEÑAS

6.10.19.4 CONFIGURACIÓN SWITCH SUCURSAL GARZOTA.

Switch>**enable**

- A nivel de modo usuario normal digitar el comando anterior para pasar a modo de usuario privilegiado.

Switch#**configure terminal**

- A nivel de modo usuario privilegiado digitar el comando que se muestra para pasar a modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.

- Aparecerán unas líneas describiendo al usuario que ingrese los comandos de configuración, uno a uno.

Switch(config)#**hostname Sw_Garzota**

- En el modo de configuración general digitar el comando anterior para establecer el nombre del dispositivo.

Sw_Garzota(config)#

- De esta manera aparecerá despues de haber dado nombre al Switch.

6.10.19.5 CREACIÓN DE VLAN.

Sw_Garzota#**vlan database**

- Permite ingresar a la base de datos de las VLAN.

Sw_Garzota(vlan)#**vlan 10 name 10**

- Crea la vlan con el nombre especificado.

6.10.19.6 CONFIGURACIÓN DE PUERTOS ASIGNANDO VLAN.

Sw_Garzota(vlan)#**exit**

- Para salir de la base de datos de las VLAN.

Sw_Garzota#**configure terminal**



BIBLIOTECA
CAMPUS
REÑAS

- A nivel de modo usuario privilegiado digitar el comando anterior para pasar a modo de configuración general

Sw_Garzota(config)#**interface fastethernet 0/1**

- Digitar el comando anterior para configurar la interfaz fastethernet 0/1.

Sw_Garzota(config-if)#**switchport mode trunk**

- Permite truncar el puerto donde se digitará este comando.

Sw_Garzota(config-if)#**switchport access vlan 10**

- Agrega este puerto a la vlan especificada.

Sw_Garzota(config)#**interface fastethernet 0/2**

- Digitar el comando anterior para configurar la interfaz fastethernet 0/2.

Sw_Garzota(config-if)#**switchport access vlan 10**

- Agrega este puerto a la vlan especificada.

GUARDAR CONFIGURACIONES HECHAS EN EL SWITCH.

Sw_Garzota(config-line)#**exit**

- Digitar lo anterior para salir del modo configuración de consola a modo configuración general.

Sw_Garzota(config)#**exit**

- Se debe ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado.

%SYS-5-CONFIG_I: Configured from console by console

- Cuando se realiza este procedimiento aparecerá el siguiente mensaje que significa que se ha configurado desde la interfaz de consola para la interfaz de consola.

Sw_Garzota#**copy running-config startup-config**

- Con el comando anterior se guarda la configuración actual a la configuración de inicio.

Building configuration...

- El siguiente mensaje significa que se esta guardando la configuración.



[OK]

- Ahora aparecerá un mensaje de aprobación.

SHOW RUN SWITCH SUCURSAL GARZOTA.

```
Sw_Garzota#show run
!
Version 12.1
```

- Indica la versión del IOS

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

- Indica que el servicio de encriptación de contraseña esta activo.

```
!
hostname Sw_Garzota
```

- Refleja el nombre que el administrador le ha asignado al router.

```
!
interface FastEthernet0/1
```

- Especifica interfaz fastethernet 0/1

```
switchport mode trunk
```

- Indica que no esta configurado el modo tipo acceso.

```
switchport access vlan 10
```

- Especifica que esta interfaz es parte de la VLAN indicada.

```
bandwidth 100000
!
```

- Valor del ancho de banda del enlace en la interfaz

```
!
interface FastEthernet0/2
```

- Especifica interfaz fastethernet0/2.

```
switchport access vlan 10
```

- Especifica que esta interfaz es parte de la VLAN indicada.



BIBLIOTECA
CAMPUS
PEÑAS

```
bandwidth 100000
```

```
!
```

- Valor del ancho de banda del enlace en la interfaz.

```
!
```

```
vtp Server
vtp domain bigdomain
```

- Especifica el dominio del puerto truncado virtual.

```
interface Vlan 1
```

- Especifica la VLAN 1 (vlan por defecto).

```
no ip address
no ip route-cache
```

- Dirección IP de la vlan por defecto.
- No almacena ip en el cache de rutas.

```
shutdown
```

- Indica que no esta levantado el servicio

```
vlan 10 name 10
```

```
!
```

- Indica VLAN configurada con su respectivo nombre.

```
!
ip classless
```

- Indica acceso a las redes no remotas con mascara de sub-red diferente.

```
no ip http server
!
```

- Especifica que no existe un servidor http.

```
!
line con 0
transport input none
```

- Configuración Puerto de consola.

```
line aux 0
line vty 0 15
!
```



- Configuración Puerto auxiliar.
- Configuración remota por telnet.

```

!
no scheduler allocate
end

```

- Fin del reporte de la configuración actual.

6.10.19.7 SHOW VLAN SWITCH SUCURSAL GARZOTA.

```

Sw_Garzota#show vlan

```

VLAN Name	Status	Ports
1 default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
10 10	active	Fa0/1, Fa0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

```

Sw_Garzota#

```

Figura 6-59: Show Vlan router Garzota.



BIBLIOTECA
CAMPUS
PEÑAS

6.10.20 ROUTER SUCURSAL AV. OLMEDO.

Router>enable

- A nivel del modo usuario normal se deberá digitar el comando anterior para pasar a modo de usuario privilegiado.

Router#configure terminal

- Digitar éste comando en el modo de usuario privilegiado para pasar al modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.

- Aparecerá un mensaje que le indica al usuario que debe ingresar los comandos de configuración, línea por línea.

Router(config)#**hostname Suc_av_Olmedo**

- En el modo de configuración general digitar el comando anterior y a continuación un nombre para el dispositivo.

CONFIGURACIÓN DE INTERFACES SERIALES.

Suc_av_Olmedo(config)#**interface serial 1**

- Digitar el comando anterior para entrar al modo de configuración de la interfaz serial 1.

Suc_av_Olmedo(config-if)#**ip address 192.168.7.10 255.255.255.252**

- Este comando permite asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

Suc_av_Olmedo(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente la interfaz. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

```
%LINK -3-UPDOWN: Interface serial1, changed state to up
```

6.10.20 .1 CONFIGURACIÓN DE FASTETHERNET SUCURSAL AV. OLMEDO

Suc_av_Olmedo(config)#**interface fastethernet 0/0**

- Digitar el comando anterior para entrar al modo de configuración de la interfaz fastethernet 0/0.

Suc_av_Olmedo(config-if)#**ip address 192.168.7.121 255.255.255.248**

- Este comando permite asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz.

Suc_av_Olmedo(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente la interfaz. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

```
%LINK -3-UPDOWN: Interface Fastethernet 0/0, changed state to up
```



6.10.20.2 CONFIGURACIÓN DE SUB-INTERFAZ.

Para poder configurar una sub-interfaz, se deberá entrar al modo de usuario privilegiado.

Suc_av_Olmedo(config)#**interface fastethernet 0.1**

- Digitar el comando anterior para entrar al modo de configuración de la sub-interfaz FastEthernet 0.1.

Suc_av_Olmedo(config-subif)#**encapsulation dot1q 20**

- Se deberá digitar el comando encapsulation dot1q para definir el tipo de encapsulamiento.

Suc_av_Olmedo(config-subif)#**ip address 192.168.8.33 255.255.255.248**

- Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz.

Suc_av_Olmedo(config-subif)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente el la interfaz.

6.10.20.3 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSION 2.

Suc_av_Olmedo# **configure Terminal**

- A nivel de modo usuario privilegiado se debe digitar el comando anterior para pasar a modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.

- Aparecerá un mensaje que indica al usuario que ingrese los comandos de configuración, línea por línea.

Suc_av_Olmedo(config-if)#**router rip**

- Se deberá habilitar el protocolo de enrutamiento con el comando anterior.

Suc_av_Olmedo(config-router)#**version 2**

- Se deberá especificar la versión del protocolo de enrutamiento.

Suc_av_Olmedo(config-router)#**network 192.168.7.0**

Suc_av_Olmedo(config-router)#**network 192.168.8.0**



BIBLIOTECA
CAMPUS
PEÑAS

- Una vez activado el protocolo de enrutamiento es preciso indicar qué redes se van a enrutar.
- Asignando las redes que seguirán el protocolo.

6.10.20.4 GUARDANDO LA CONFIGURACIÓN DEL ROUTER.

Suc_av_Olmedo#wr

- Con el comando anterior se guarda la configuración actual a la configuración de inicio.

Building configuration...

- El siguiente mensaje indica que se está guardando la configuración.

[OK]

- Ahora aparece un mensaje de aprobación

SHOW RUN ROUTER SUCURSAL AV. OLMEDO

```
Suc_av_Olmedo#show run
Building configuration...
```

```
!
Version 12.1
```

- Indica la versión del IOS.

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

- Indica que el servicio de encriptación de contraseña está activo.

```
!
hostname Suc_av_Olmedo
!
```

- Refleja el nombre que el administrador le ha asignado al router

```
!
ip subnet-zero
!
interface Serial1
```



- Especifica interfaz serial 1

```
ip address 192.168.7.10 255.255.255.252
```

- Dirección ip y máscara de de sub-red de la interfaz.

```
no ip directed-broadcast
```

- Indica la velocidad de la interfaz en bits por segundo. Se lo encuentra en interfaces DCE.

```
bandwidth 1544
```

```
!
```

- Valor del ancho de banda del enlace en la interfaz.

```
!
```

```
interface FastEthernet0/0
```

- Especifica interfaz fastethernet 0 slot 0

```
ip address 192.168.7.121 255.255.255.248
```

- Dirección ip y máscara de de sub-red de la Fastethernet.

```
no ip directed-broadcast
```

```
bandwidth 1544
```

```
!
```

- Valor del ancho de banda del enlace en la interfaz.

```
!
```

```
interface FastEthernet0/0.1
```

- Especifica sub-interfaz fastethernet 0.1 slot 0.

```
encapsulation dot1q 20
```

- Define el tipo de encapsulamiento asignado a la VLAN 20.

```
ip address 192.168.8.33 255.255.255.248
```

```
!
```

- Dirección ip y máscara de de sub-red de la sub-interfaz.

```
!
```

```
router rip
```

- Indica que se ha configurado el protocolo de enrutamiento rip.



version 2

- Define la versión 2 del protocolo de enrutamiento.

```
network 192.168.7.0
network 192.168.8.0
!
```

- Indica qué redes enruta el protocolo de enrutamiento.

```
!
ip classless
```

- Indica acceso a las redes no remotas con máscara de sub-red diferente.

```
no ip http server
!
```

- Especifica que no existe un servidor http.

```
!
line con 0
transport input none
```

- Configuración Puerto de consola.
- Ningún transporte impuesto.

```
line aux 0
line vty 0 4
!
```

- Configuración Puerto auxiliar.
- Configuración remota por telnet.

```
!
no scheduler allocate
end
```

- Fin del reporte de la configuración actual



BIBLIOTECA
CAMPUS
PEÑAS

SHOW IP ROUTE SUCURSAL AV. OLMEDO

```

Suc_av_Olmedo#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

Gateway of last resort is not set

192.168.8.0/29 is subnetted, 4 subnets
C    192.168.8.32 is directly connected, 192.168.8.33
R    192.168.8.24 [120/2] via 192.168.7.9, 00:06:42, Serial1
R    192.168.8.40 [120/3] via 192.168.7.9, 00:08:34, Serial1
R    192.168.8.48 [120/3] via 192.168.7.9, 00:07:26, Serial1
192.168.7.0/0 is variably subnetted, 8 subnets
C    192.168.7.8/30 is directly connected, Serial1
C    192.168.7.120/29 is directly connected, FastEthernet0/0
R    192.168.7.4/30 [120/1] via 192.168.7.9, 00:01:23, Serial1
R    192.168.7.0/30 [120/1] via 192.168.7.9, 00:02:31, Serial1
R    192.168.7.32/29 [120/1] via 192.168.7.9, 00:08:39, Serial1
R    192.168.7.112/29 [120/2] via 192.168.7.9, 00:06:21, Serial1
R    192.168.7.136/29 [120/3] via 192.168.7.9, 00:03:19, Serial1
R    192.168.7.128/29 [120/3] via 192.168.7.9, 00:07:30, Serial1

Suc_av_Olmedo#

```

Figura 6-60: Show IP route Olmedo.

- **C:** Especifica que la interfaz está conectada directamente, **192.168.x.x:** la dirección de la sub-red a la cual está conectado y **Serial 0/x:** la interfaz de salida por la cual se accede a la red de destino.
- **R:** Especifica el protocolo de enrutamiento usado para conectarse a la red destino (RIP), **192.168.x.x:** la dirección ip de la sub-red, **[120/1]:** La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente.

6.10.20.5 CONFIGURACIÓN SWITCH SUCURSAL AV. OLMEDO

Switch>enable

- A nivel de modo usuario normal digitar el comando anterior para pasar a modo de usuario privilegiado.

Switch#configure terminal

- A nivel de modo usuario privilegiado digitar el comando que se muestra para pasar a modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.



BIBLIOTECA
CAMPUS
PEÑAS

- Aparecerán unas líneas describiendo al usuario que ingrese los comandos de configuración, uno a uno.

Switch(config)#**hostname Sw_Olmedo**

- En el modo de configuración general digitar el comando anterior para establecer el nombre del dispositivo.

Sw_Olmedo(config)#

- Así deberá aparecer después de haber dado nombre al Switch.

6.10.20.6 CREACIÓN DE VLAN.

Sw_Olmedo#**vlan database**

- Permite ingresar a la base de datos de las VLAN.

Sw_Olmedo(vlan)#**vlan 20 name 20**

- Crea la vlan con el nombre especificado.

6.10.20.7 CONFIGURACIÓN DE PUERTOS ASIGNANDO VLAN.

Sw_Olmedo(vlan)#**exit**

- Para salir de la base de datos de las VLAN.

Sw_Olmedo#**configure terminal**

- A nivel de modo usuario privilegiado digitar el comando anterior para pasar a modo de configuración general

Sw_Olmedo(config)#**interface fastethernet 0/1**

- Digitar el comando anterior para configurar la interfaz fastethernet 0/1.

Sw_Olmedo(config-if)#**switchport mode trunk**

- Permite truncar el puerto donde se digita este comando.

Sw_Olmedo(config-if)#**switchport access vlan 20**

- Agrega este puerto a la vlan especificada.



Sw_Olmedo(config)#**interface fastethernet 0/2**

- Digitar el comando anterior para configurar la interfaz fastethernet de puerto 0/2.

Sw_Olmedo(config-if)#**switchport access vlan 20**

- Agrega este puerto a la vlan especificada.

GUARDAR CONFIGURACIONES HECHAS EN EL SWITCH.

Sw_Olmedo(config-line)#**exit**

- Digitar lo anterior para salir del modo configuración de consola a modo configuración general.

Sw_Olmedo(config)#**exit**

- Se deberá ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado.

```
%SYS-5-CONFIG_I: Configured from console by console
```

- Cuando se realiza este procedimiento aparecerá el siguiente mensaje que significa que se ha configurado desde la interfaz de consola para la interfaz de consola.

Sw_Olmedo#**copy running-config startup-config**

- Con el comando anterior se guarda la configuración actual a la configuración de inicio.

Building configuration...

- El siguiente mensaje significa que se esta guardando la configuración.

[OK]

- Ahora aparece un mensaje de aprobación.

SHOW RUN SWITCH SUCURSAL AV. OLMEDO.

```
Sw_Olmedo#show run
!
Version 12.1
```

- Indica la versión del IOS

```

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

- Indica que el servicio de encriptación de contraseña esta activo.

```

!
hostname Sw_Olmedo
```

- Refleja el nombre que el administrador le ha asignado al router.

```

!
interface FastEthernet0/1
```

- Especifica interfaz fastethernet 0/1

```

switchport mode trunk
```

- Indica que no esta configurado el modo tipo acceso.

```

switchport access vlan 20
```

- Especifica que esta interfaz es parte de la VLAN indicada.

```

bandwidth 100000
!
```

- Valor del ancho de banda del enlace en la interfaz

```

!
interface FastEthernet0/2
```

- Especifica interfaz fastethernet0/2.

```

switchport access vlan 20
```

- Especifica que esta interfaz es parte de la VLAN indicada.

```

bandwidth 100000
!
```

- Valor del ancho de banda del enlace en la interfaz.

```

!
vtp Server
vtp domain bigdomain
```

- Especifica el dominio del puerto truncado virtual.

```

interface Vlan 1
```



BIBLIOTECA
CAMPUS
PEÑAS

- Especifica la VLAN 1 (vlan por defecto).

```
no ip address
no ip route-cache
```

- Dirección IP de la vlan por defecto.
- No almacena ip en el cache de rutas.

```
shut down
```

- Indica que no esta levantado el servicio

```
vlan 20 name 20
!
```

- Indica VLAN configurada con su respectivo nombre.

```
!
ip classless
```

- Indica acceso a las redes no remotas con mascara de sub-red diferente.

```
no ip http server
!
```

- Especifica que no existe un servidor http.

```
!
line con 0
transport input none
```

- Configuración Puerto de consola.

```
line aux 0
line vty 0 15
!
```

- Configuración Puerto auxiliar.
- Configuración remota por telnet.

```
!
no scheduler allocate
end
```

- Fin del reporte de la configuración actual.

SHOW VLAN SWITCH SUCURSAL AV. OLMEDO.

```
Sw_Olmedo#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
20	20	active	Fa0/1, Fa0/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

```
Sw_Olmedo#
```

Figura 6-61: Show VLAN Av Olmedo.



BIBLIOTECA
CAMPUS
PEÑAS

VLAN:	Identificación vlan.
Name:	Nombre de vlan.
Status:	Estado de la Vlan.
Ports:	Puertos asignados a la vlan.
Type:	Tipo de interfaces.
SIAD:	Encabezado para identificar vlan.
MTU:	Tamaño máximo de los paquetes transmitidos por el puerto expresado en bytes.
Parent:	Parentela.
RingNo:	Número de anillo si hay.
BridgeNO:	Número de puente si hay.
Stp:	STP usado
BrdgMode:	Modo de puente.
Trans:	TRANS, o si es una VLAN que cambia de topología Token Ring / FDDI a Ethernet.

6.10.21 CONFIGURACIÓN DEL ROUTER SUCURSAL GRAN COLOMBIA.

Router>**enable**

- A nivel del modo usuario normal se deberá digitar el comando anterior para pasar a modo de usuario privilegiado.

Router#**configure terminal**

- Digitar éste comando en el modo de usuario privilegiado para pasar al modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.

- Aparecerá un mensaje que le indica al usuario que deberá ingresar los comandos de configuración, línea por línea.

Router(config)#**hostname Suc_Gran_Colombia**

- En el modo de configuración general digitar el comando anterior y a continuación un nombre para el dispositivo.



6.10.21.1 CONFIGURACIÓN DE INTERFACES SERIALES.

BIBLIOTECA
CAMPUS
PEÑAS

Suc_Gran_Colombia(config)#**interface serial 1**

- Digitar el comando anterior para entrar al modo de configuración de la interfaz serial 1.

Suc_Gran_Colombia(config-if)#**ip address** 192.168.7.14 255.255.255.252

- Este comando permitirá asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

Suc_Gran_Colombia(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente la interfaz. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

```
%LINK -3-UPDOWN: Interface serial1, changed state to up
```

6.10.21.2 CONFIGURACIÓN DE FASTETHERNET SUCURSAL GRAN COLOMBIA

Suc_Gran_Colombia(config)#**interface fastethernet 0/0**

- Digitar el comando anterior para entrar al modo de configuración de la interfaz fastethernet 0/0.

Suc_Gran_Colombia(config-if)#**ip address 192.168.7.129 255.255.255.248**

- Este comando permitirá asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz.

Suc_Gran_Colombia(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente la interfaz. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

%LINK -3-UPDOWN: Interface Fastethernet 0/0, changed state to up

6.10.21.3 CONFIGURACIÓN DE SUB-INTERFAZ.

Para poder configurar una sub-interfaz, se deberá entrar al modo de usuario privilegiado.

Suc_Gran_Colombia(config)#**interface fastethernet 0.1**

- Digitar el comando anterior para entrar al modo de configuración de la sub-interfaz FastEthernet 0.1.

Suc_Gran_Colombia(config-subif)#**encapsulation dot1q 30**

- Se deberá digitar el comando encapsulation dot1q para definir el tipo de encapsulamiento.

Suc_Gran_Colombia(config-subif)#**ip address 192.168.8.41 255.255.255.248**

- Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz.

Suc_Gran_Colombia(config-subif)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente el la interfaz.



POLITECNIA DEL LITORAL

BIBLIOTECA
CAMPUS
PEÑAS

6.10.21.4 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSION 2.

Suc_Gran_Colombia# **configure terminal**

- A nivel de modo usuario privilegiado se deberá digitar el comando anterior para pasar a modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.

- Aparecerá un mensaje que indicará al usuario que ingrese los comandos de configuración, línea por línea.

Suc_Gran_Colombia(config-if)#**router rip**

- Se deberá habilitar el protocolo de enrutamiento con el comando anterior.

Suc_Gran_Colombia(config-router)#**version 2**

- Se deberá especificar la versión del protocolo de enrutamiento.

Suc_Gran_Colombia(config-router)#**network 192.168.7.0**

Suc_Gran_Colombia(config-router)#**network 192.168.8.0**

- Una vez activado el protocolo de enrutamiento es preciso indicar qué redes se van a enrutar.
- Asignando las redes que seguirán el protocolo.

GUARDANDO LA CONFIGURACIÓN DEL ROUTER.

Suc_Gran_Colombia #**wr**

- Con el comando anterior se guardará la configuración actual a la configuración de inicio.

Building configuration...

- El siguiente mensaje indica que se está guardando la configuración.

[OK]

- Ahora aparece un mensaje de aprobación

SHOW RUN ROUTER SUCURSAL GRAN COLOMBIA

```
Suc_Gran_Colombia#show run
Building configuration...
```

```
!
Version 12.1
```

- Indica la versión del IOS.

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

- Indica que el servicio de encriptación de contraseña está activo.

```
!
hostname Suc_Gran_Colombia
!
```

- Refleja el nombre que el administrador le ha asignado al router

```
!
ip subnet-zero
!
interface Serial1
```

- Especifica interfaz serial 1

```
ip address 192.168.7.14 255.255.255.252
```

- Dirección ip y máscara de de sub-red de la interfaz.

```
no ip directed-broadcast
```

- Indica la velocidad de la interfaz en bits por segundo. Se lo encuentra en interfaces DCE.

```
bandwidth 1544
!
```

- Valor del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/0
```

- Especifica interfaz fastethernet 0 slot 0



BIBLIOTECA
CAMPUS
PEÑAS

```
ip address 192.168.7.129 255.255.255.248
```

- Dirección ip y máscara de de sub-red de la Fastethernet.

```
no ip directed-broadcast
bandwidth 1544
!
```

- Valor del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/0.1
```

- Especifica sub-interfaz fastethernet 0.1 slot 0.

```
encapsulation dot1q 30
```

- Define el tipo de encapsulamiento asignado a la VLAN 30.

```
ip address 192.168.8.41 255.255.255.248
!
```

- Dirección ip y máscara de de sub-red de la sub-interfaz.

```
!
router rip
```

- Indica que se ha configurado el protocolo de enrutamiento rip.

```
version 2
```

- Define la versión 2 del protocolo de enrutamiento.

```
network 192.168.7.0
network 192.168.8.0
!
```

- Indica qué redes enruta el protocolo de enrutamiento.

```
!
ip classless
```

- Indica acceso a las redes no remotas con máscara de sub-red diferente.

```
no ip http server
!
!
```

- Especifica que no existe un servidor http.



BIBLIOTECA
CAMPUS
PEÑAS

```

!
line con 0
  transport input none

```

- Configuración Puerto de consola.
- Ningún transporte impuesto.

```

line aux 0
line vty 0 4
!

```

- Configuración Puerto auxiliar.
- Configuración remota por telnet.

```

!
no scheduler allocate
end

```

- Fin del reporte de la configuración actual



SHOW IP ROUTE SUCURSAL GRAN COLOMBIA

```

Suc_Gran_Colombia#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

Gateway of last resort is not set

  192.168.8.0/29 is subnetted, 4 subnets
C       192.168.8.40 is directly connected, 192.168.8.41
R       192.168.8.48 [120/2] via 192.168.7.13, 00:05:40, Serial1
R       192.168.8.24 [120/3] via 192.168.7.13, 00:09:30, Serial1
R       192.168.8.32 [120/3] via 192.168.7.13, 00:09:16, Serial1
  192.168.7.0/0 is variably subnetted, 8 subnets
C       192.168.7.12/30 is directly connected, Serial1
C       192.168.7.128/29 is directly connected, FastEthernet0/0
R       192.168.7.0/30 [120/1] via 192.168.7.13, 00:07:29, Serial1
R       192.168.7.16/30 [120/1] via 192.168.7.13, 00:07:43, Serial1
R       192.168.7.88/29 [120/1] via 192.168.7.13, 00:04:19, Serial1
R       192.168.7.136/29 [120/2] via 192.168.7.13, 00:06:43, Serial1
R       192.168.7.112/29 [120/3] via 192.168.7.13, 00:06:39, Serial1
R       192.168.7.120/29 [120/3] via 192.168.7.13, 00:09:40, Serial1

Suc_Gran_Colombia#

```

Figura 6-62: Show IP Route Gran Colombia.

- **C**: Especifica que la interfaz está conectada directamente, **192.168.x.x**: la dirección de la sub-red a la cual está conectado y **Serial 0/x**: la interfaz de salida por la cual se accede a la red de destino.

- **R:** Especifica el protocolo de enrutamiento usado para conectarse a la red destino (RIP), **192.168.x.x:** la dirección ip de la sub-red, **[120/1]:** La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente.

6.10.21.5 CONFIGURACIÓN SWITCH SUCURSAL GRAN COLOMBIA

Switch>**enable**

- A nivel de modo usuario normal digitar el comando anterior para pasar a modo de usuario privilegiado.

Switch#**configure terminal**

- A nivel de modo usuario privilegiado digitar el comando que se muestra para pasar a modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.

- Aparecerá unas líneas describiendo al usuario que ingrese los comandos de configuración, uno a uno.

Switch(config)#**hostname Sw_Gran_Colombia**

- En el modo de configuración general digitar el comando anterior para establecer el nombre del dispositivo.

Sw_Gran_Colombia(config)#

- Así deberá aparecer después de haber dado nombre al Switch.

CREACIÓN DE VLAN.

Sw_Gran_Colombia#**vlan database**

- Permite ingresar a la base de datos de las VLAN.

Sw_Gran_Colombia(vlan)#**vlan 30 name 30**

- Crea la vlan con el nombre especificado.

6.10.21.6 CONFIGURACIÓN DE PUERTOS ASIGNANDO VLAN.

Sw_Gran_Colombia(vlan)#**exit**

- Para salir de la base de datos de las VLAN.

Sw_Gran_Colombia#configure terminal

- A nivel de modo usuario privilegiado digitar el comando anterior para pasar a modo de configuración general

Sw_Gran_Colombia(config)#interface fastethernet 0/1

- Digitar el comando anterior para configurar la interfaz fastethernet 0/1.

Sw_Gran_Colombia(config-if)#switchport mode trunk

- Permite truncar el puerto donde se digitará este comando.

Sw_Gran_Colombia(config-if)#switchport access vlan 30

- Agregar este puerto a la vlan especificada.

Sw_Gran_Colombia(config)#interface fastethernet 0/2

- Digitar el comando anterior para configurar la interfaz fastethernet de puerto 0/2.

Sw_Gran_Colombia(config-if)#switchport access vlan 30

- Agregar este puerto a la vlan especificada.

GUARDAR CONFIGURACIONES HECHAS EN EL SWITCH.**Sw_Gran_Colombia(config-line)#exit**

- Digitar lo anterior para salir del modo configuración de consola a modo configuración general.

Sw_Gran_Colombia(config)#exit

- Se deberá ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado.

```
%SYS-5-CONFIG_I: Configured from console by console
```

- Cuando se realiza este procedimiento aparecerá el siguiente mensaje que significa que se ha configurado desde la interfaz de consola para la interfaz de consola.

Sw_Gran_Colombia#copy running-config startup-config

- Con el comando anterior se guardará la configuración actual a la configuración de inicio.



Building configuration...

- El siguiente mensaje significa que se esta guardando la configuración.

[OK]

- Ahora aparecerá un mensaje de aprobación.

SHOW RUN SWITCH SUCURSAL GRAN COLOMBIA.

```
Sw_Gran_Colombia#show run
!
Version 12.1
```

- Indica la versión del IOS

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

- Indica que el servicio de encriptación de contraseña esta activo.

```
!
hostname Sw_Gran_Colombia
```

- Refleja el nombre que el administrador le ha asignado al router.

```
!
interface FastEthernet0/1
```

- Especifica interfaz fastethernet 0/1

```
switchport mode trunk
```

- Indica que no esta configurado el modo tipo acceso.

```
switchport access vlan 30
```

- Especifica que esta interfaz es parte de la VLAN indicada.

```
bandwidth 100000
!
```

- Valor del ancho de banda del enlace en la interfaz

```
!
interface FastEthernet0/2
```

- Especifica interfaz fastethernet0/2.



```
switchport access vlan 30
```

- Especifica que esta interfaz es parte de la VLAN indicada.

```
bandwidth 100000
!
```

- Valor del ancho de banda del enlace en la interfaz.

```
!
vtp Server
vtp domain bigdomain
```

- Especifica el dominio del puerto truncado virtual.

```
interface Vlan 1
```

- Especifica la VLAN 1 (vlan por defecto).

```
no ip address
no ip route-cache
```

- Dirección IP de la vlan por defecto.
- No almacena ip en el cache de rutas.

```
shut down
```

- Indica que no esta levantado el servicio

```
vlan 30 name 30
!
```

- Indica VLAN configurada con su respectivo nombre.

```
!
ip classless
```

- Indica acceso a las redes no remotas con mascara de sub-red diferente.

```
no ip http server
!
```

- Especifica que no existe un servidor http.

```
!
line con 0
transport input none
```

- Configuración Puerto de consola.



BIBLIOTECA
CAMPUS
PEÑAS

```

line aux 0
line vty 0 15
!
```

- Configuración Puerto auxiliar.
- Configuración remota por telnet.

```

!
no scheduler allocate
end
```

- Fin del reporte de la configuración actual.



SHOW VLAN SWITCH SUCURSAL GRAN COLOMBIA.

```
Sw_Gran_Colombia#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
30	30	active	Fa0/1, Fa0/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fdnet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

```
Sw_Gran_Colombia#
```

Figura 6-63: Show VLAN Switch Gran Colombia.

VLAN:	Identificación vlan.
Name:	Nombre de vlan.
Status:	Estado de la Vlan.
Ports:	Puertos asignados a la vlan.
Type:	Tipo de interfaces.
SIAD:	Encabezado para identificar vlan.
MTU:	Tamaño máximo de los paquetes transmitidos por el puerto expresado en bytes.
Parent:	Parentela.
RingNo:	Número de anillo si hay.
BridgeNO:	Número de puente si hay.
Stp:	STP usado
BrdgMode:	Modo de puente.
Trans:	TRANS, o si es una VLAN que cambia de topología Token Ring / FDDI a Ethernet.

6.10.22 CONFIGURACIÓN DEL ROUTER SUCURSAL MAGDALENA.

Router>**enable**

- A nivel del modo usuario normal se deberá digitar el comando anterior para pasar a modo de usuario privilegiado.

Router#**configure terminal**

- Digitar éste comando en el modo de usuario privilegiado para pasar al modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.

- Aparecerá un mensaje que indicará al usuario que debe ingresar los comandos de configuración, línea por línea.

Router(config)#**hostname Suc_Magdalena**

- En el modo de configuración general digitar el comando anterior y a continuación un nombre para el dispositivo.



BIBLIOTECA
CAMPUS
PEÑAS

6.10.22.1 CONFIGURACIÓN DE INTERFACES SERIALES.

Suc_Magdalena(config)#**interface serial 1**

- Digitar el comando anterior para entrar al modo de configuración de la interfaz serial 1.

Suc_Magdalena(config-if)#**ip address 192.168.7.18 255.255.255.252**

- Este comando permite asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

Suc_Magdalena(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente la interfaz. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

```
%LINK -3-UPDOWN: Interface serial1, changed state to up
```

6.10.22.2 CONFIGURACIÓN DE FASTETHERNET SUCURSAL GRAN COLOMBIA

Suc_Magdalena(config)#**interface fastethernet 0/0**

- Digitar el comando anterior para entrar al modo de configuración de la interfaz fastethernet 0/0.

Suc_Magdalena(config-if)#**ip address 192.168.7.137 255.255.255.248**

- Este comando permitirá asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz.

Suc_Magdalena(config-if)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente la interfaz. Luego de digitar éste comando, aparecerá el siguiente mensaje el cual realizará un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down**, quiere decir que existe algún tipo de problema en el enlace.

```
%LINK -3-UPDOWN: Interface Fastethernet 0/0, changed state to up
```

6.10.22.3 CONFIGURACIÓN DE SUB-INTERFAZ.

Para poder configurar una sub-interfaz, se deberá entrar al modo de usuario privilegiado.

Suc_Magdalena(config)#**interface fastethernet 0.1**

- Digitar el comando anterior para entrar al modo de configuración de la sub-interfaz FastEthernet 0.1.

Suc_Magdalena(config-subif)#**encapsulation dot1q 40**

- Se deberá digitar el comando encapsulation dot1q para definir el tipo de encapsulamiento.

Suc_Magdalena(config-subif)#**ip address 192.168.8.49 255.255.255.248**

- Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz.

Suc_Magdalena(config-subif)#**no shutdown**

- Se deberá ingresar éste comando para habilitar administrativamente el la interfaz.



BIBLIOTECA
CAMPUS
PEÑAS

6.10.22.4 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSION 2.

Suc_Magdalena# **configure terminal**

- A nivel de modo usuario privilegiado se debe digitar el comando anterior para pasar a modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.

- Aparecerá un mensaje que indica al usuario que ingrese los comandos de configuración, línea por línea.

Suc_Magdalena(config-if)#**router rip**

- Se deberá habilitar el protocolo de enrutamiento con el comando anterior.

Suc_Magdalena(config-router)#**version 2**

- Se deberá especificar la versión del protocolo de enrutamiento.

Suc_Magdalena(config-router)#**network 192.168.7.0**

Suc_Magdalena(config-router)#**network 192.168.8.0**

- Una vez activado el protocolo de enrutamiento es preciso indicar qué redes se van a enrutar.
- Asignando las redes que seguirán el protocolo.

GUARDANDO LA CONFIGURACIÓN DEL ROUTER.

Suc_Magdalena#**wr**

- Con el comando anterior se guarda la configuración actual a la configuración de inicio.

Building configuration...

- El siguiente mensaje indica que se está guardando la configuración.

[OK]

- Ahora aparece un mensaje de aprobación



BIBLIOTECA
CAMPUS
SEPEÑAS

SHOW RUN ROUTER SUCURSAL MAGDALENA

```
Suc_Magdalena#show run
Building configuration...
```

```
!
Version 12.1
```

- Indica la versión del IOS.

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

- Indica que el servicio de encriptación de contraseña está activo.

```
!
hostname Suc_Magdalena
!
```

- Refleja el nombre que el administrador le ha asignado al router

```
!
ip subnet-zero
!
interface Serial1
```

- Especifica interfaz serial 1

```
ip address 192.168.7.18 255.255.255.252
```

- Dirección ip y máscara de de sub-red de la interfaz.

```
no ip directed-broadcast
```

- Indica la velocidad de la interfaz en bits por segundo. Se lo encuentra en interfaces DCE.

```
bandwidth 1544
!
```

- Valor del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/0
```

- Especifica interfaz fastethernet 0 slot 0



```
ip address 192.168.7.137 255.255.255.248
```

- Dirección ip y máscara de de sub-red de la Fastethernet.

```
no ip directed-broadcast
bandwidth 1544
!
```

- Valor del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/0.1
```

- Especifica sub-interfaz fastethernet 0.1 slot 0.

```
encapsulation dot1q 40
```

- Define el tipo de encapsulamiento asignado a la VLAN 30.

```
ip address 192.168.8.49 255.255.255.248
!
```

- Dirección ip y máscara de de sub-red de la sub-interfaz.

```
!
router rip
```

- Indica que se ha configurado el protocolo de enrutamiento rip.

```
version 2
```

- Define la versión 2 del protocolo de enrutamiento.

```
network 192.168.7.0
network 192.168.8.0
!
```

- Indica qué redes enruta el protocolo de enrutamiento.

```
!
ip classless
```

- Indica acceso a las redes no remotas con máscara de sub-red diferente.

```
no ip http server
!
!
```



BIBLIOTECA
CAMPUS
PEÑAS

- Especifica que no existe un servidor http.

```
!
line con 0
transport input none
```

- Configuración Puerto de consola.
- Ningún transporte impuesto.

```
line aux 0
line vty 0 4
!
```

- Configuración Puerto auxiliar.
- Configuración remota por telnet.

```
!
no scheduler allocate
end
```

- Fin del reporte de la configuración actual



SHOW IP ROUTE SUCURSAL MAGDALENA

```
Suc_Magdalena#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

Gateway of last resort is not set

192.168.8.0/29 is subnetted, 4 subnets
C       192.168.8.48 is directly connected, 192.168.8.49
R       192.168.8.40 [120/2] via 192.168.7.17, 00:03:19, Serial1
R       192.168.8.24 [120/3] via 192.168.7.17, 00:07:27, Serial1
R       192.168.8.32 [120/3] via 192.168.7.17, 00:08:21, Serial1
192.168.7.0/0 is variably subnetted, 8 subnets
C       192.168.7.16/30 is directly connected, Serial1
C       192.168.7.136/29 is directly connected, FastEthernet0/0
R       192.168.7.0/30 [120/1] via 192.168.7.17, 00:02:29, Serial1
R       192.168.7.12/30 [120/1] via 192.168.7.17, 00:06:31, Serial1
R       192.168.7.88/29 [120/1] via 192.168.7.17, 00:06:13, Serial1
R       192.168.7.128/29 [120/2] via 192.168.7.17, 00:08:27, Serial1
R       192.168.7.112/29 [120/3] via 192.168.7.17, 00:07:25, Serial1
R       192.168.7.120/29 [120/3] via 192.168.7.17, 00:02:43, Serial1

Suc_Magdalena#
```

Figura 6-64: Show IP Route Sucursal Magdalena

- **C:** Especifica que la interfaz está conectada directamente, **192.168.x.x:** la dirección de la sub-red a la cual está conectado y **Serial 0/x:** la interfaz de salida por la cual se accede a la red de destino.

- **R:** Especifica el protocolo de enrutamiento usado para conectarse a la red destino (RIP), **192.168.x.x:** la dirección ip de la sub-red, **[120/1]:** La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente.

6.10.22.5 CONFIGURACIÓN SWITCH SUCURSAL MAGDALENA

Switch>**enable**

- A nivel de modo usuario normal digitar el comando anterior para pasar a modo de usuario privilegiado.

Switch#**configure terminal**

- A nivel de modo usuario privilegiado digitar el comando que se muestra para pasar a modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.

- Aparecerán unas líneas describiendo al usuario que ingrese los comandos de configuración, uno a uno.

Switch(config)#**hostname Sw_Magdalena**

- En el modo de configuración general digitar el comando anterior para establecer el nombre del dispositivo.

Sw_Magdalena(config)#

- Así deberá aparecer después de haber dado nombre al Switch.

6.10.22.6 CREACIÓN DE VLAN.

Sw_Magdalena#**vlan database**

- Permite ingresar a la base de datos de las VLAN.

Sw_Magdalena(vlan)#**vlan 40 name 40**

- Crea la vlan con el nombre especificado.

6.10.22.7 CONFIGURACIÓN DE PUERTOS ASIGNANDO VLAN.

Sw_Magdalena(vlan)#**exit**

- Para salir de la base de datos de las VLAN.

Sw_Magdalena#**configure terminal**

- A nivel de modo usuario privilegiado digitar el comando anterior para pasar a modo de configuración general

Sw_Magdalena(config)#**interface fastethernet 0/1**

- Digitar el comando anterior para configurar la interfaz fastethernet 0/1.

Sw_Magdalena(config-if)#**switchport mode trunk**

- Permite truncar el puerto donde se digita este comando.

Sw_Magdalena(config-if)#**switchport access vlan 40**

- Agrega este puerto a la vlan especificada.

Sw_Magdalena(config)#**interface fastethernet 0/2**

- Digitar el comando anterior para configurar la interfaz fastethernet de puerto 0/2.

Sw_Magdalena(config-if)#**switchport access vlan 40**

- Agrega este puerto a la vlan especificada.

GUARDAR CONFIGURACIONES HECHAS EN EL SWITCH.

Sw_Magdalena(config-line)#**exit**

- Digitar lo anterior para salir del modo configuración de consola a modo configuración general.

Sw_Magdalena(config)#**exit**

- Se debe ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado.

```
%SYS-5-CONFIG_I: Configured from console by console
```

- Cuando se realiza este procedimiento aparecerá el siguiente mensaje que significa que se ha configurado desde la interfaz de consola para la interfaz de consola.

```
Sw_Magdalena#copy running-config startup-config
```

- Con el comando anterior se guarda la configuración actual a la configuración de inicio.

```
Building configuration...
```

- El siguiente mensaje significa que se esta guardando la configuración.

```
[OK]
```

- Ahora aparece un mensaje de aprobación.

```
SHOW RUN SWITCH SUCURSAL MAGDALENA.
```

```
Sw_Magdalena#show run
!
Version 12.1
```

- Indica la versión del IOS

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

- Indica que el servicio de encriptación de contraseña esta activo.

```
!
hostname Sw_Magdalena
```

- Refleja el nombre que el administrador le ha asignado al router.

```
!
interface FastEthernet0/1
```

- Especifica interfaz fastethernet 0/1

```
switchport mode trunk
```

- Indica que no esta configurado el modo tipo acceso.

```
switchport access vlan 40
```

- Especifica que esta interfaz es parte de la VLAN indicada.

```
bandwidth 100000
```

```
!
```

- Valor del ancho de banda del enlace en la interfaz

```
!
```

```
interface FastEthernet0/2
```

- Especifica interfaz fastethernet0/2.

```
switchport access vlan 40
```

- Especifica que esta interfaz es parte de la VLAN indicada.

```
bandwidth 100000
```

```
!
```

- Valor del ancho de banda del enlace en la interfaz.

```
!
```

```
vtp Server
```

```
vtp domain bigdomain
```

- Especifica el dominio del puerto truncado virtual.

```
interface Vlan 1
```

- Especifica la VLAN 1 (vlan por defecto).

```
no ip address
```

```
no ip route-cache
```

- Dirección IP de la vlan por defecto.
- No almacena ip en el cache de rutas.

```
shut down
```

- Indica que no esta levantado el servicio

```
vlan 40 name 40
```

```
!
```

- Indica VLAN configurada con su respectivo nombre.

```
!
```

```
ip classless
```

- Indica acceso a las redes no remotas con mascara de sub-red diferente.

```
no ip http server
!
```

- Especifica que no existe un servidor http.

```
!
line con 0
transport input none
```

- Configuración Puerto de consola.

```
line aux 0
line vty 0 15
!
```

- Configuración Puerto auxiliar.
- Configuración remota por telnet.

```
!
no scheduler allocate
end
```

- Fin del reporte de la configuración actual.

SHOW VLAN SWITCH SUCURSAL MAGDALENA.

```
Sw_Magdalena#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
40 40	active	Fa0/1, Fa0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
40	enet	100040	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

```
Sw_Magdalena#
```

Figura 6-65: Show VLAN Switch Magdalena

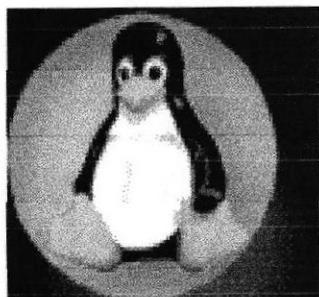


BIBLIOTECA
CAMPUS
PEÑAS

CAPÍTULO 7 LINUX

7 LINUX

7.1 INTRODUCCIÓN A LINUX



Linux es un Unix libre, es decir, un sistema operativo, como el Windows o el MS-DOS (sin embargo, a diferencia de estos y otros sistemas operativos propietarios, ha sido desarrollado por miles de usuarios de computadores a través del mundo, y la desventaja de estos es que lo que te dan es lo que tu obtienes, dicho de otra forma no existe posibilidad de realizar modificaciones ni de saber como se realizó dicho sistema), que fue creado inicialmente como un hobby por un estudiante joven, Linus Torvalds, en la universidad de Helsinki en

Finlandia, con asistencia por un grupo de hackers a través de Internet. Linus tenía un interés en Minix, un sistema pequeño o abreviado del UNIX (desarrollado por Andy Tanenbaum); y decidido a desarrollar un sistema que excedió los estándares de Minix. Quería llevar a cabo un sistema operativo que aprovecharse la arquitectura de 32 bits para multitarea y eliminar la barrera del direccionamiento de memoria. Torvalds empezó escribiendo el núcleo del proyecto en ensamblador, y luego comenzó a añadir código en C, lo cual incrementó la velocidad de desarrollo, e hizo que empezara a tomarse en serio su idea.

Él comenzó su trabajo en 1991 cuando él realizó la versión 0,02, la cual no la dió a conocer porque ni siquiera tenía drivers de disquette, además de llevar un sistema de almacenamiento de archivos muy defectuoso.

Trabajó constantemente hasta 1994 en que la versión 1,0 del núcleo o (KERNEL) de Linux se concretó. La versión completamente equipada actual es 2,2 (versión concluida el 25 de enero de 1999), y el desarrollo continúa.

Linux tiene todas las prestaciones que se pueden esperar de un Unix moderno y completamente desarrollado: multitarea real, memoria virtual, bibliotecas compartidas, carga de sistemas a-demanda, compartimiento, manejo de debido de la memoria y soporte de redes TCP/IP.

Linux corre principalmente en PCs basados en procesadores 386/486/586, usando las facilidades de proceso de la familia de procesadores 386 (segmentación TSS, etc.) para implementar las funciones nombradas.

La parte central de Linux (conocida como núcleo o Kernel) se distribuye a través de la Licencia Pública General GNU, lo que básicamente significa que puede ser copiado libremente, cambiado y distribuido, pero no es posible imponer restricciones adicionales a los productos obtenidos y, adicionalmente, se debe dejar el código fuente disponible, de la misma forma que está disponible el código de Linux. Aún cuando Linux tenga registro de Copyright, y no sea estrictamente de dominio público. La licencia tiene por objeto asegurar que Linux siga siendo gratuito y a la vez estándar. Por su naturaleza Linux se distribuye libremente y puede ser obtenido y utilizado sin restricciones por cualquier persona, organización o empresa que así lo desee, sin necesidad de que tenga que firmar ningún documento ni inscribirse como usuario. Por todo ello, es muy difícil establecer quiénes son los principales usuarios de Linux. No obstante se sabe que actualmente Linux está siendo utilizado ampliamente en soportar servicios en Internet, lo utilizan Universidades alrededor del todo el mundo para sus redes y sus clases, lo utilizan empresas productoras de equipamiento industrial para vender como software de apoyo a su maquinaria, lo utilizan cadenas de supermercados, estaciones de servicio y muchas instituciones del gobierno y militares de varios países.

Obviamente, también es utilizado por miles de usuarios en sus computadores personales.

El apoyo más grande, sin duda, ha sido Internet ya que a través de ella se ha podido demostrar que se puede crear un sistema operativo para todos los usuarios sin la necesidad de fines lucrativos.

Linux tiene una mascota oficial, el pingüino de Linux, que fue seleccionado por Linus Torvalds para representar la imagen que se asocia al sistema operativo que él creó.

7.2 REQUERIMIENTO PARA INSTALAR UN SERVIDOR LINUX

REQUERIMIENTO MINIMO	
Memoria	64 MB
Disco Duro	5 GB
Procesador	Pentium II de 300 Mhz

Tabla 7-1: Requerimiento mínimo

REQUERIMIENTO ÓPTIMO	
Memoria	512 MB
Disco Duro	10 GB
Procesador	Pentium D

Tabla 7-2: Requerimiento óptimo



7.3 CONFIGURACIÓN DEL BIOS

Para iniciar la instalación se deberá ingresar al bios pulsando varias veces la tecla suprimir (Equipo Clon) o F2 (Equipo de Marca) dependiendo de la marca.

Una vez que se ingresa al **BIOS** aparecerá una pantalla de configuración parecida a la que se muestra a continuación:

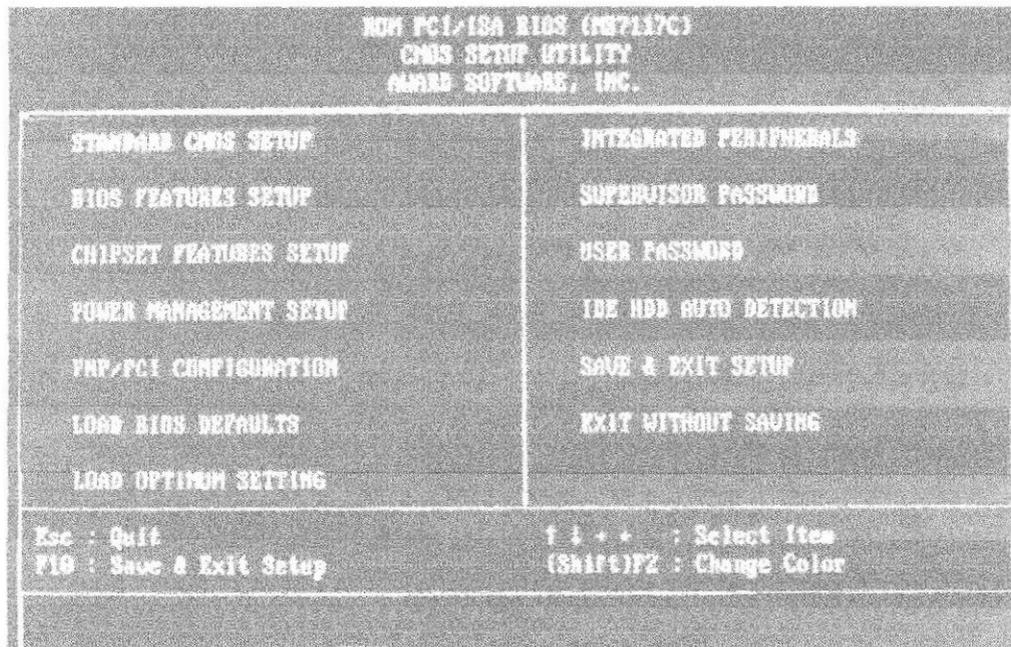


Figura 7-1: Configuración del BIOS

Pulsar **ENTER**, en la opción **BIOS FEATURES SETUP**, tal como se muestra en la gráfica siguiente.

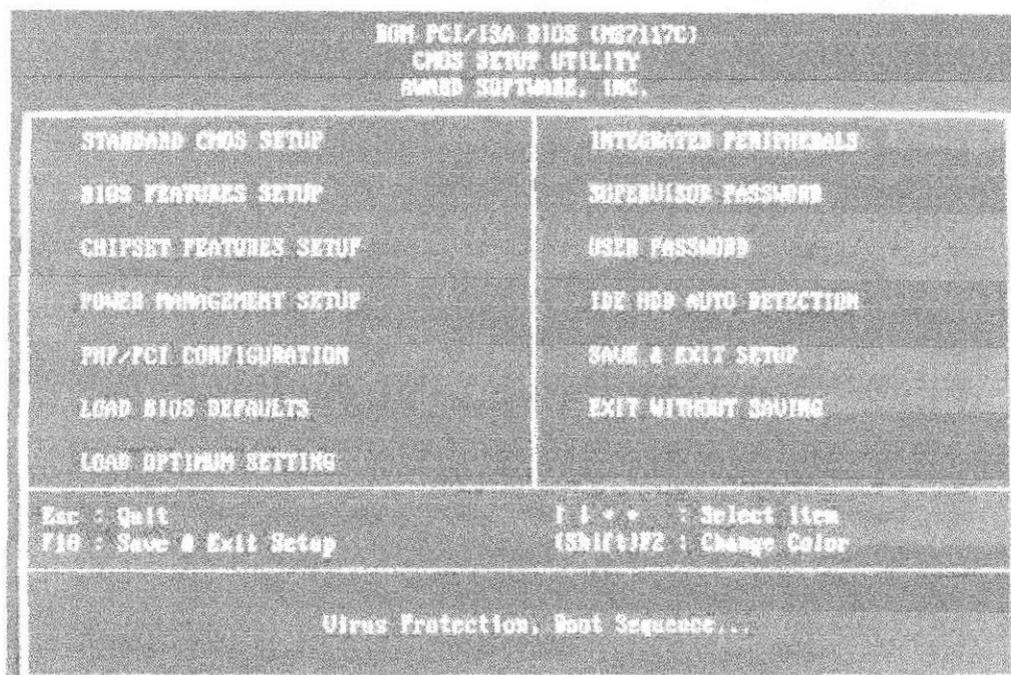


Figura 7-2: BIOS FEATURES SETUP

Ubicarse en Boot Sequence y con AvPág seleccionar CDROM,C,A para que el PC arranque desde el CDROM (además, deberá quitar la protección antivirus, para volver a poner al acabar la instalación del sistema operativo).

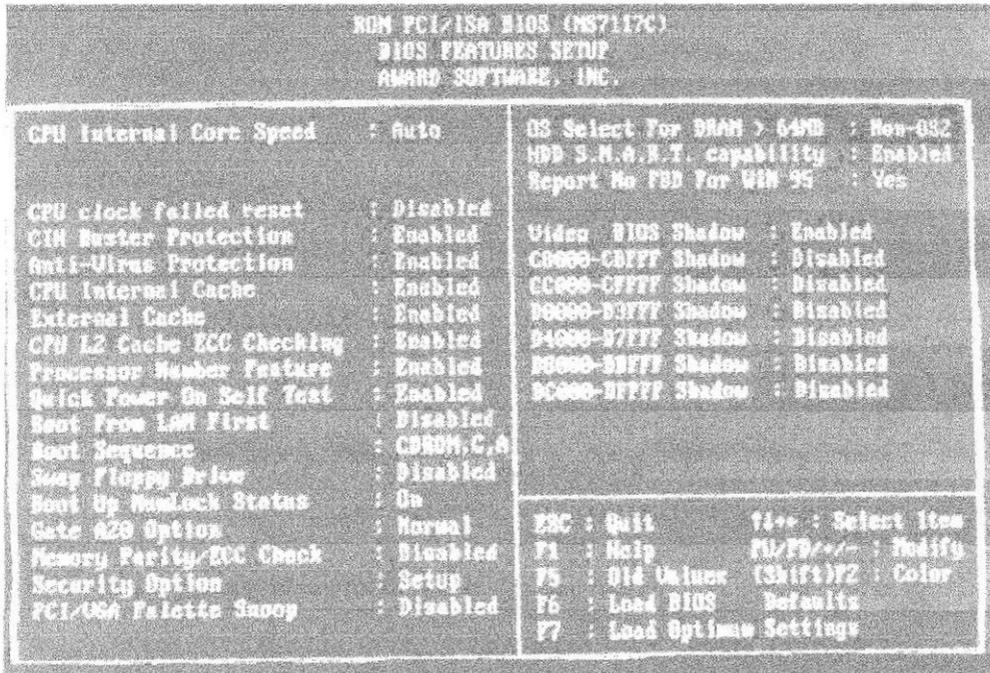


Figura 7-3: Selección del CDROM

Pulsar ESC y mostrar la siguiente pantalla, donde resalta SAVE & EXIT SETUP, pulsar ENTER, y el PC arranca de nuevo.

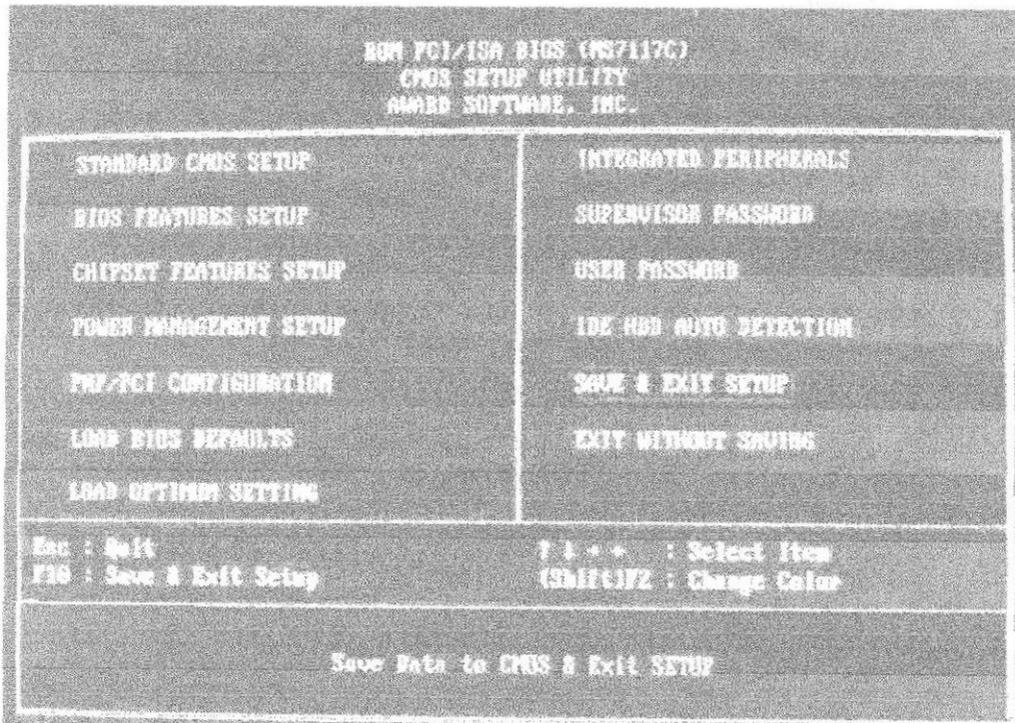


Figura 7-4: Selección SAVE & EXIT

7.4 INSTALACIÓN DE LINUX FEDORA CORE 3

Esta es la primera pantalla que muestra la instalación del sistema operativo Linux Fedora Core 3, para continuar con la instalación presionar la tecla enter.

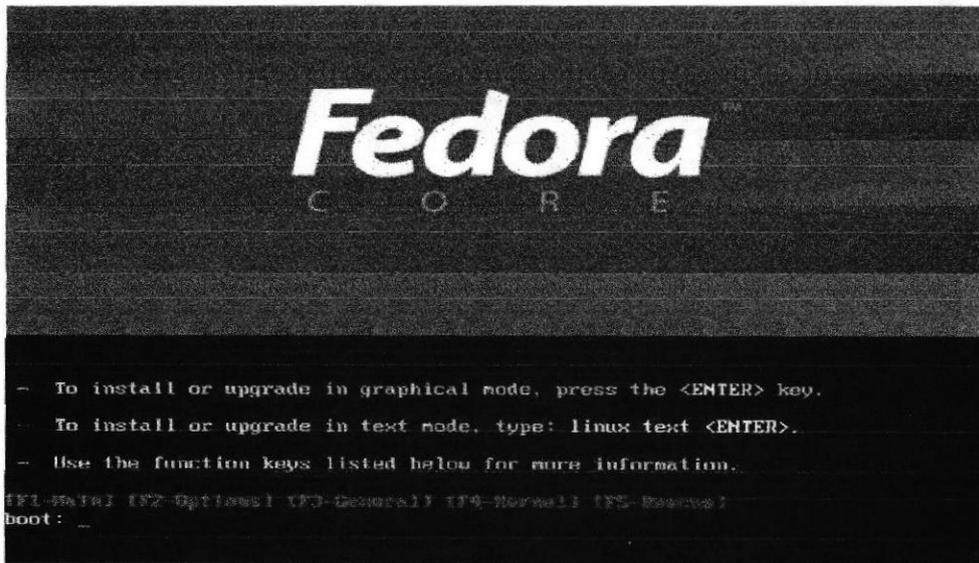
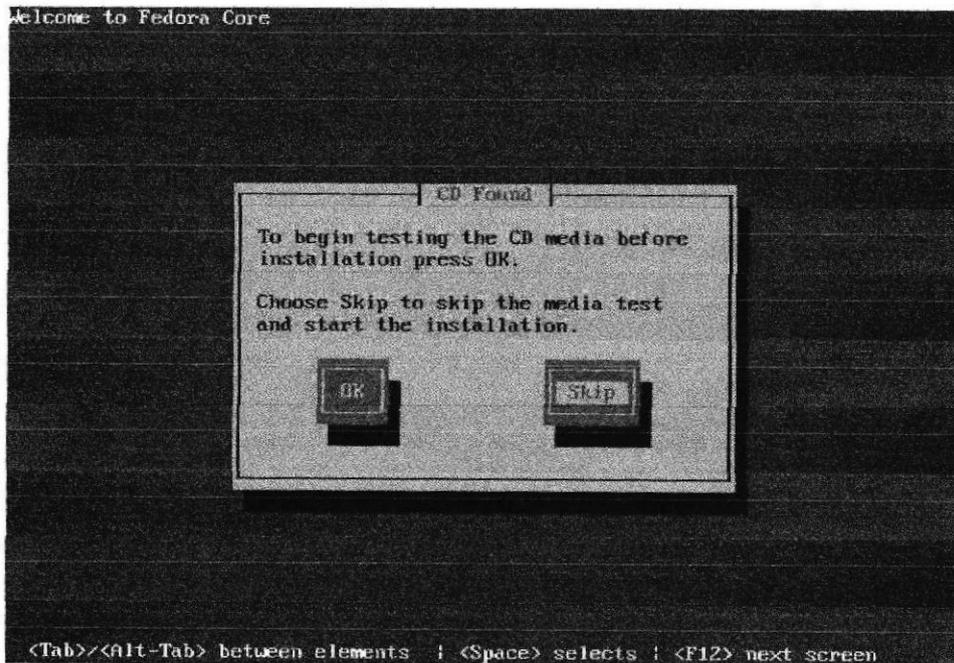


Figura 7-5: Instalación

Esta pantalla pregunta si quiere hacer un skandisk al disco o si se quiere omitir ese paso, para este caso ubicarse en Skip y presionar la tecla enter.



BIBLIOTECA
CAMPUS
PEÑAS

Figura 7-6: Skandisk

En esta pantalla el asistente da la bienvenida a la instalación de Linux Fedora Core 3, para continuar con la instalación dar clic en Next.

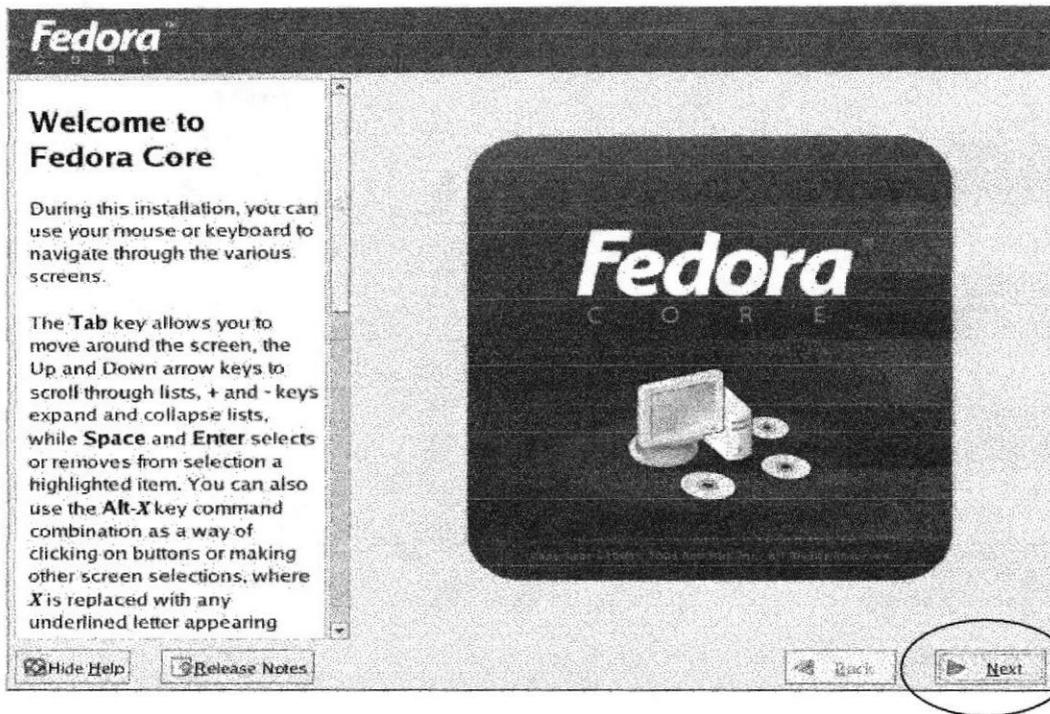


Figura 7-7: Bienvenida

En esta pantalla el asistente permite elegir el idioma en el que va a ser instalado el Sistema Operativo, para continuar con la instalación dar clic en Next.

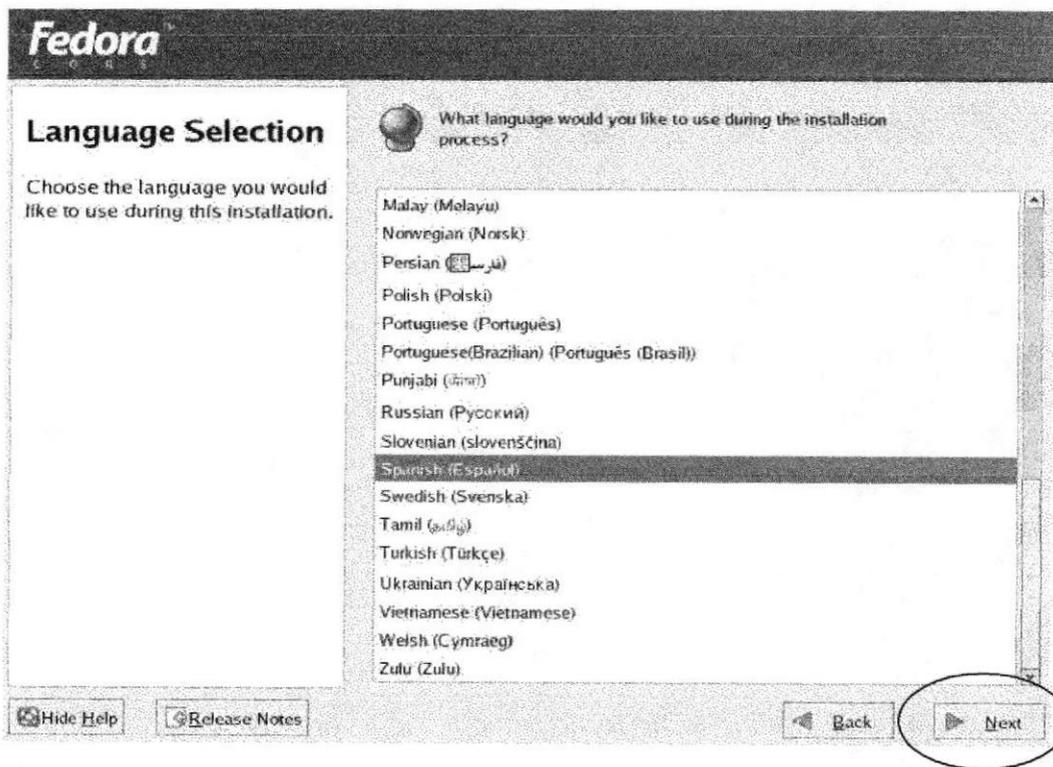


Figura 7-8: Selección de Idioma



BIBLIOTECA
CAMPUS
PEÑAS

En esta pantalla el asistente muestra la configuración del teclado el cual puede elegir el idioma según el teclado que tenga, para continuar con la instalación dar clic en Siguiente.

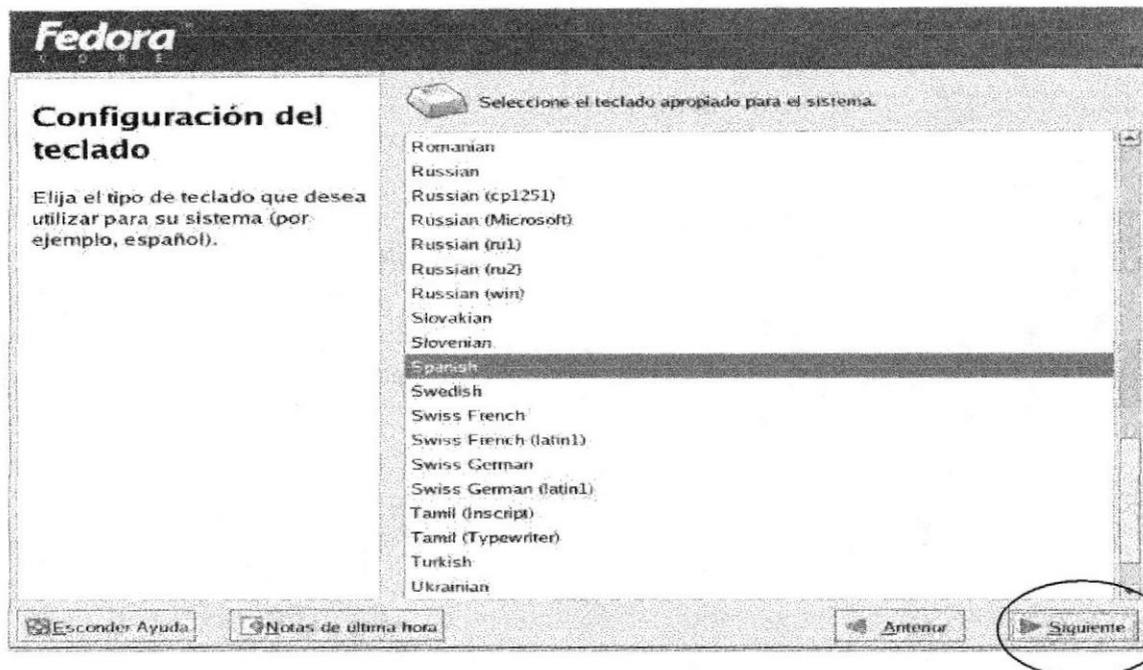


Figura 7-9: Selección de Idioma del teclado

En esta pantalla el asistente muestra el tipo de instalación que quiera realizar para el Servidor, para este caso seleccionar personalizado, para continuar con la instalación dar clic en Siguiente.

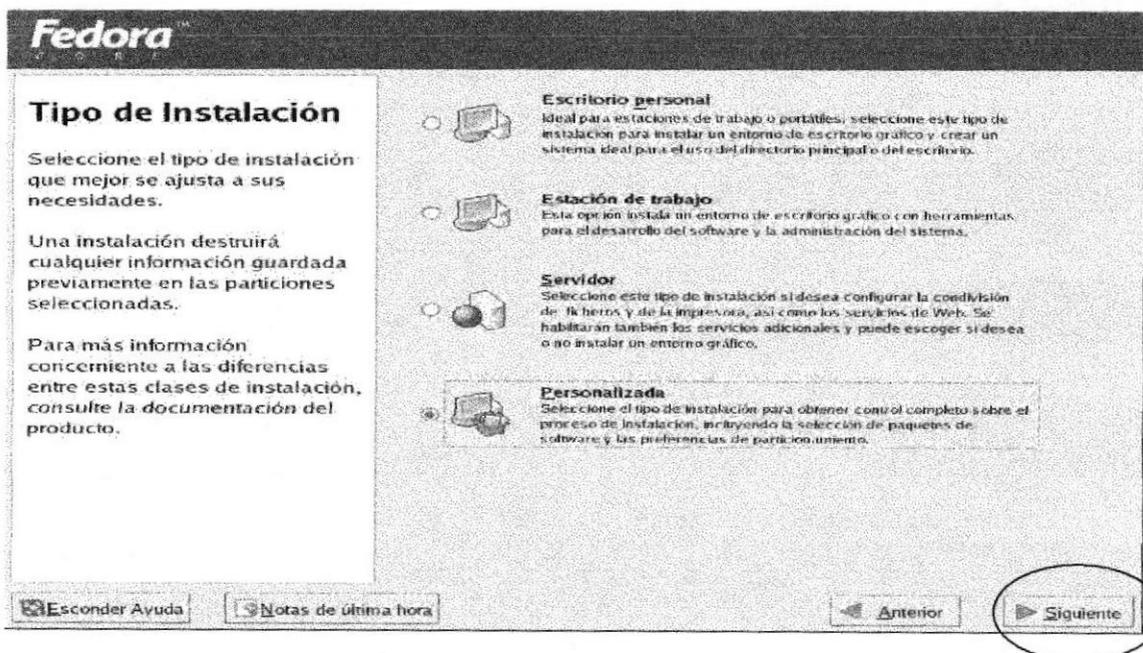


Figura 7-10: Tipo de Instalación



POLITECNICO DEL ESTADO

BIBLIOTECA
CAMPUS
PEÑAS

Si elige esta opción de Servidor, el asistente instalará todos los paquetes relacionados con un Servidor, incluyendo paquetes que el administrador no usará.

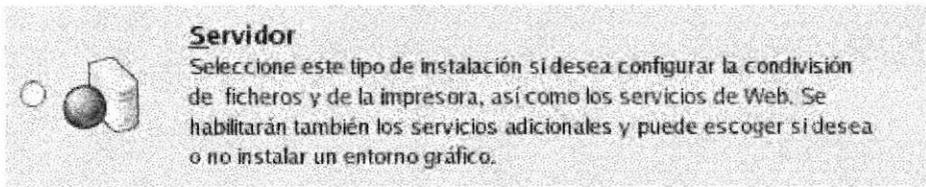


Figura 7-11: Opción Servidor

Esta opción permite elegir paso a paso las herramientas y paquetes que se vaya a instalar en el Servidor.

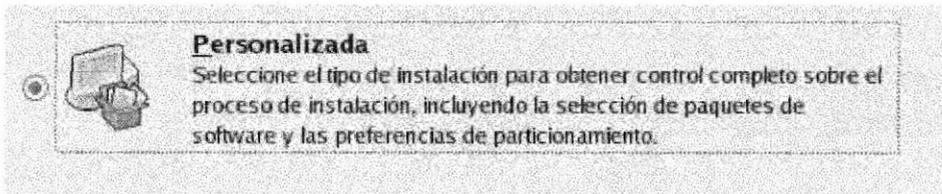


Figura 7-12: Opción Personalizada

En esta pantalla el asistente permite la configuración y particionamiento del disco duro, elegir la opción de Partición Manual con Disk Druid, para continuar con la instalación dar clic en Siguiente.

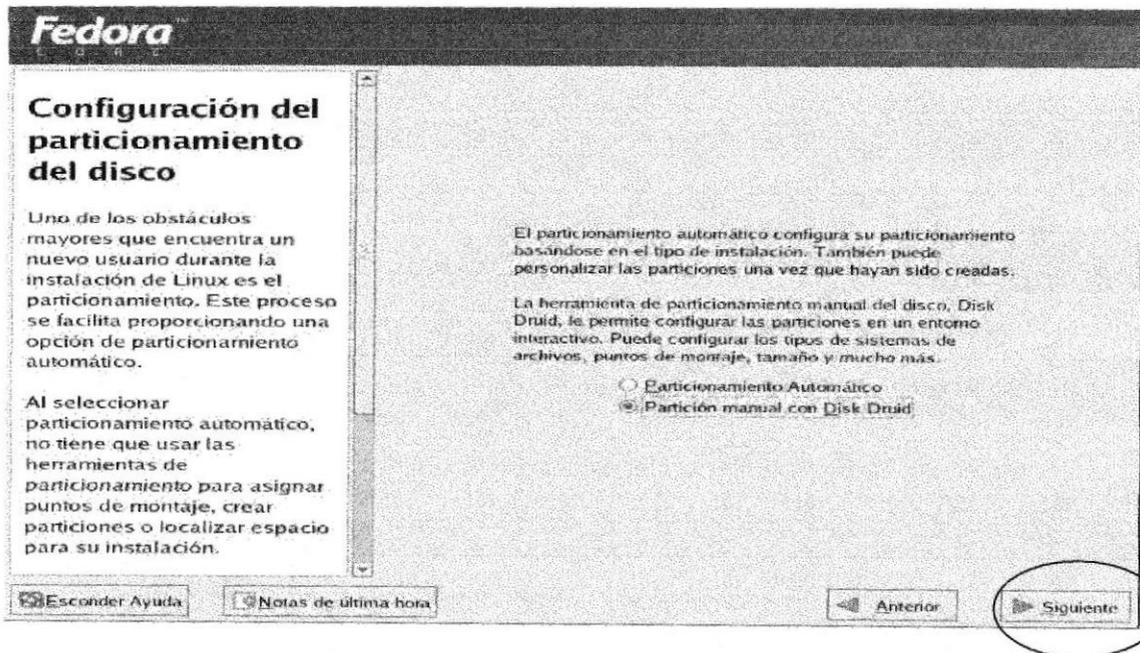


Figura 7-13: Configuración Particionamiento del Disco

En esta pantalla el asistente permite asignar un espacio en el disco duro en el cual el sistema operativo va a ser instalado, dar clic en Nuevo para comenzar la creación de las particiones.

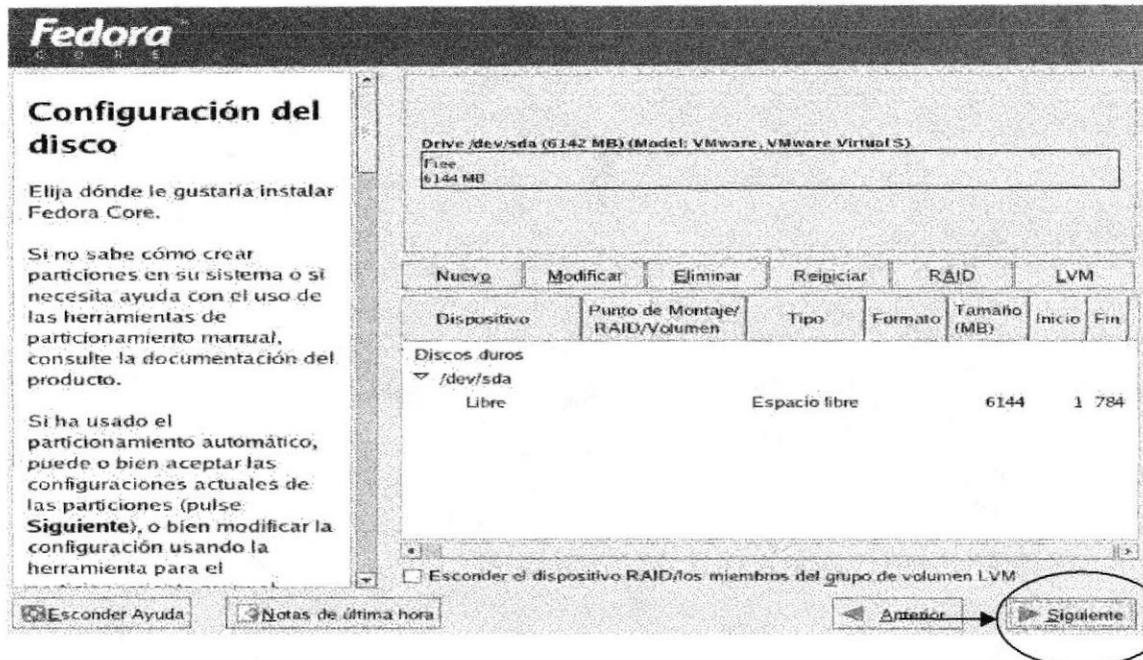


Figura 7-14: Configuración del disco

En esta pantalla comenzar a crear la partición Boot, que es la que maneja el sistema de bueteo de Linux, asignar el tamaño por defecto de 100 MB, dar clic en aceptar.

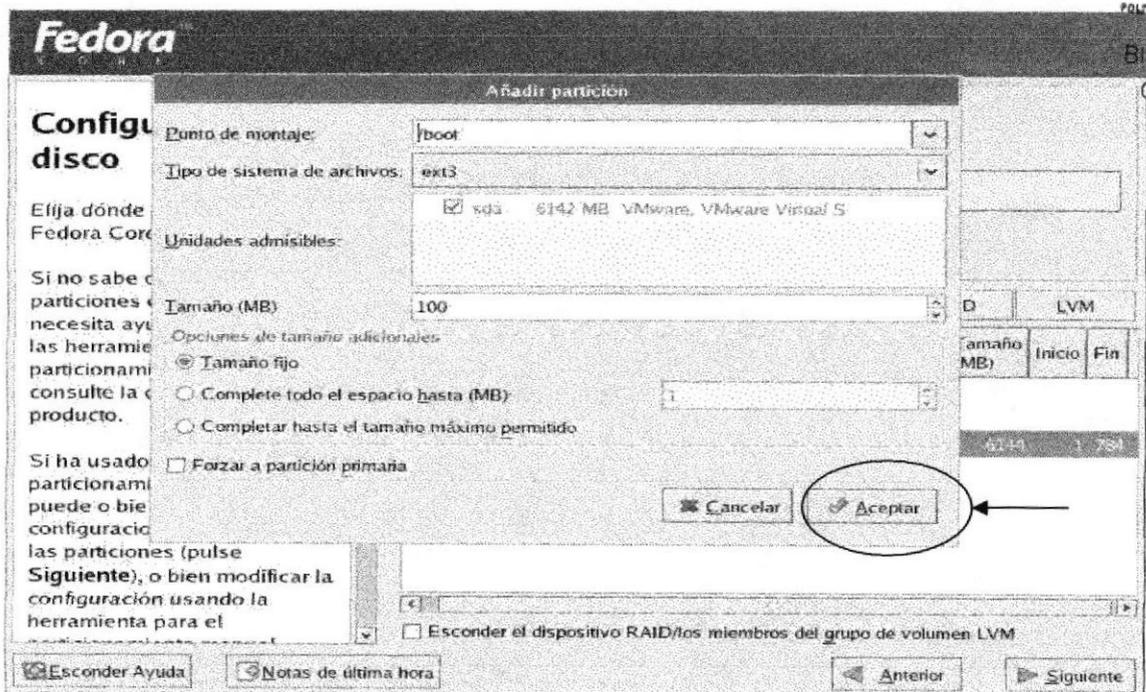


Figura 7-15: Añadir Partición



BIBLIOTECA
CAMPUS
PEÑAS

En esta pantalla comenzar a crear la partición Swap, que es la partición que maneja la memoria virtual del sistema, se le asigna el tamaño dependiendo de la Memoria Ram que tenga el Servidor, dar clic en aceptar.

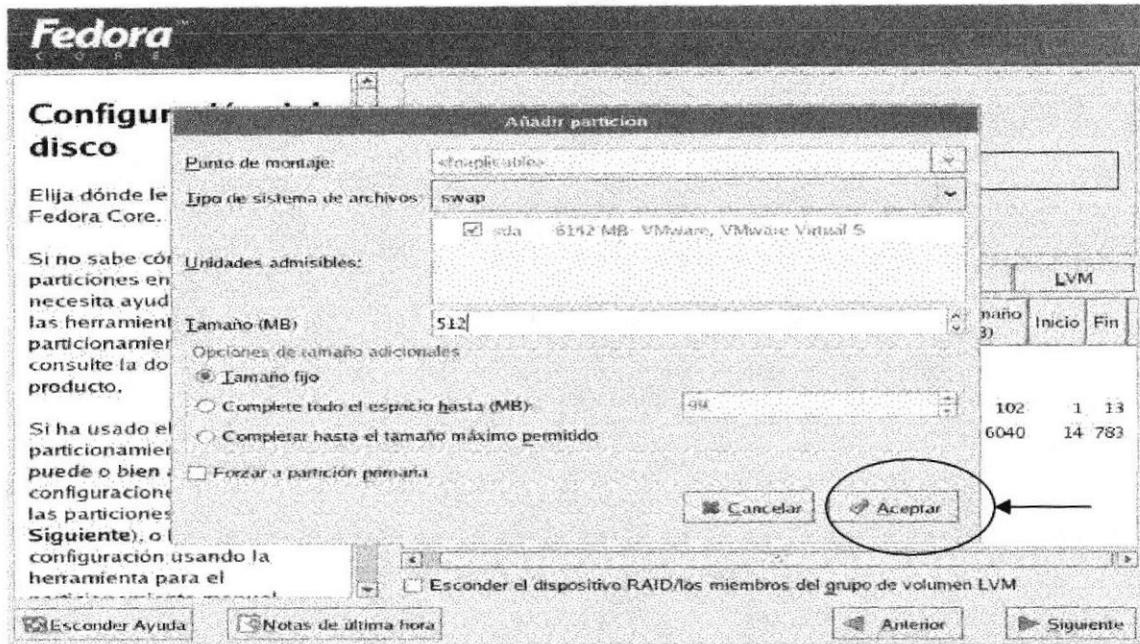


Figura 7-16: Creación Swap

En esta pantalla comenzar a crear la partición Raíz, esta partición permite crear la estructura de directorios en Linux, se recomienda un espacio mínimo de 5 Gb, dar clic en aceptar.

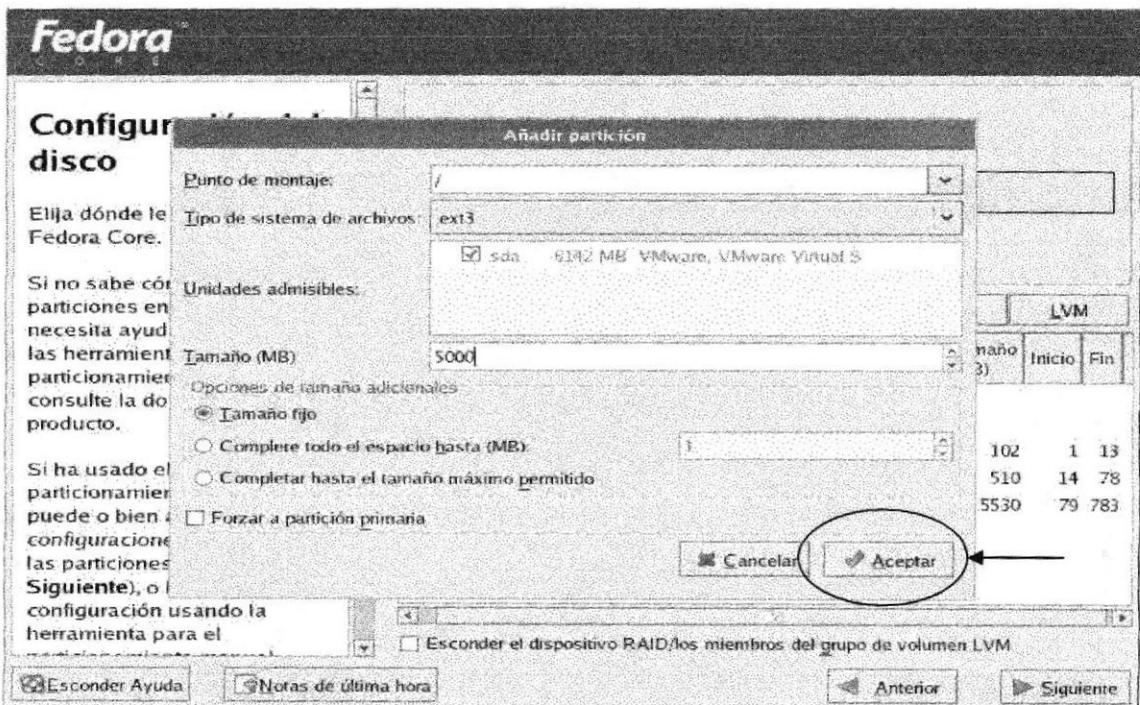


Figura 7-17: Creación partición raiz



BIBLIOTECA
CAMPUS
PEÑAS

Si todas las particiones fueron creadas con éxito el asistente mostrará una pantalla como esta, en el cual mostrará todas las particiones creadas, para continuar con la instalación dar clic en Siguiente.

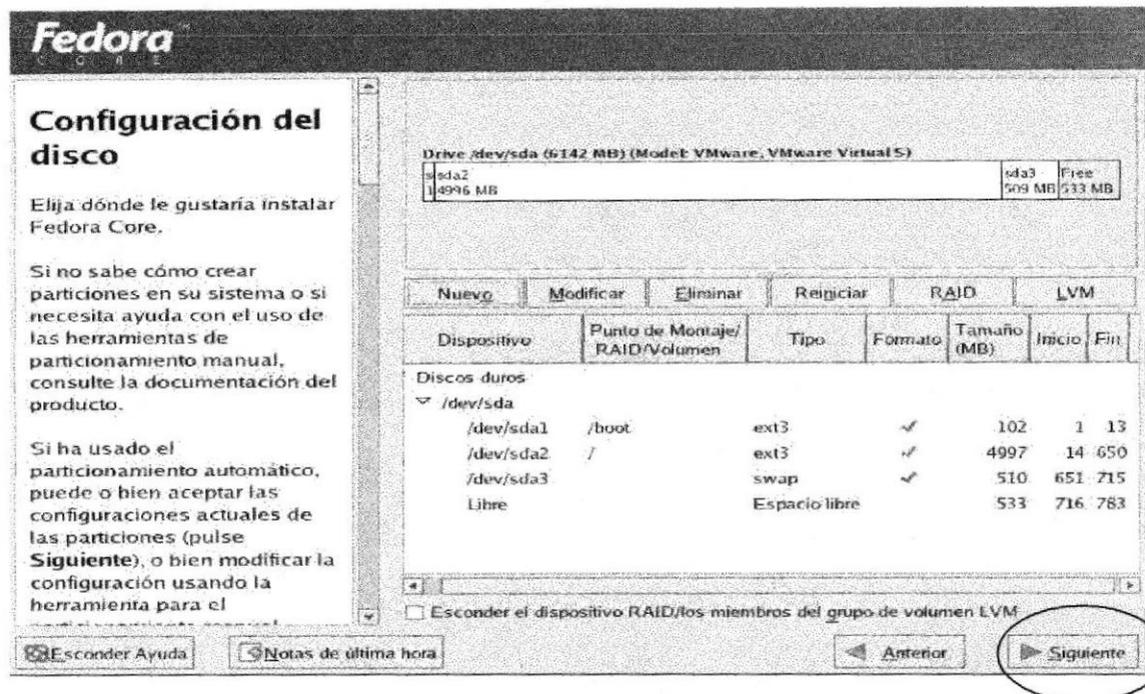


Figura 7-18: Configuración del Disco

En esta pantalla el asistente permite configurar el gestor de arranque, en caso de estar instalado otro sistema operativo el asistente permitirá elegir con cual sistema el Servidor arrancará, para continuar con la instalación dar clic en Siguiente.

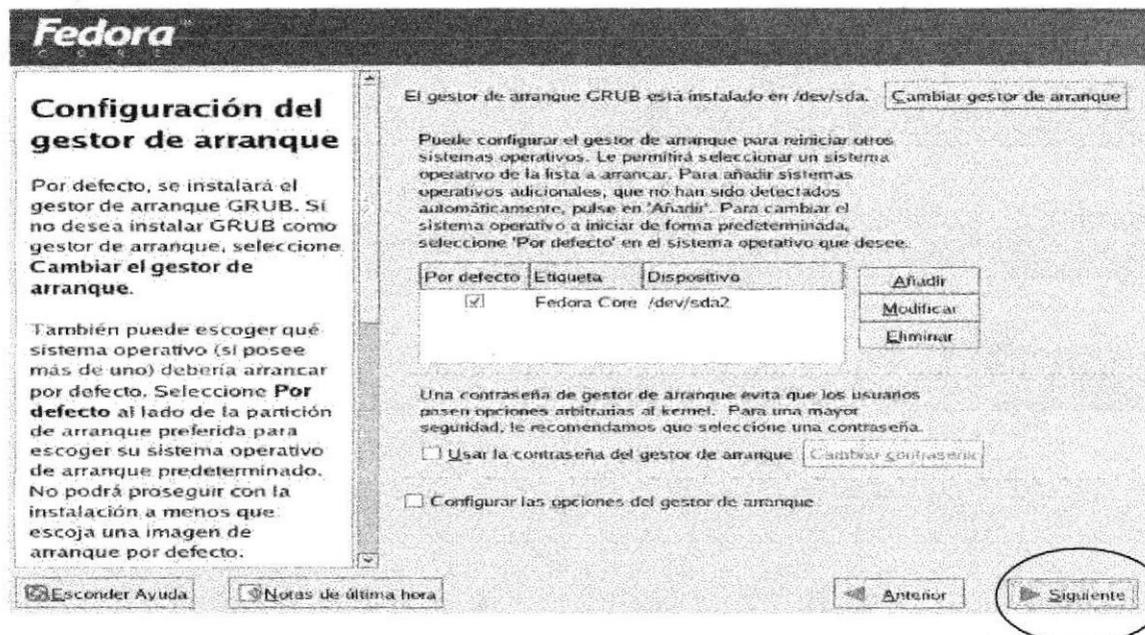


Figura 7-19: Configuración del Gestor de Arranque



BIBLIOTECA
CAMPUS
PEÑAS

Gestor de Arranque: Es aquel que permite butear entre varios Sistemas Operativos.

En esta pantalla el asistente permite configurar la dirección IP del Servidor, para este caso solo dar clic en siguiente porque asignará la IP más adelante de forma manual.

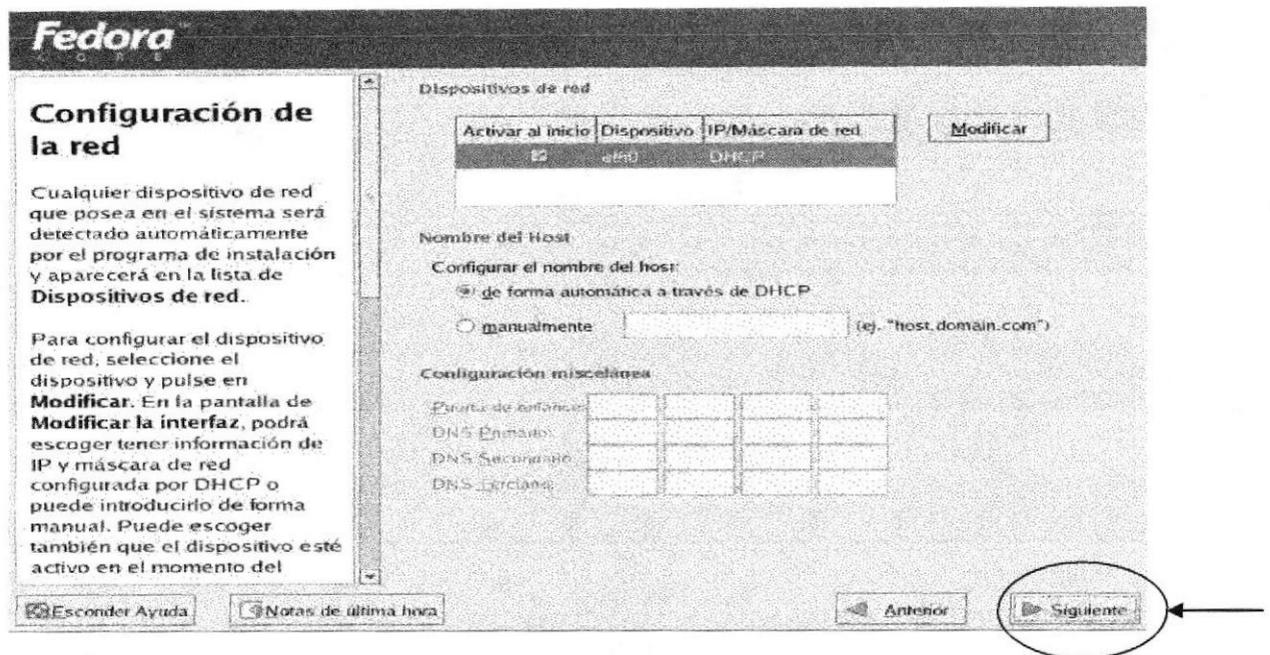


Figura 7-20: Configuración de Red

En esta pantalla el asistente permitirá configurar un Firewall para proteger el Servidor en la Red, para este caso dar clic en Ningún Cortafuego ya que lo se configurará de forma manual más adelante, para continuar con la instalación dar clic en Siguiente.

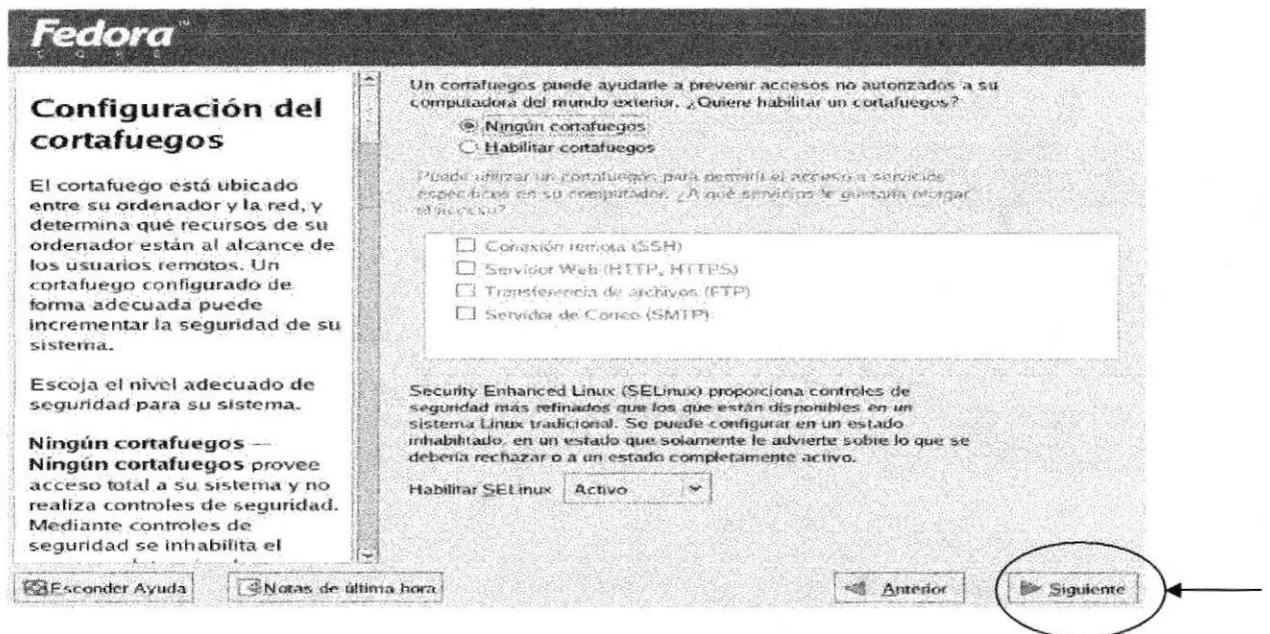


Figura 7-21: Configuración de Firewall

En esta pantalla el asistente pregunta si se desea continuar con la instalación, para continuar con la instalación dar clic en Proceder.

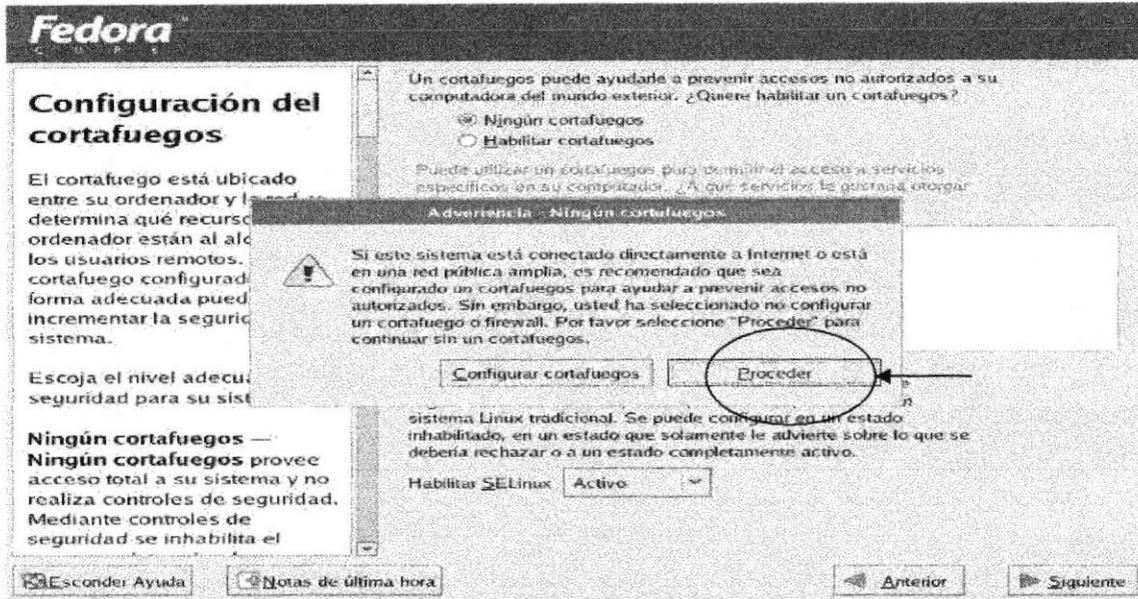


Figura 7-22: Advertencia

En esta pantalla el asistente permite escoger el idioma en el cual el sistema operativo permitirá trabajar y realizar todas las configuraciones, para continuar con la instalación dar clic en Siguiente.

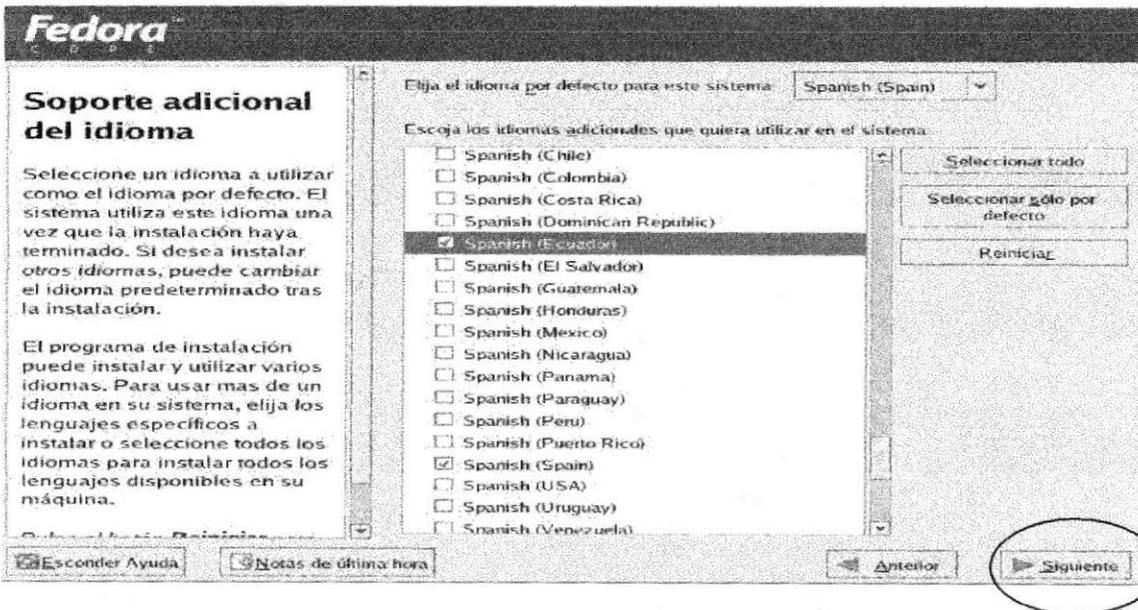


Figura 7-23: Idioma

En esta pantalla el asistente permitirá elegir la zona horaria en la que se va a trabajar, para continuar con la instalación dar clic en Siguiente.

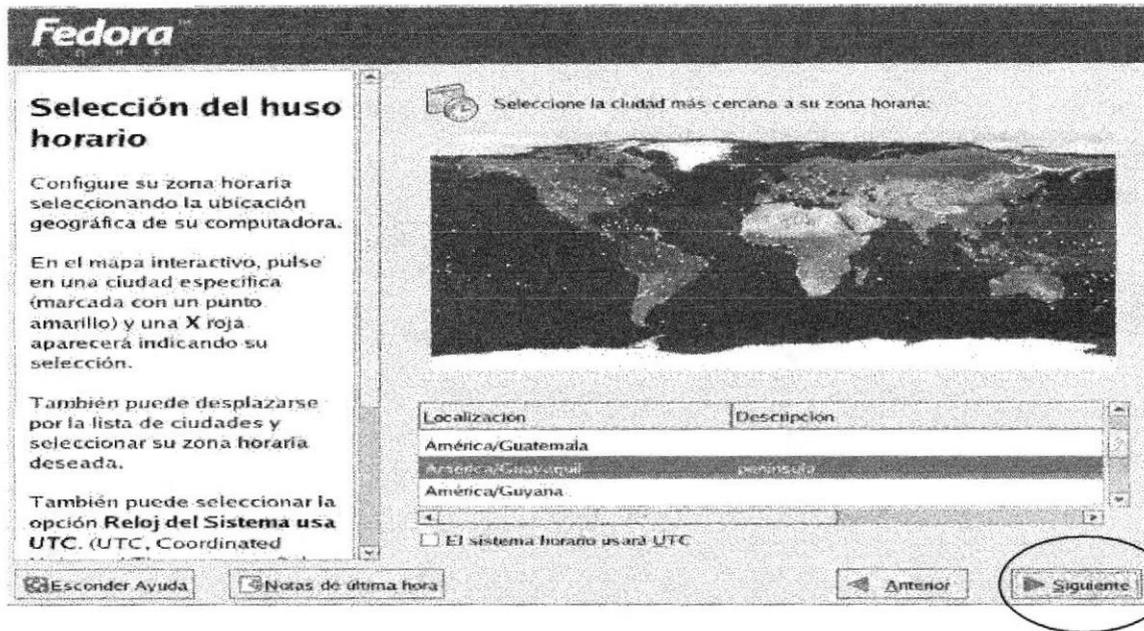


Figura 7-24: Huso Horario

En esta pantalla el asistente permitirá signar una clave al usuario privilegiado root el cual es el Administrador del sistema Operativo, para continuar con la instalación dar clic en Siguiente.

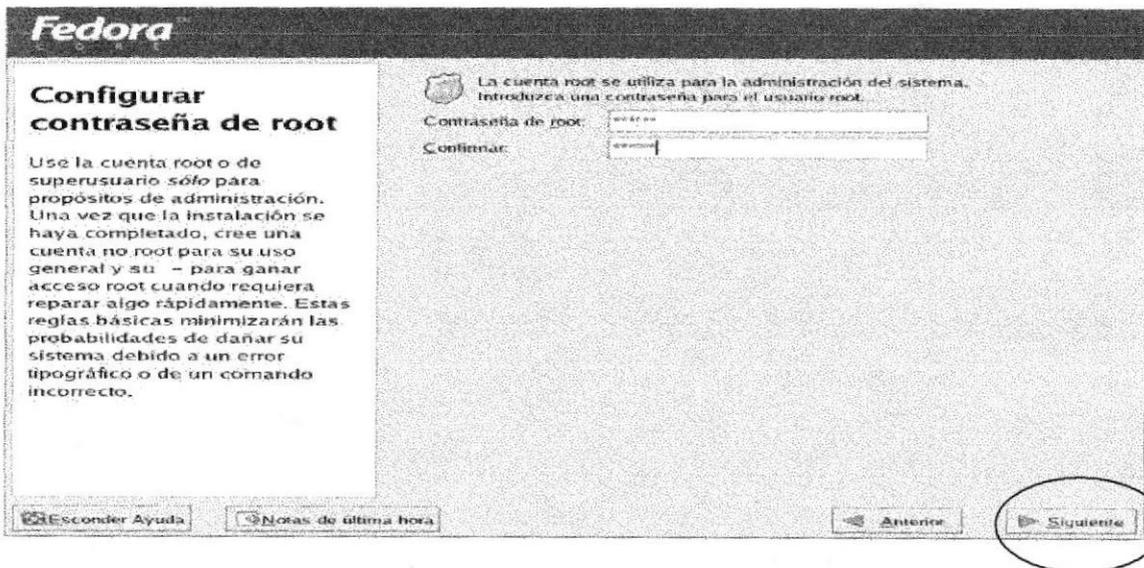


Figura 7-25: Asignación de Clave

En esta pantalla el asistente da las opciones de elegir los paquetes que se necesitará para la configuración de los servicios, para continuar con la instalación dar clic en Siguiente.

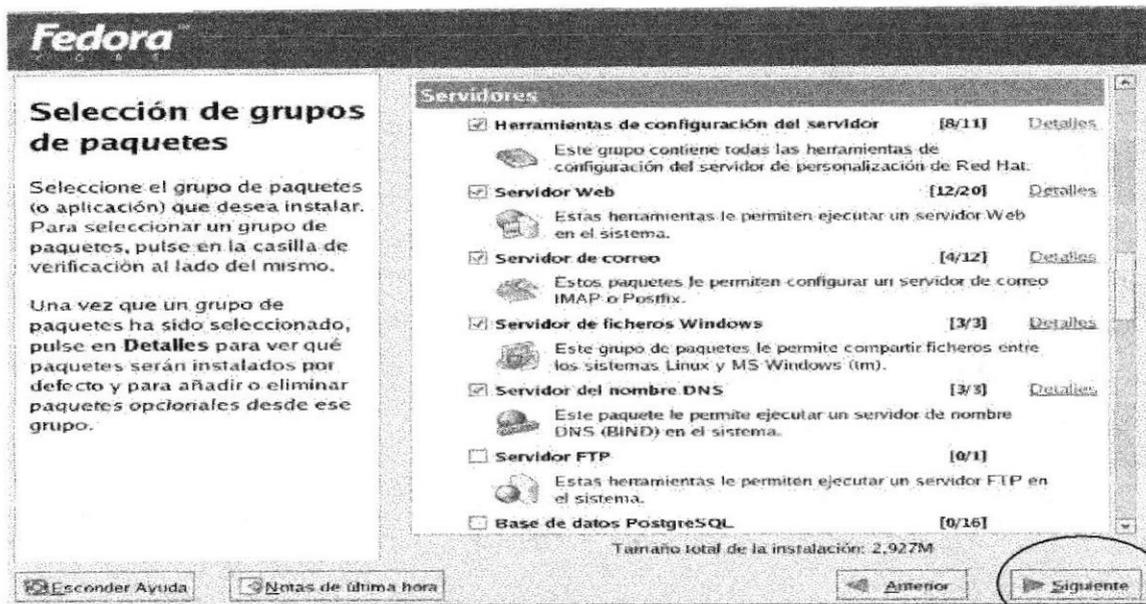


Figura 7-26: Pantalla Selección de Paquetes

Por defecto el servicio de DHCP no viene marcado en las opciones para instalarse, en esta pantalla se marca la opción de dhcp Servidor y agente DHCP, para continuar con la instalación dar clic en Aceptar.

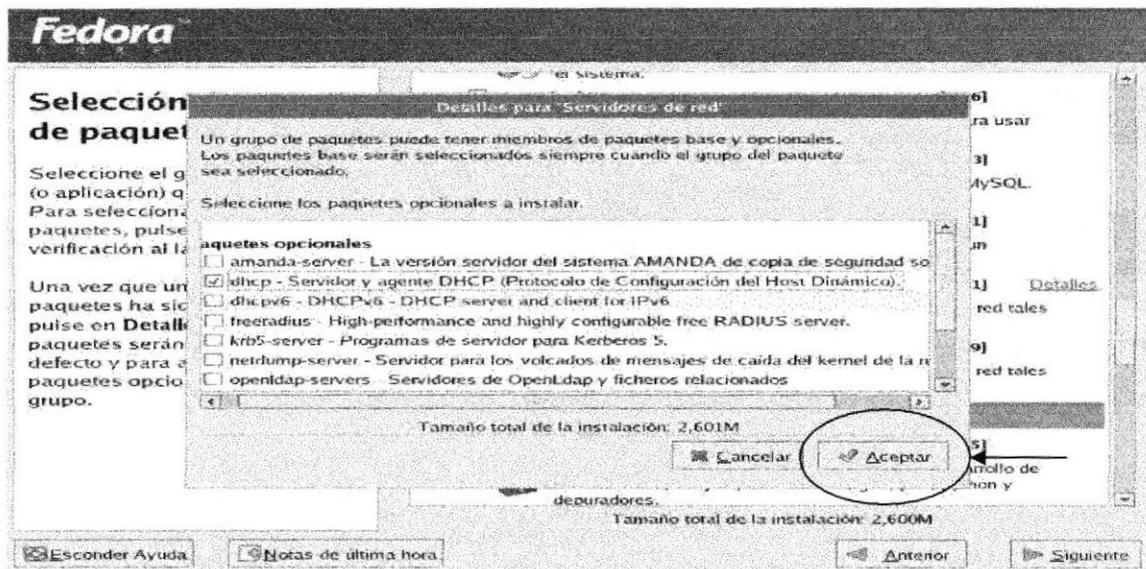


Figura 7-27: Servidores de Red

En esta pantalla el asistente pregunta si se ha realizado toda la configuración respectiva para la instalación del sistema operativo, para continuar con la instalación dar clic en Siguiente.

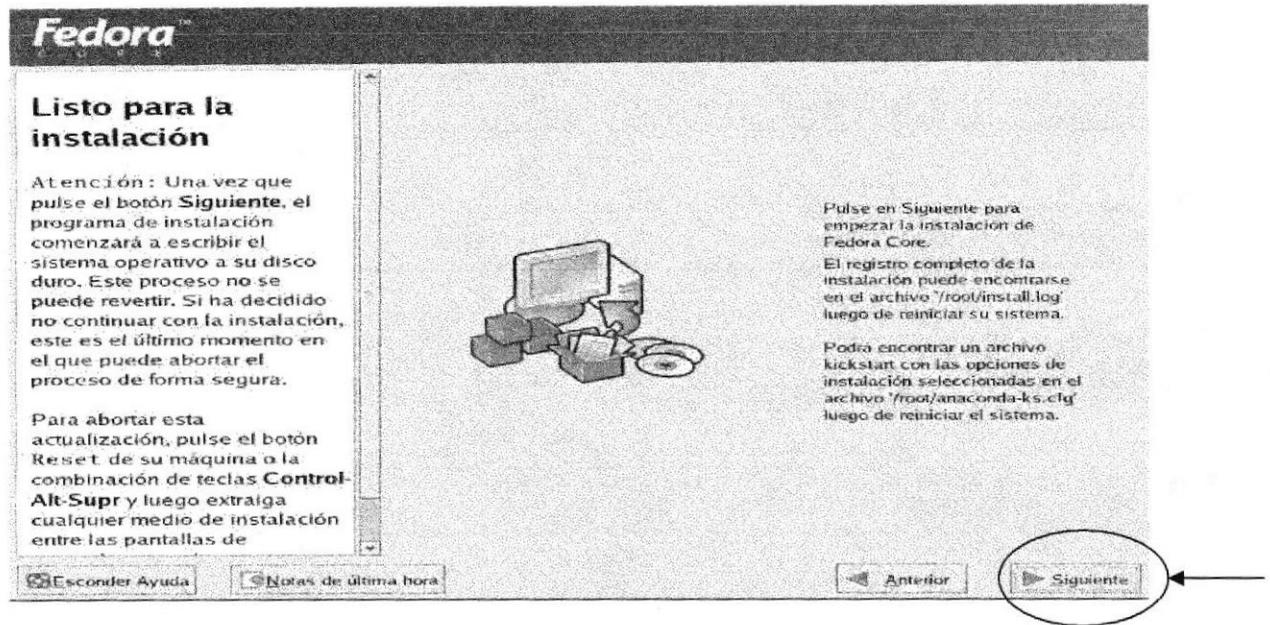


Figura 7-28: Comienzo de Instalación

En esta pantalla el asistente indica que va a necesitar los CDs #1, 2, 3 para la instalación del sistema operativo, para continuar con la instalación dar clic en Continuar.

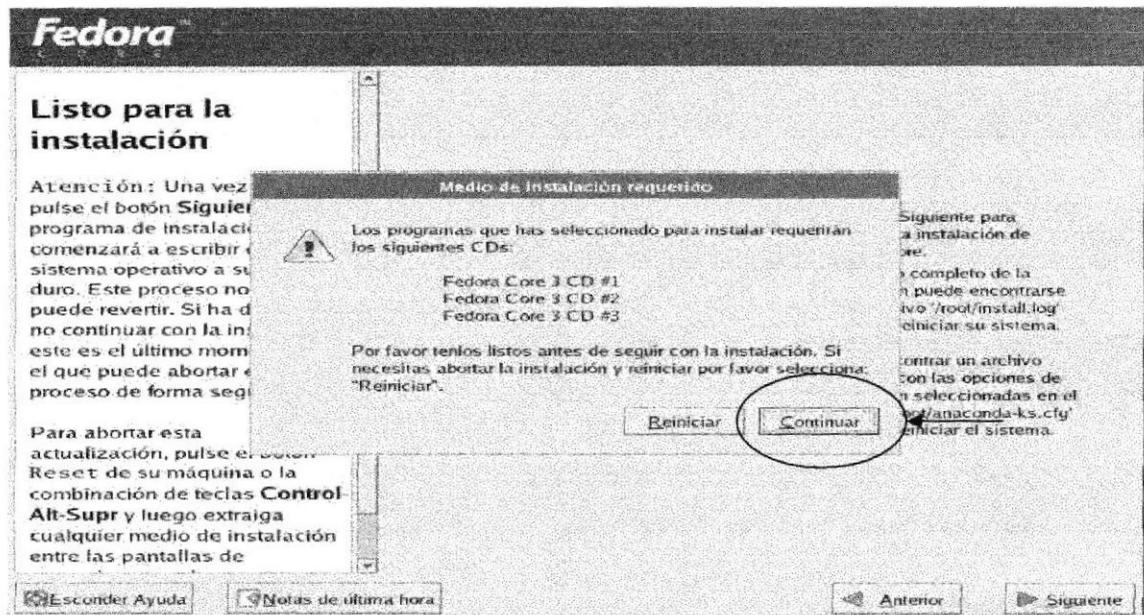


Figura 7-29: Medio de instalación requerido

En esta pantalla el asistente muestra la creación y formateo de las particiones.

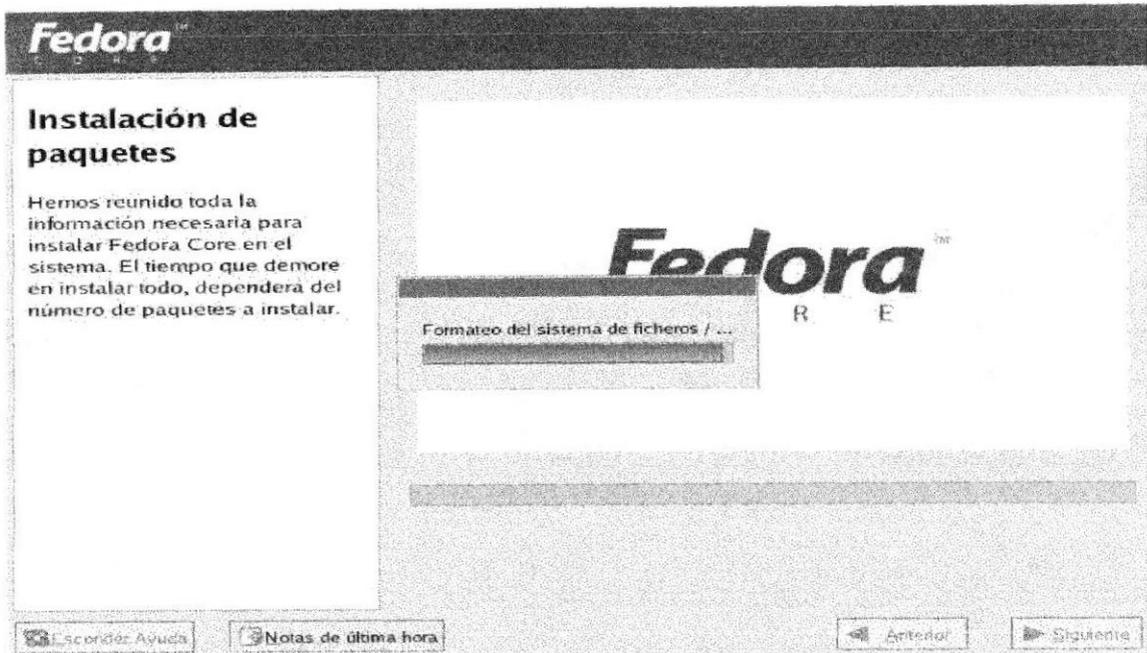


Figura 7-30: Creación y formateo de unidades

Esta pantalla indica que ya ha comenzado la instalación del sistema operativo.

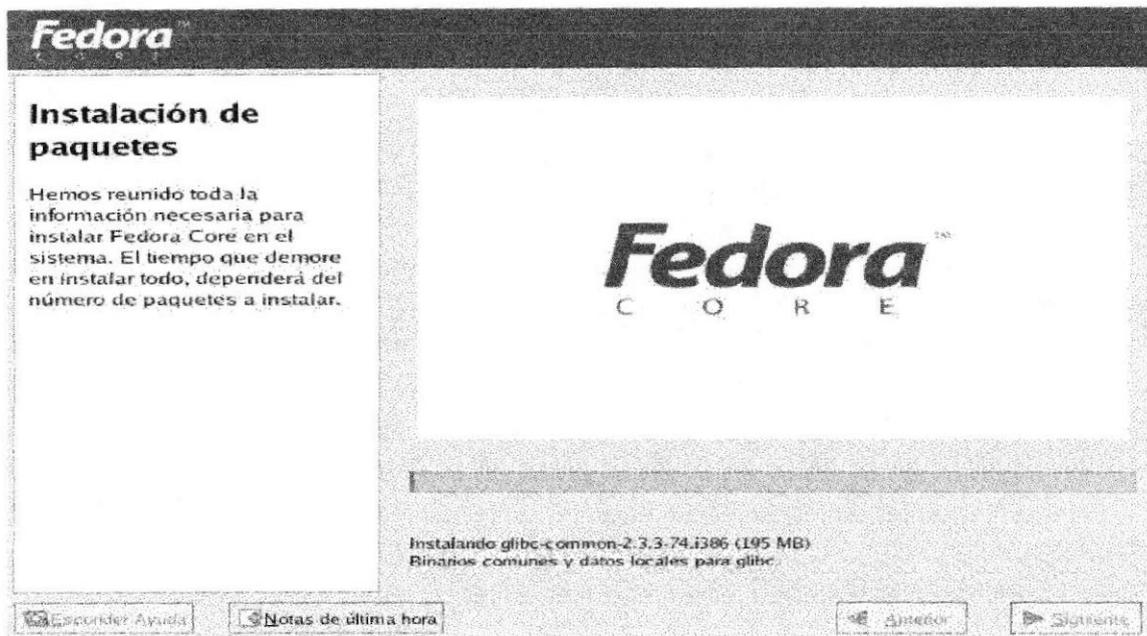


Figura 7-31: Instalación Sistema Operativo



Esta pantalla el asistente indica que la instalación de los paquetes esta finalizando, y comienza la post-configuración del sistema.

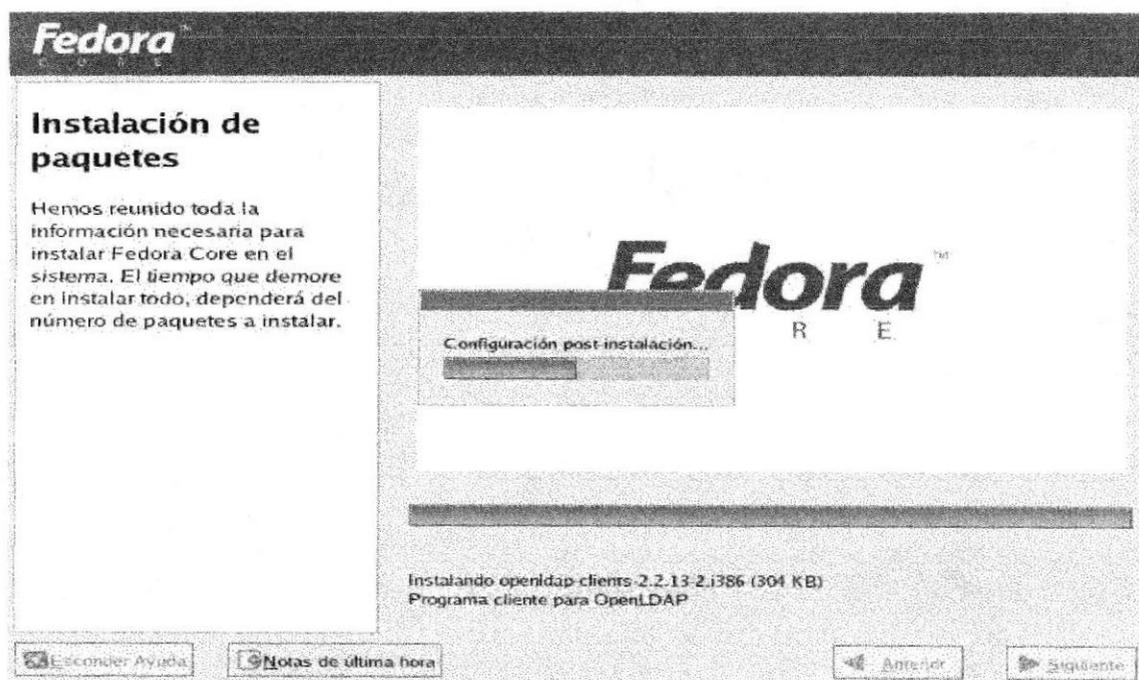


Figura 7-32: Finalización de instalación de paquetes

En esta pantalla muestra que la instalación fue terminada con éxito, y el sistema comienza a cargar.



Figura 7-33: Instalación terminada con éxito



Esta pantalla muestra el gestor de arranque.

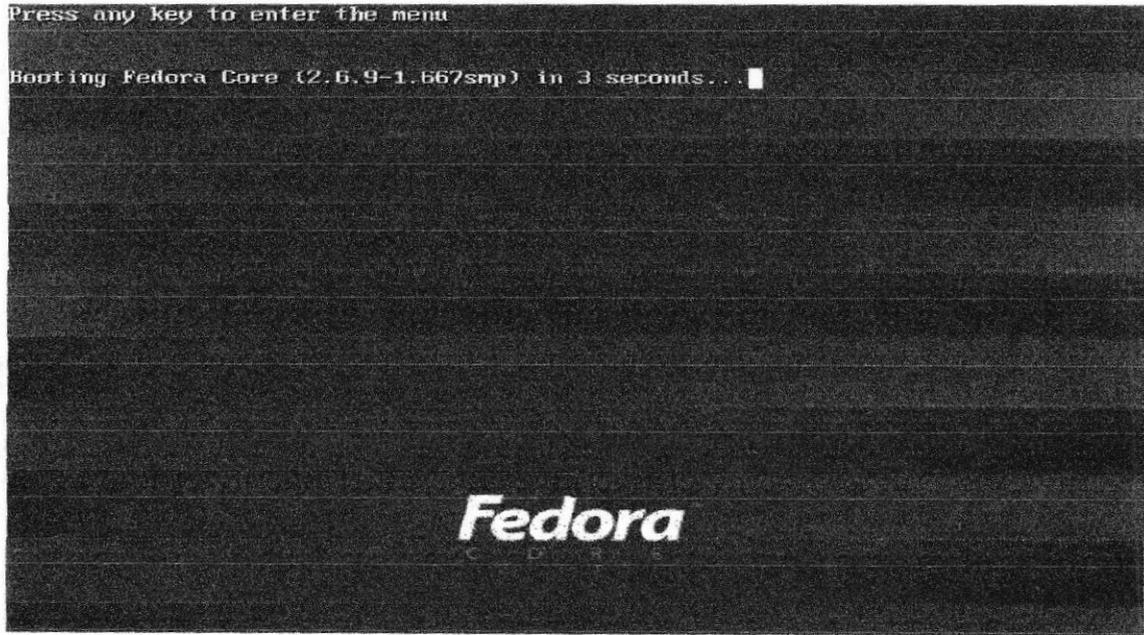


Figura 7-34: Gestor de Arranque



7.5 POST-CONFIGURACIÓN DE LINUX FEDORA CORE 3

En esta pantalla el asistente da la bienvenida a la post-configuración del sistema, para continuar con la instalación dar clic en Siguiente.

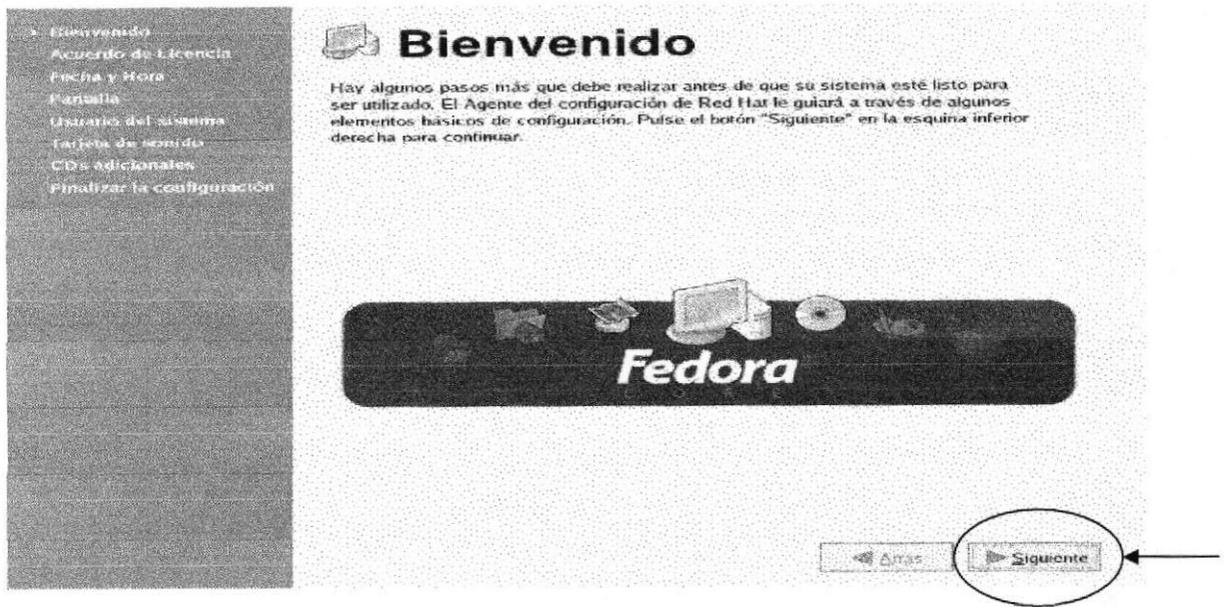


Figura 7-35: Bienvenida

En esta pantalla el asistente pregunta si aceptará el acuerdo de la licencia, seleccionar si, acepto el acuerdo, para continuar con la instalación dar clic en Siguiente.

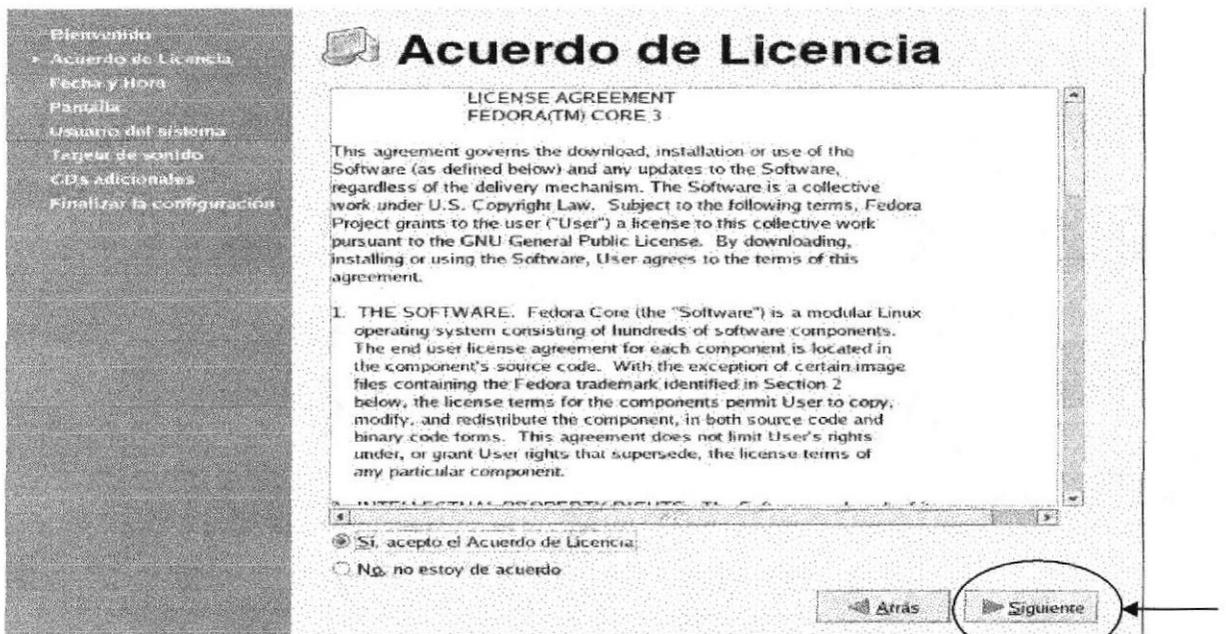


Figura 7-36: Acuerdo de Licencia

En esta pantalla el asistente dará la opción de poner la hora y fecha actual, para continuar con la instalación dar clic en Siguiente.

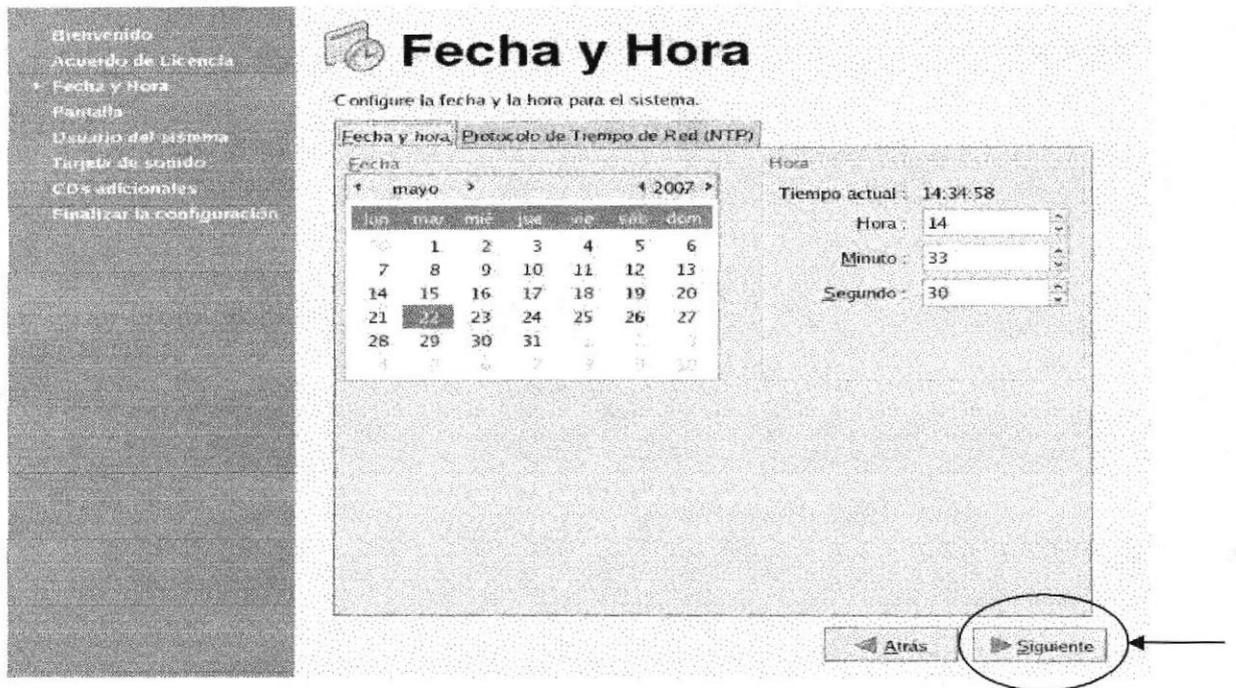


Figura 7-37: Configuración fecha y hora

En esta pantalla el asistente permitirá configurar la resolución de la pantalla, para continuar con la instalación dar clic en Siguiente.

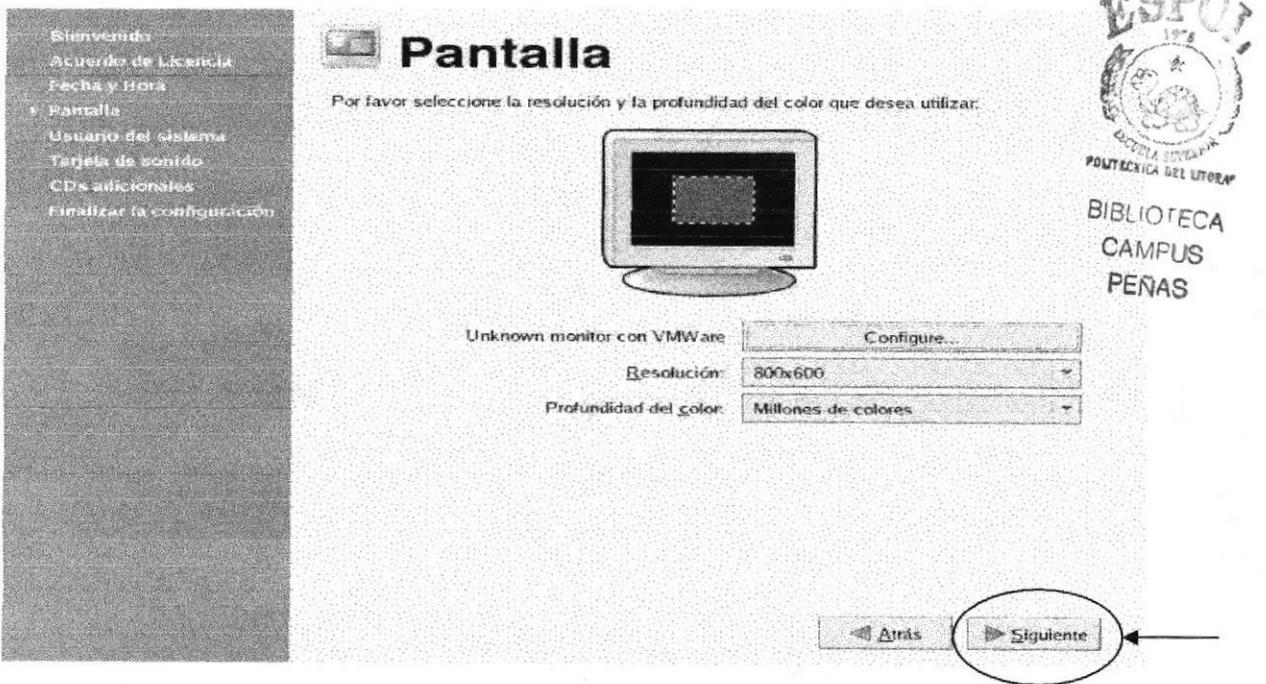


Figura 7-38: Resolución de Pantalla

En esta pantalla el asistente indica la creación de un usuario del sistema con su respectiva contraseña, para continuar con la instalación dar clic en Siguiente.

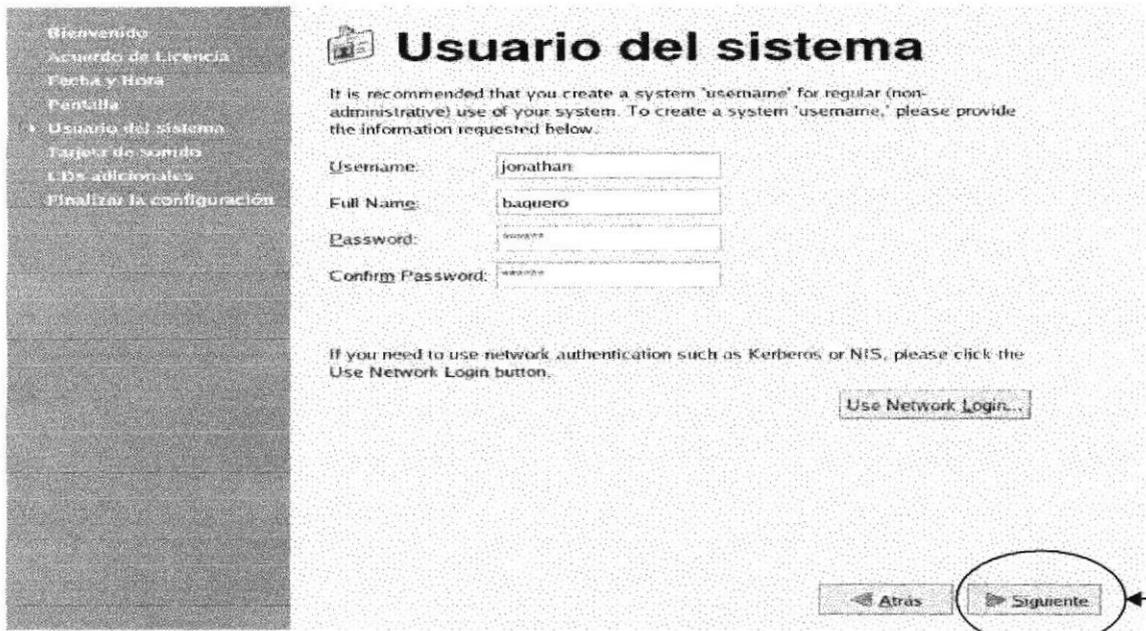


Figura 7-39: Creación Usuario del Sistema

En esta pantalla el asistente dará la opción de configurar la tarjeta de sonido, para continuar con la instalación dar clic en Siguiente.

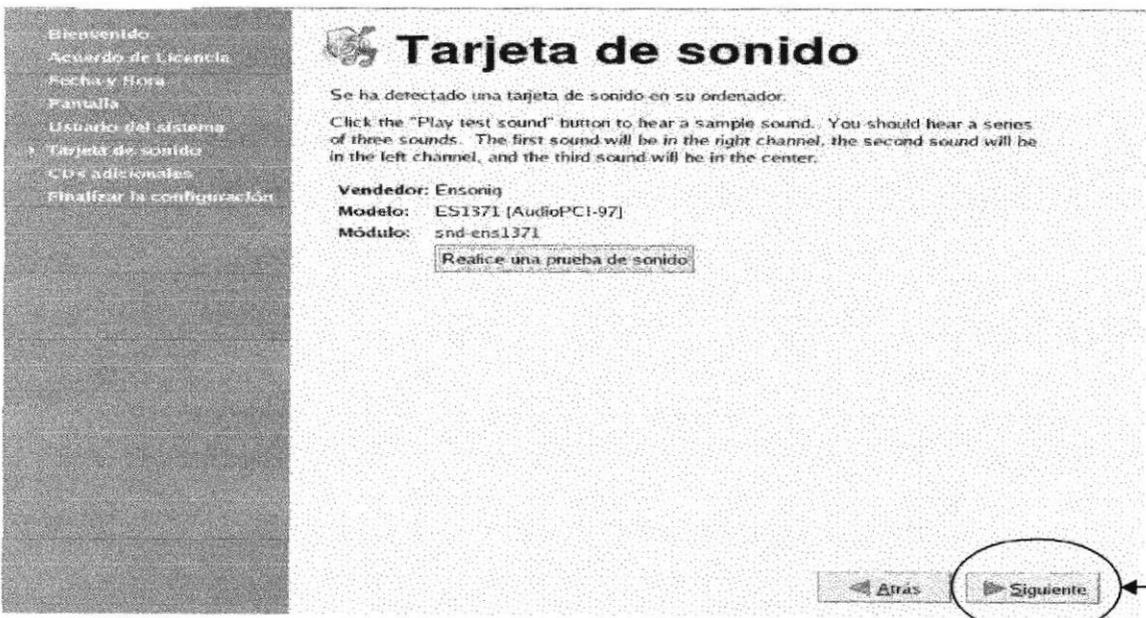


Figura 7-40: Configuración tarjeta de Sonido

En esta pantalla el asistente preguntará si se desea agregar algún paquete que se haya olvidado en la instalación anterior, para continuar con la instalación dar clic en Siguiente.

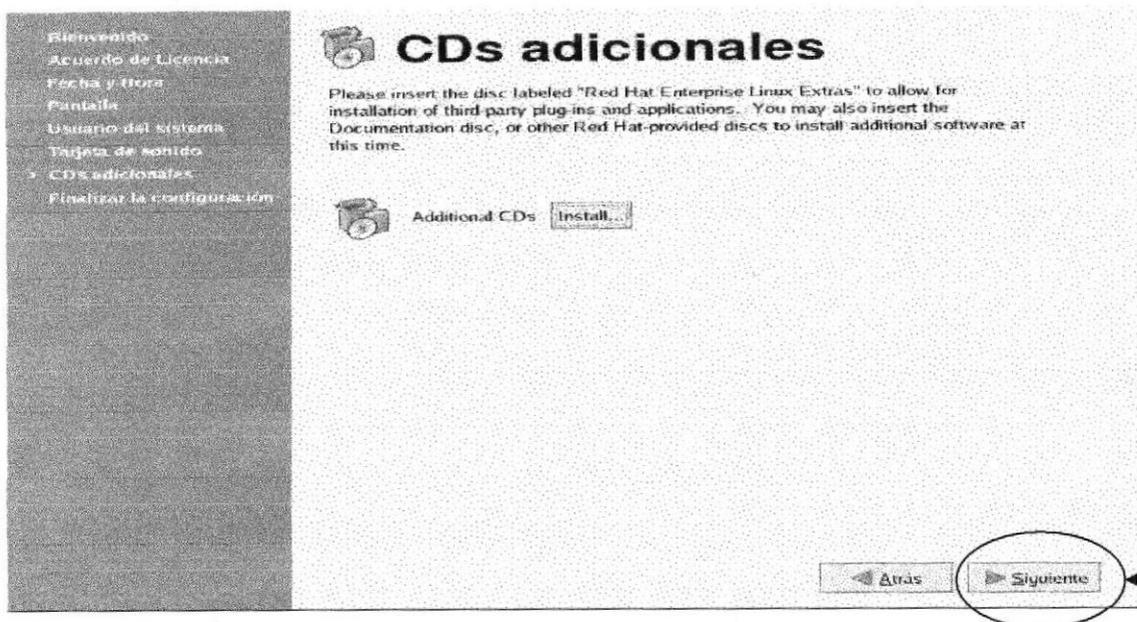


Figura 7-41: Agregar paquetes adicionales

En esta pantalla el asistente muestra la finalización de la post-configuración del sistema, para continuar con la instalación dar clic en Siguiente.



Figura 7-42: Finalización de la configuración

INICIALIZACIÓN DEL SISTEMA FEDORA EN MODO GRÁFICO

En esta pantalla el sistema preguntará con qué usuario se desea ingresar en este caso se ingresa con el usuario privilegiado root.

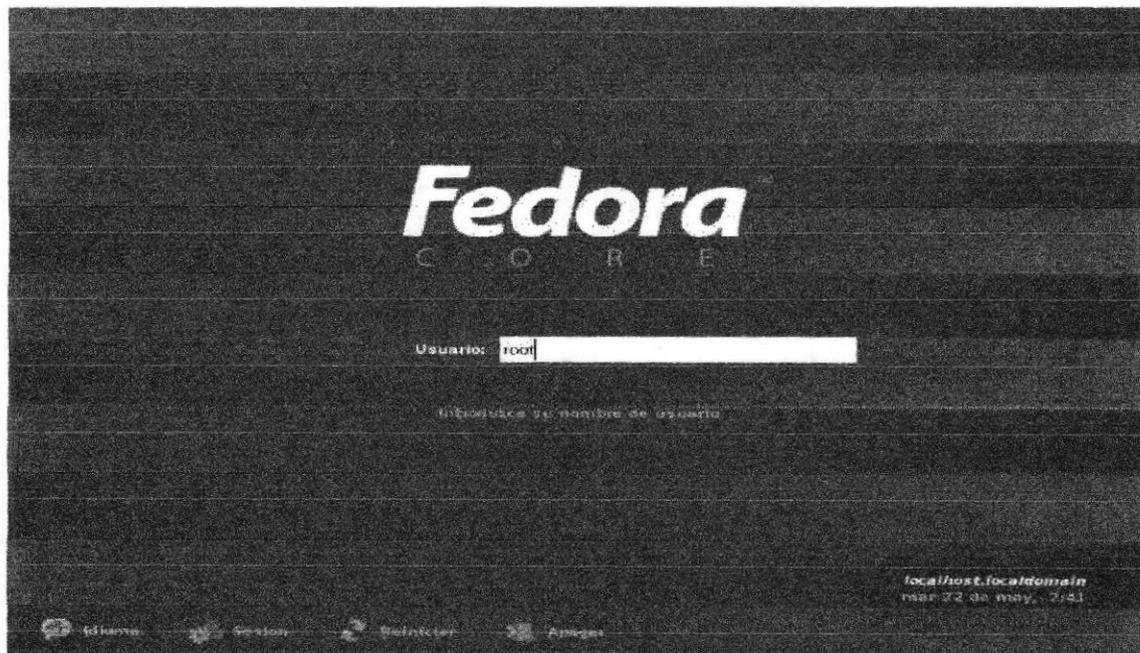


Figura 7-42: Introducir nombre de usuario

En esta pantalla el sistema preguntará con que contraseña desea ingresar en este caso ingresar con la contraseña dada anteriormente al usuario privilegiado.

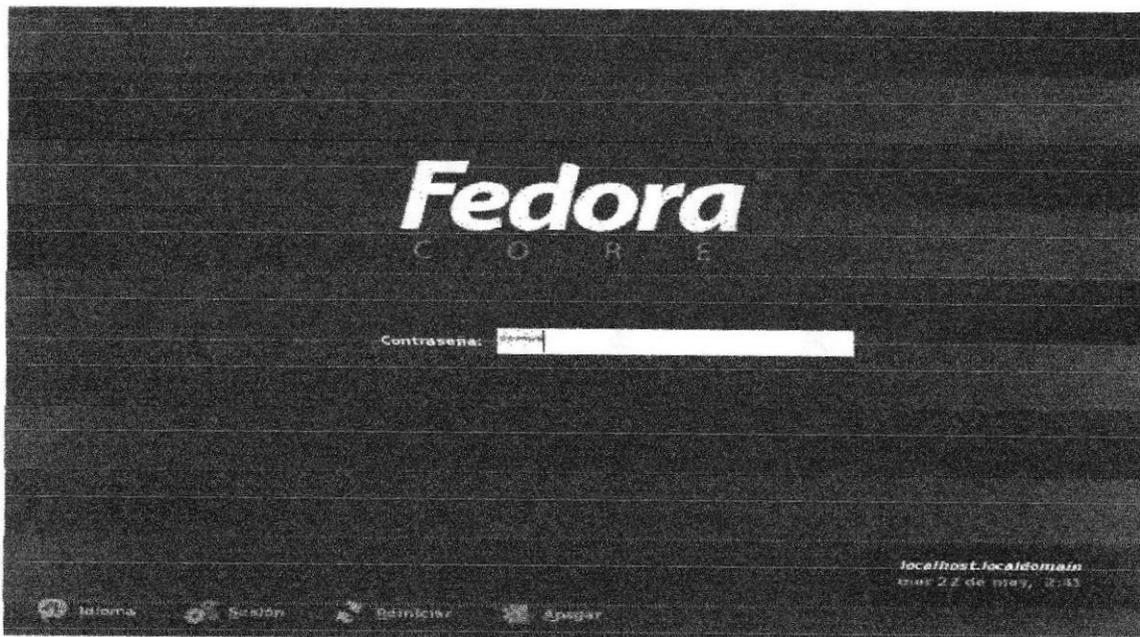


Figura 7-43: Introducir contraseña de usuario



Esta pantalla muestra que el sistema operativo Linux ya está iniciado y listo para trabajar.

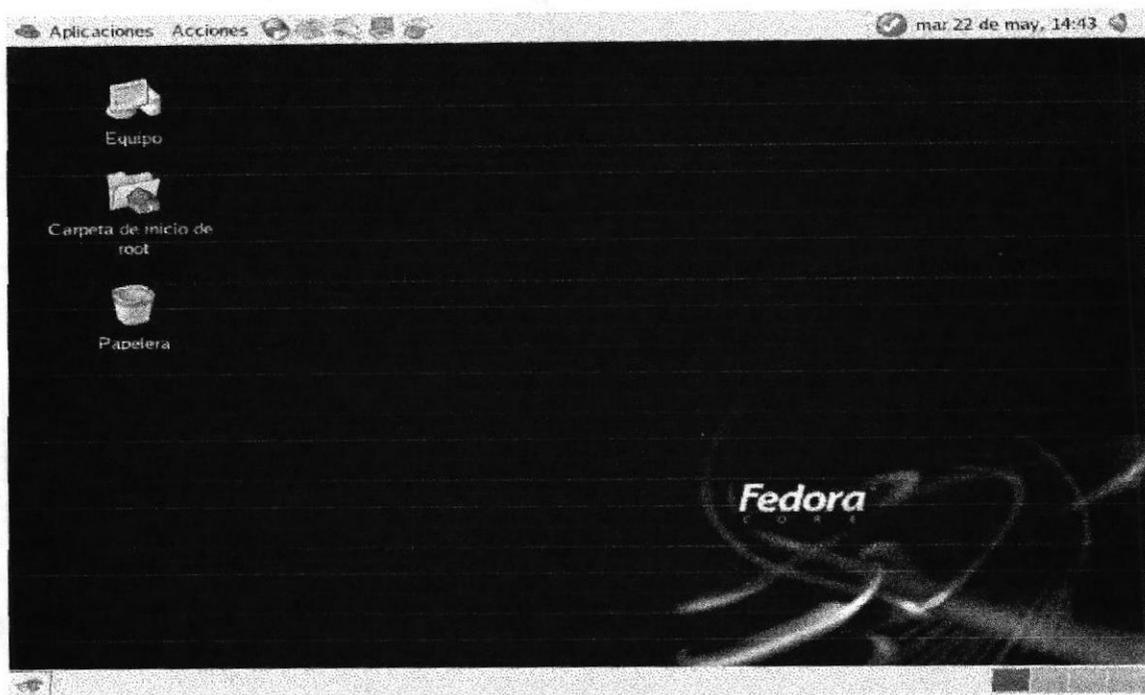


Figura 7-44: Sistema Operativo listo

Para abrir un Terminal se hace los siguientes pasos:

- 1.- Ubicarse en Aplicaciones.
- 2.- Herramientas del Sistema.
- 3.- Terminal.
- 4.- Empezar a configurar todos los Servicios en Linux.

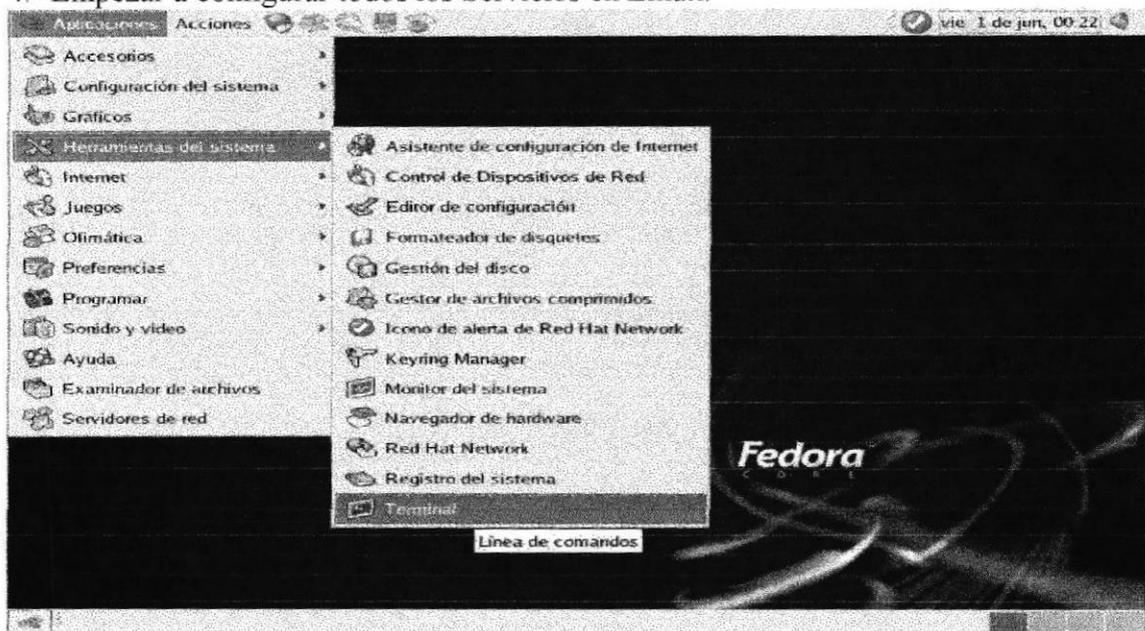


Figura 7-45: Abrir terminal



INICIALIZACION DEL SISTEMA FEDORA EN MODO TEXTO

Para poder inicializar el sistema Operativo en modo texto, debe digitar la combinación de teclas ctrl + alt + F1 al F6.

Después de haber digitado la combinación de teclas para ingresar al Sistema Operativo en modo texto aparecerá una pantalla parecida a esta, en la cual pide el usuario.

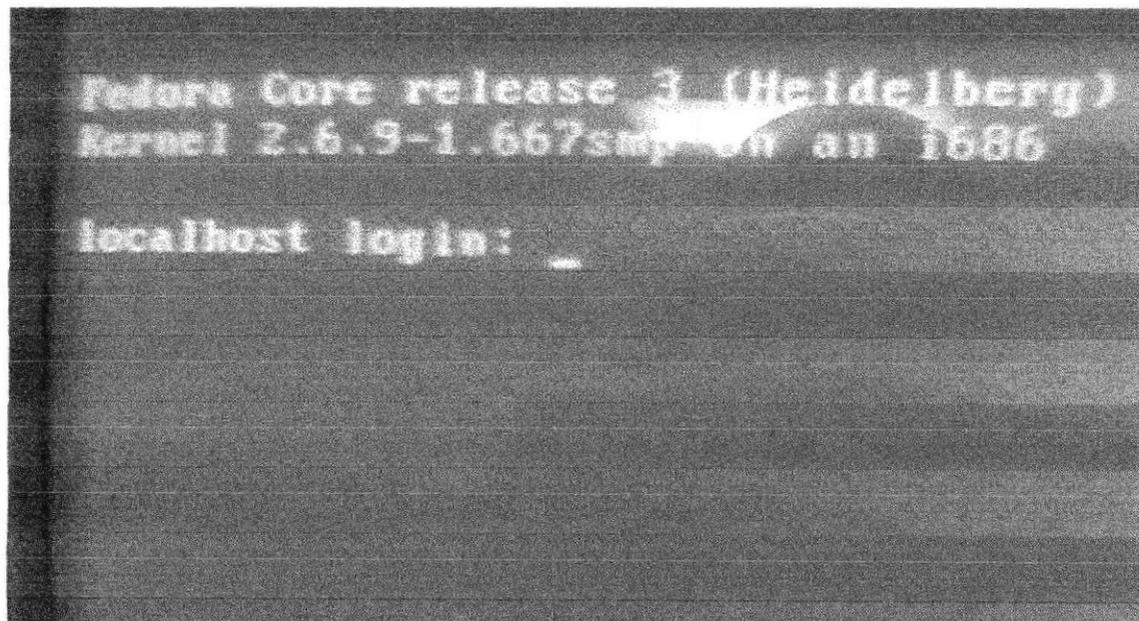


Figura 7-46: Modo texto

Luego ingresar el usuario root el cual es usuario privilegiado root.

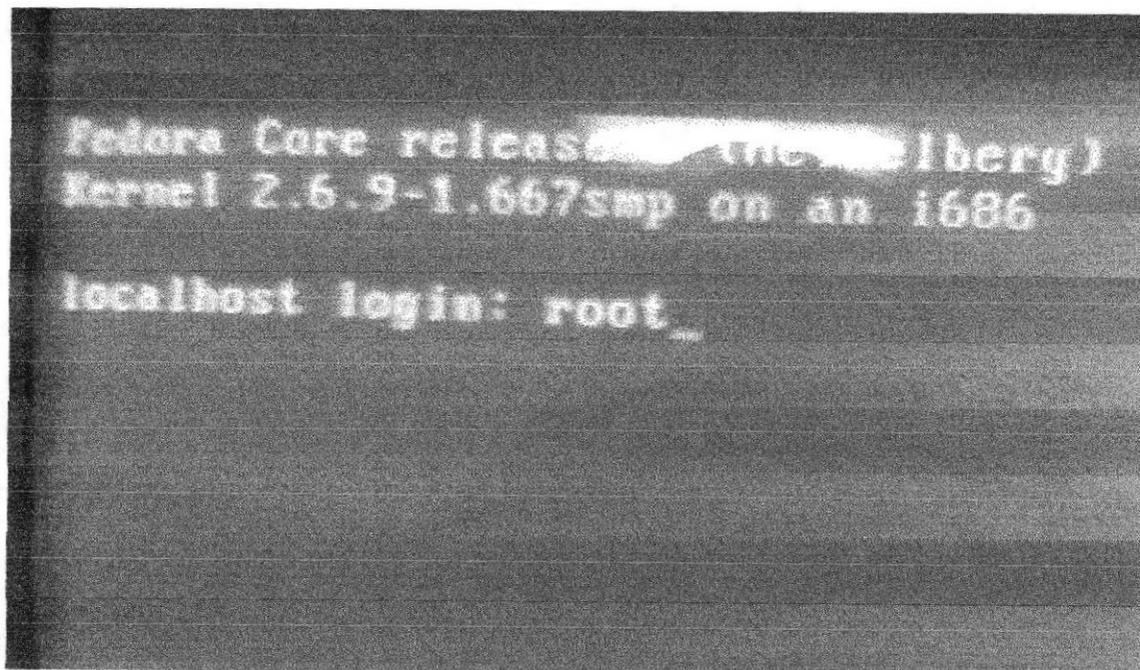


Figura 7-47: Ingresar al root

Luego pedirá una contraseña la cual ya se la ha asignado al usuario usuario privilegiado.

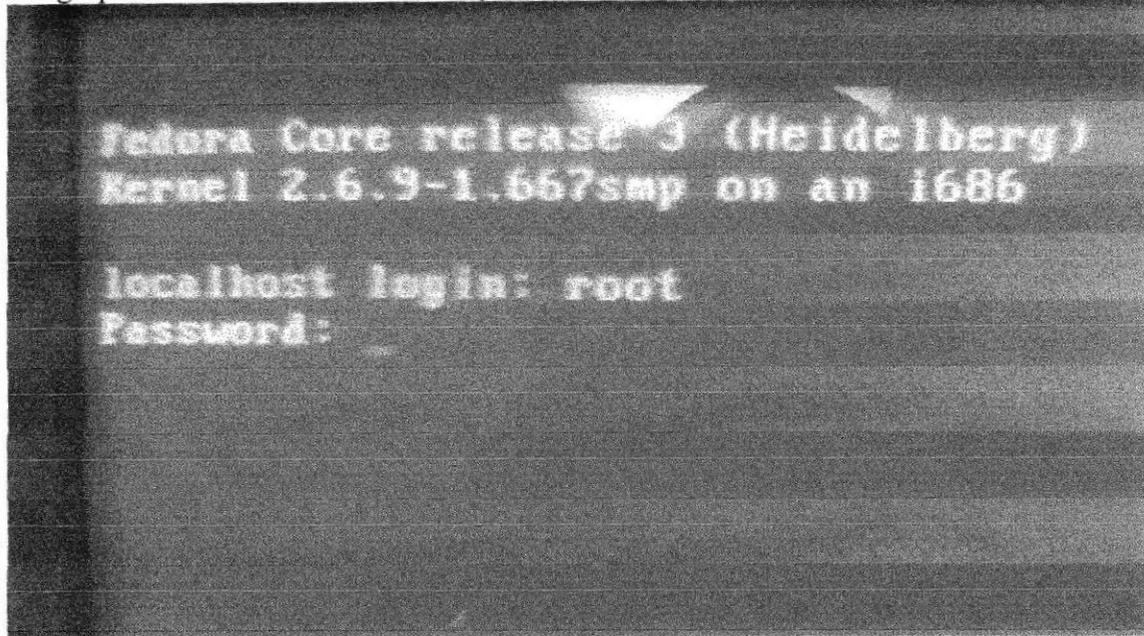


Figura 7-48: Ingresar password

Después de haber ingresado aparecerá una pantalla parecida a esta, en la cual se puede visualizar que ha ingresado al Sistema Operativo.

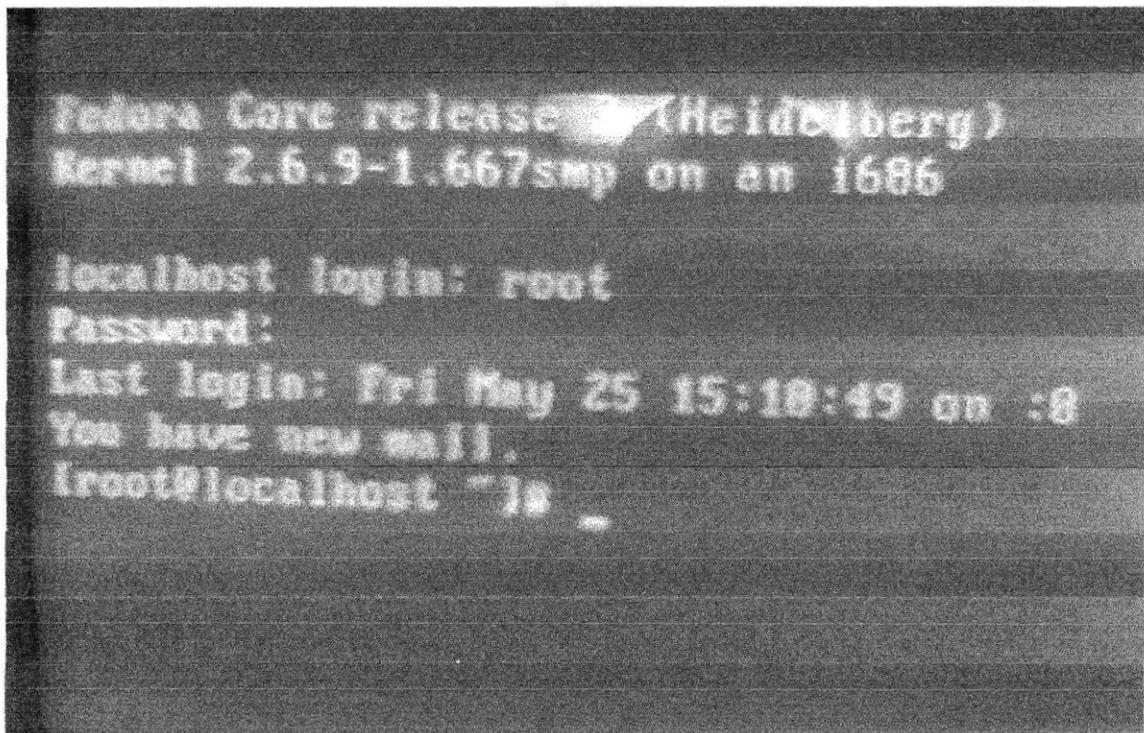


Figura 7-49: Visualización del Sistema Operativo

7.6 COMANDOS BASICOS DE LINUX FEDORA CORE 3

COMANDO	SINTAXIS	DESCRIPCIÓN
adduser	adduser jonathan	crea usuario
cd	cd /etc	entrar a un directorio
clear	clear	limpiar pantalla
cp	cp localhost.zone tia.com	copia de un archivo con otro nombre
ifconfig	ifconfig	verifica si esta habilitada la ip del servidor
ls	ls	muestra información sobre los archivos
mkdir	mkdir jonathan	crea directorios
chown	chown root:root jonathan	para dar los permisos de usuario
passwd	passwd jonathan	crea una contraseña
ping	ping 192.168.7.1	mensaje de prueba para verificar el estado de la tarjeta de red
telnet	telnet 192.168.7.1	Permite conectarse de forma remota a cualquier pc especificando la dirección IP
touch	touch deber.txt	crea archivos



BIBLIOTECA
CAMPUS
PEÑAS

vi	vi deber.txt	edita el contenido de un archivo
wq	:wq	sale y guarda cambios desde el editor
x	:x	sale y guarda cambios desde el editor
q!	q!	Este comando sale de un fichero sin guardar cambios realizados
i	i	Este comando inserta, indica al fichero que se comenzará a escribir en el.
p	p	esta tecla pega líneas copiadas con anterioridad
yy + numero	yy jonathan o yy 5	copia un número de líneas, especificado con anterioridad
chmod	chmod +777 /jonathan chmod +777 /jonathan/deber.txt	Este comando da permisos de lectura, escritura a cualquier archivo especificado
service <servicio> start	service squid start	Sirve para levantar un servicio.
rpm -q	rpm -q samba	Sirve para verificar si están instalados los paquetes.
slocate	slocate /etc/jonathan.txt	Sirve para buscar archivo, directorios.
rmdir	rmdir jonathan	Sirve para borrar directorios



date	date	Sirve para ver y poder configurar la fecha actual.
gunzip	gunzip jonathan.txt	Sirve para descomprimir archivos compatibles con zip.
mail	Mail	Sirve para enviar y leer correo electrónico.
userdel	userdel jonathan	Sirve para borrar los usuarios de sistema creados.
mount	mount media/cdrom	Sirve para poder montar o tener acceso a unidades como cdrom, diskettes, disco duros.
umount	umount media/cdrom	Sirve para desmontar las unidades como cdrom, diskettes, disco duro
find	find jonathan.txt	Sirve como buscador de ficheros con demasiados parámetros
lsmod	lsmod	Muestra los modulos de kernel que estan cargados.
mv	mv jonathan/baquero	Sirve para mover o renombrar ficheros/directorios.

Tabla 7-1: Comandos Básicos



7.7 CONFIGURACIONES GENERALES DE LINUX FEDORA

7.7.1 CONFIGURACIÓN DE LA TARJETA DE RED MODO TEXTO

Para trabajar en el ambiente texto de Linux debe abrir un Terminal, dar clic derecho sobre el escritorio y seleccionar abrir un nuevo Terminal.

Una de las formas de configurar la tarjeta de red es la siguiente:

Digitar la siguiente línea especificando la dirección IP que dará al Servidor. Ifconfig eth0 192.168.7.1 up

ifconfig: Es un comando que sirve para dar direcciones a la tarjeta de red.

eth0: es como reconoce Linux a la tarjeta de red.

192.168.7.1: Dirección IP la cual será asignada al servidor.

up: sirve para levantar el servicio.

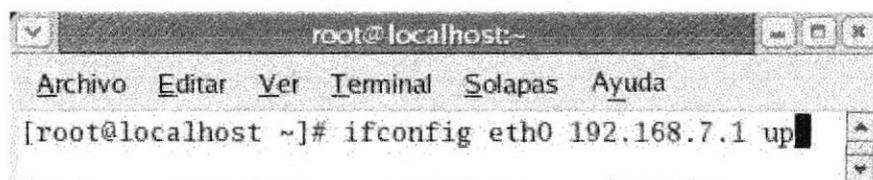


Figura 7-50: Configuración tarjeta de red modo texto

Luego de haber dado la dirección IP, realizar la debida verificación si la tarjeta de red está levantada con el comando ifconfig

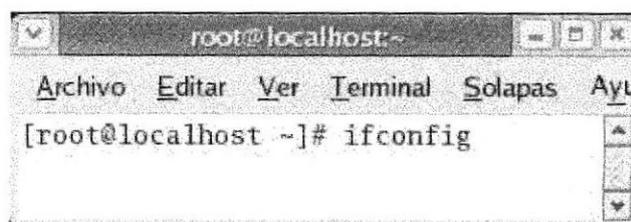


Figura 7-51: Ruta para verificar la tarjeta



BIBLIOTECA
CAMPUS
PEÑAS

En esta ventana nos muestra que se a levantado la tarjeta de red y la mascara se levanta por defecto.

```
root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:92:29:CD
          inet addr:192.168.7.1  Bcast:192.168.7.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe92:29cd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2885 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:445418 (434.9 KiB)  TX bytes:2484 (2.4 KiB)
          Interrupt:185 Base address:0x1080

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:10752 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10752 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14151548 (13.4 MiB)  TX bytes:14151548 (13.4 MiB)

[root@localhost ~]#
```

Figura 7-52: Verificación de la tarjeta levantada



7.7.2 MODO GRÁFICO

Otra manera de levantar la tarjeta de red, es digitar el comando setup

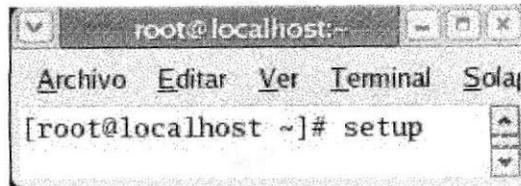


Figura 7-53: Ingresar al Setup

En esta pantalla muestra una ventana en la cual se podrá configurar las diversas herramientas, tales como: configuración de la tarjeta de red

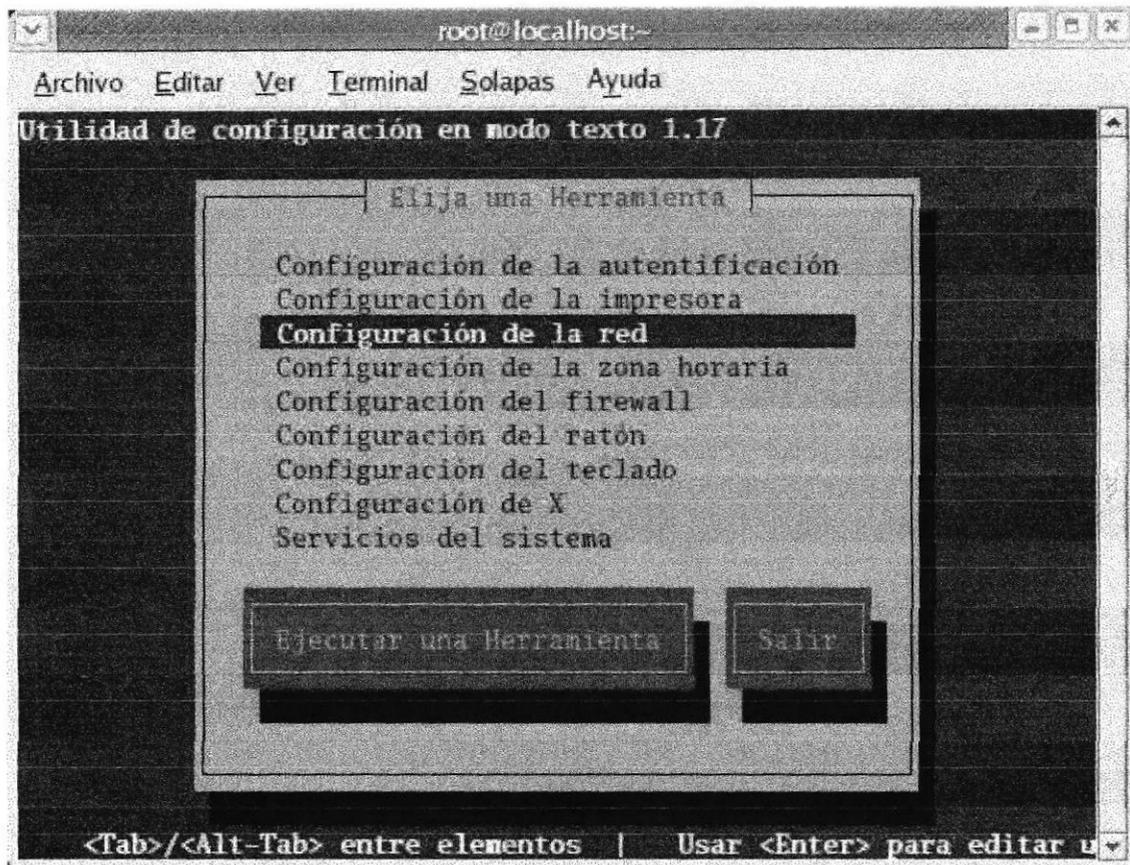
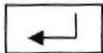


Figura 7-54: Setup



En esta pantalla el asistente pregunta si desea configurar la tarjeta de red, dar clic en Si.

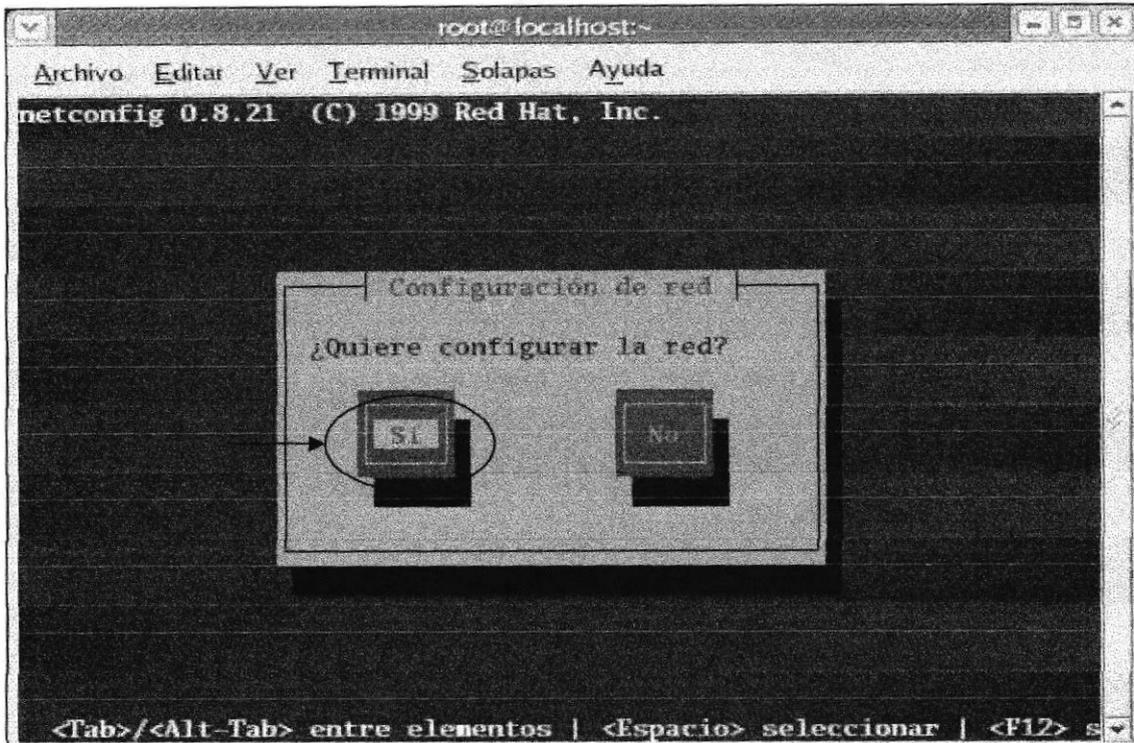


Figura 7-55: Consulta de configuración de la tarjeta

En esta pantalla se podrá asignar una dirección IP que desea dar al servidor con su respectiva máscara de red.

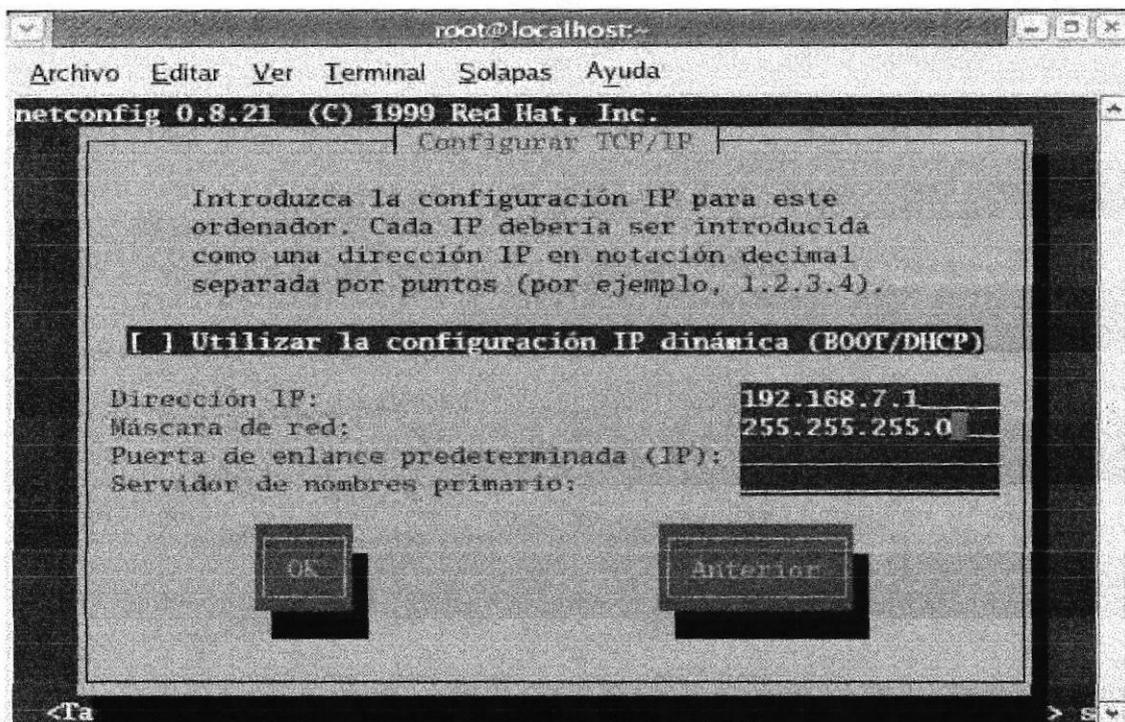


Figura 7-56: Asignación de IP

Luego de haber asignado la dirección IP al Servidor, ubicarse en la opción OK para continuar con la configuración de la tarjeta de red.

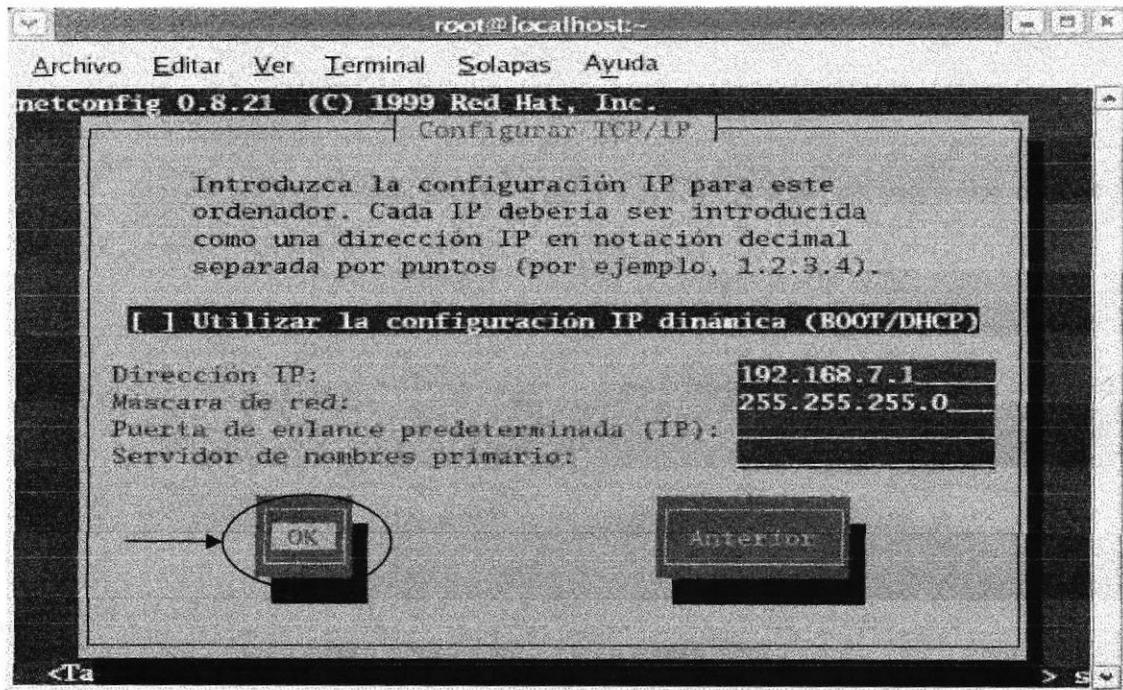


Figura 7-57: Opción OK

Después de haber aceptado los cambios se ha hecho a la tarjeta de red, seleccionar la opción salir para finalizar la configuración de la tarjeta de red.

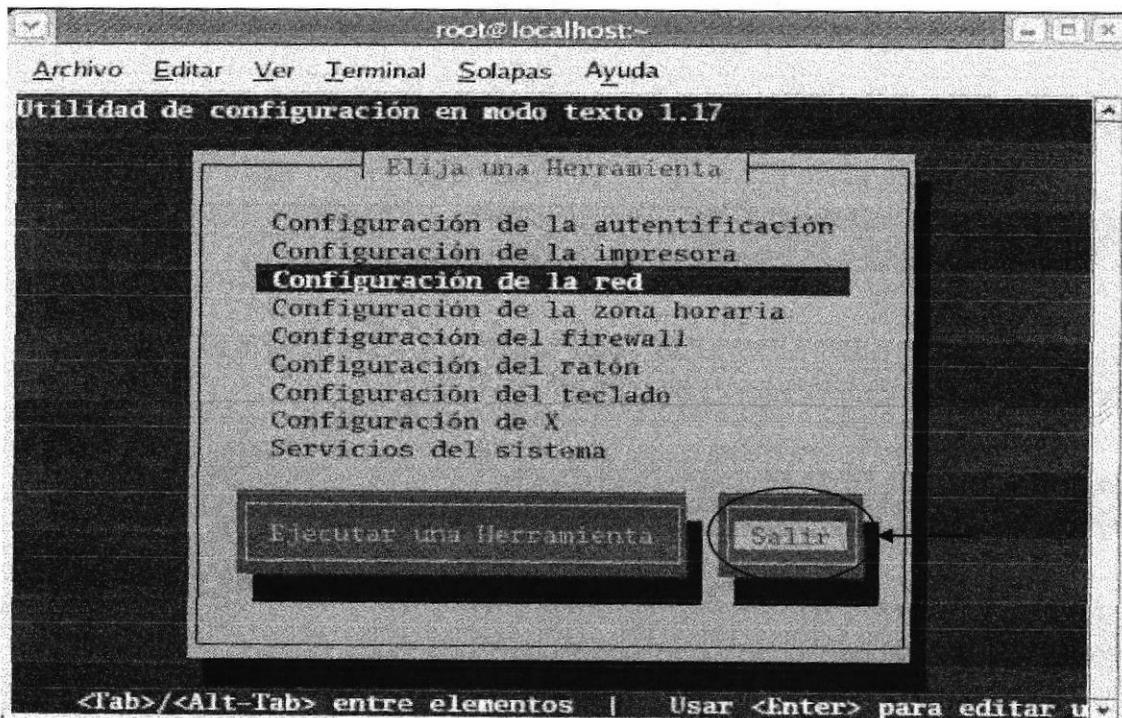


Figura 7-58: Configuración con opción Salir

Para que la tarjeta de red acepte los cambios deberá digitar el comando:
service network restart

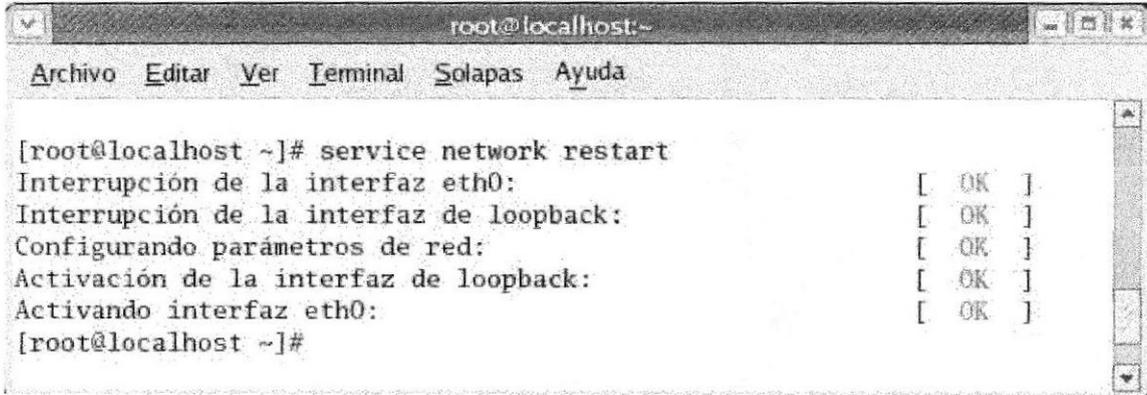


Figura 7-59: Comando network



BIBLIOTECA
CAMPUS
PEÑAS

7.8 CONFIGURACIONES DE LOS SERVIDORES EN LINUX

7.8.1 CONFIGURACIÓN DEL SERVIDOR SAMBA

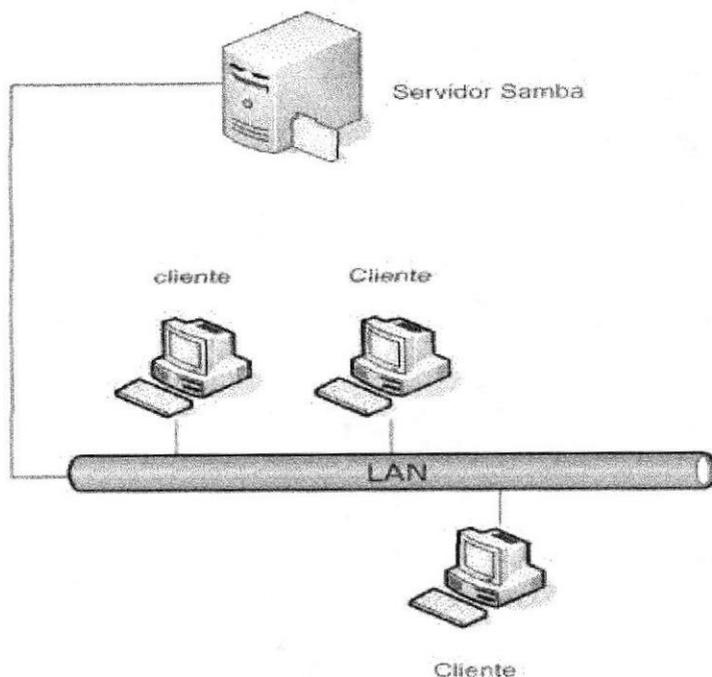


Figura 7-60: Esquema Samba

Samba son un conjunto de aplicaciones libres para Linux que implementan el protocolo de comunicación SMB utilizado por los sistemas operativos Microsoft Windows para compartir carpetas e impresoras.

Básicamente **samba** permite a PCs que utilizan Linux conectarse a carpetas compartidas en PCs con Windows y compartir carpetas como si de un Windows se tratara. Gracias a **samba**, en una red se puede tener PCs con Windows y PCs con Linux de forma que puedan intercambiar información en carpetas compartidas de la misma forma que se haría si todos los PCs fueran Windows.

Cuando en una misma red conviven sistemas Unix con equipos Windows, se utiliza **samba** para integrarlos y poder intercambiar información. Como alternativa, sería posible utilizar protocolos estándar como el ftp que es utilizado tanto equipos Windows como equipos Linux. “

Las funcionalidades de **samba** no se quedan solo en una simple compartición de archivos e impresoras sino que permite a un PC con Linux comportarse como un controlador de dominio de Windows para redes Microsoft con prestaciones superiores a las que nos ofrecería un servidor con Windows NT Server 4.0. En las páginas siguientes se verá como hacer que un PC con Linux haga las veces de controlador de dominio de la red Windows.

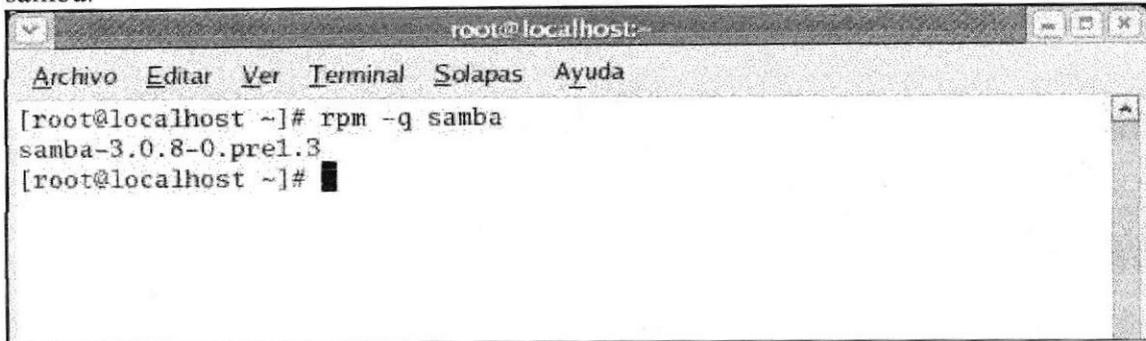
REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR SAMBA

- 1 Pc con Linux Fedora Core 3
- 1 Tarjeta de Red
- Tener una IP Estática
- Tener instalados los paquetes Samba
 - Samba-2.2.1a
 - Samba-client-2.2.1a



7.8.1.1 CONFIGURACIÓN EN LINUX

Para verificar si está instalado el paquete de samba, debe digitar el comando `rpm -q samba`.

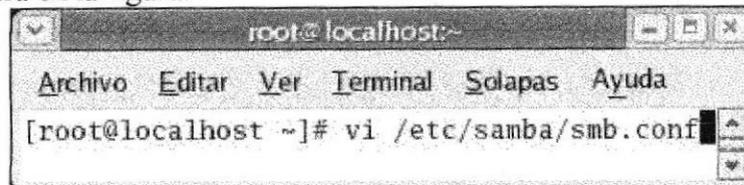


```

root@localhost:~# rpm -q samba
samba-3.0.8-0.pre1.3
root@localhost:~#
  
```

Figura 7-61: Verificación del paquete Samba

Después de haber verificado el paquete de samba, editar el archivo del `smb.conf` tal como se muestra en la figura.



```

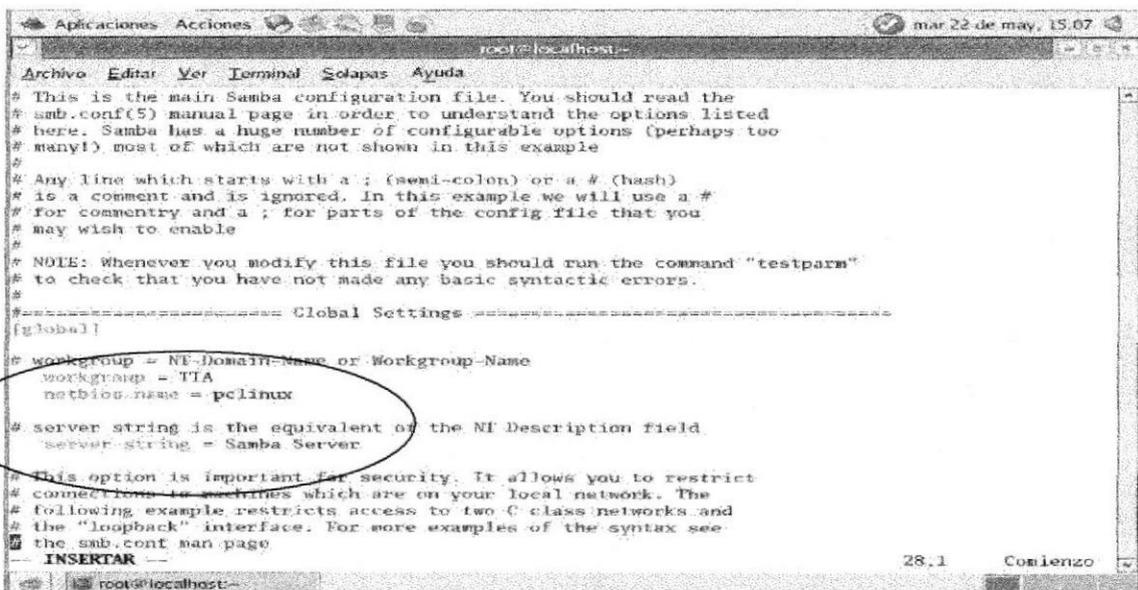
root@localhost:~# vi /etc/samba/smb.conf
  
```

Figura 7-62: Editar el archivo smb

Una vez dentro del archivo `smb.conf`, ubicarse en la sección de GLOBAL SETTING y modificar las siguientes líneas.

workgroup: Es aquel que permite elegir el tipo de grupo de trabajo a trabajar en el Servidor Samba.

netbiosname: Es aquel que permite definir el nombre de la maquina en este caso al momento de buscar la máquina lo hará mediante el nombre que agregue.



```

# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options (perhaps too
# many!) most of which are not shown in this example
#
# Any line which starts with a ; (semi-colon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentary and a ; for parts of the config file that you
# may wish to enable
#
# NOTE: Whenever you modify this file you should run the command "testparm"
# to check that you have not made any basic syntactic errors.
#----- Global Settings -----
[global]
# workgroup = NT-Domain-Name or Workgroup-Name
workgroup = TTA
netbios.name = pclinux
# server string is the equivalent of the MI Description field
server string = Samba Server
# This option is important for security. It allows you to restrict
# connections to machines which are on your local network. The
# following example restricts access to two C class networks and
# the "loopback" interface. For more examples of the syntax see
# the smb.conf man page
-- INSERTAR --
  
```

Figura 7-63: Sección global Settings

Después de haber modificado la sección del GLOBAL SETTING, ubicarse en la última parte del archivo en la sección SHARE DEFINITION y agregar las siguientes líneas tal como se muestra en la figura.

path: Es aquel que permite definir en que directorio desee compartirlo.

valid users: Es aquel que permite definir cual es el usuario que podrán acceder al servidor.

writable: Es aquel que permite que en el servidor podrán tener acceso de escritura.

comment: Permite agregar un comentario del Servidor en este caso Samba.

public: Es aquel que permite que el servidor sea público.

browseable: Es aquel que permite definir si el servidor será visible para los usuarios, después de haber editado este archivo guardar los cambios y salir con el comando :x

```

===== Share Definitions =====
idmap uid = 16777216-33554431
idmap gid = 16777216-33554431
template shell = /bin/false
winbind use default domain = no
[homes]
comment = Home Directories
browseable = no
writable = yes
[tias]
path = /tias
valid users = jonathan
writable = yes
comment = Home Directories
browseable = yes
writable = yes
public = yes
# (In comment the following and create the netlogon directory for Domain Logons
[netlogon]
comment = Network Logon Service
path = /home/netlogon
guest ok = yes
writable = no
share modes = no
:x

```

Figura 7-64: Sección Share definition

Para levantar el servicio de samba digitar el comando `service smb start`.

```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda

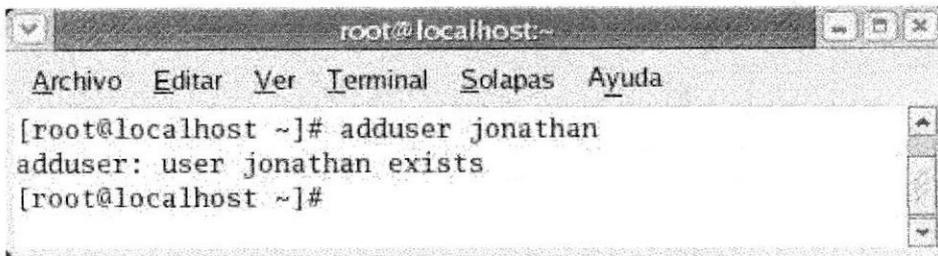
[root@localhost ~]# service smb start
Iniciando servicios SMB:
OK ]
Iniciando servicios NMB:
OK ]

```

Figura 7-65: Levantar el servicio Samba



Si todo salió bien al momento de levantar los servicios de samba, ahora se procede a crear los usuarios que tendrán acceso al servidor, con el comando `adduser`.

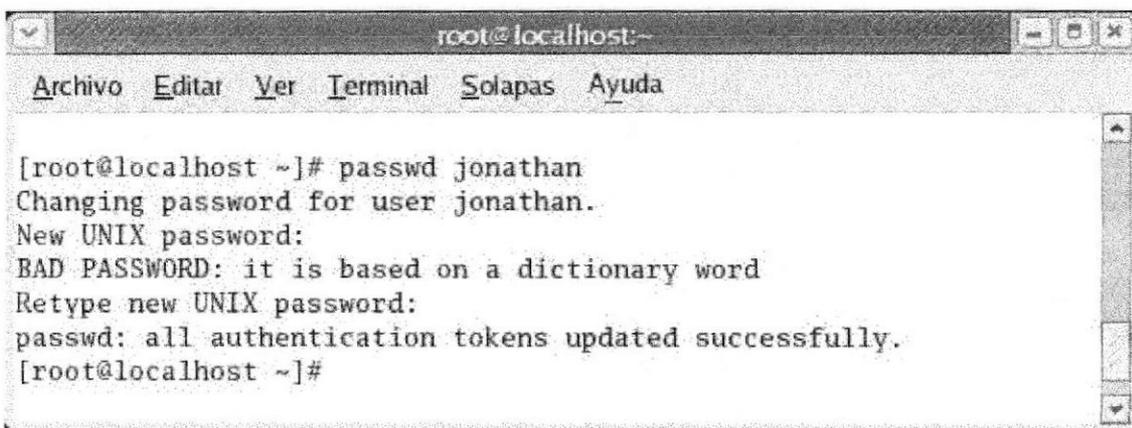


```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# adduser jonathan
adduser: user jonathan exists
[root@localhost ~]#
  
```

Figura 7-66: Crear usuario

Luego de haber creado su usuario, asignar su respectiva contraseña con el comando `passwd`.

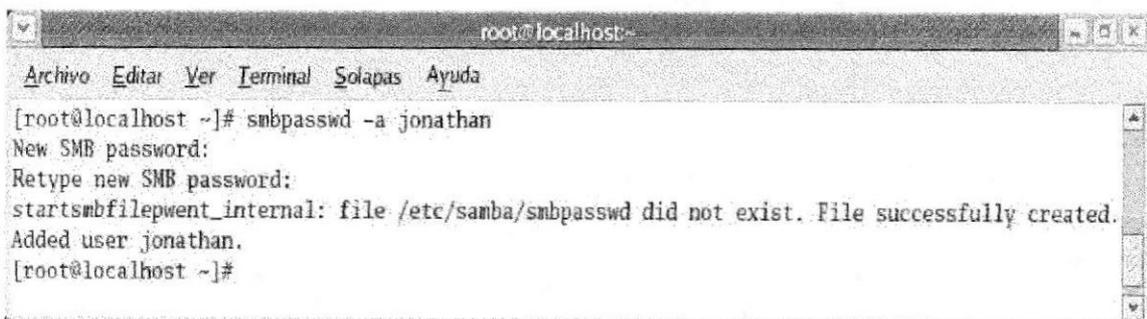


```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# passwd jonathan
Changing password for user jonathan.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
  
```

Figura 7-67: Asignar password

Para asignar una clave tipo samba al usuario digitar el comando `smbpasswd -a`



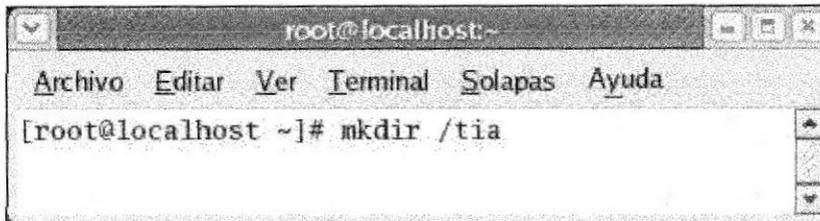
```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# smbpasswd -a jonathan
New SMB password:
Retype new SMB password:
startsmfilepwent_internal: file /etc/samba/smbpasswd did not exist. File successfully created.
Added user jonathan.
[root@localhost ~]#
  
```

Figura 7-68: Asignar usuario samba



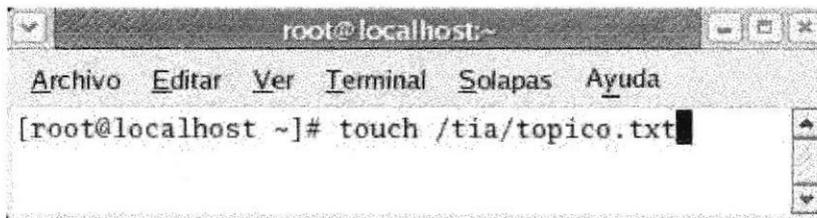
Luego de haber creado el usuario y contraseña crear el directorio el cual será compartido por el servidor samba para toda la red, dicho directorio a crear tiene que llevar el mismo nombre definido en la sección SHARE DEFINITIONS.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# mkdir /tia
```

Figura 7-69: Crear una carpeta

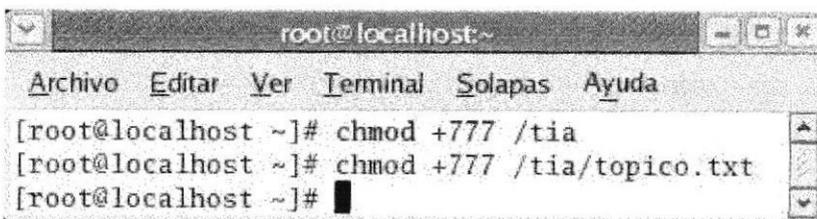
Luego se procede a crear un archivo como prueba para verlo mediante el cliente Windows.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# touch /tia/topico.txt
```

Figura 7-70: Crear archivo

Después de haber creado el archivo, proceder a darles sus debidos permisos generales, se hace con el comando chmod.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# chmod +777 /tia  
[root@localhost ~]# chmod +777 /tia/topico.txt  
[root@localhost ~]#
```

Figura 7-71: Dar permisos



7.8.1.1 CONFIGURACIÓN EN EL CLIENTE WINDOWS

En el cliente Windows se debe asignar su respectiva dirección IP, para esto dar clic derecho en el icono de mis sitios de red y elegir la opción propiedades.

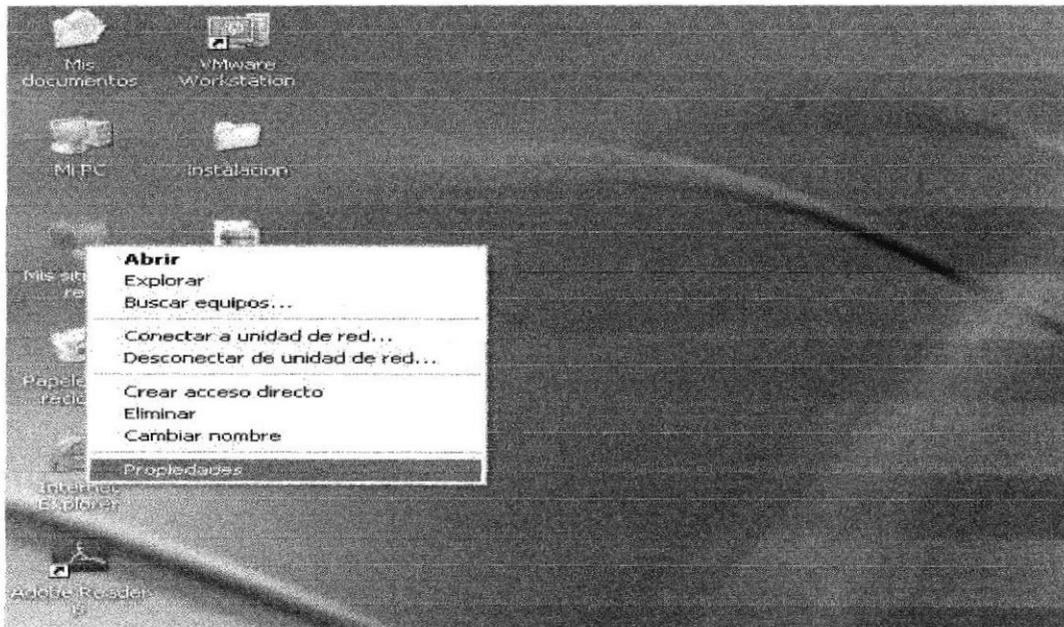


Figura 7-72: Propiedades de Mis sitios de red

Una vez ingresado en las propiedades de mis sitios de red, dar clic derecho sobre el icono de conexión de área local y seleccionar propiedades.

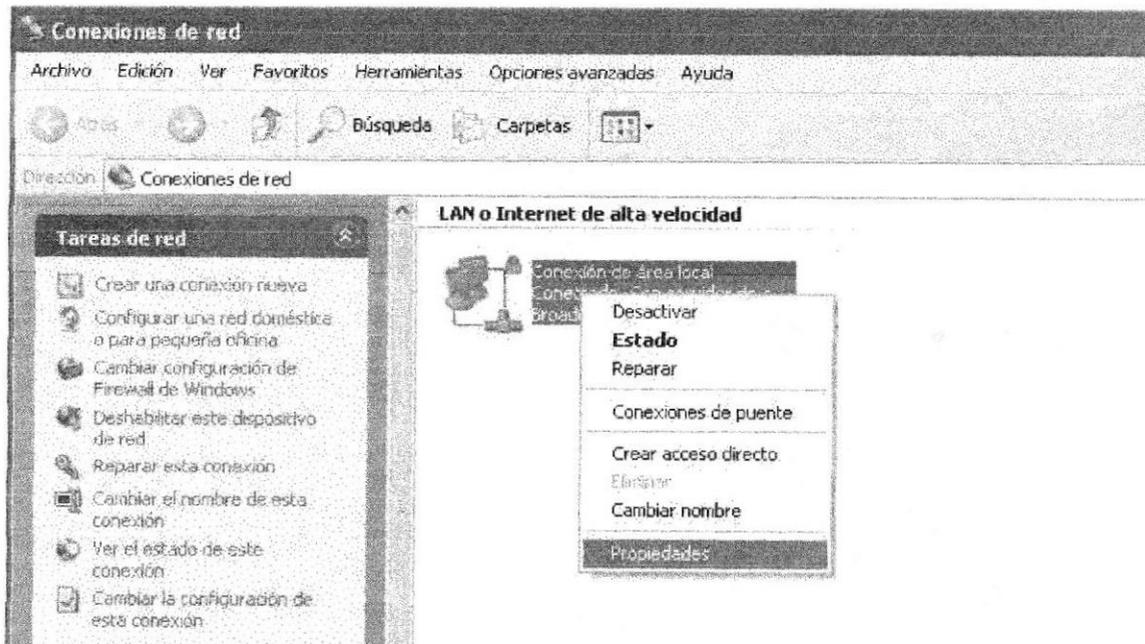


Figura 7-73: Propiedades de conexiones de red

Luego de esto aparecerá un recuadro de propiedades de Conexión de área local en el cual deberá ubicarse en la opción de protocolos de Internet tcp/ip y dar clic en propiedades.

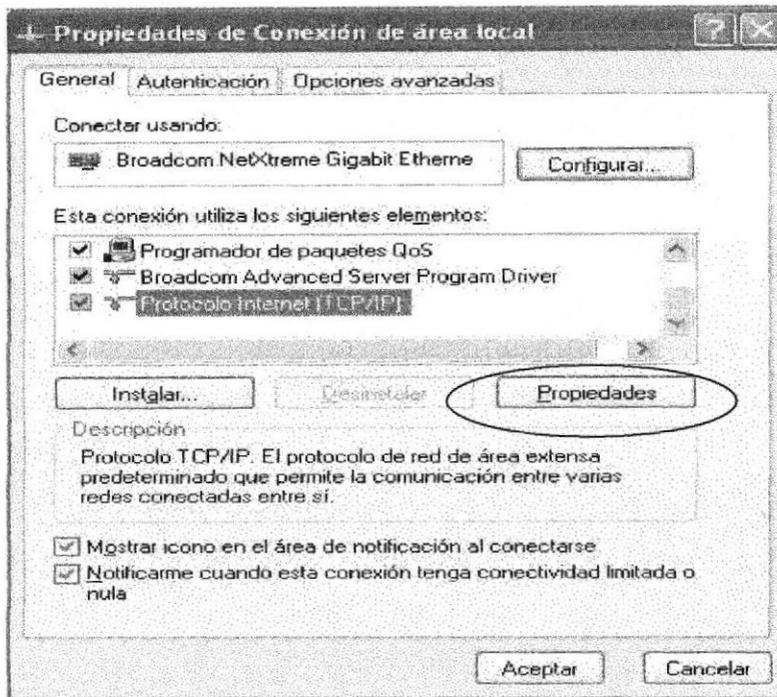


Figura 7-74: Propiedades de Protocolo de Internet

Luego de esto aparecerá otro recuadro en el cual asignar una dirección IP al cliente Windows tal como se muestra en la figura y aceptar los cambios realizados.

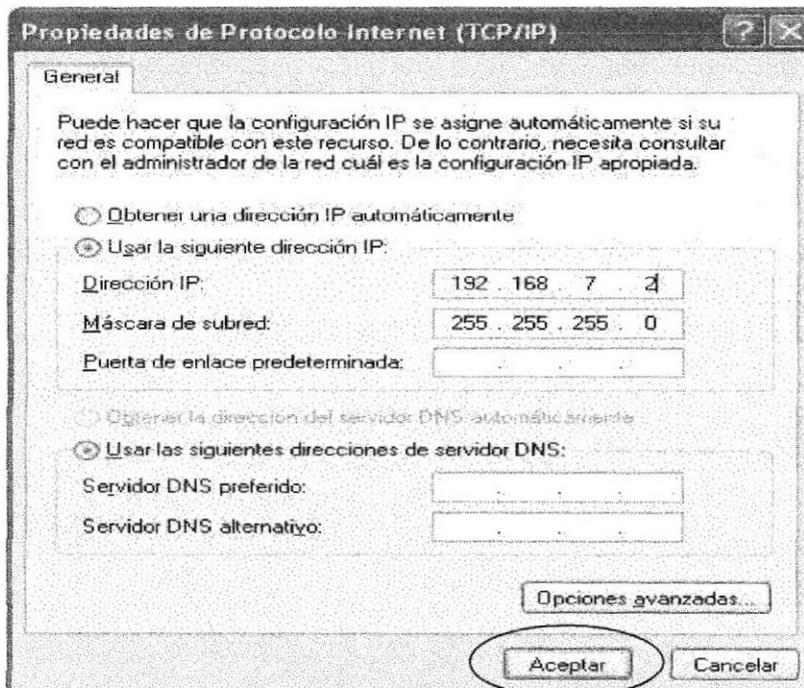


Figura 7-75: Asignación IP

El siguiente paso es buscar el Servidor samba, para ello dar clic derecho sobre el icono de mis sitios de red y seleccionar la opción buscar equipos.

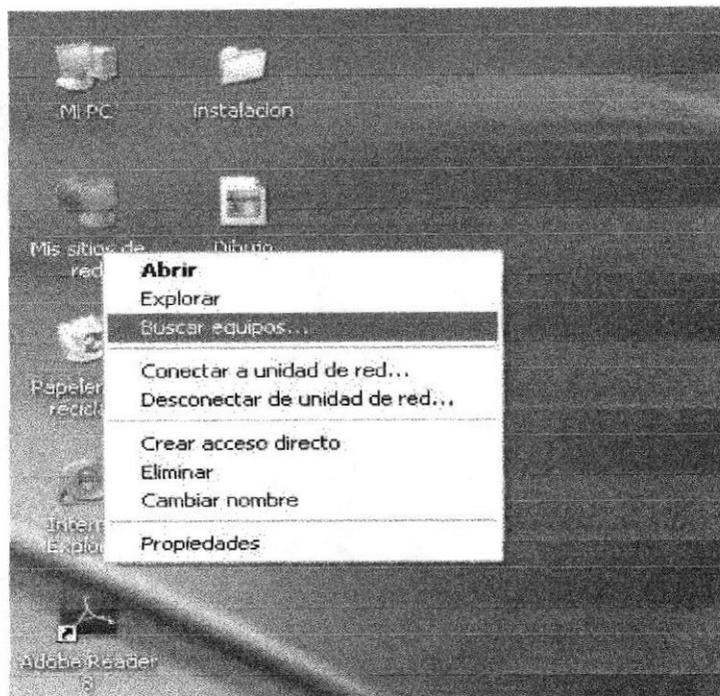


Figura 7-76: Buscar equipos

Aparecerá una ventana en el cual se procede a buscar el servidor samba, ya sea por nombre o por IP.

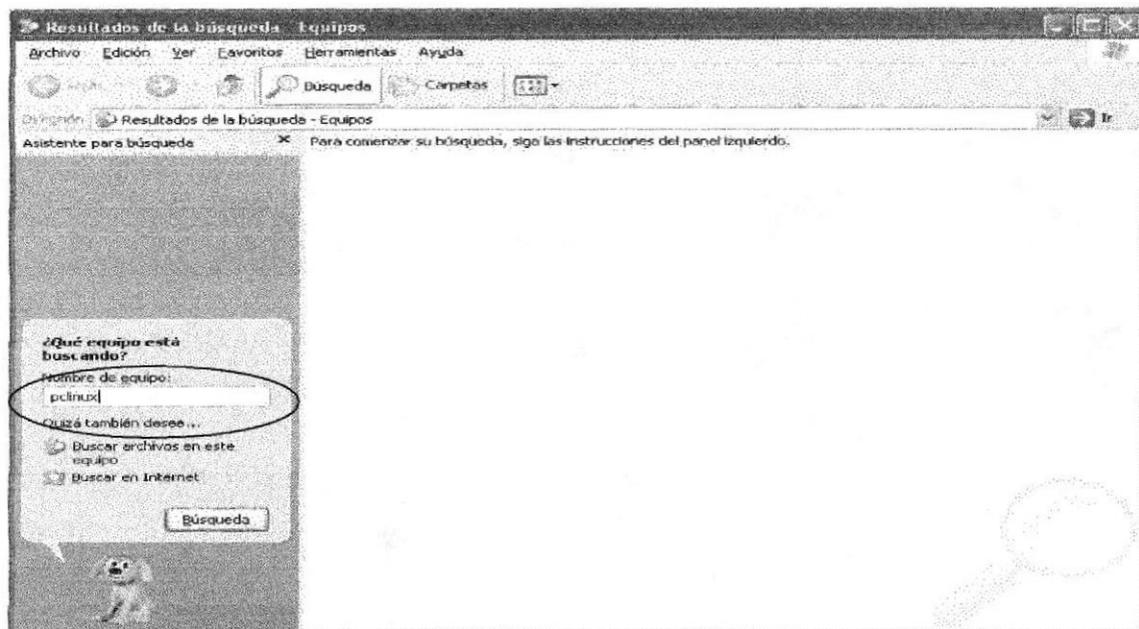


Figura 7-77: Búsqueda del servidor

Una vez encontrado el servidor samba dar doble clic sobre el icono del servidor encontrado.

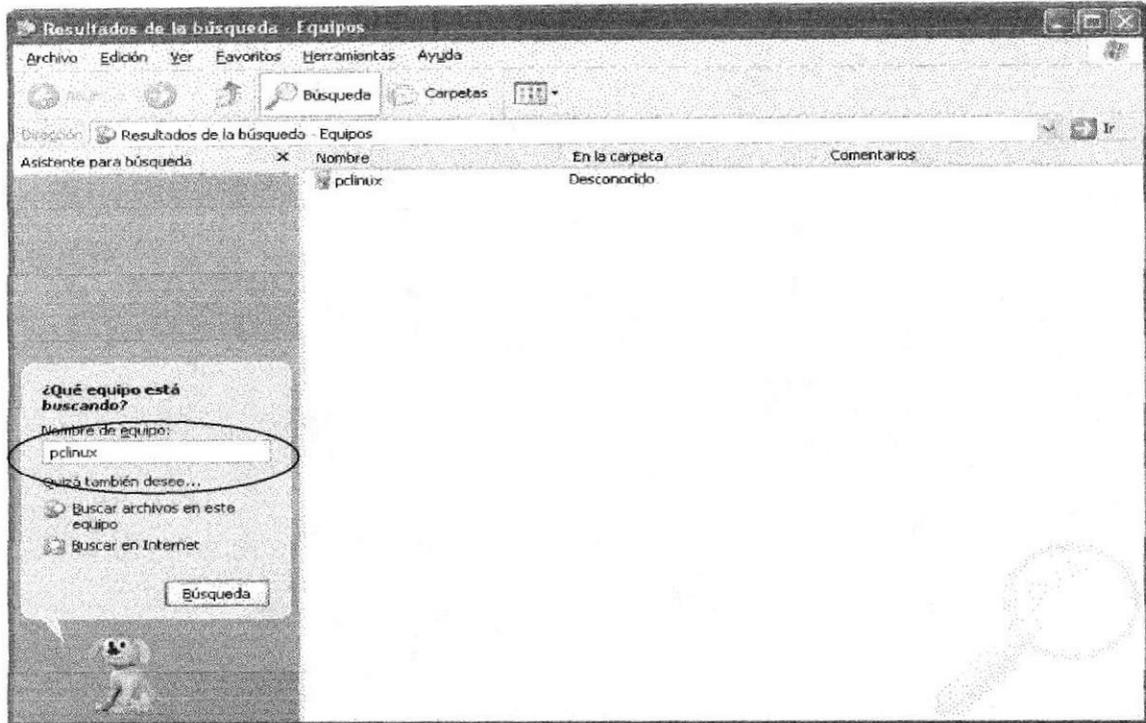


Figura 7-78: Servidor

Después de haber encontrado el servidor samba, aparecerá un recuadro solicitando un usuario y contraseña para poder acceder a dicho servidor.



Figura 7-79: Conexión a Linux



Una vez ingresado al servidor mostrará el directorio compartido por el mismo en el cual estarán todos los archivos compartidos.

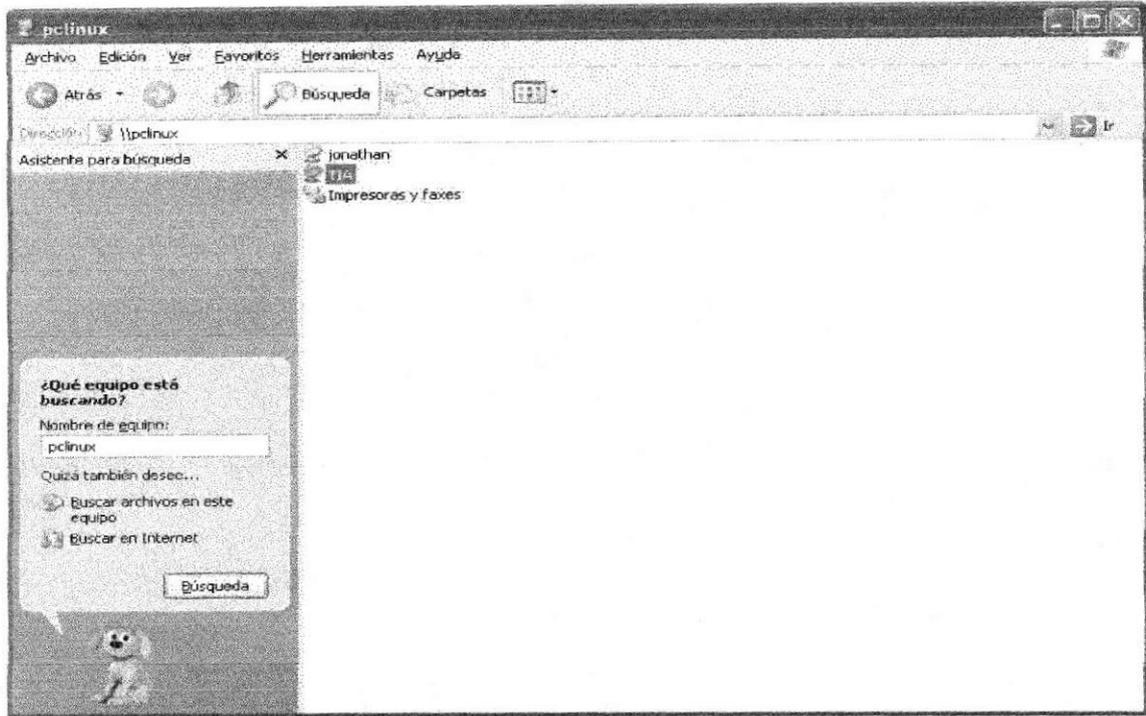


Figura 7-80: Archivos compartidos

Para realizar una prueba, ingresar al directorio compartido y dar doble clic sobre el archivo existente.

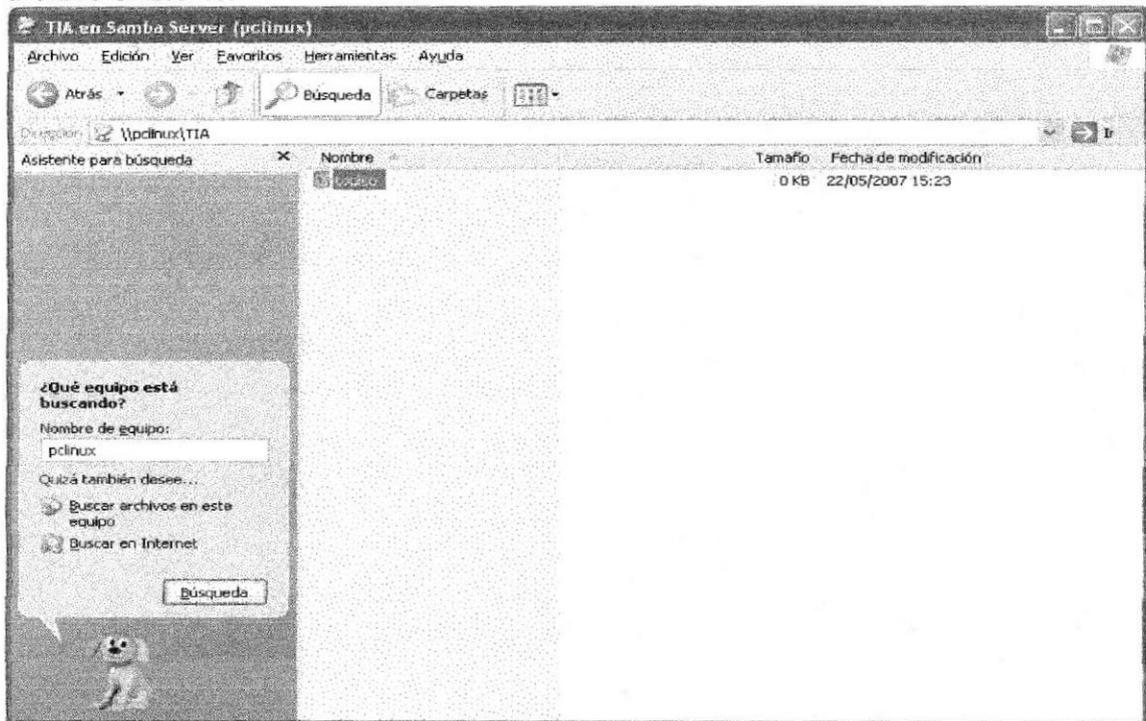


Figura 7-81: Crear usuario



Luego de esto proceder a editar el archivo, agregar algún mensaje.

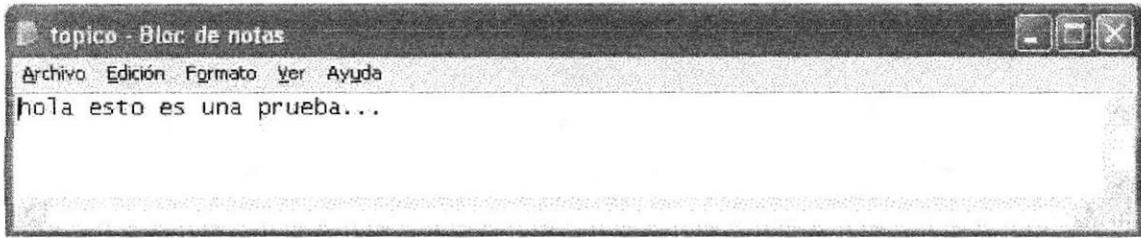


Figura 7-82: Agregar mensaje

Después de esto en el servidor samba, ir al directorio donde se encuentra el archivo.

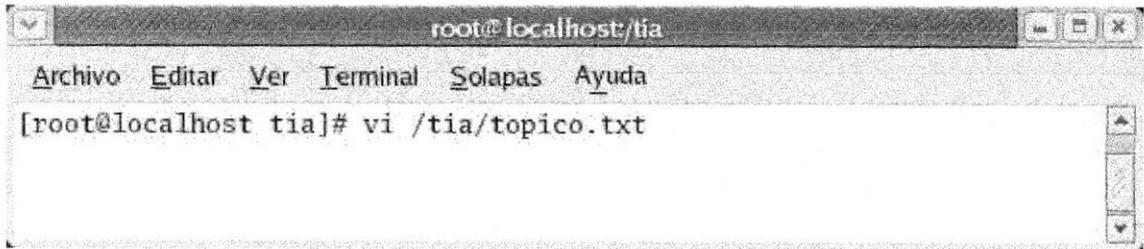


Figura 7-83: Directorio del archivo

Aquí observar que se puede tener acceso al archivo compartido por el servidor.

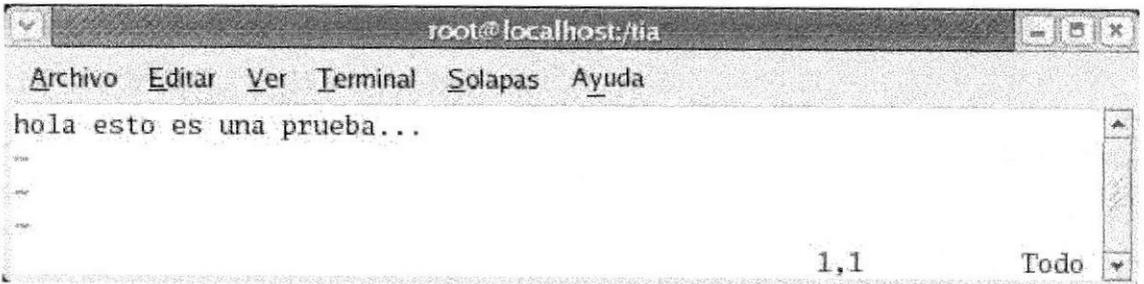


Figura 7-84: Comprobación



7.8.2 CONFIGURACIÓN DEL SERVIDOR DNS

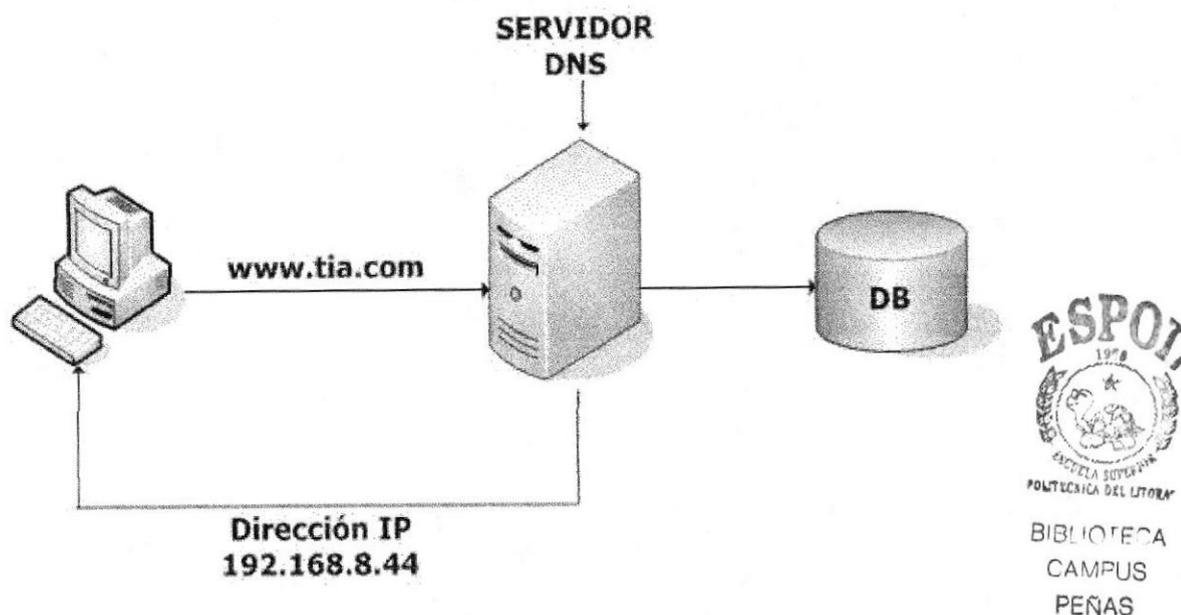


Figura 7-85: Pantalla esquema DNS

El DNS usa el concepto de espacio de nombres distribuido. Los nombres simbólicos se agrupan en zonas de autoridad, o más comúnmente, zonas. En cada una de estas zonas, uno o más hosts tienen la tarea de mantener una base de datos de nombres simbólicos y direcciones IP y de suministrar la función de servidor para los clientes que deseen traducir nombres simbólicos a direcciones IP. Estos servidores de nombres locales se interconectan lógicamente en un árbol jerárquico de dominios.

BIND (acrónimo de **Berkeley Internet Name Domain**) es una implementación del protocolo DNS y provee una implementación libre de los principales componentes del Sistema de Nombres de Dominio, los cuales incluyen:

- Un servidor de sistema de nombres de dominio (named).
- Una biblioteca resolutoria de sistema de nombres de dominio.
- Herramientas para verificar la operación adecuada del servidor DNS (bind-utils).

El Servidor DNS BIND es ampliamente utilizado en la Internet (99% de los servidores DNS) proporcionando una robusta y estable solución.

DNS (Domain Name System).

DNS (acrónimo de **Domain Name System**) es una base de datos distribuida y jerárquica que almacena la información necesaria para los nombre de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico correspondientes para cada dominio. El **DNS** nació de la necesidad de facilitar a los seres humanos el acceso hacia los servidores disponibles a través de Internet permitiendo hacerlo por un nombre, algo más fácil de recordar que una dirección **IP**.

Los **Servidores DNS** utilizan **TCP** y **UDP** en el puerto 53 para responder las consultas. Casi todas las consultas consisten de una sola solicitud **UDP** desde un **Cliente DNS** seguida por una sola respuesta **UDP** del servidor. **TCP** interviene cuando el tamaño de los datos de la respuesta excede los 512 bytes, tal como ocurre con tareas como **transferencia de zonas**.

NIC (Network Information Center).

NIC (acrónimo de Network Information Center o Centro de Información sobre la Red) es una institución encargada de asignar los nombres de dominio en Internet, ya sean nombres de dominio genérico o por países, permitiendo personas o empresas montar sitios de Internet mediante a través de un **ISP** mediante un DNS. Técnicamente existe un **NIC** por cada país en el mundo y cada uno de éstos es responsable por todos los dominios con la terminación correspondiente a su país. Por ejemplo: **NIC MEXICO** es la entidad encargada de gestionar todos los dominios con terminación **.mx**, la cual es la terminación correspondiente asignada a los dominios de México.

FQDN (Fully Qualified Domain Name).

FQDN (acrónimo de Fully Qualified Domain Name o Nombre de Dominio Plenamente Calificado) es un Nombre de Dominio ambiguo que especifica la posición absoluta del nodo en el árbol jerárquico del DNS. Se distingue de un nombre regular porque lleva un punto al final.

Como ejemplo: suponiendo que se tiene un dispositivo cuyo nombre de anfitrión es «maquina1» y un dominio llamado «dominio.com», el **FQDN** sería «**maquina1.dominio.com.**», así es que se define de forma única al dispositivo mientras que pudieran existir muchos anfitriones llamados «maquina1», solo puede haber uno llamado «**maquina1.dominio.com.**». La ausencia del punto al final definiría que se pudiera tratar tan solo de un prefijo, es decir «**maquina1.dominio.com**» pudiera ser un dominio de otro más largo como «**maquina1.dominio.com.mx**».

La longitud máxima de un **FQDN** es de 255 bytes, con una restricción adicional de 63 bytes para cada etiqueta dentro del nombre del dominio. Solo se permiten los caracteres A-Z de ASCII, dígitos y el carácter «-». No se distinguen mayúsculas y minúsculas.

Desde 2004, a solicitud de varios países de Europa, existe el estándar **IDN** (acrónimo de Internationalized Domain Name) que permite caracteres no-ASCII, codificando caracteres **Unicode** dentro de cadenas de bytes dentro del conjunto normal de caracteres de **FQDN**. Como resultado, los límites de longitud de los nombres de dominio **IDN** dependen directamente del contenido mismo del nombre.

Componentes de un DNS.

Los DNS operan a través de tres componentes: Clientes DNS, Servidores DNS y Zonas de Autoridad.

Clientes DNS.

Son programas que ejecuta un usuario y que generan peticiones de consulta para resolver nombres. Básicamente preguntan por la dirección IP que corresponde a un nombre determinado.

Servidores DNS.

Son servicios que contestan las consultas realizadas por los **Clientes DNS**. Hay dos tipos de servidores de nombres:

- **Servidor Maestro:** También denominado **Primario**. Obtiene los datos del dominio a partir de un fichero hospedado en el mismo servidor.
- **Servidor Esclavo:** También denominado **Secundario**. Al iniciar obtiene los datos del dominio a través de un Servidor Maestro (o primario), realizando un proceso denominado **transferencia de zona**.

Un gran número de problemas de operación de servidores DNS se atribuyen a las pobres opciones de servidores secundarios para la zona de DNS. De acuerdo al RFC



BIBLIOTECA
CAMPUS
PEÑAS

2182 el DNS requiere que **al menos tres servidores existan** para todos los dominios delegados (o zonas).

Una de las principales razones para **tener al menos tres servidores** para cada zona es permitir que la información de la zona misma esté disponible siempre y forma confiable hacia los **Cientes DNS** a través de Internet cuando un servidor DNS de dicha zona falle, no esté disponible y/o esté inalcanzable.

Contar con múltiples servidores también facilita la **propagación** de la zona y mejoran la eficiencia del sistema en general al brindar opciones a los **Cientes DNS** si acaso encontrarán dificultades para realizar una consulta en un **Servidor DNS**. En otras palabras: tener múltiples servidores para una zona permite **contar con redundancia y respaldo del servicio**.

Con múltiples servidores, por lo general uno actúa como **Servidor Maestro o Primario** y los demás como **Servidores Esclavos o Secundarios**. Correctamente configurados y una vez creados los datos para una zona, no será necesario copiarlos a cada **Servidor Esclavo o Secundario**, pues éste se encargará de transferir los datos de manera automática cuando sea necesario.

Los **Servidores DNS** responden dos tipos de consultas:

- **Consultas Iterativas (no recursivas):** El cliente hace una consulta al **Servidor DNS** y este le responde con la mejor respuesta que pueda darse basada sobre su caché o en las zonas locales. Si no es posible dar una respuesta, la consulta se reenvía hacia otro Servidor DNS repitiéndose este proceso hasta encontrar al **Servidor DNS** que tiene la **Zona de Autoridad** capaz de resolver la consulta.
- **Consultas Recursivas:** El **Servidor DNS** asume toda la carga de proporcionar una respuesta completa para la consulta realizada por el **Ciente DNS**. El **Servidor DNS** desarrolla entonces **Consultas Iterativas** separadas hacia otros **Servidores DNS** (en lugar de hacerlo el **Ciente DNS**) para obtener la respuesta solicitada.

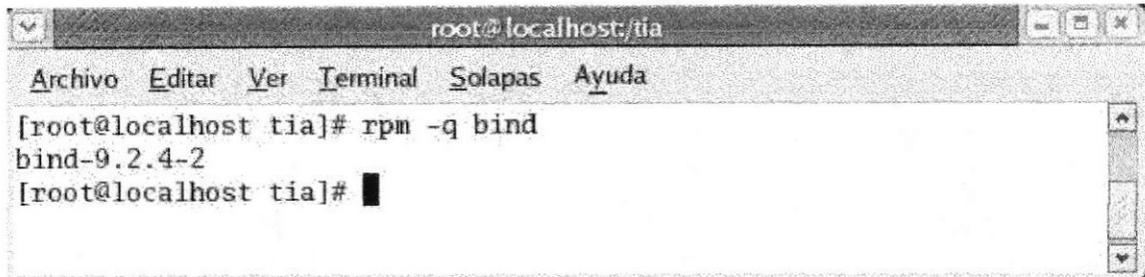
REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR DNS

- 1 Pc con Linux Fedora Core 3
- 1 Tarjeta de Red
- Tener una IP Estática
- Tener instalados los paquetes DNS
 - Bind
 - Bind-chroot



7.8.2.1 CONFIGURACIÓN DEL BIND

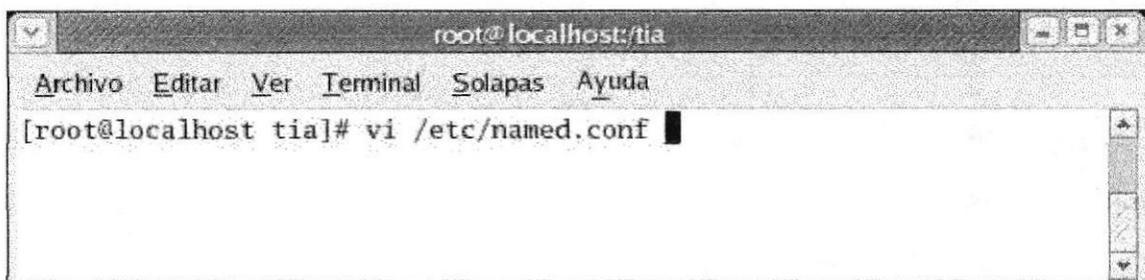
Antes de comenzar con la configuración del archivo, se debe verificar si está instalado el paquete, hacerlo con el comando `rpm -q bind`.



```
root@localhost:/tia
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost tia]# rpm -q bind
bind-9.2.4-2
[root@localhost tia]#
```

Figura 7-86: Verificación del paquete bind

Si el paquete está instalado se procede a editar el archivo del `named.conf` con el comando `vi` tal como se muestra en la figura.



```
root@localhost:/tia
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost tia]# vi /etc/named.conf
```

Figura 7-87: Editar archivo named

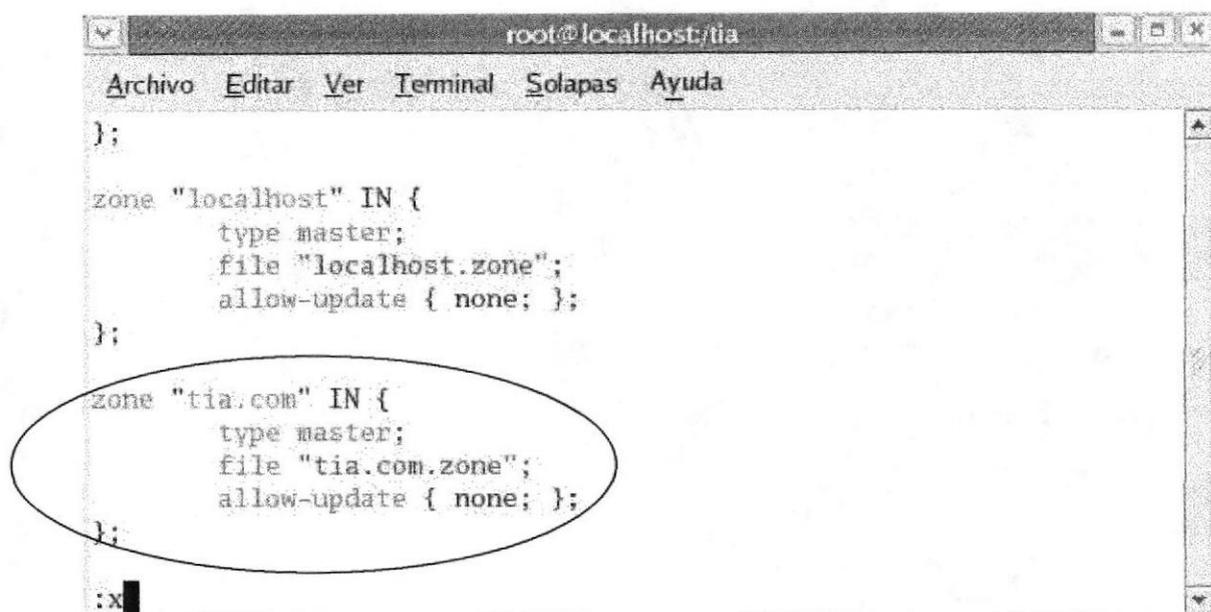
Una vez dentro del archivo del `named.conf` agregar las siguientes líneas para levantar el dominio.

zone "tia.com" IN {: Es el nombre del dominio o la zona.

type master: Tipo de la Zona, en este caso zona principal.

file "tia.com.zone": Es el nombre del archivo que se va a editar.

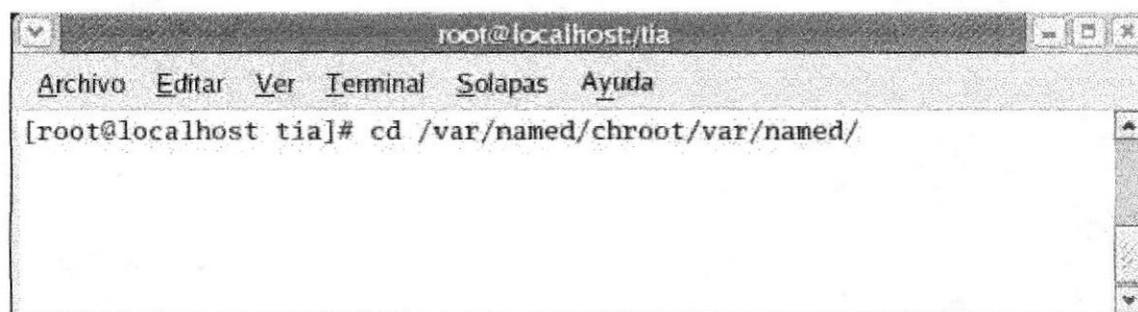
Allow-update { none; }: Es el que permite actualizar la zona.



```
root@localhost:/tia
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
};
zone "localhost" IN {
    type master;
    file "localhost.zone";
    allow-update { none; };
};
zone "tia.com" IN {
    type master;
    file "tia.com.zone";
    allow-update { none; };
};
:x
```

Figura 7-88: Archivo para editar

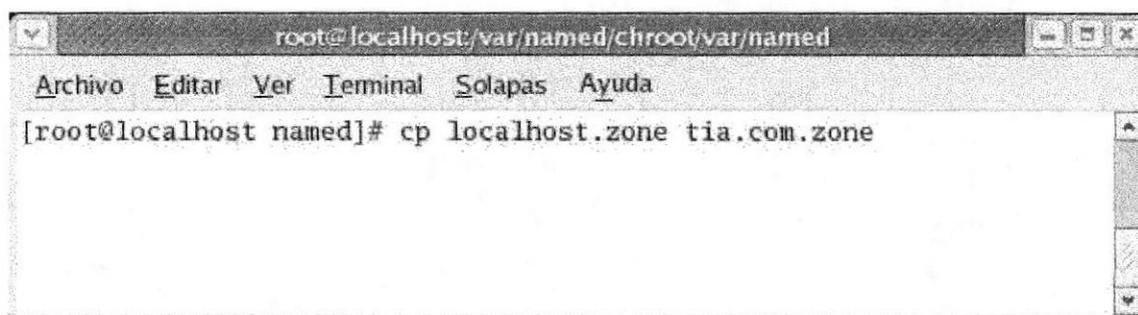
Después de haber editado el archivo del named.conf, se procede a buscar el archivo del localhost.zone ubicado en var/named/chroot/var/named/



```
root@localhost:/tia
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost tia]# cd /var/named/chroot/var/named/
```

Figura 7-89: Ruta para entrar al localhost

Una vez encontrado el archivo de localhost.zone se procede a copiar y renombrar con el nombre del dominio, para este caso tia.com.zone.



```
root@localhost:/var/named/chroot/var/named
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost named]# cp localhost.zone tia.com.zone
```

Figura 7-90: Copiar archivo

Después de esto se procede a edita el archivo de zona con el comando `vi tia.com.zone`

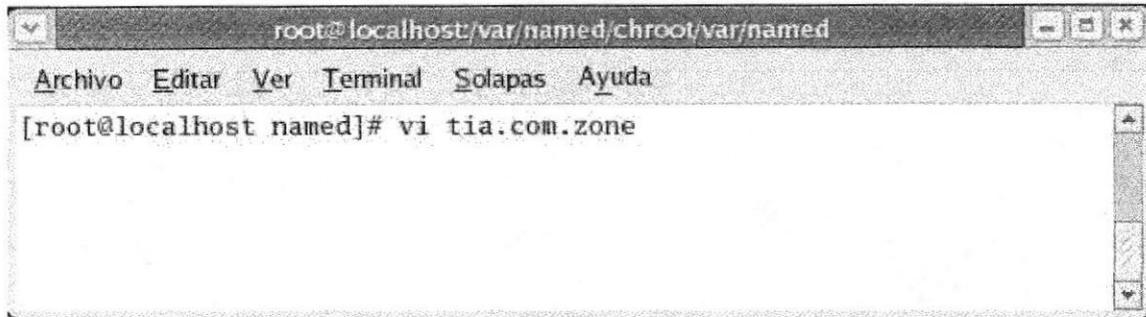


Figura 7-91: Ruta para editar el archivo

Dentro del archivo de la zona aparecerá algo parecido a esto:

SOA (Start of Authority): Registro de inicio de autoridad que especifica el **Servidor DNS Maestro** (o Primario) que proporcionará la información con autoridad acerca de un dominio de Internet, dirección de correo electrónico del administrador, número de serie del dominio y parámetros de tiempo para la zona.

NS (Name Server): Registro de servidor de nombres que sirve para definir una lista de servidores de nombres con autoridad para un dominio.

A (Address): Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección IP.

CNAME (Canonical Name): Registro de nombre canónico que hace que un nombre sea alias de otro. Los dominios con alias obtienen los sub-dominios y registros DNS del dominio original.

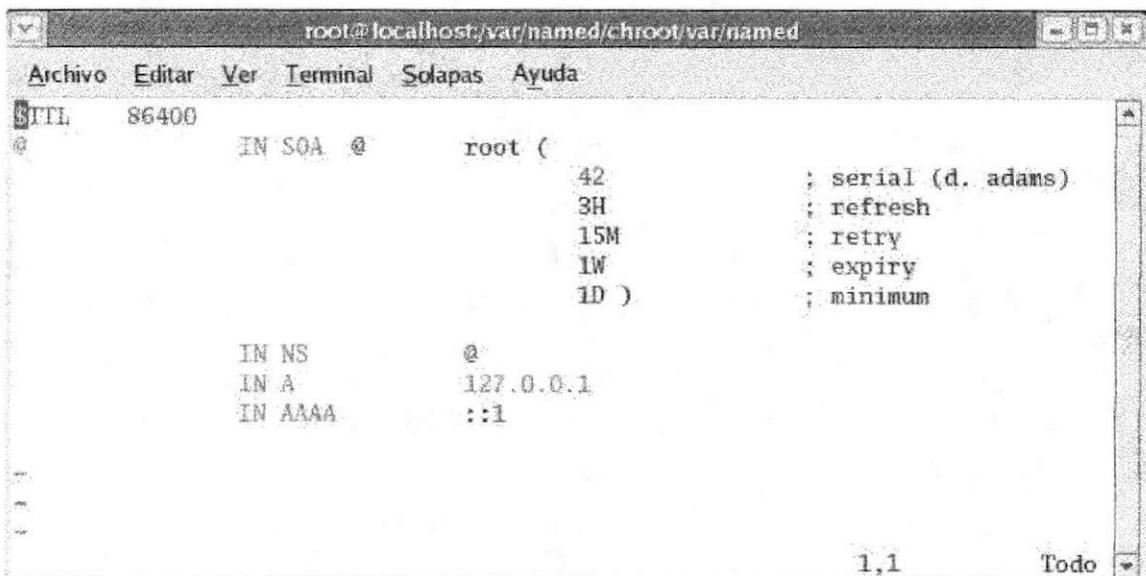


Figura 7-92: Archivo

ESPOL
1978
BIBLIOTECA
CAMPUS
PEÑAS

Proceder a editar el archivo de zona agregando lo siguiente tal y como lo muestra en la figura y guardar los cambios.

```

root@localhost:/var/named/chroot/var/named
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
$TTL 86400
@      IN SOA  tia.com.  root.tia.com. (
                        42      ; serial (d. adams)
                        3H      ; refresh
                        15M     ; retry
                        1W      ; expiry
                        1D      ; minimum

localhost IN NS   tia
localhost IN A   127.0.0.1
tia       IN A   192.168.7.1
www       CNAME  tia
:~
:~
:~
:x

```

Figura 7-93: Archivo editada

Luego de haber terminado de editar el archivo de la zona, se procede a editar el archivo del resolv, el cual indica la resolución del nombre.

```

root@localhost:/var/named/chroot/var/named
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost named]# vi /etc/resolv.conf

```

Figura 7-94: Ruta de archivo resolv.conf

Dentro del archivo resolv.conf aparecerá algo parecido a esto:

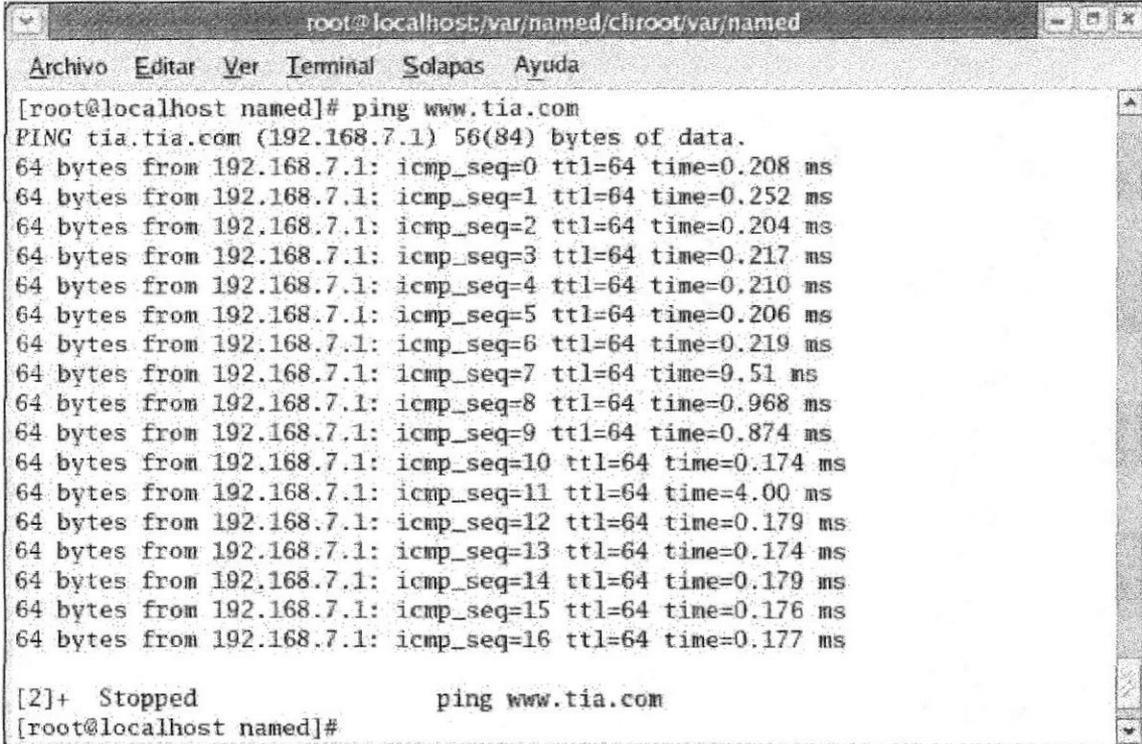
```

root@localhost:/var/named/chroot/var/named
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
search localdomain
:~
:~
:~
1,18      Todo

```

Figura 7-95: Archivo resolv.conf

Si el dominio está bien levantado deberá mostrar algo parecido a esto.

A screenshot of a terminal window titled "root@localhost:/var/named/chroot/var/named". The window has a menu bar with "Archivo", "Editar", "Ver", "Terminal", "Solapas", and "Ayuda". The terminal content shows a ping command being executed: [root@localhost named]# ping www.tia.com. The output displays 17 successful ping responses from 192.168.7.1 to tia.tia.com (192.168.7.1) with 56(84) bytes of data. Each response shows the ICMP sequence number, TTL, and response time in milliseconds. The times are mostly below 1 ms, with one outlier at 9.51 ms for sequence 7. The terminal ends with "[2]+ Stopped ping www.tia.com" and the prompt [root@localhost named]#.

```
root@localhost:/var/named/chroot/var/named
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost named]# ping www.tia.com
PING tia.tia.com (192.168.7.1) 56(84) bytes of data.
64 bytes from 192.168.7.1: icmp_seq=0 ttl=64 time=0.208 ms
64 bytes from 192.168.7.1: icmp_seq=1 ttl=64 time=0.252 ms
64 bytes from 192.168.7.1: icmp_seq=2 ttl=64 time=0.204 ms
64 bytes from 192.168.7.1: icmp_seq=3 ttl=64 time=0.217 ms
64 bytes from 192.168.7.1: icmp_seq=4 ttl=64 time=0.210 ms
64 bytes from 192.168.7.1: icmp_seq=5 ttl=64 time=0.206 ms
64 bytes from 192.168.7.1: icmp_seq=6 ttl=64 time=0.219 ms
64 bytes from 192.168.7.1: icmp_seq=7 ttl=64 time=9.51 ms
64 bytes from 192.168.7.1: icmp_seq=8 ttl=64 time=0.968 ms
64 bytes from 192.168.7.1: icmp_seq=9 ttl=64 time=0.874 ms
64 bytes from 192.168.7.1: icmp_seq=10 ttl=64 time=0.174 ms
64 bytes from 192.168.7.1: icmp_seq=11 ttl=64 time=4.00 ms
64 bytes from 192.168.7.1: icmp_seq=12 ttl=64 time=0.179 ms
64 bytes from 192.168.7.1: icmp_seq=13 ttl=64 time=0.174 ms
64 bytes from 192.168.7.1: icmp_seq=14 ttl=64 time=0.179 ms
64 bytes from 192.168.7.1: icmp_seq=15 ttl=64 time=0.176 ms
64 bytes from 192.168.7.1: icmp_seq=16 ttl=64 time=0.177 ms

[2]+  Stopped                  ping www.tia.com
[root@localhost named]#
```

Figura 7-99: Resultado del ping

7.8.2.2 CONFIGURACIÓN EN EL CLIENTE WINDOW

En el cliente Windows se debe asignar su respectiva dirección IP, para esto dar clic derecho en el icono de mis sitios de red y elegir la opción propiedades.

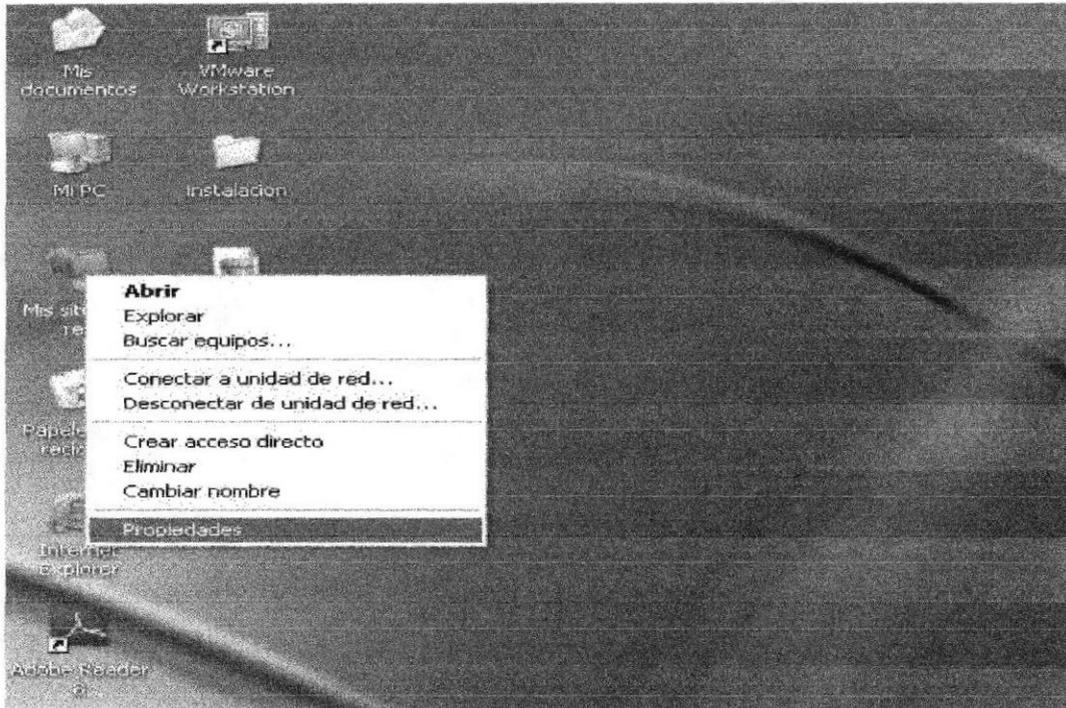


Figura 7-100: Propiedades de mis sitios de red

Una vez ingresado en las propiedades de mis sitios de red, dar clic derecho sobre el icono de conexión de área local y seleccionar propiedades.

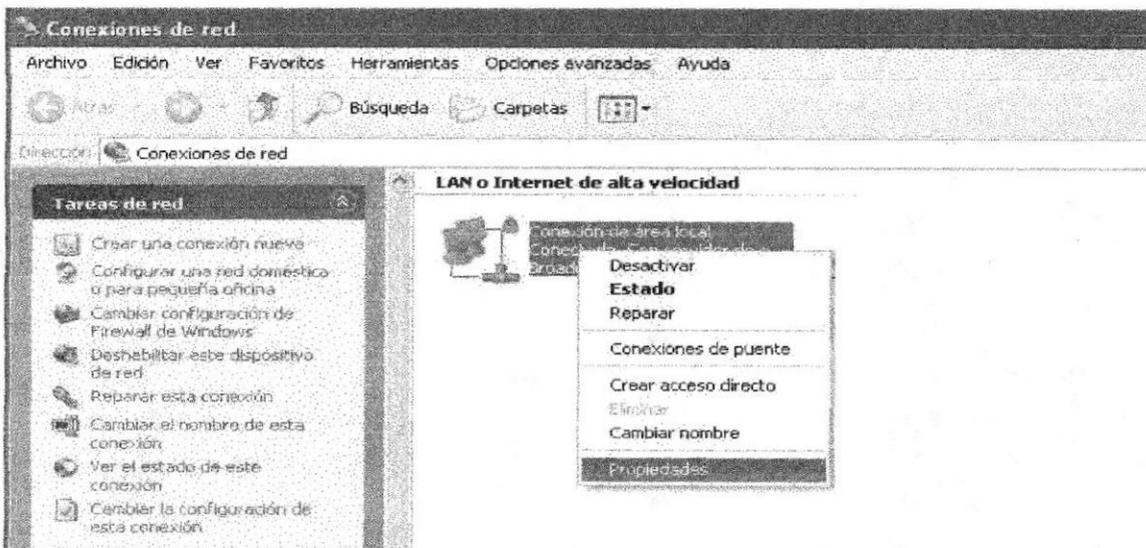


Figura 7-101: Pantalla propiedades de conexión

Luego de esto aparecerá un recuadro de propiedades de Conexión de área local en el cual ubicarse en la opción de protocolos de Internet tcp/ip y dar clic en propiedades.

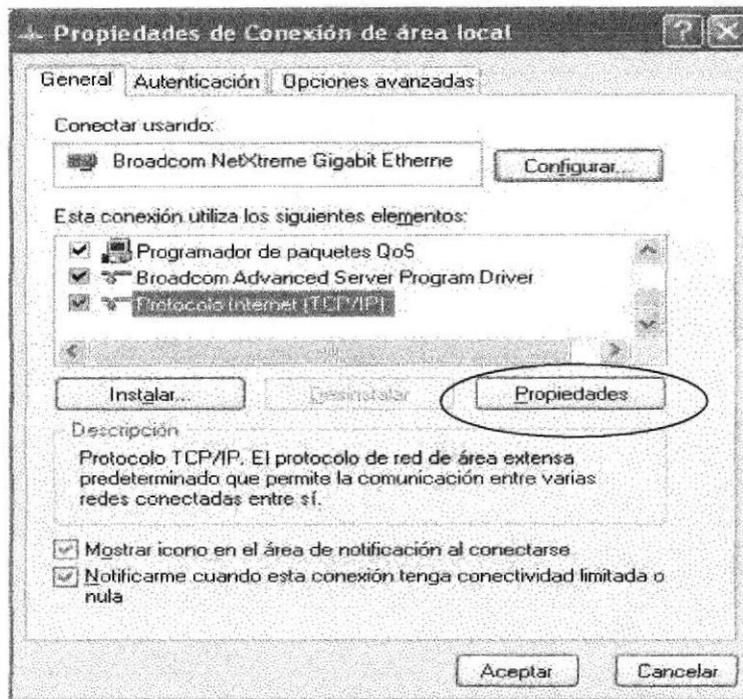


Figura 7-102: Propiedades de TCP/IP

En esta ventana se procede a agregar la dirección IP al cliente, con su respectiva máscara de subred y con el dns preferido el cual es la dirección IP del servidor.

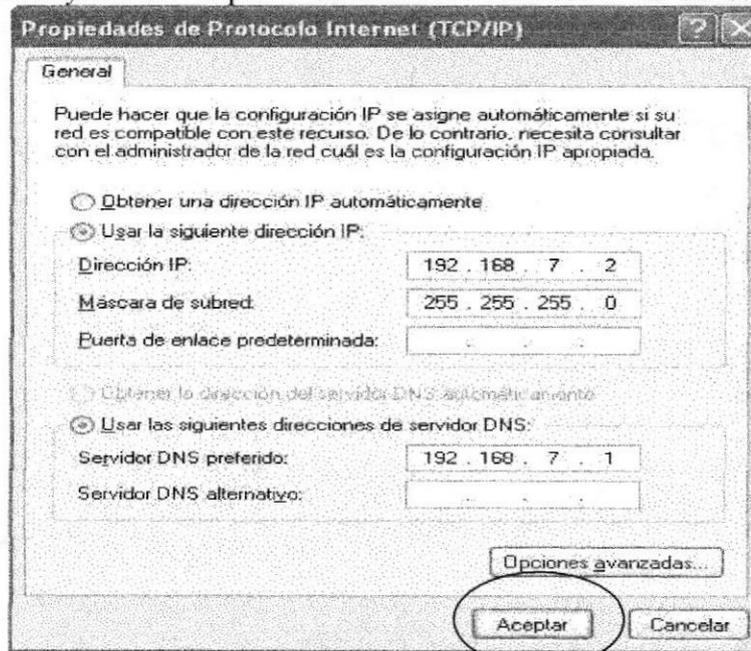


Figura 7-103: Pantalla para agregar IP



Luego de haber dado la dirección DNS se procede a probar haciendo ping desde el equipo cliente.

Para poder hacer la comprobación de estar bien levantado el servidor DNS deberá hacer los siguientes pasos ir a menú inicio del cliente y dar clic en ejecutar.



Figura 7-104: Inicio opción Ejecutar

Luego aparecerá algo parecido a esta ventana donde debe digitar cmd para que se abra el ambiente texto del cliente.

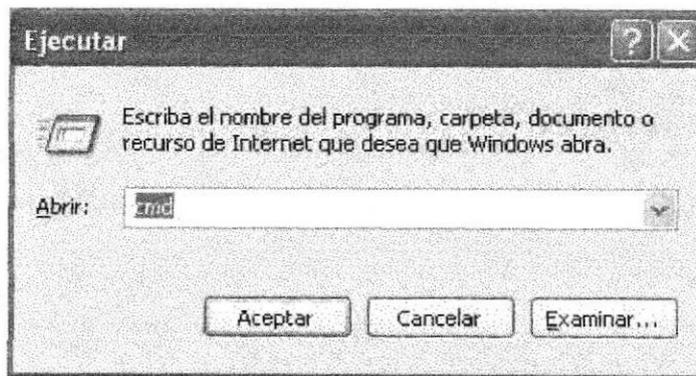
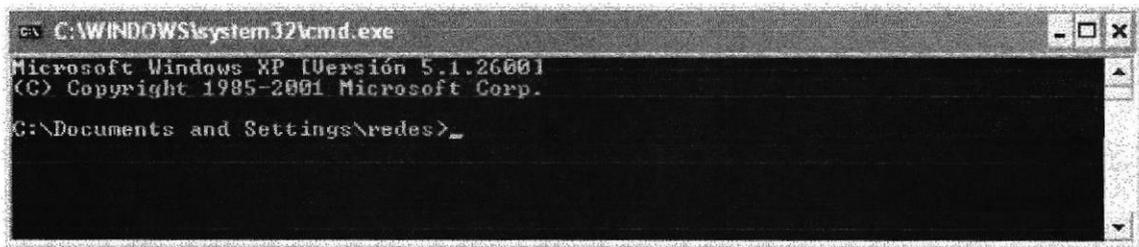


Figura 7-105: Comando para abrir ambiente texto

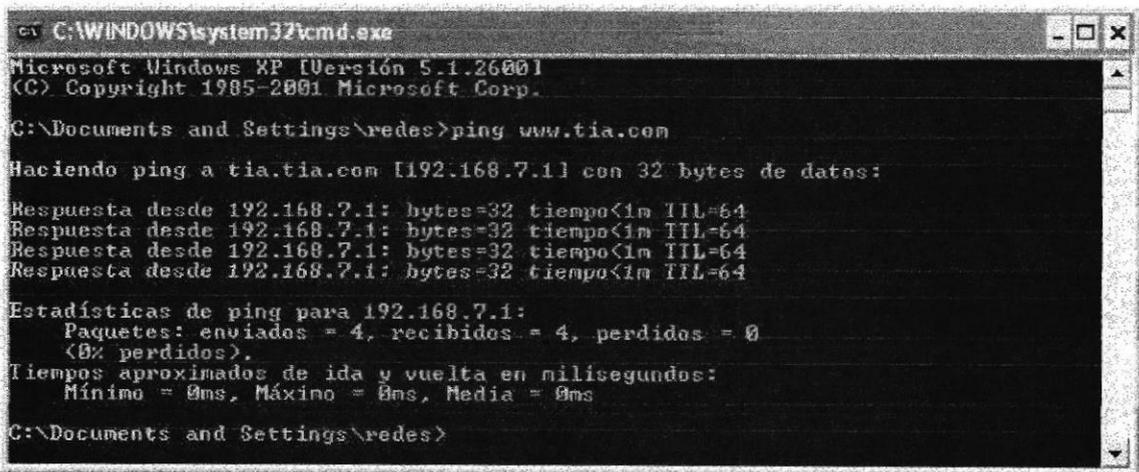
Luego de haber ingresado aparecerá una pantalla parecida a esta donde se realizará la comprobación.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\redes>
```

Figura 7-106: Realizar la comprobación

Luego de haber ingresado digitar ping el dominio creado en el Servidor para poder comprobar que esta bien configurado el servidor Dns.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\redes>ping www.tia.com
Haciendo ping a tia.tia.com [192.168.7.1] con 32 bytes de datos:
Respuesta desde 192.168.7.1: bytes=32 tiempo<1m TTL=64
Estadísticas de ping para 192.168.7.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos).
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
C:\Documents and Settings\redes>
```

Figura 7-107: Comprobación

BENEFICIOS

- Nombres conocidos por el usuario son más fácil de recordar que sus respectivas direcciones IP.
- Las direcciones IP pueden cambiar pero los nombres permanecen constantes.

7.8.3 CONFIGURACIÓN DEL SERVIDOR WEB

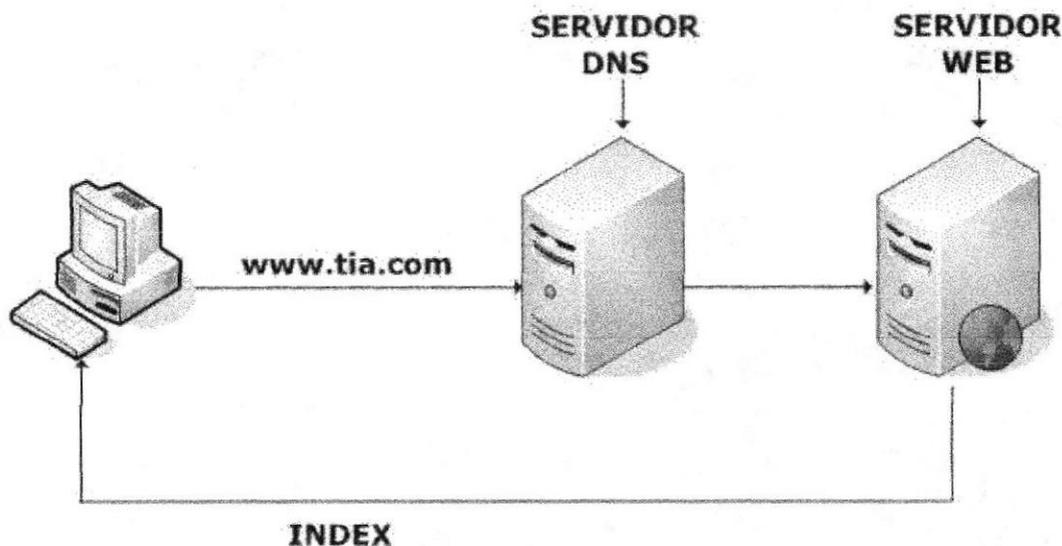


Figura 7-108: Pantalla de esquema Servidor Web

Básicamente, un servidor Web sirve contenido estático a un navegador, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP. Se pueden utilizar varias tecnologías en el servidor para aumentar su potencia más allá de su capacidad de entregar páginas HTML; éstas incluyen scripts CGI, seguridad SSL y páginas activas del servidor (ASP).

Los Servidores Web son aquéllos que permiten a los clientes compartir datos, documentos y multimedia en formato Web. Aunque es parte de la tecnología Cliente-Servidor, el servidor Web aporta algunas ventajas adicionales; como acceso más simple a la información (con un simple clic).

Versatilidad

En GNU/Linux, no se está atado a un solo servidor Web. Desde el popular Apache (utilizado por más del 65 % de los servidores Web de todo el mundo) hasta servidores web basados en Java como Tomcat, pueden ser configurados dependiendo de la necesidad. Esto quiere decir que el servidor Web se adapta a su aplicación y necesidades y no al revés.

Confiabilidad

Un servidor Web bien programado y configurado, sobre una plataforma estable, conjugan para que la estabilidad y confiabilidad de un servidor Web Linux sean insuperables. Meses o años. Ese es el tiempo que puede llegar a estar corriendo el servidor sin necesidad de reiniciar y sin fallas.

Seguridad

Seguridad. La palabra clave en servidores Web, especialmente si corre sitios de e-commerce o maneja información valiosa. El servidor web Apache, a pesar de ser el más ampliamente utilizado, registra muchos menos incidentes de seguridad por año que su principal competidor propietario (IIS), el cual a pesar de poseer menor cuota de mercado registra las mayores fallos de seguridad.

Economía

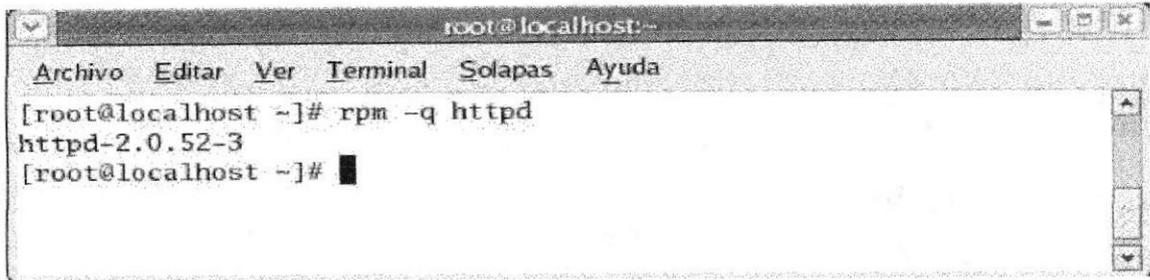
Instalar un servidor Web Linux no sólo es más económico desde el punto de vista de la inversión inicial. El hecho de que requiera muy poco mantenimiento (si no es nulo) abarata costos y de que sea más seguro y confiable también ayuda a reducir el presupuesto, ya que el servidor nunca está off-line, evitando pérdidas de dinero. Además, al ser el rendimiento superior (y atender a más usuarios) se evitan actualizaciones de hardware y software.

REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR WEB

- 1 Pc con Linux Fedora Core 3
- 1 Tarjeta de Red
- Tener una IP Estática
- Tener levantado previamente DNS.
- Tener habilitado los servicios necesarios (httpd).

7.8.3.1 CONFIGURACIÓN EN LINUX

Antes de comenzar con la configuración del archivo, se debe verificar si está instalado el paquete con el comando `rpm -q httpd`.

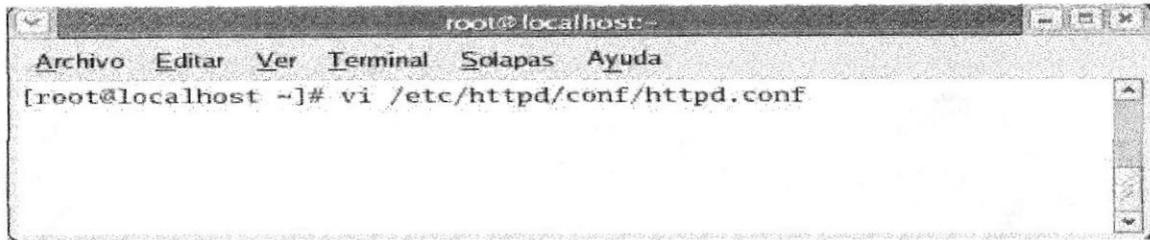


```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost ~]# rpm -q httpd
httpd-2.0.52-3
[root@localhost ~]#
  
```

Figura 7-109: Pantalla verificación del paquete

Para comenzar a editar el archivo de configuración de `httpd.conf` hacerlo con el comando `vi` en la siguiente ruta:



```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost ~]# vi /etc/httpd/conf/httpd.conf
  
```

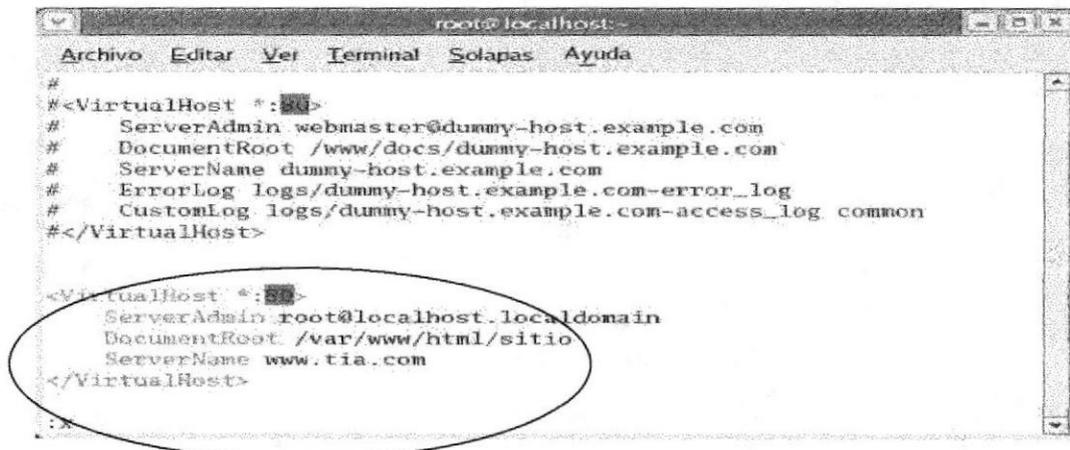
Figura 7-110: Ruta del `httpd.conf`

Luego de haber ingresado al archivo `httpd.conf`, ubicarse en la última parte del archivo y proceder a agregar las siguientes líneas.

ServerAdmin: Es aquel donde se especifica el nombre del equipo y del usuario.

DocumentRoot: Es aquel donde se crea la carpeta en donde se va a alojar el sitio Web de prueba.

ServerName: En esta línea se especifica la dirección de la página Web.



```

#
#<VirtualHost *:80>
#   ServerAdmin webmaster@dummy-host.example.com
#   DocumentRoot /www/docs/dummy-host.example.com
#   ServerName dummy-host.example.com
#   ErrorLog logs/dummy-host.example.com-error_log
#   CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>

<VirtualHost *:80>
  ServerAdmin root@localhost.localdomain
  DocumentRoot /var/www/html/sitio
  ServerName www.tia.com
</VirtualHost>
:~
  
```

Figura 7-111: Texto agregado

Después de haber agregado las líneas de configuración en el archivo httpd.conf, proceder a crear el directorio al cual va a contener el sitio Web en la siguiente ruta.

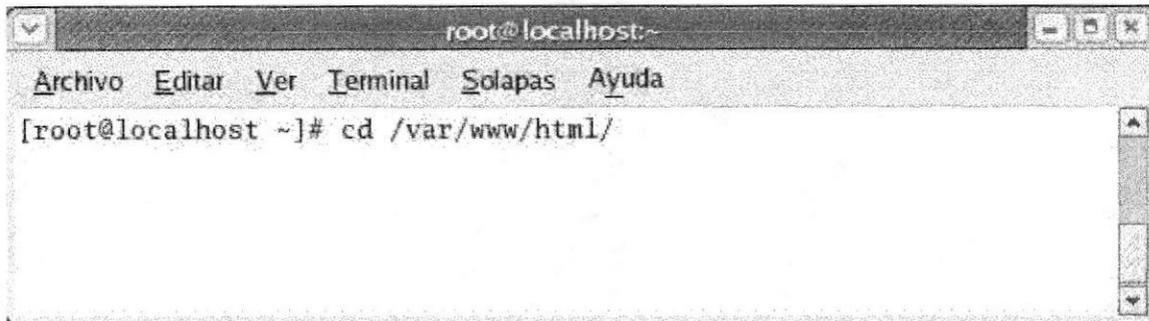


Figura 7-112: Ruta para crear directorio

Después de ingresar a la ruta donde se alojará el sitio Web crear un directorio con el comando mkdir.

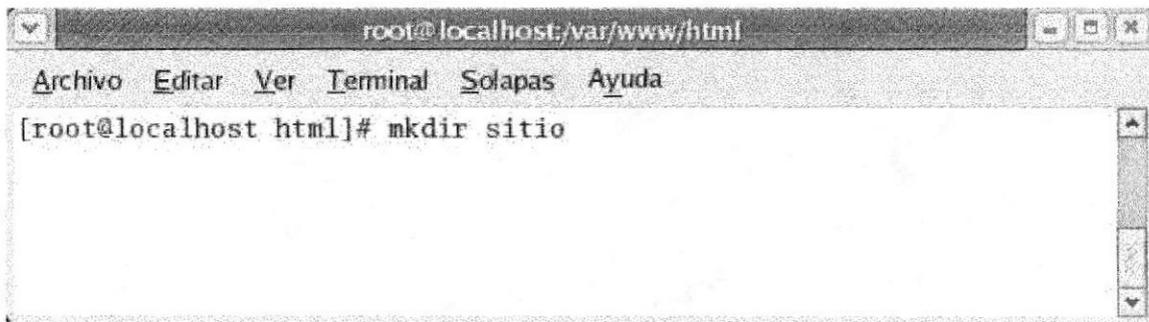


Figura 7-113: Creación de carpeta sitio

Una vez creado el directorio se procede a ingresar para crear la página de prueba.

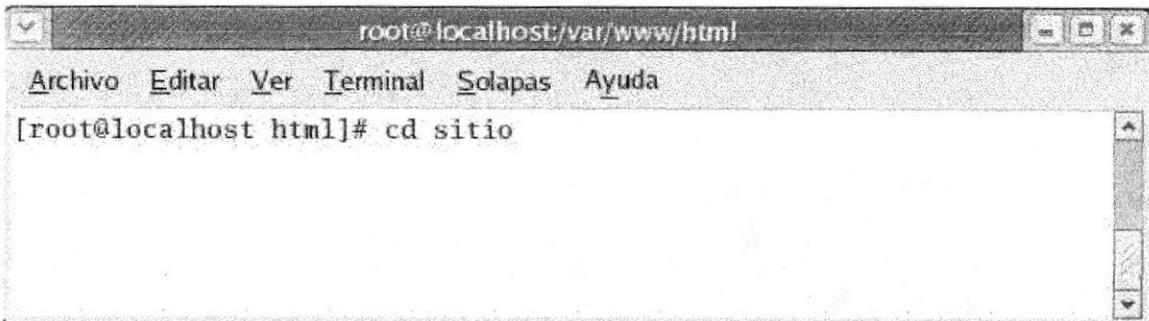


Figura 7-114: Ingresar al sitio



Luego crear un archivo con el nombre index.html el cual será la página de prueba.

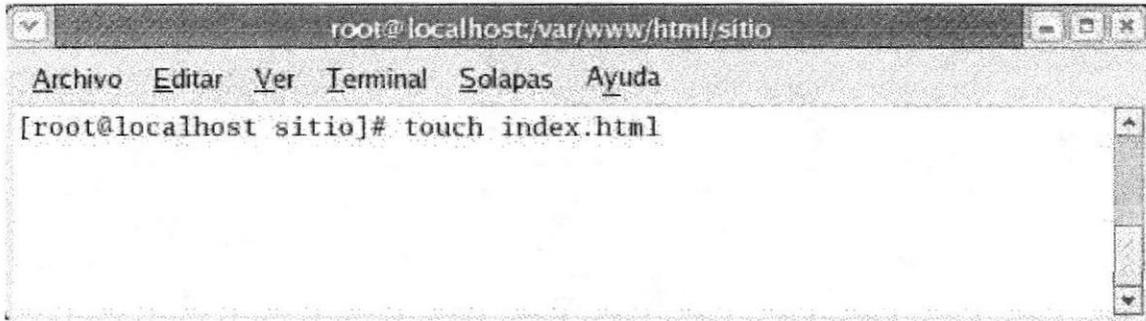


Figura 7-115: Creación del archivo index

Luego proceder a editar dicho archivo con el comando vi.

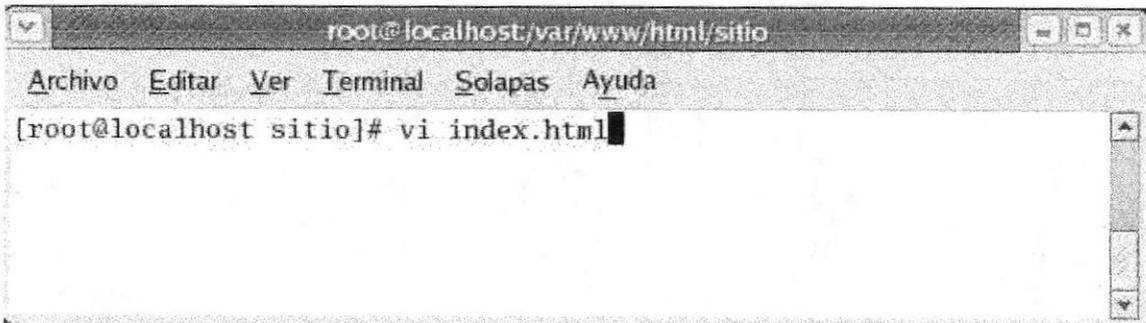


Figura 7-116: Editar archivo

Dentro del archivo index.html agregar un mensaje descriptivo para la prueba, el cual mostrará el navegador web.

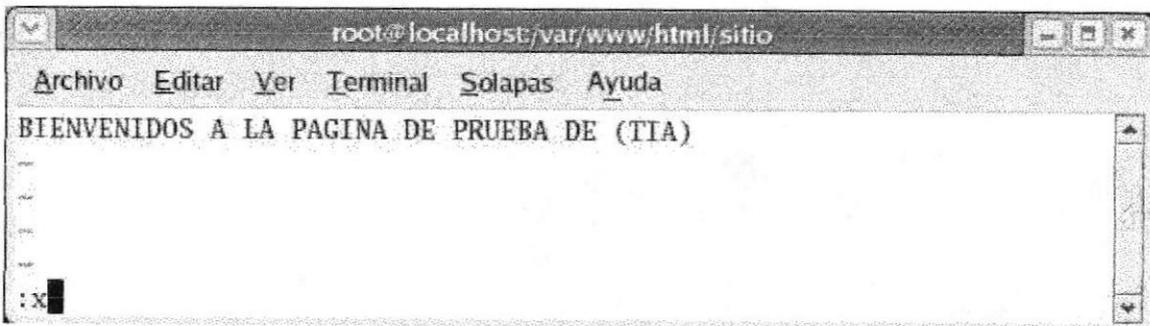


Figura 7-117: Agregar texto

Para levantar el servicio apache hacerlo con el comando `service httpd start`.

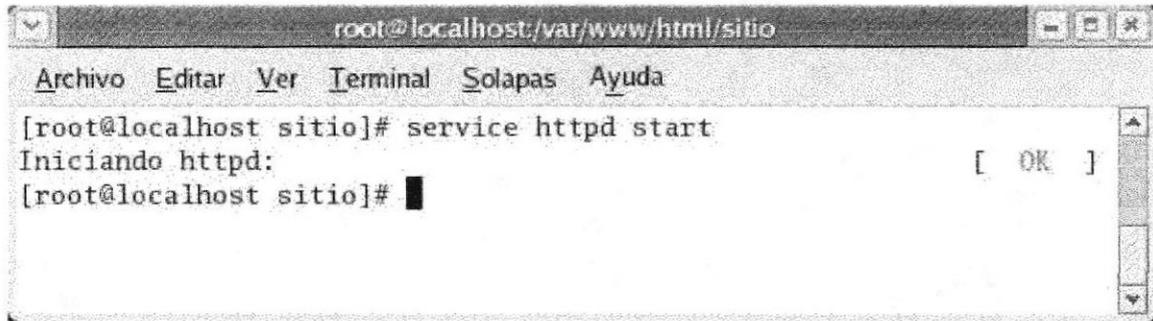


Figura 7-118: Restaurar el servicio

7.8.3.2 CONFIGURACIÓN EN EL CLIENTE WINDOW

Para realizar la prueba en el cliente Windows dar doble clic sobre el icono de Internet Explorer.

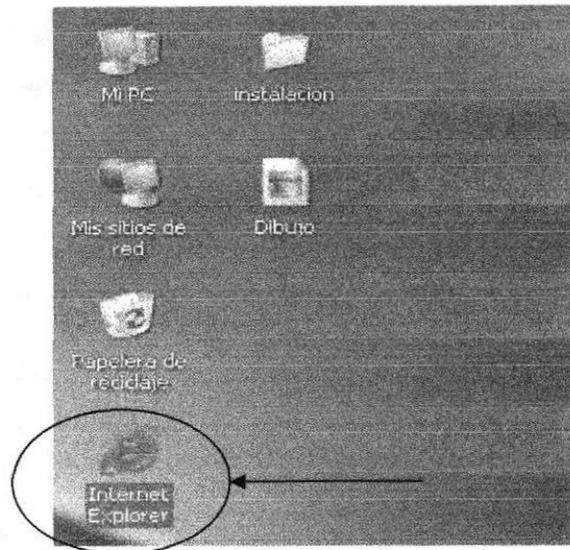


Figura 7-119: Internet Explorer

En la barra de direcciones del explorador, escribir la dirección de el dominio y deberá mostrar algo como esto.

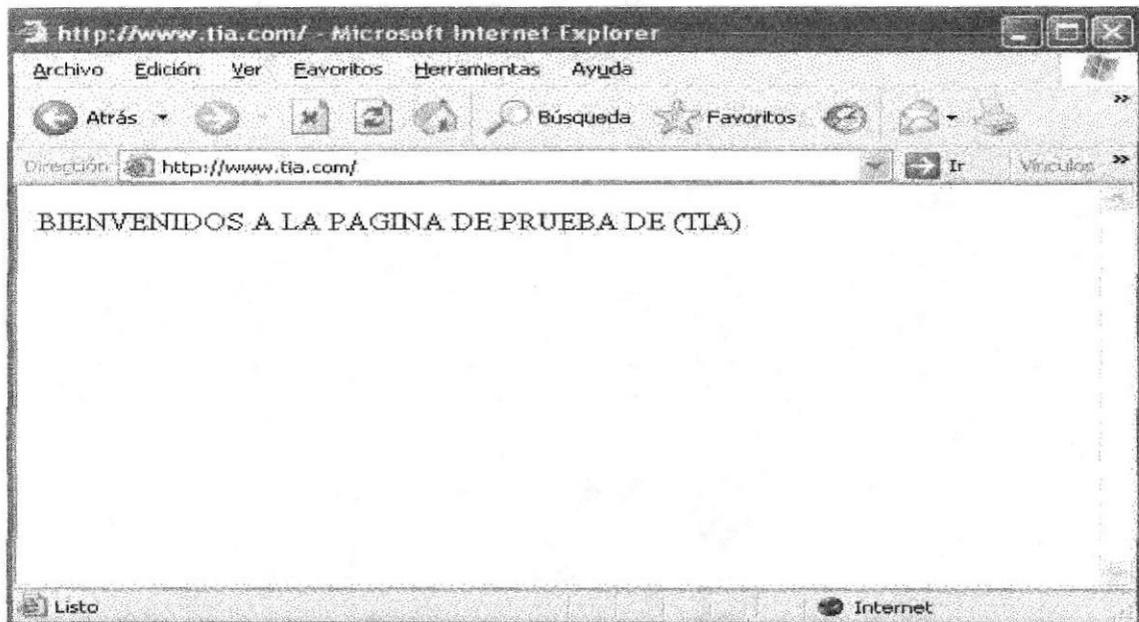


Figura 7-120: Bienvenida

7.8.4 CONFIGURACIÓN DEL SERVIDOR PROXY

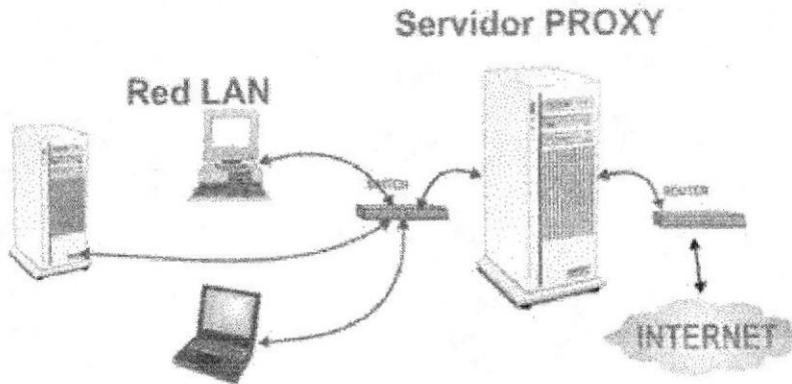


Figura 7-121: Pantalla esquema Proxy

Un **Servidor Intermediario** (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. Durante el proceso ocurre lo siguiente:

Cliente se conecta hacia un **Servidor Intermediario** (Proxy).

Cliente solicita una conexión, fichero u otro recurso disponible en un servidor distinto.

Servidor Intermediario (Proxy) proporciona el recurso ya sea conectándose hacia el servidor especificado o sirviendo éste desde un caché.

En algunos casos el **Servidor Intermediario** (Proxy) puede alterar la solicitud del cliente o bien la respuesta del servidor para diversos propósitos.

Los **Servidores Intermediarios** (Proxy) generalmente se hacen trabajar simultáneamente como muro cortafuegos operando en el **Nivel de Red**, actuando como filtro de paquetes, como en el caso de **iptables**, o bien operando en el **Nivel de Aplicación**, controlando diversos servicios, como es el caso de **TCP Wrapper**. Dependiendo del contexto, el muro cortafuegos también se conoce como **BPD** o **Border Protección Device** o simplemente **filtro de paquetes**.

Aplique políticas de seguridad

Restrinja la navegación mediante la política que más le guste: combinación usuario/contraseña, restricción de horarios, listas de control de acceso o por dirección de máquina.

Obtenga mayor información

Genere reportes y gráficos de uso para determinar los sitios visitados, y la cantidad de tiempo en cada uno de ellos.

Administre eficientemente la navegación

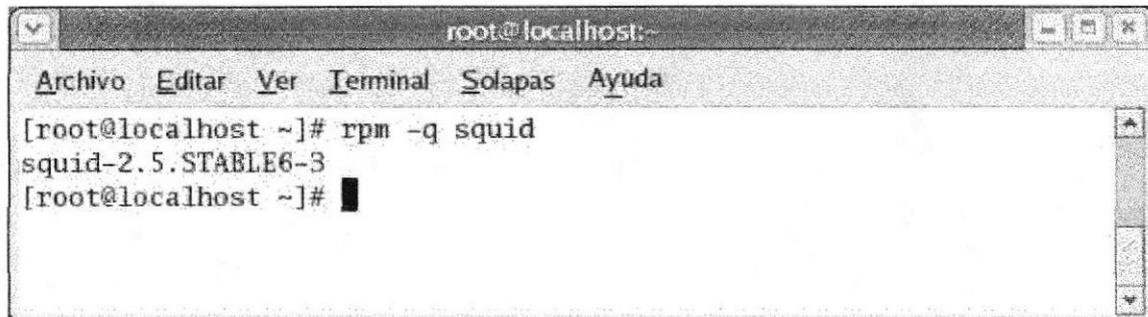
Puede administrar todo lo mencionado anteriormente desde cualquier navegador, a través de una herramienta web intuitiva y amigable. También puede hacerlo desde la línea de comandos si lo desea.

REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR PROXY

- 1 Pc con Linux Fedora Core 3
- 2 Tarjeta de Red
- Tener una IP Estática
- Tener levantado previamente DNS Y WEBSERVER.
- Tener habilitado los servicios.
 - squid-2.5.STABLE1

7.8.4.1 CONFIGURACIÓN PARA LEVANTAR EL SQUID

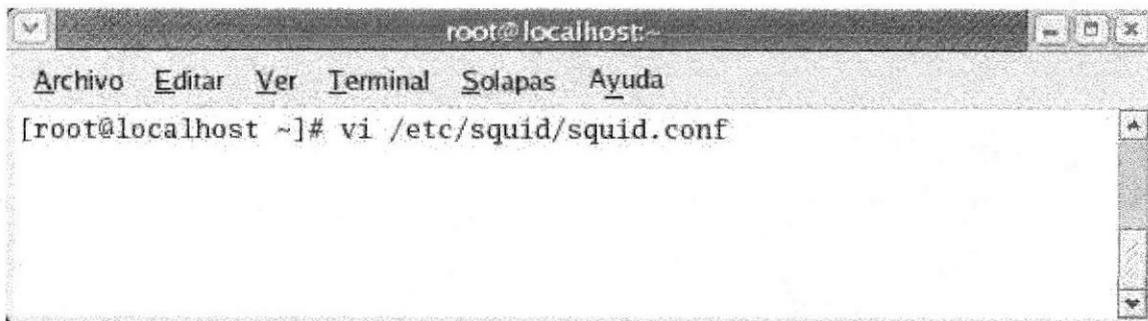
Para empezar con la configuración del Squid, se debe verificar si está instalado el paquete propio de squid.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# rpm -q squid  
squid-2.5.STABLE6-3  
[root@localhost ~]#
```

Figura 7-122: Verificación del squid

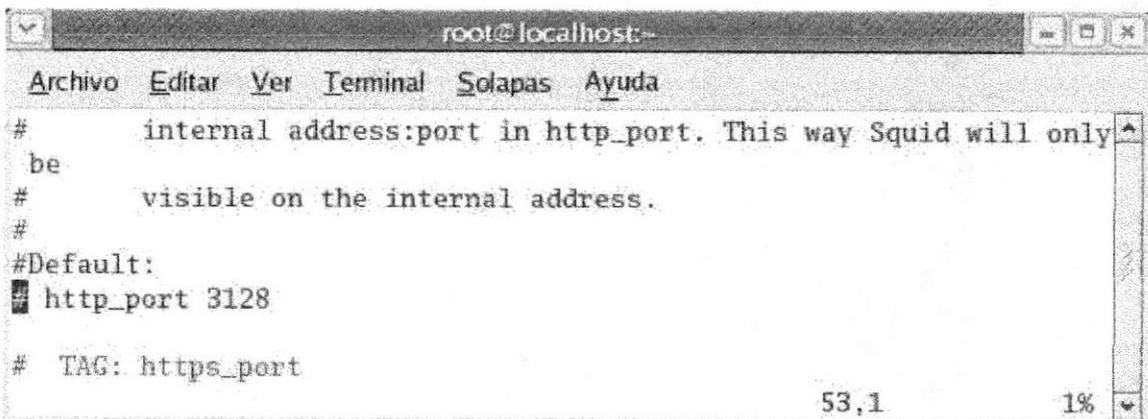
Luego de haber comprobado que está instalado el paquete squid, proceder a editar el archivo squid.conf que se encuentra en etc/squid/ como lo muestra el gráfico.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# vi /etc/squid/squid.conf
```

Figura 7-123: Ruta del squid

Después de haber entrado a la configuración del squid.conf, empezar a configurar, buscar la línea http_port.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
# internal address:port in http_port. This way Squid will only  
be  
# visible on the internal address.  
#  
#Default:  
# http_port 3128  
# TAG: https_port  
53,1 1%
```

Figura 7-124: Squid línea 53

En esta línea proceder a descomentar y cambiar de 3128 a 8080 que es el puerto que permitirá por donde tendrá salida el proxy.

http_port 8080: Es el que habilita el puerto por donde escucha el Servidor.

```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# internal address:port in http_port. This way Squid will only
be
# visible on the internal address.
#
#Default:
http_port 8080
# TAG: https_port
-- INSERTAR --
52,1 1%

```

Figura 7-125: Squid línea 52

Luego de haber habilitado el puerto buscar la línea `cache_mem`.

cache mem: es donde se establece la memoria caché.

```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
#
#Default:
# cache_mem 8 MB
# TAG: cache_swap_low (percent, 0-100)
482,31-32 14%

```

Figura 7-126: Squid línea 482

En esta línea descomentar y cambiar de 8MB a 16 MB para asignar la memoria virtual del squid.

```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
#
#Default:
cache_mem 16 MB
# TAG: cache_swap_low (percent, 0-100)
-- INSERTAR --
480,1 14%

```

Figura 7-127: Squid línea 480

Después de haber editado las líneas anteriores en el mismo archivo buscar la línea de configuración `cache_dir`.

cache_dir: Es aquel que permite establecer que tamaño desea tener el el disco duro.

```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
#
#Default:
# cache_dir ufs /var/spool/squid 100 16 256
# TAG: cache_access_log
695,2 20%

```

Figura 7-128: Squid línea 695,2

Una vez encontrada la línea de configuración proceder a descomentar, esta línea asigna un espacio en el disco duro para el proxy.

```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
#
#Default:
cache_dir ufs /var/spool/squid 100 16 256
# TAG: cache_access_log
-- INSERTAR --
695,33 20%

```

Figura 7-129: Squid línea 695,33

Luego de editar las líneas de `cache_dir`, ubicarse en la parte de las `acl` donde se agrega la línea para asignar el puerto por donde va a salir.

acl puerto myport 8080: Esta línea es donde se define que puerto va a usarse para el Servidor.

```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
acl puerto myport 8080
# TAG: http_access
# Allowing or Denying access based on defined access lists
#
-- INSERTAR --
1818,1 53%

```

Figura 7-130: Squid línea 1818

Luego de haber editado en las acl proceder a buscar y agregar la línea `http_access allow puerto`, donde se declara el mismo nombre de las acl, en esta listas se definen que lista de control tendrán acceso a Internet.

```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks

# And finally deny all other access to this proxy
http_access allow puerto
http_access allow localhost
http_access deny all

-- INSERTAR --                               1864,25           55%

```

Figura 7-131: Squid línea 1864

Luego volver a las acl y declarar el segmento de red, para poder dar Internet a todo el segmento de red, agregar la siguiente línea.

`acl mired src 192.168.7.0/255.255.255.0`: en esta línea definir el segmento de red que va a tener acceso a Internet.

```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
acl puerto myport 8080
acl mired src 192.168.7.0/255.255.255.0
# TAG: http_access
# Allowing or Denying access based on defined access lists
#

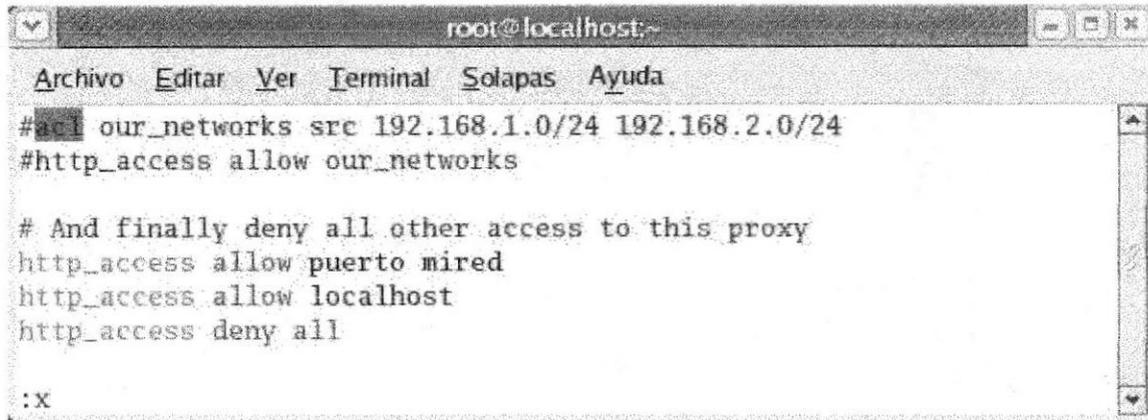
-- INSERTAR --                               1818,40           53%

```

Figura 7-132: Squid línea 1818



Luego de haber asignado el puerto por donde va a salir y dar acceso a toda la red ir a las `http_access` y en la misma línea creada agregar el nombre creado en las `acl`, guardar los cambios y salir.



```

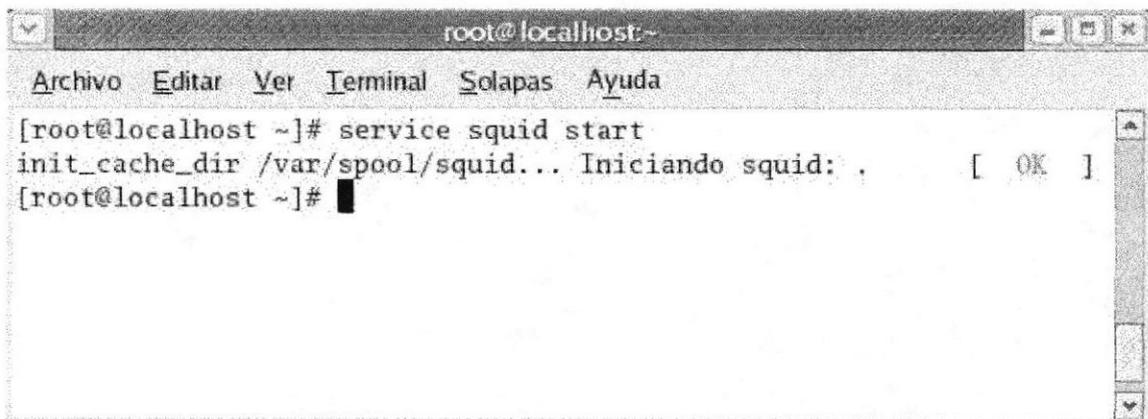
root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks

# And finally deny all other access to this proxy
http_access allow puerto mired
http_access allow localhost
http_access deny all

:x
  
```

Figura 7-133: Access

En esta parte para poder levantar la configuración que ha realizado, hacerlo con el comando `service squid start`.



```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# service squid start
init_cache_dir /var/spool/squid... Iniciando squid: . [ OK ]
[root@localhost ~]#
  
```

Figura 7-134: Restauración del servicio



7.8.4.1 CONFIGURACIÓN EN EL CLIENTE WINDOWS

En el lado del cliente realizar las siguientes configuraciones:

Ingresar al Explorador de Windows, Herramientas, opciones de Internet como se puede en la siguiente gráfica.

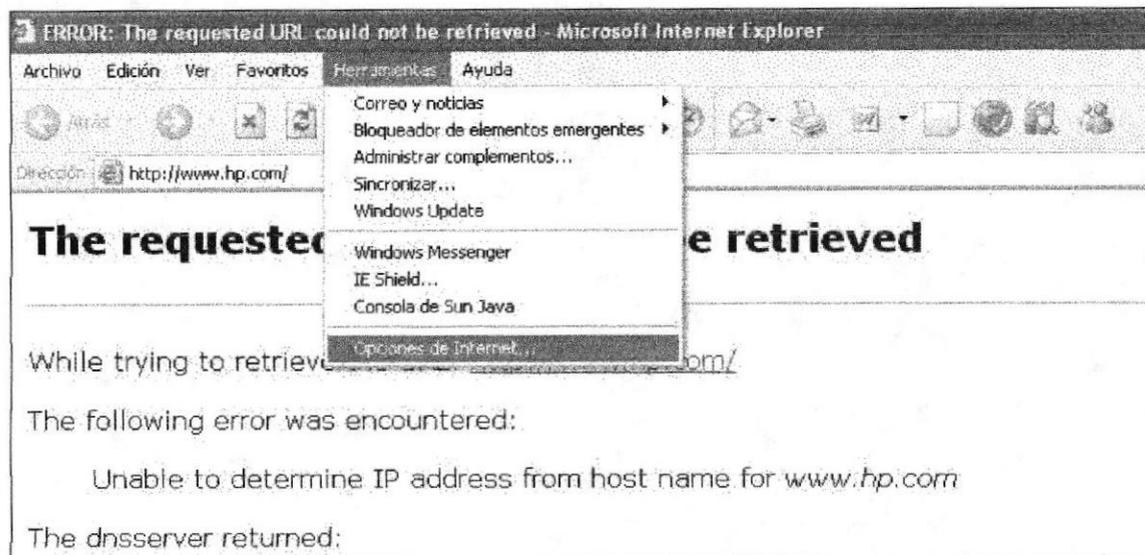


Figura 7-135: Opción de Internet

Dentro de opciones de Internet escoger la pestaña “conexiones”, configuración de la red LAN como se puede observar en la grafica.

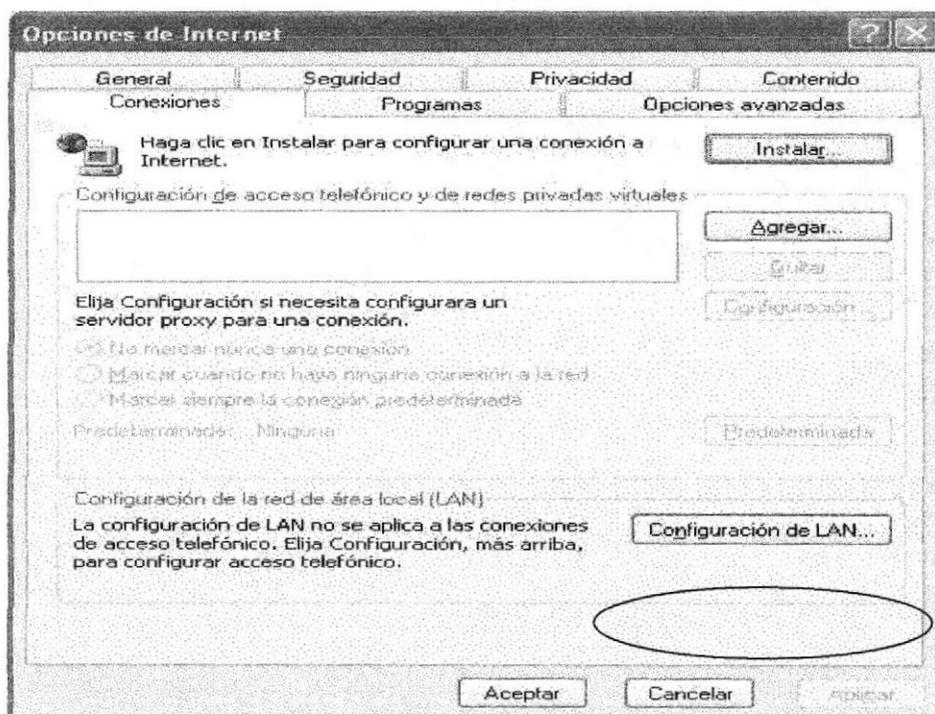


Figura 7-136: Configuración LAN



BIBLIOTECA
CAMPUS
PEÑAS

Aquí seleccionar Configuración LAN donde se digitará la dirección del servidor y el Puerto de comunicación en este caso para Proxy es el 8080, luego aceptar y guardar los cambios.

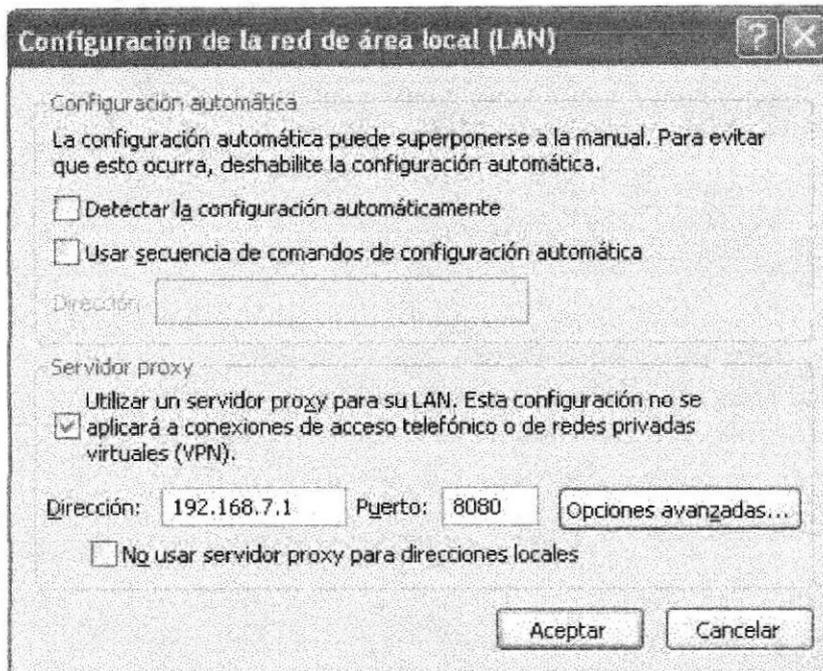


Figura 7-137: Configuración de la red LAN

Para hacer la comprobación cargar en el explorador el dominio o dirección Web.

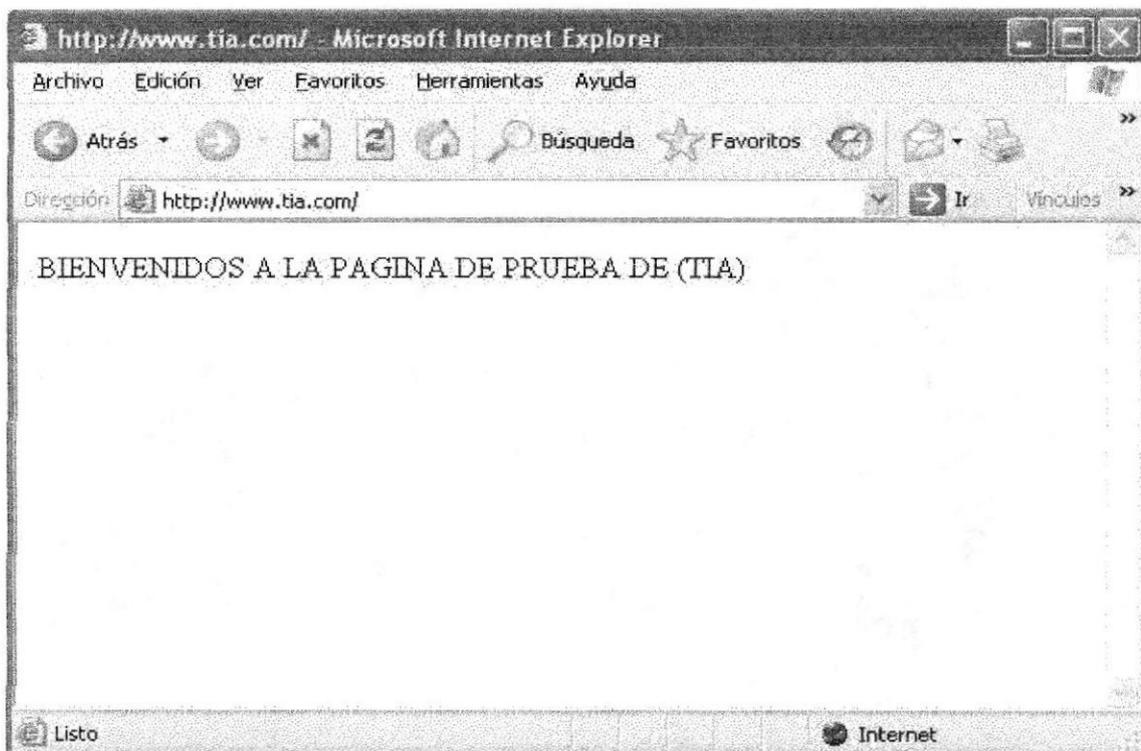


Figura 7-138: Dirección web

RESTRINCIONES POR HORARIO

Los días están determinados por las letras los cuales son los siguientes:

- Lunes M
 - Martes T
 - Miércoles W
 - Jueves H
 - Viernes F
 - Sábado A
 - Domingo S
- Pueden combinarse los días

La hora inicio y hora fin debe ser asignados en formato 24:00

Para poder empezar a configurar por horario se debe digitar el archivo de configuración squid.conf, como lo muestra la gráfica.

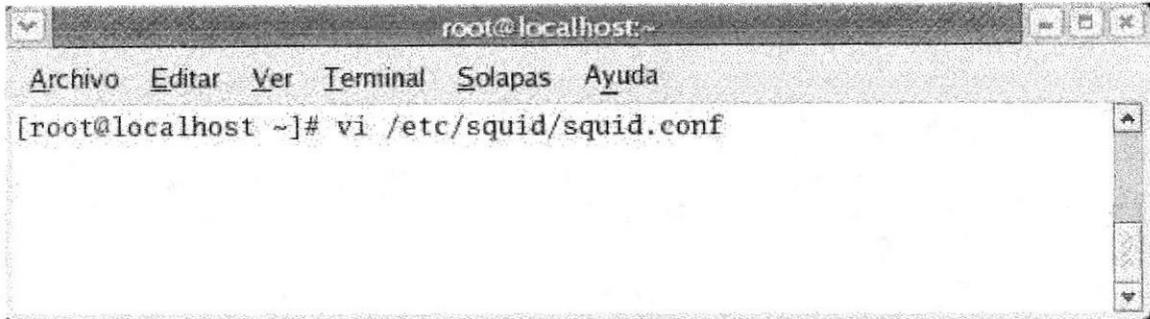


Figura 7-139: Ruta squid.conf

En la parte de las acl, proceder a crear una línea donde se asignará el rango de días y horas que va a denegar.

acl horario time MTWHF 17:35-18:00: Esta línea permite denegar el acceso a Internet mediante la hora del Servidor.

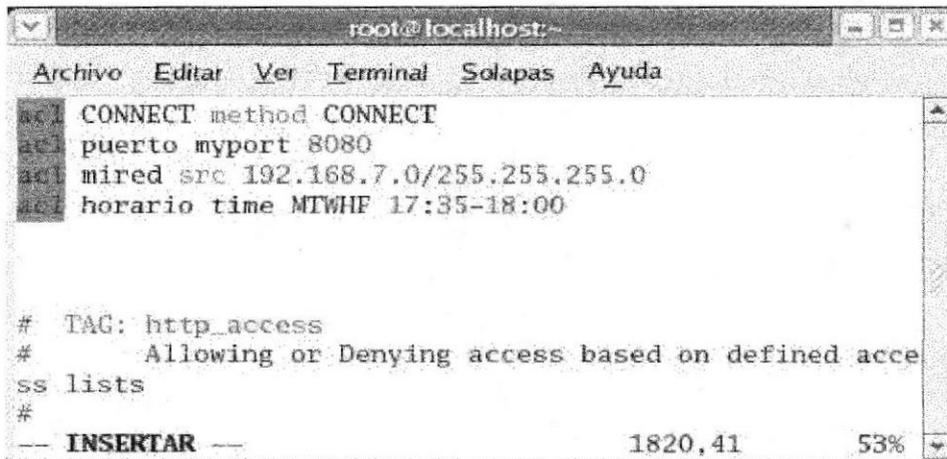


Figura 7-140: Sección acl

Luego de haber insertado la línea en las acl, ir a las http_access donde se agregará el nombre de la acl creada, guardar los cambios y salir.

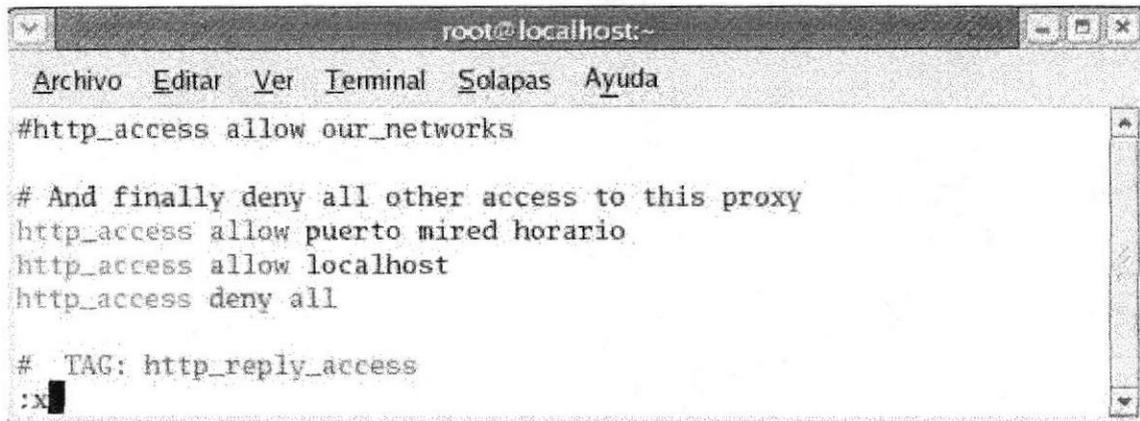


Figura 7-141: Sección http

Luego de denegar por horario levantar el servicio squid, cabe indicar que cada configuración que realice debe levantar el servicio para que tome efecto.

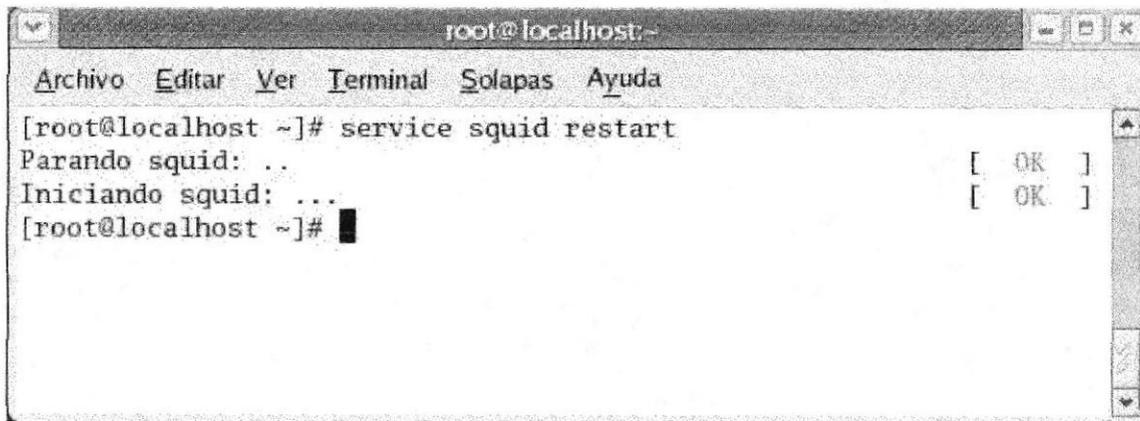


Figura 7-142: Restauración squid

Luego de haber levantado el servicio, ir al equipo cliente para verificar si está bien hecha la configuración, debe salir una ventana muy parecida a esta.

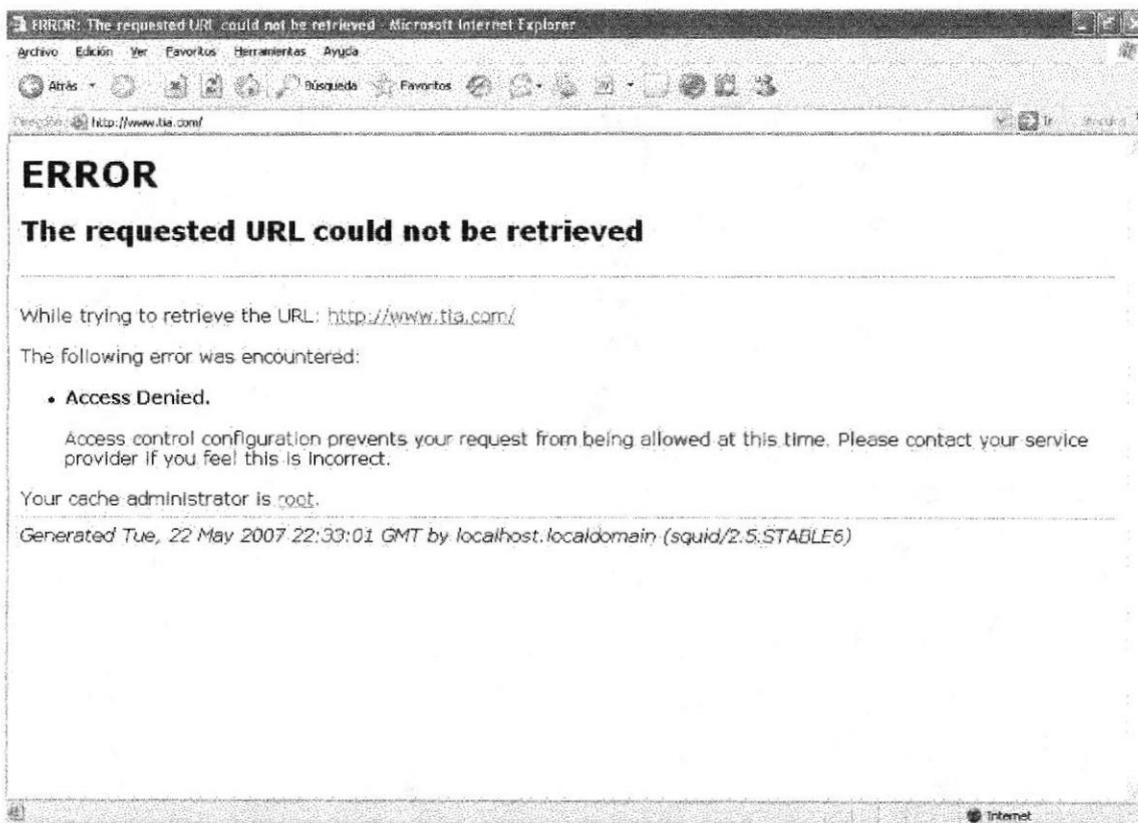
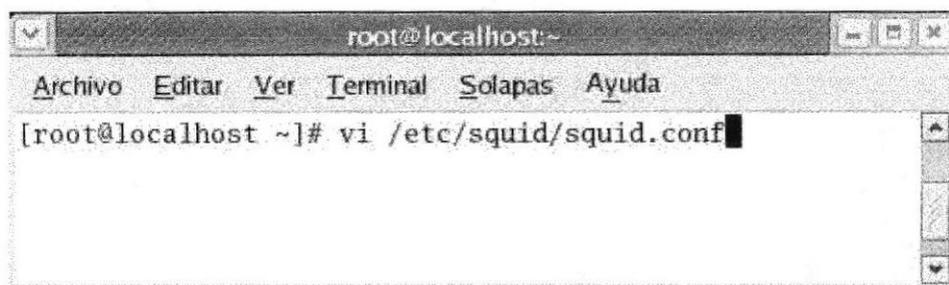


Figura 7-143: Verificación

RESTRICION POR PÁGINAS PROHIBIDAS

Para poder empezar a configurar por bloqueo de página deberá digitar el archivo de configuración squid.conf, como lo muestra la gráfica.

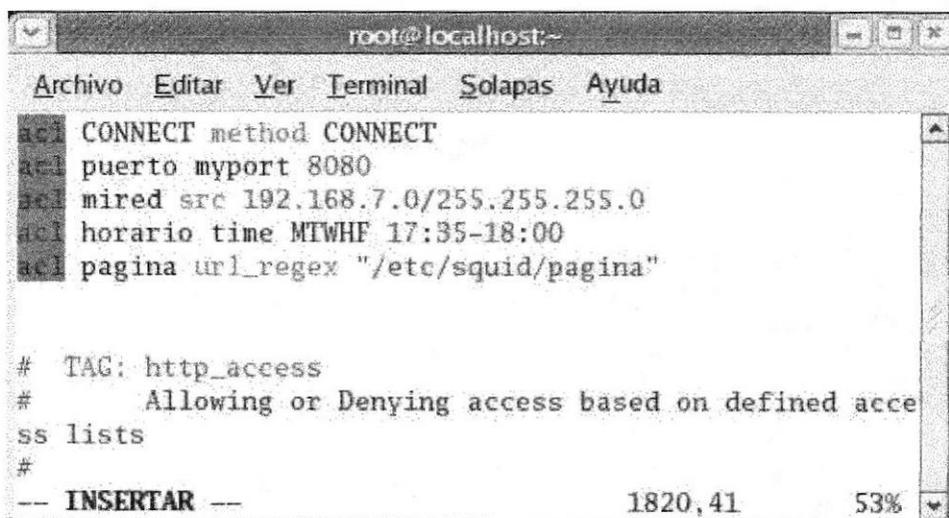


```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# vi /etc/squid/squid.conf
```

Figura 7-144: Ruta squid

Luego de haber ingresado a la configuración del squid agregar la línea en la cual agregar una lista de páginas a las cuales no deben tener acceso los clientes.

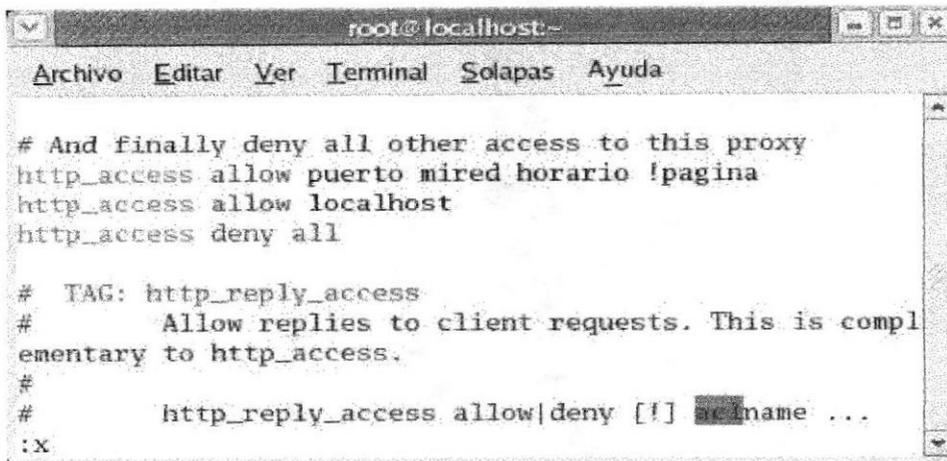
acl pagina url_regex "/etc/squid/pagina": Esta línea declarar una ruta donde se guardarán las direcciones Web que no se desea tener acceso.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
acl CONNECT method CONNECT  
acl puerto myport 8080  
acl mired src 192.168.7.0/255.255.255.0  
acl horario time MTWHF 17:35-18:00  
acl pagina url_regex "/etc/squid/pagina"  
  
# TAG: http_access  
# Allowing or Denying access based on defined access lists  
#  
-- INSERTAR -- 1820, 41 53%
```

Figura 7-145: Sección acl

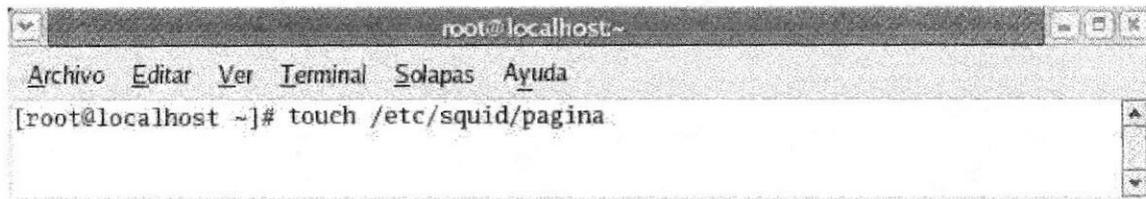
Después de haber asignado en las acl la ruta proceder a denegar el nombre asignado en las acl, guardar los cambios y salir.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
# And finally deny all other access to this proxy  
http_access allow puerto mired horario !pagina  
http_access allow localhost  
http_access deny all  
  
# TAG: http_reply_access  
# Allow replies to client requests. This is complementary to http_access.  
# http_reply_access allow|deny [!] ac:iname ...  
:x
```

Figura 7-147: Sección http

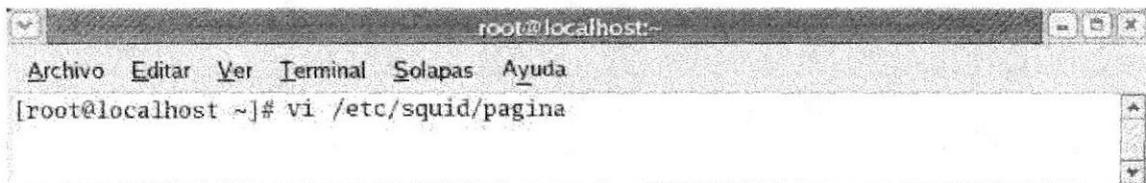
Luego de haber guardado los cambios, crear un archivo con la ruta dada en las acl, crear el archivo con el comando touch, como lo muestra la gráfica.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# touch /etc/squid/pagina
```

Figura 7-148: Creación pagina

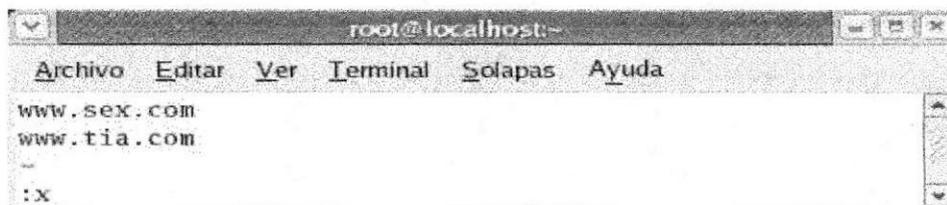
Luego proceder a editar el archivo, en el cual agregar la lista de direcciones web que no se deben cargar.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# vi /etc/squid/pagina
```

Figura 7-149: Editar pagina

Agregar la lista de direcciones web a la cual no debe el cliente tener acceso.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
www.sex.com  
www.tia.com  
~  
:x
```

Figura 7-150: Lista de direcciones



Luego de haber editado el archivo donde se alojarán las páginas negadas, reiniciar el servicio squid.

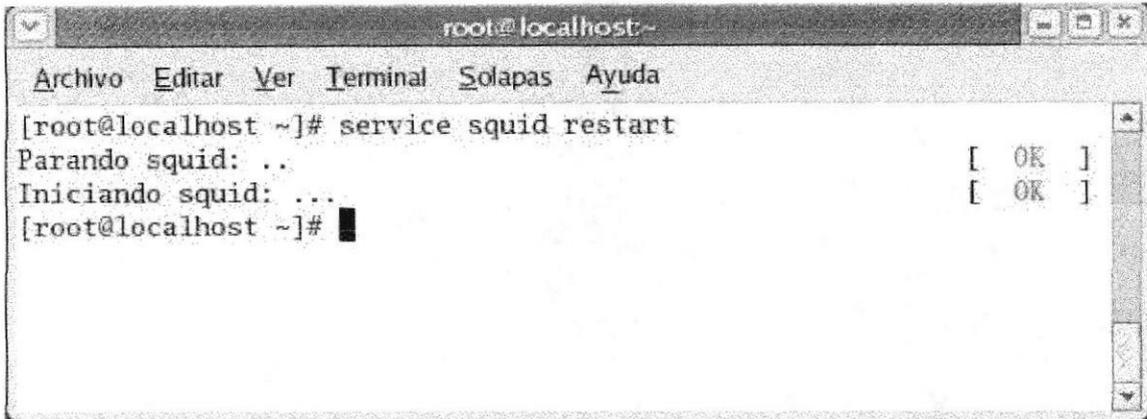


Figura 7-151: Restauración del servicio

Luego de haber levantado el servicio squid, proceder a abrir el explorador de Windows para cargar la página, debe salir una pantalla como esta.

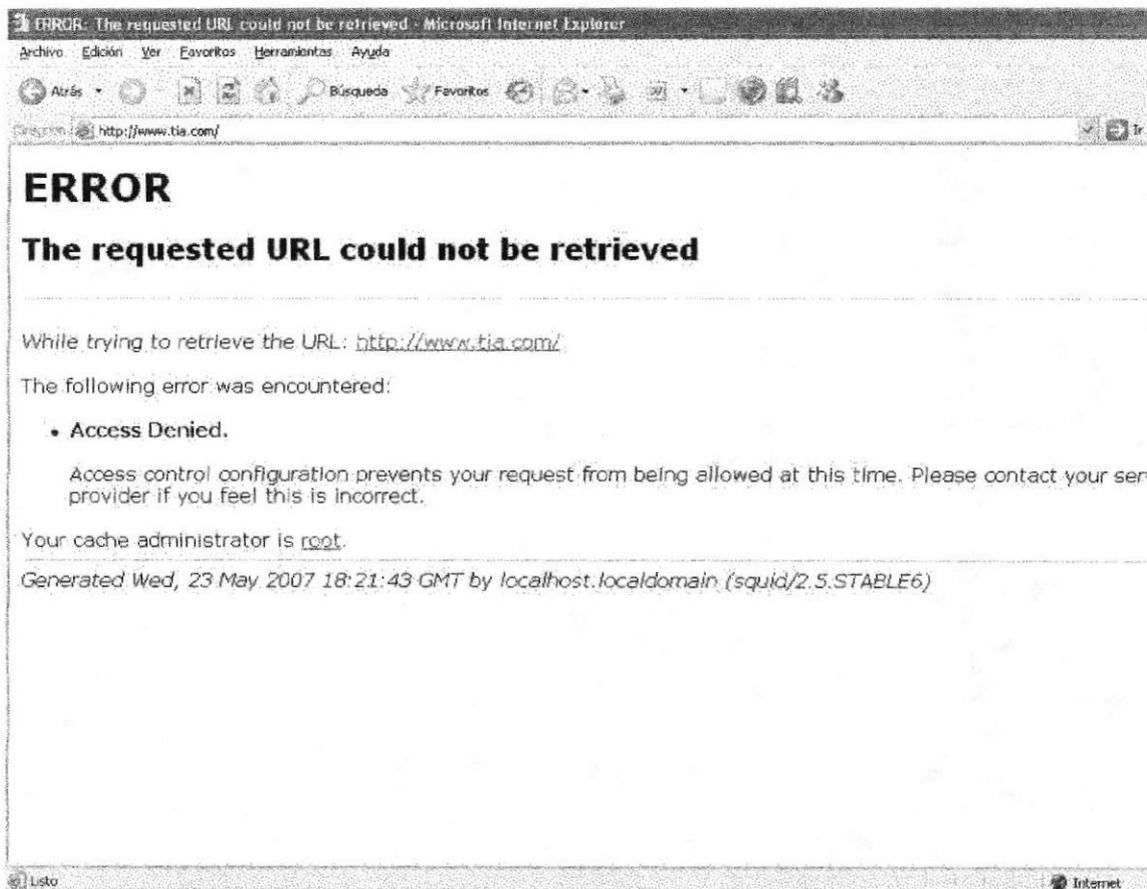


Figura 7-152: Internet explorer

userdel	userdel jonathan	Sirve para borrar los usuarios de sistema creados.
mount	mount media/cdrom	Sirve para poder montar o tener acceso a unidades como cdrom, diskettes, disco duros.
umount	umount media/cdrom	Sirve para desmontar las unidades como cdrom, diskettes, disco duro
find	find jonathan.txt	Sirve como buscador de ficheros con demasiados parámetros
lsmod	lsmod	Muestra los modulos de kernel que estan cargados.
mv	mv jonathan/baquero	Sirve para mover o renombrar ficheros/directorios.

Tabla 7-1: Comandos Básicos



x	:x	sale y guarda cambios desde el editor
q!	q!	Este comando sale de un fichero sin guardar cambios realizados
i	i	Este comando inserta, indica al fichero que se comenzará a escribir en el.
p	p	esta tecla pega líneas copiadas con anterioridad
yy + numero	yy jonathan o yy 5	copia un número de líneas, especificado con anterioridad
chmod	chmod +777 /jonathan chmod +777 /jonathan/deber.txt	Este comando da permisos de lectura, escritura a cualquier archivo especificado
service <servicio> start	service squid start	Sirve para levantar un servicio.
rpm -q	rpm -q samba	Sirve para verificar si están instalados los paquetes.
slocate	slocate /etc/jonathan.txt	Sirve para buscar archivo, directorios.
rmdir	rmdir jonathan	Sirve para borrar directorios
date	date	Sirve para ver y poder configurar la fecha actual.
gunzip	gunzip jonathan.txt	Sirve para descomprimir archivos compatibles con zip.
mail	Mail	Sirve para enviar y leer correo electrónico.

7.6 COMANDOS BASICOS DE LINUX FEDORA CORE 3

COMANDO	SINTAXIS	DESCRIPCIÓN
adduser	adduser jonathan	crea usuario
cd	cd /etc	entrar a un directorio
clear	clear	limpiar pantalla
cp	cp localhost.zone tia.com	copia de un archivo con otro nombre
ifconfig	ifconfig	verifica si esta habilitada la ip del servidor
ls	ls	muestra información sobre los archivos
mkdir	mkdir jonathan	crea directorios
chown	chown root:root jonathan	para dar los permisos de usuario
passwd	passwd jonathan	crea una contraseña
ping	ping 192.168.7.1	mensaje de prueba para verificar el estado de la tarjeta de red
telnet	telnet 192.168.7.1	Permite conectarse de forma remota a cualquier pc especificando la dirección IP
touch	touch deber.txt	crea archivos
vi	vi deber.txt	edita el contenido de un archivo
wq	:wq	sale y guarda cambios desde el editor



BIBLIOTECA
CAMPUS
PEÑAS

AUTENTIFICACIÓN

Para poder empezar a configurar por autenticación deberá digitar el archivo de configuración squid.conf, como lo muestra la gráfica.

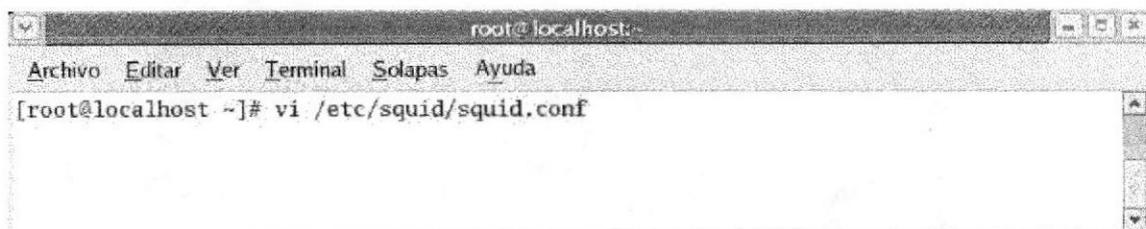


Figura 7-153: Ruta del squid

Luego de haber ingresado al archivo de configuración del squid, buscar la línea auth_param.

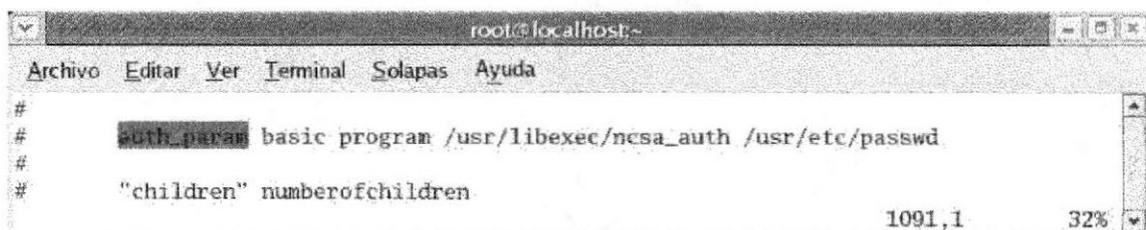


Figura 7-154: Squid línea 1091

Luego de haber encontrado la línea auth_param, copiar y editar esta línea como lo indica la gráfica.

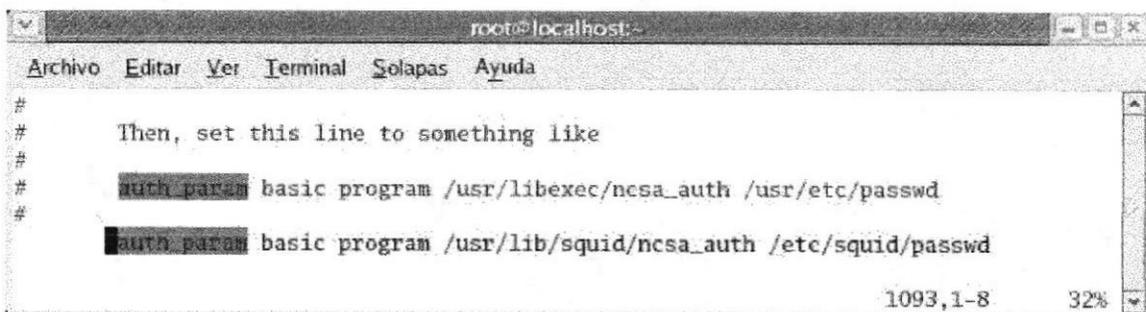


Figura 7-155: Squid línea 1093



Después de haber editado la línea `auth_param`, dirigirse a las `acl` donde insertará la línea para poder realizar la autenticación, cabe indicar que se puede poner un nombre descriptivo en las `acl`.

acl autenticación Proxy auth REQUIRED: Es donde define la autenticación al Proxy.

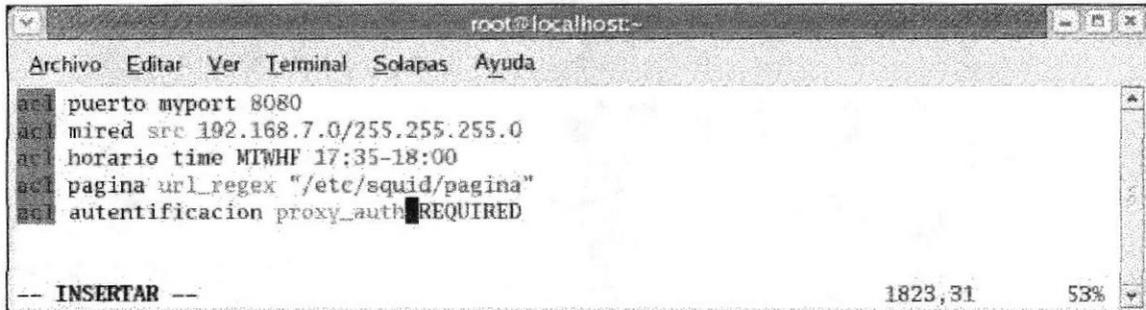


Figura 7-156: Squid línea 1823

Luego ira las `http_access` donde agregará el mismo nombre asignado a las `acl`, guardar los cambios y salir.

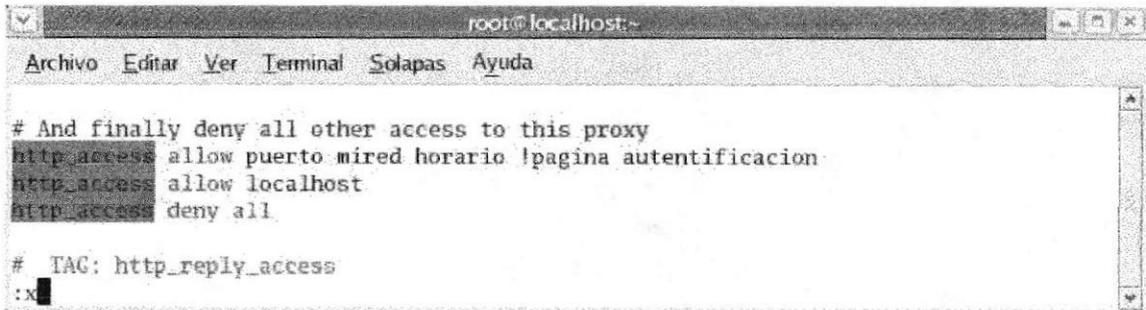


Figura 7-157: Squid sección http

Luego de haber editado el archivo de configuración del squid, proceder a levantar el servicio.

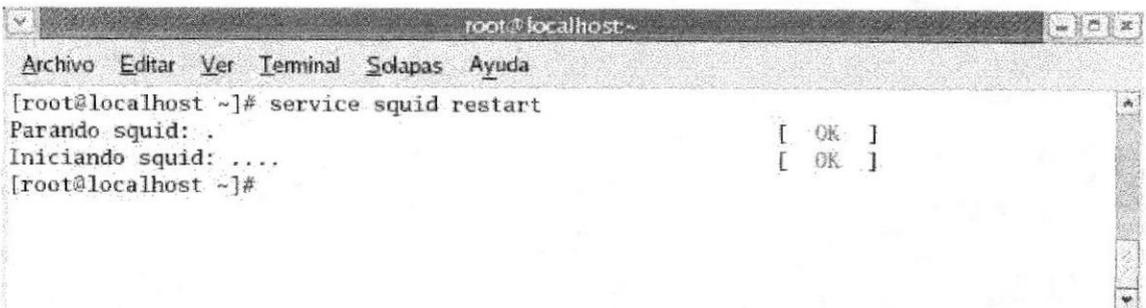


Figura 7-158: Pantalla Restauración squid

Después de levantar el servicio squid, proceder a entrar al directorio squid donde creará el archivo donde se alojará el usuario y contraseña de la autenticación.

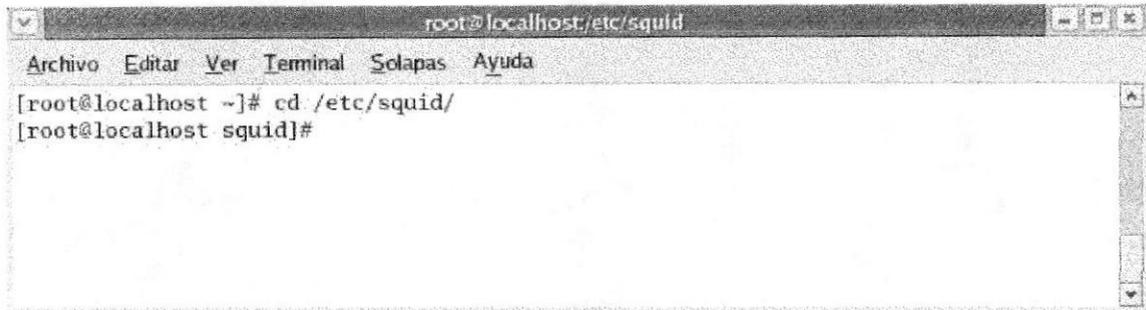


Figura 7-159: Ingreso squid

Crear el archivo con el comando touch, como lo muestra la gráfica.

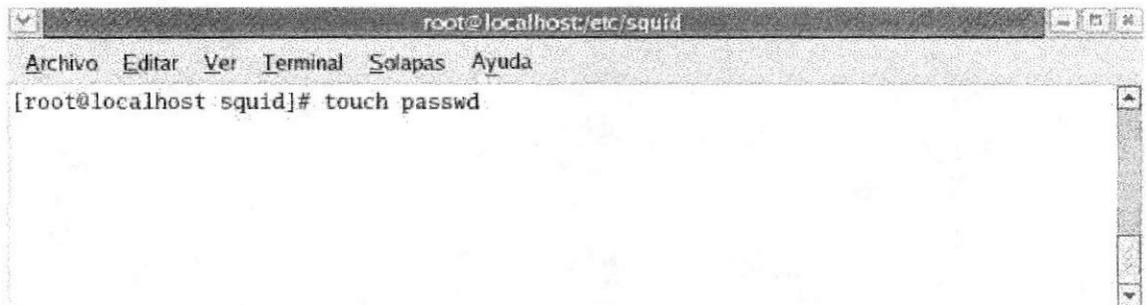


Figura 7-160: Creación del archivo

Luego de haber creado el archivo donde se alojará el usuario y contraseña, proceder a crear el usuario y contraseña de la siguiente manera.

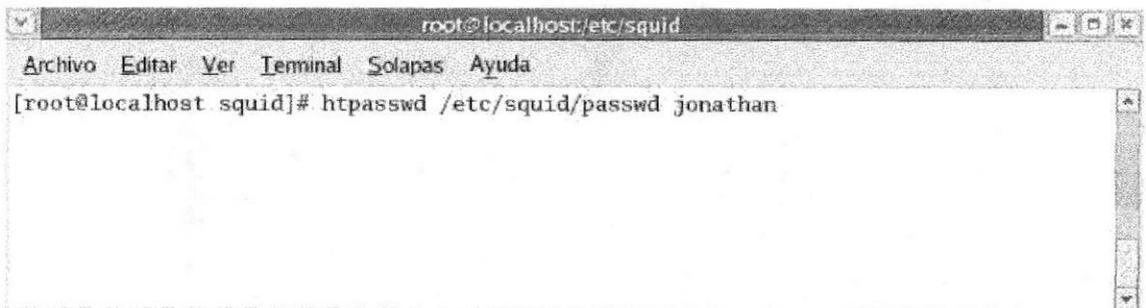


Figura 7-161: Creación usuario



En esta parte asignar la contraseña que se usará al momento de querer cargar el explorador.

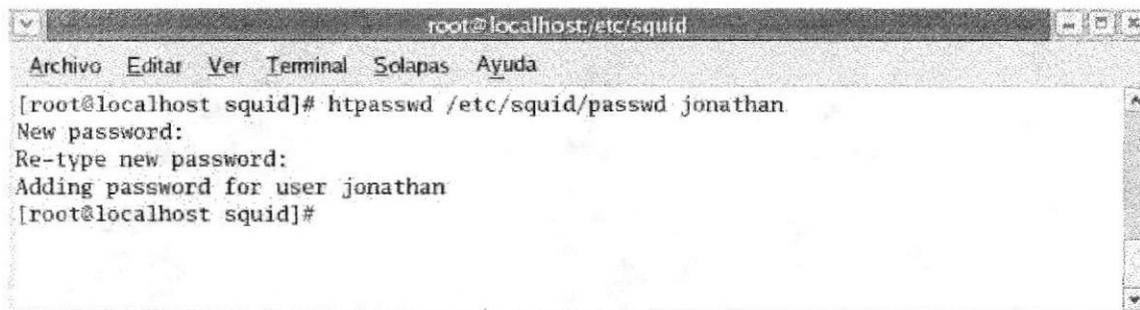


Figura 7-162: Creación contraseña

Al momento de cargar el explorador de Windows pide un usuario y contraseña el cual es la que se creará en el servidor.

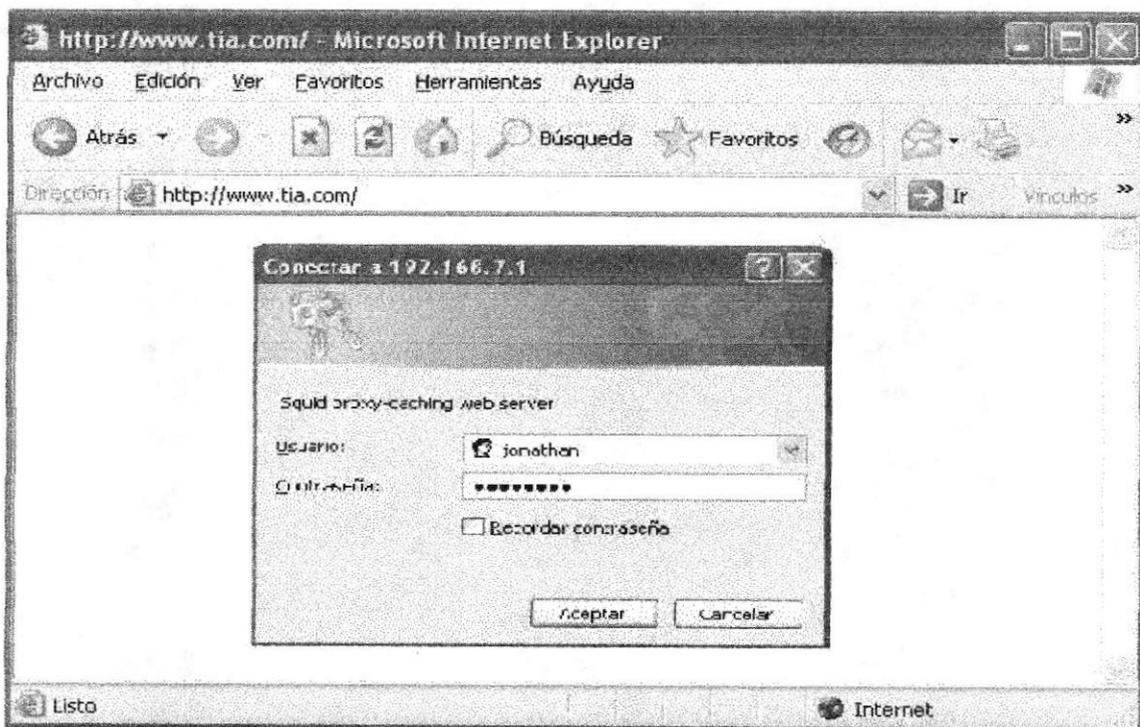


Figura 7-163: Conectar



Luego de haber ingresado el usuario y contraseña debe tener acceso a la página Web solicitada, en este caso debe cargar algo como esto.

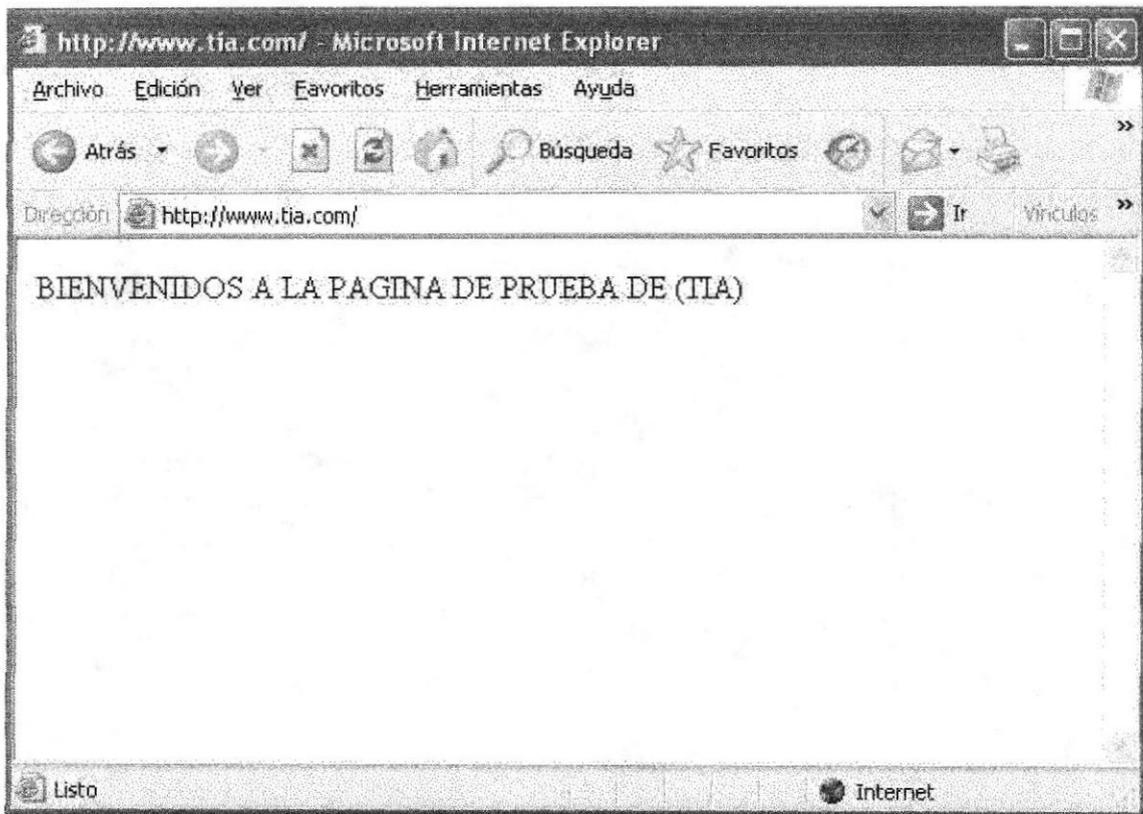


Figura 7-164: Acceso a la página



7.8.5 CONFIGURACIÓN DEL SERVIDOR SENDMAIL

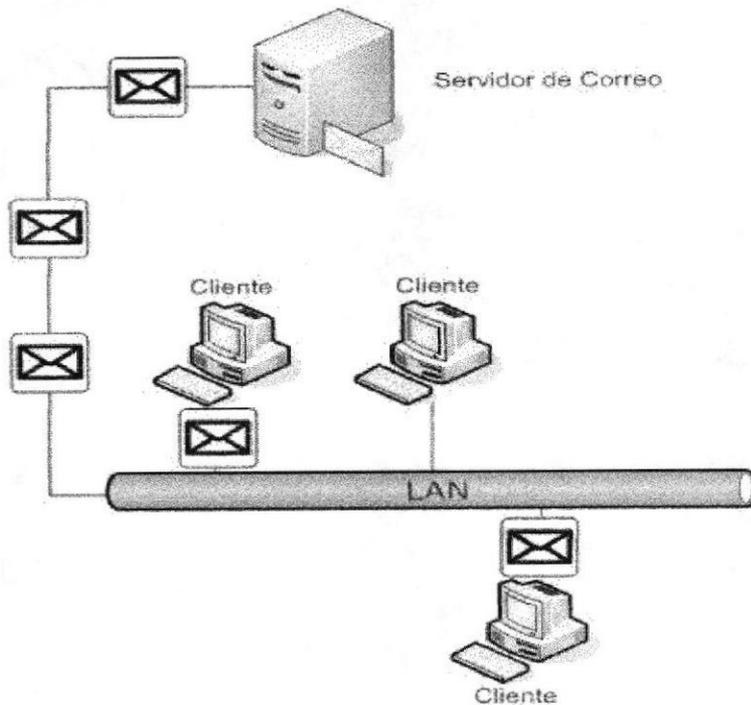


Figura 7-165: Esquema Sendmail

Sendmail es el agente de transporte de correo más común de Internet en los sistemas Linux. Aunque actúa principalmente como MTA (Mail Transport Agent), que son los encargados de transferir los mail a su correcto destino.

Un servidor de correo es una aplicación que nos permite enviar mensajes de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

Para lograrlo se definen una serie de protocolos, cada uno con una finalidad concreta:

SMTP, Simple Mail Transfer Protocol: Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes.

POP, Post Office Protocol: Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

IMAP, Internet Message Access Protocol: Su finalidad es la misma que la de POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes.

Mail Server es un servidor de mail POP3 y SMTP que soporta un número ilimitado de dominios, casillas de mail, y listas de correo.

Sendmail es el agente de transporte de correo más común de Internet en los sistemas Linux. Aunque actúa principalmente como MTA (Mail Transport Agent), que son los encargados de transferir los mail a su correcto destino.

Versatilidad

Desde pequeñas oficinas a grandes empresas, en GNU/Linux hay un servidor de correo para cada necesidad y presupuesto, manteniendo siempre una excelente calidad.

Confiabilidad

"No se cae". Eso es lo que le responde un Administrador de Sistema satisfecho luego de unos pocos meses de probar un servidor de correo corriendo sobre GNU/Linux. Siendo usualmente éste uno de los servicios más castigados, la confiabilidad es fundamental.

Seguridad

IMAP/POP con SSL, SMTP autenticado, claves encriptadas con CRAM-MD5, DIGEST-MD5, Kerberos, NT-Login o POP-before-SMTP.

Lo que quiera en materia de seguridad y control de relay puede ser realizado, siempre con el máximo rendimiento.

Rapidez

En un servidor de correo, la rapidez es fundamental. Largas colas de mensajes pueden saturar hasta el más potente de los servidores. Por eso, los servidores de correo más grandes del mundo utilizan plataformas basadas en GNU/Linux.

Economía

Menor costo de instalación, menor costo de mantenimiento y menor costo medio por usuario (debido a que atiende más usuarios por equipo) hacen de los servidores de correo basados en GNU/Linux la mejor opción.

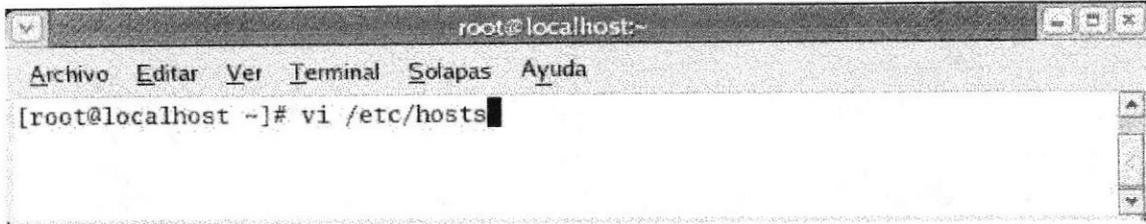
REQUERIMIENTOS PARA CONFIGURAR UN SENDMAIL

- 1 Pc con Linux Fedora Core 3
- 1 Tarjeta de Red
- Tener una IP Estática
- Tener habilitado los servicios necesarios (SendMail y Dovecot).



7.8.5.1 CONFIGURACIÓN DE SENDMAIL EN SERVIDOR LINUX

Para comenzar con la configuración de sendmail debe editar el hosts para dar un nombre descriptivo a el Servidor.

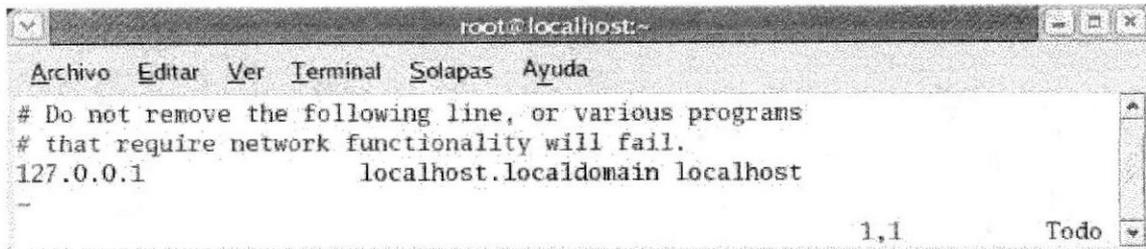


```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# vi /etc/hosts
  
```

Figura 7-166: Creación del archivo

Después de haber ingresado al archivo del hosts aparecerá algo como esto.

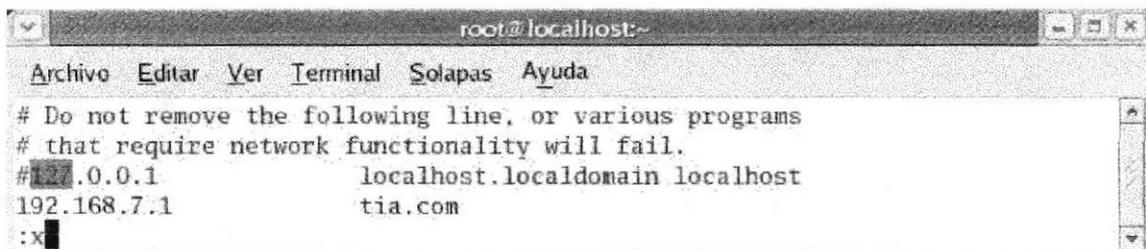


```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1          localhost.localdomain localhost
-
1,1              Todo
  
```

Figura 7-167: Creación del archivo

En esta parte proceder a comentar la dirección loopback y agregar la IP y el nombre del servidor.



```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
# Do not remove the following line, or various programs
# that require network functionality will fail.
#127.0.0.1          localhost.localdomain localhost
192.168.7.1        tia.com
:x
  
```

Figura 7-168: Agregar IP

Después de haber editado el hosts, se procederá a editar el archivo del sendmail.cf que se encuentra en la ruta /etc/mail/ como lo muestra la gráfica.



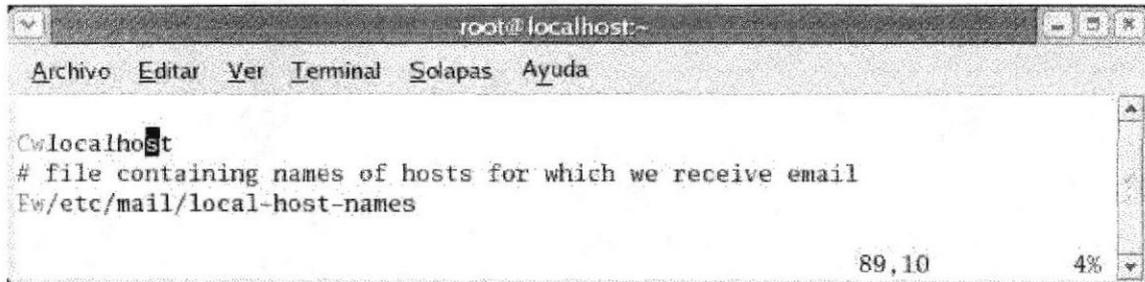
```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# vi /etc/mail/sendmail.cf
  
```

Figura 7-169: Ruta para editar sendmail.cf



Después de haber ingresado al archivo del sendmail, buscar la línea del Cwlocalhost.

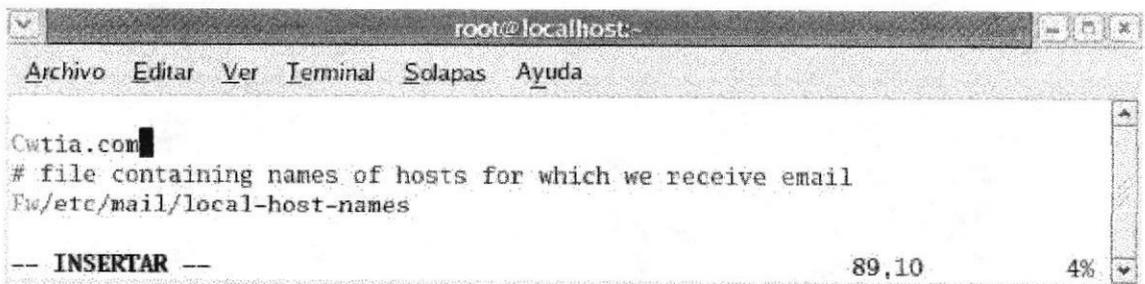


```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
Cwlocalhost
# file containing names of hosts for which we receive email
Fw/etc/mail/local-host-names
89,10  4%
  
```

Figura 7-170: Creación del archivo

Una vez ubicado en la línea Cwlocalhost reemplazará por Cw y nombre del dominio, tal como se encuentra en la pantalla.

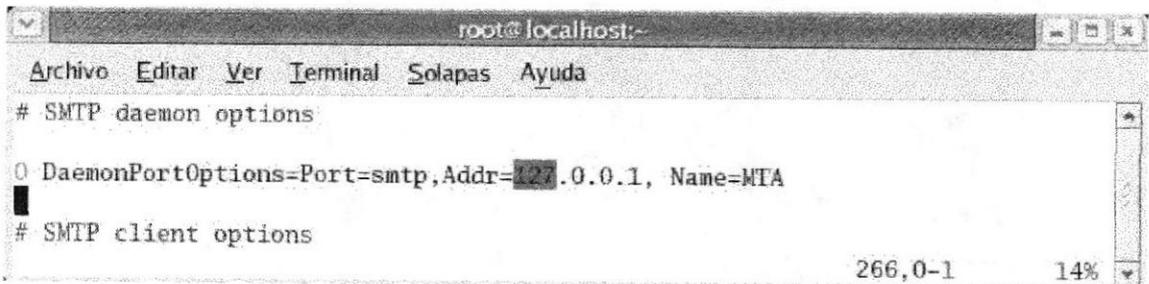


```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
Cwtia.com
# file containing names of hosts for which we receive email
Fw/etc/mail/local-host-names
-- INSERTAR --
89,10  4%
  
```

Figura 7-171: Sendmail línea 89

Luego buscar la línea #SMTP daemon options

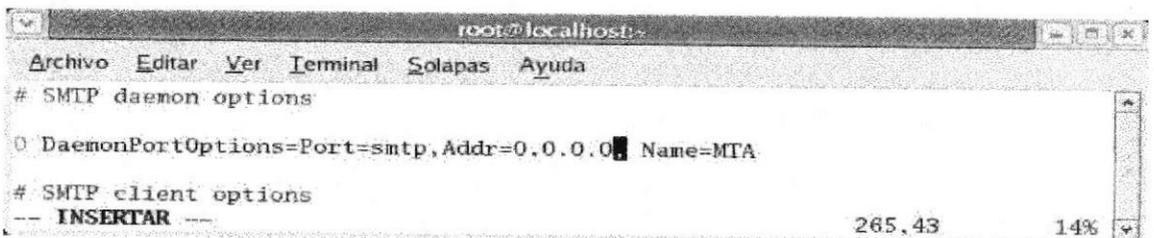


```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# SMTP daemon options
O DaemonPortOptions=Port=smtp,Addr=127.0.0.1, Name=MTA
# SMTP client options
266,0-1  14%
  
```

Figura 7-172: Pantalla sendmail línea 266

Luego de haber encontrado la línea #SMTP daemon options, proceder a cambiar la dirección de la loopback por la 0.0.0.0 tal como se muestra en la figura.

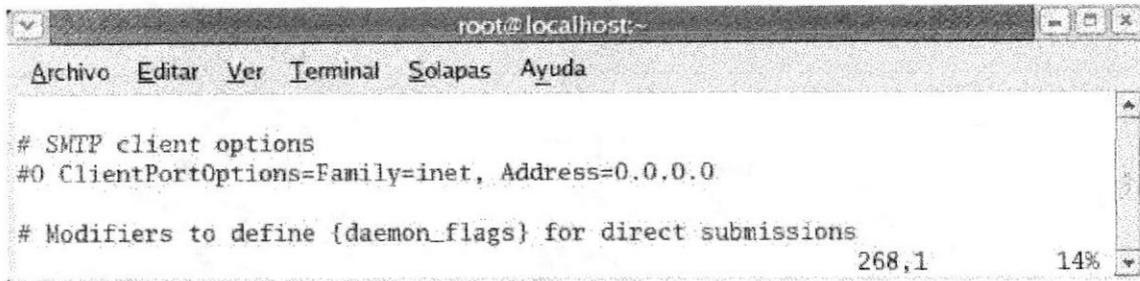


```

root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# SMTP daemon options
O DaemonPortOptions=Port=smtp,Addr=0.0.0.0, Name=MTA
# SMTP client options
-- INSERTAR --
265,43  14%
  
```

Figura 7-173: Pantalla sendmail línea 265

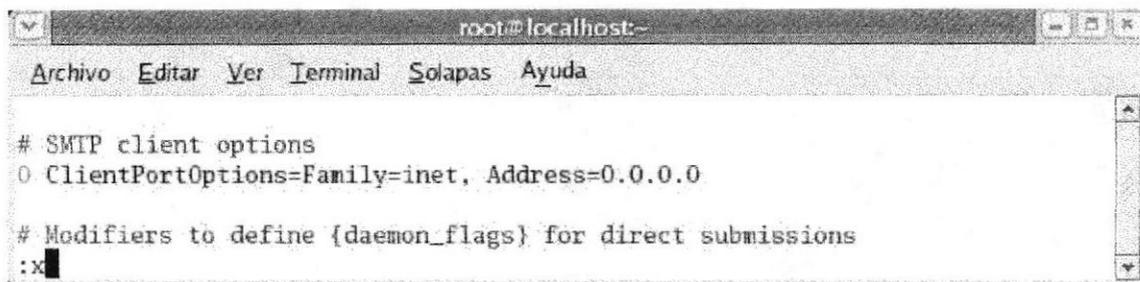
Luego en el mismo archivo buscar la línea # SMTP client options.



```
root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# SMTP client options
#0 ClientPortOptions=Family=inet, Address=0.0.0.0
# Modifiers to define {daemon_flags} for direct submissions
268,1 14%
```

Figura 7-174: Sendmail línea 268

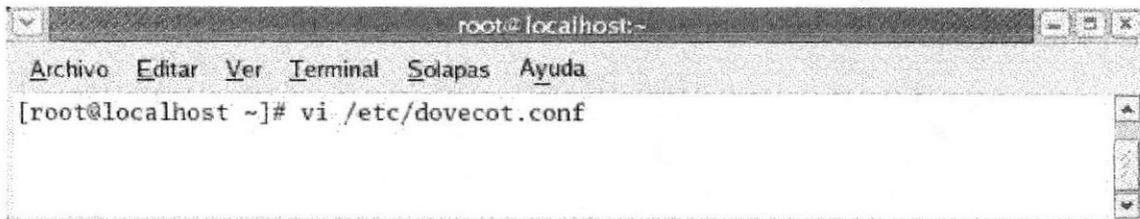
Una vez encontrada la línea # SMTP client options, proceder a descomentarla, salir y guardar los cambios.



```
root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# SMTP client options
0 ClientPortOptions=Family=inet, Address=0.0.0.0
# Modifiers to define {daemon_flags} for direct submissions
:x
```

Figura 7-175: Sendmail modificada

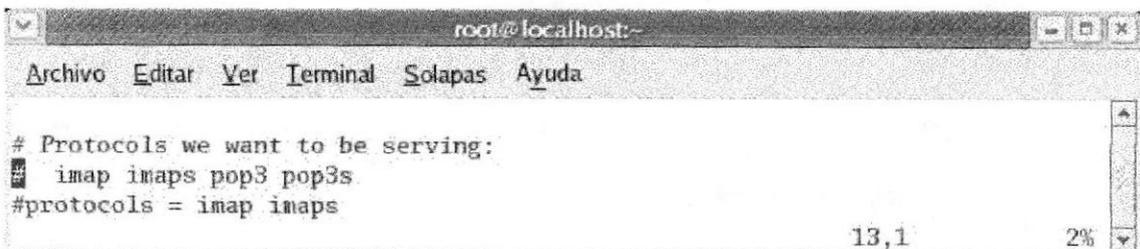
Luego se procede a editar el archivo del dovecot.conf que se encuentra en la siguiente ruta, /etc/.



```
root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost ~]# vi /etc/dovecot.conf
```

Figura 7-176: Ruta dovecot

Una vez adentro del archivo dovecot proceder a buscar la línea de #protocols = imap imaps

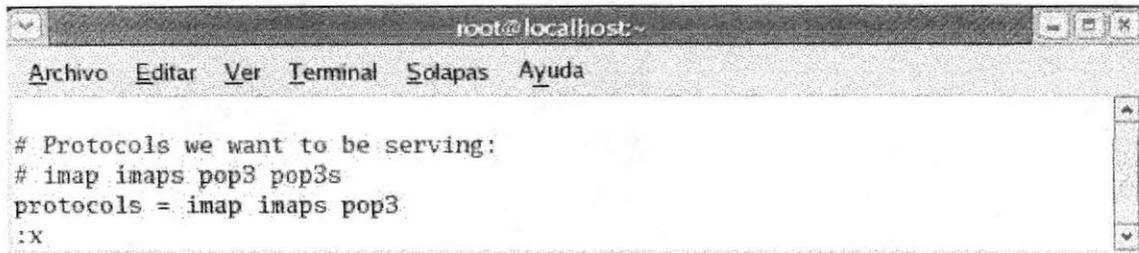


```
root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# Protocols we want to be serving:
imap imaps pop3 pop3s
#protocols = imap imaps
13,1 2%
```

Figura 7-177: Dovecot línea 13



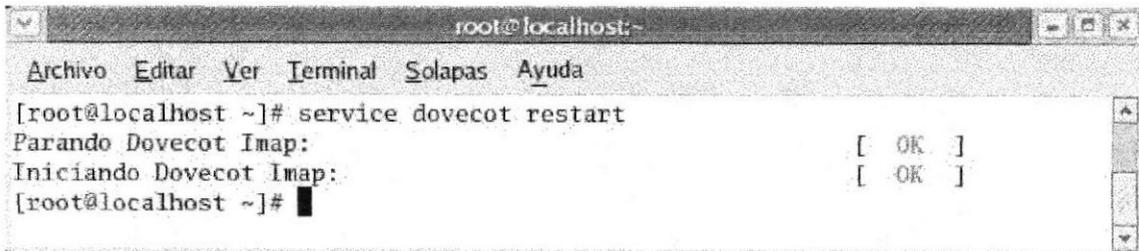
Una vez encontrada esa ruta proceder a descomentar y agregar el pop3, salir y guardar los cambios.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
# Protocols we want to be serving:  
# imap imaps pop3 pop3s  
protocols = imap imaps pop3  
:x
```

Figura 7-178: Dovecot modificada

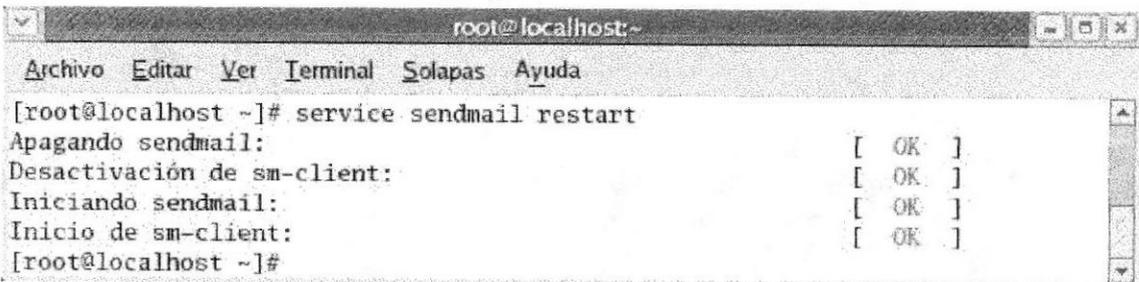
Luego de haber guardado los cambios del archivo dovecot proceder a levantar los servicios del dovecot.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# service dovecot restart  
Parando Dovecot Imap: [ OK ]  
Iniciando Dovecot Imap: [ OK ]  
[root@localhost ~]# █
```

Figura 7-179: Restauración dovecot

Después también levantar el servicio sendmail



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# service sendmail restart  
Apagando sendmail: [ OK ]  
Desactivación de sm-client: [ OK ]  
Iniciando sendmail: [ OK ]  
Inicio de sm-client: [ OK ]  
[root@localhost ~]#
```

Figura 7-180: Restauración sendmail

7.8.5.2 CONFIGURACIÓN Y CREACION DE USUARIO EN PC CLIENTE

Abrir Outlook Express para crear un usuario con el dominio tia.com

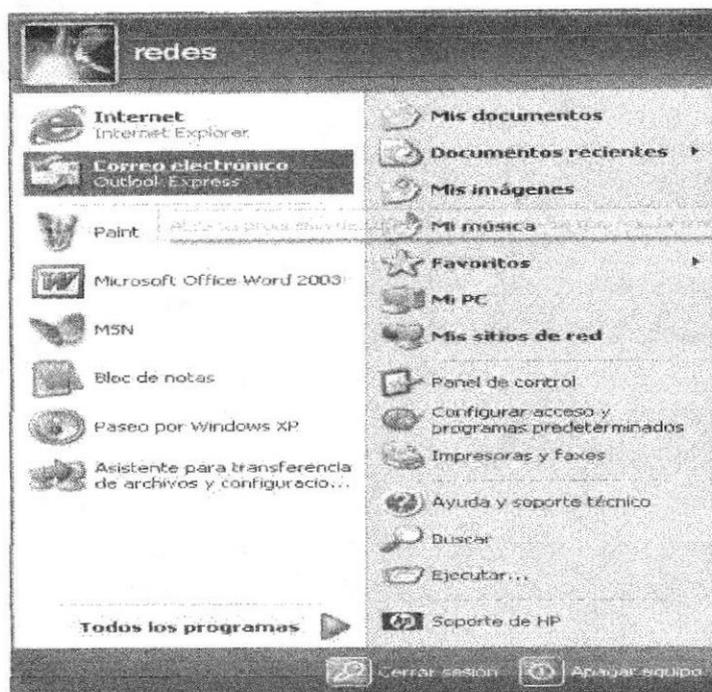


Figura 7-181: Inicio opción correo

Esta es la pantalla de bienvenida de Outlook Express, esta pantalla se carga por defecto.

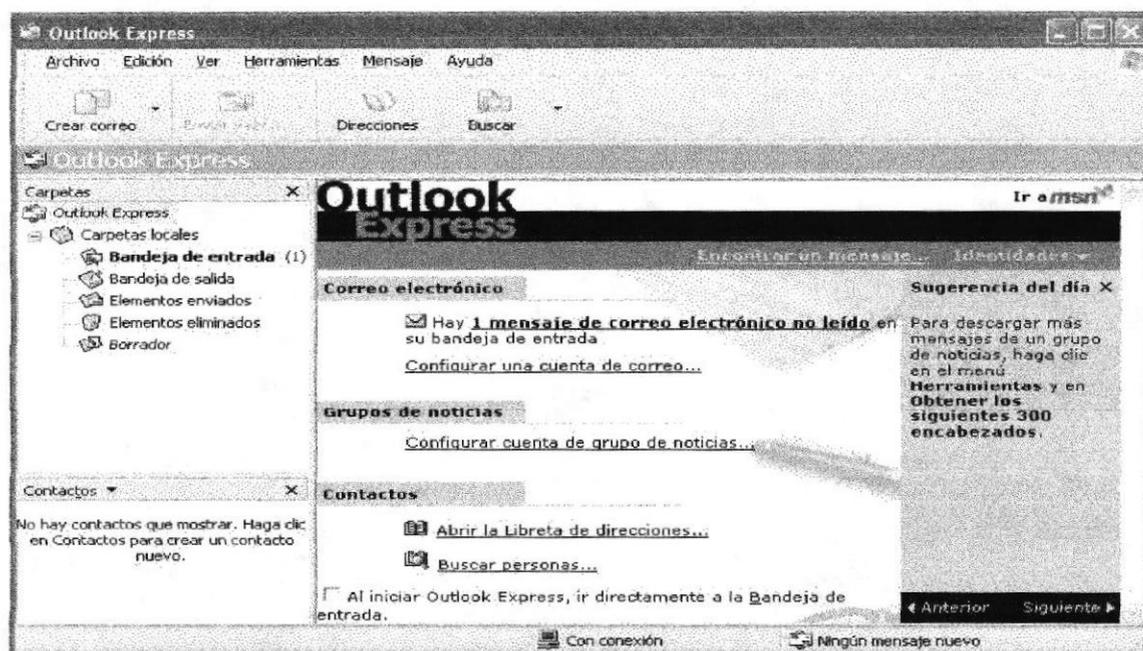


Figura 7-182: Outlook



Para proceder con la creación de una cuenta de usuario, ir a la pestaña Herramientas y seleccionar la opción cuentas.

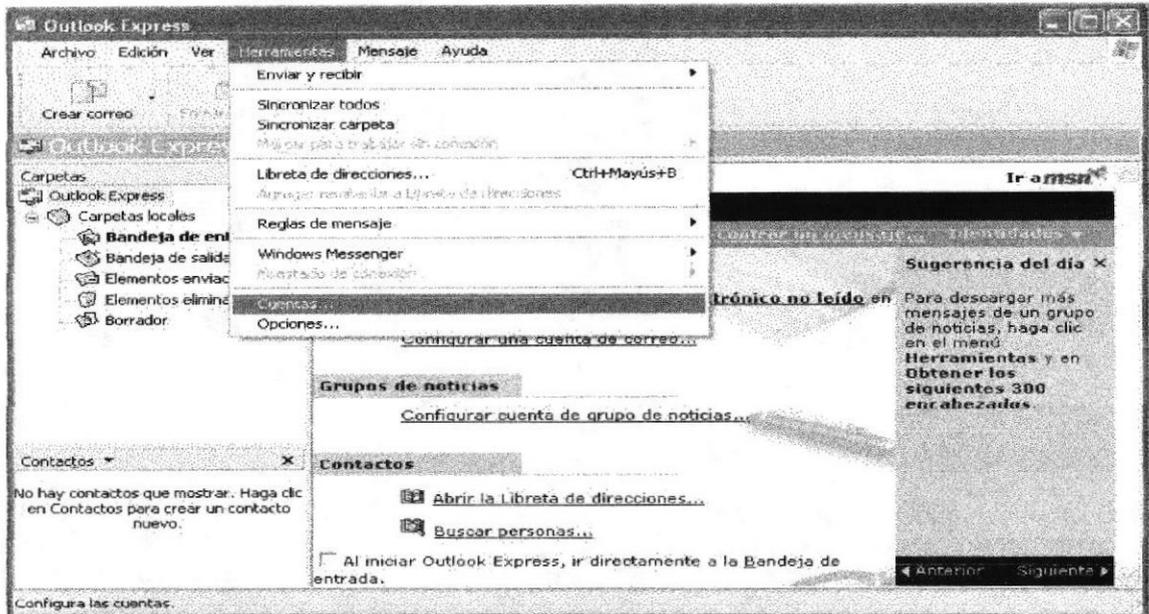


Figura 7-182: Outlook opción cuentas

Luego aparecerá una ventana parecida a esta en la cual debe agregar la cuenta de usuario.

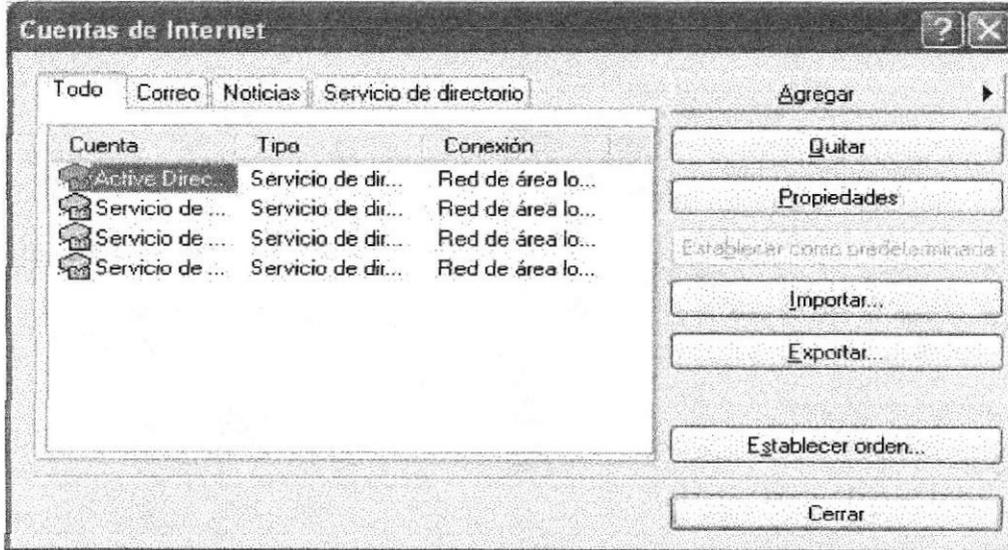


Figura 7-183: Cuenta de Internet



Seleccionar la opción correo para continuar con la creación de la cuenta.

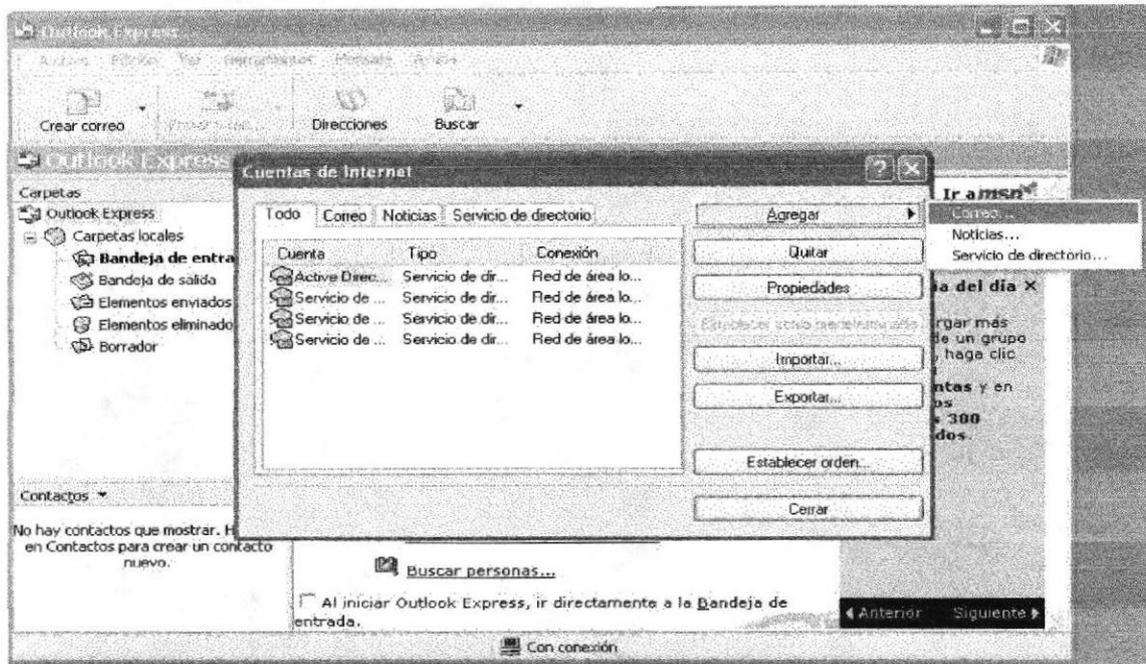


Figura 7-184: Cuentas de Internet opción agregar

En esta pantalla debe agregar el nombre que aparecerá en el campo de mensaje saliente, clic en siguiente.

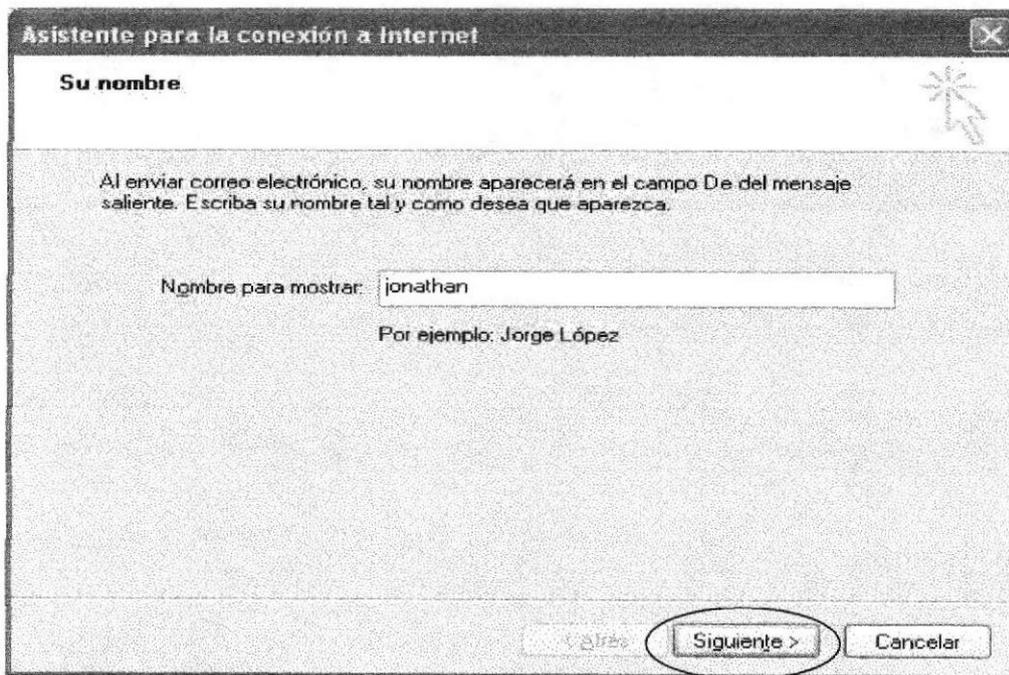


Figura 7-185: Asistente de conexión



En este caso agregar la dirección de correo electrónico con el respectivo dominio como lo muestra en esta pantalla, clic en siguiente.

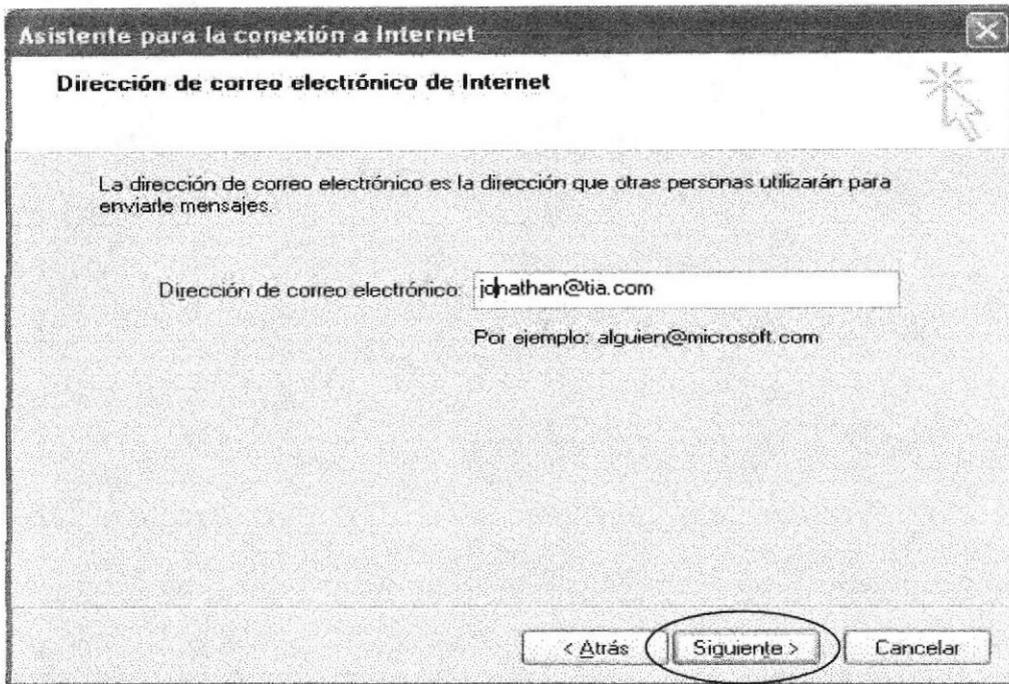


Figura 7-186: Correo electronico

Especificar el servidor de correo entrante (POP3) y el servidor de correo saliente (SMTP), en este caso los dos son la misma dirección del servidor Linux, clic en siguiente.

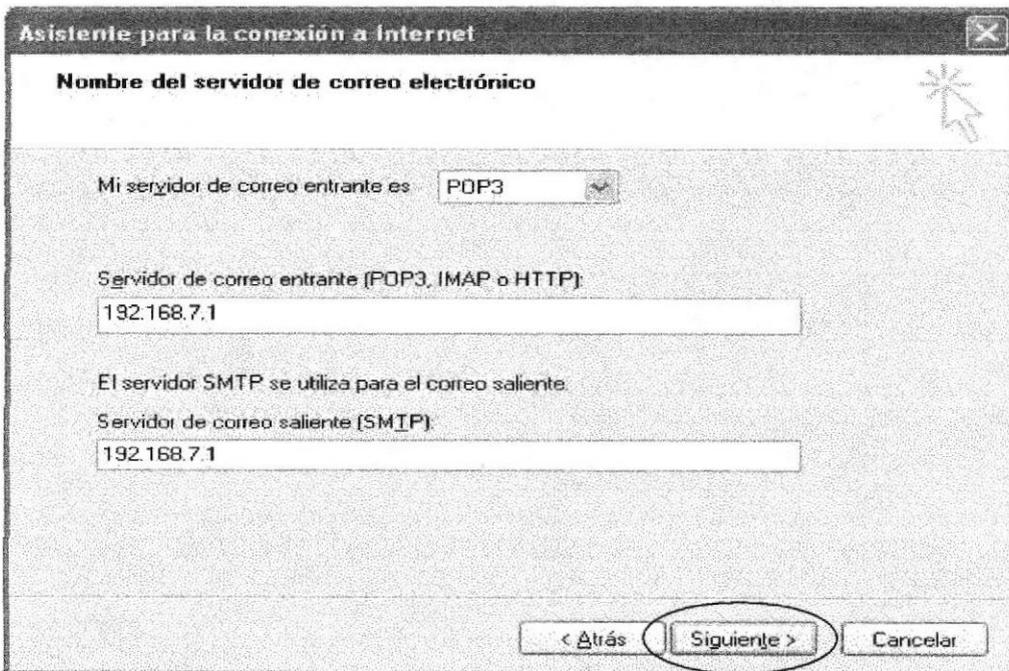


Figura 7-187: Nombre del servidor

Ingresa el nombre de usuario y contraseña proporcionado por el servidor Linux, clic en siguiente.

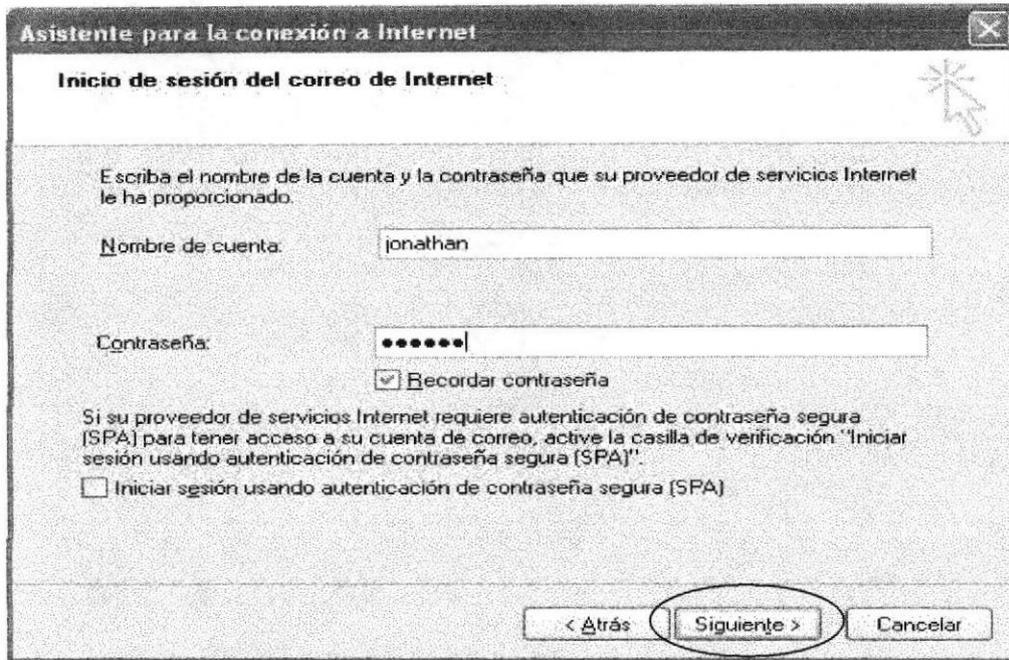


Figura 7-188: Inicio de Sesión

Clic en finalizar para verificar que la información escrita anteriormente esta correcta.

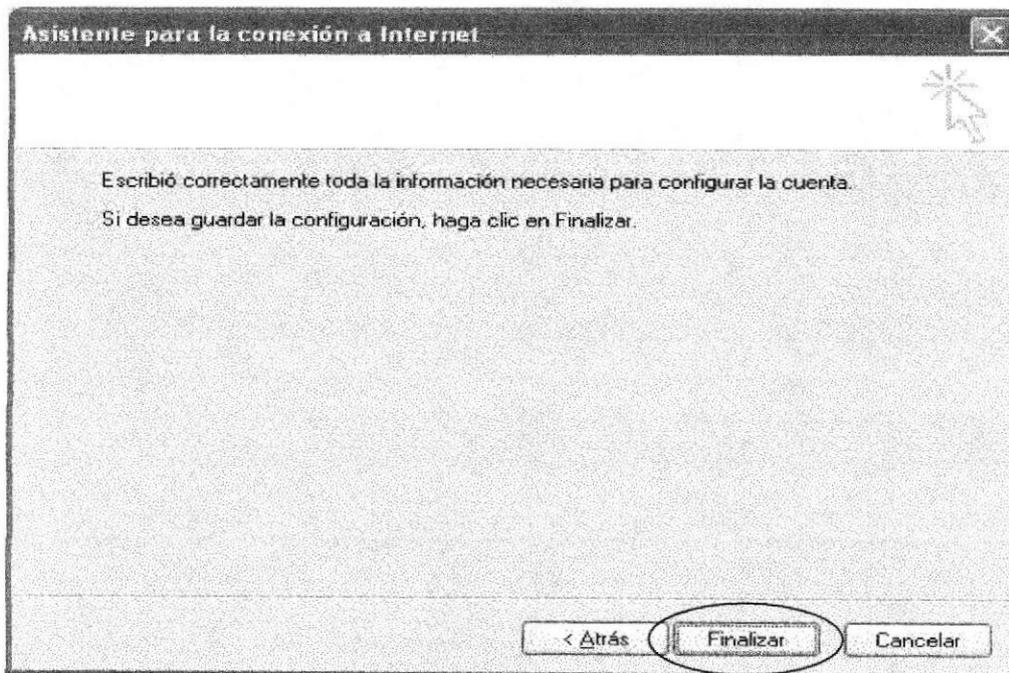


Figura 7-189: Asistente opción finalizar



Para crear un nuevo mensaje de correo electrónico realizar los pasos que muestran a continuación.

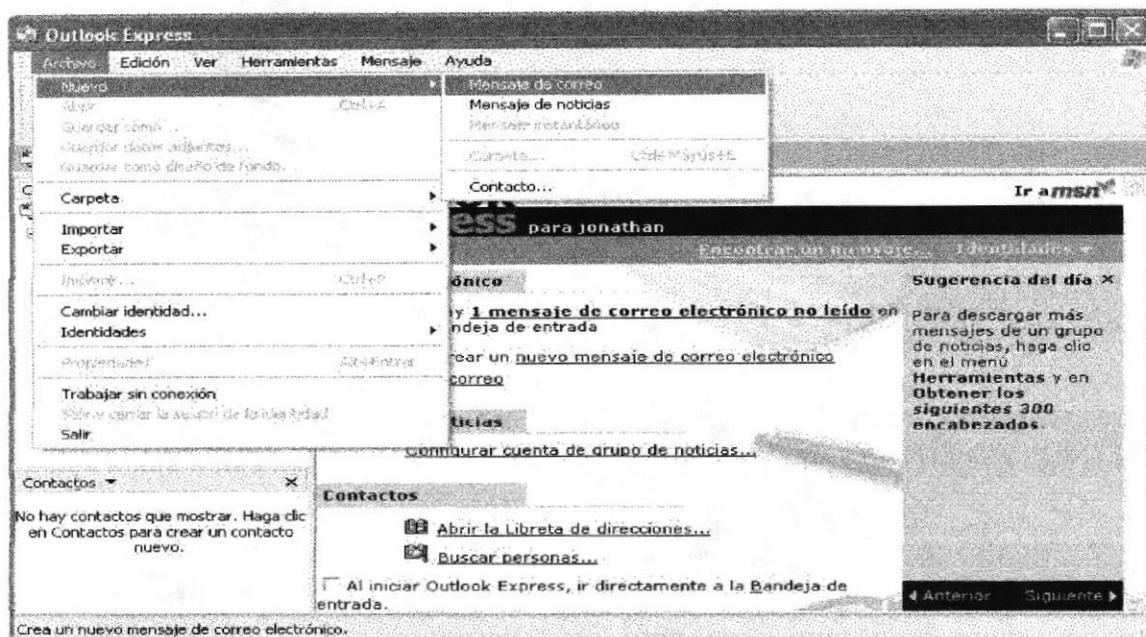


Figura 7-190: Outlook Express

En esta pantalla proceder a enviar un mensaje de prueba, en este caso a la dirección del root.

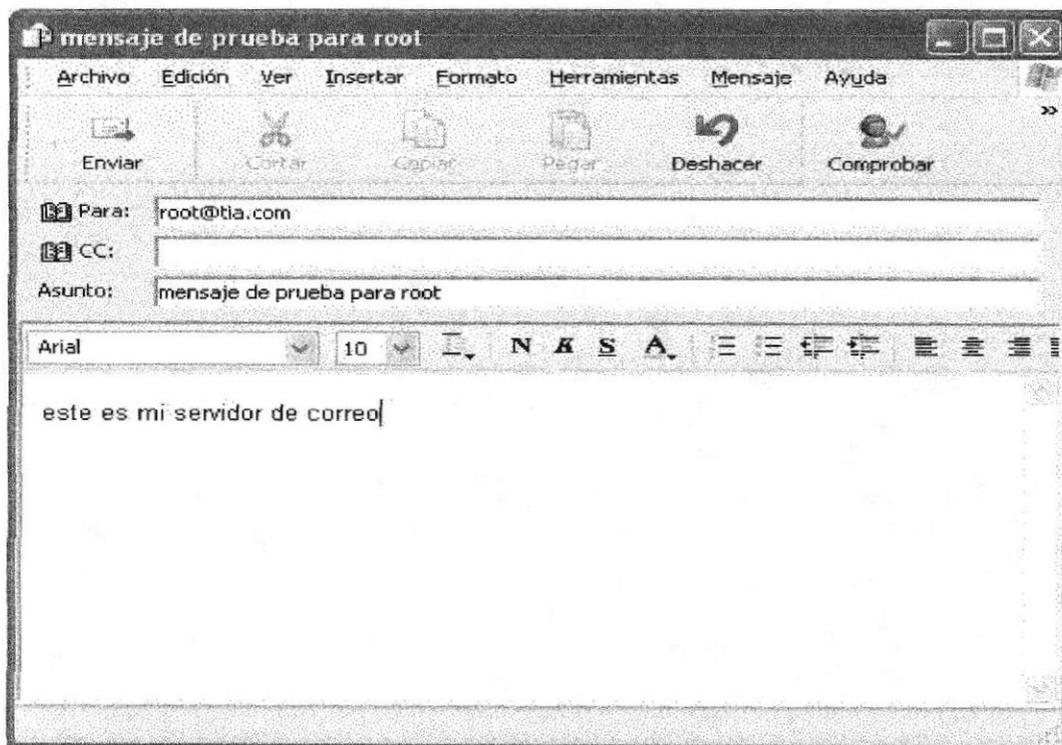


Figura 7-191: Mensaje de prueba

Para poder hacer una comprobación si llegó el mail al usuario root, hacerlo con el comando mail, como lo muestra en la siguiente gráfica.

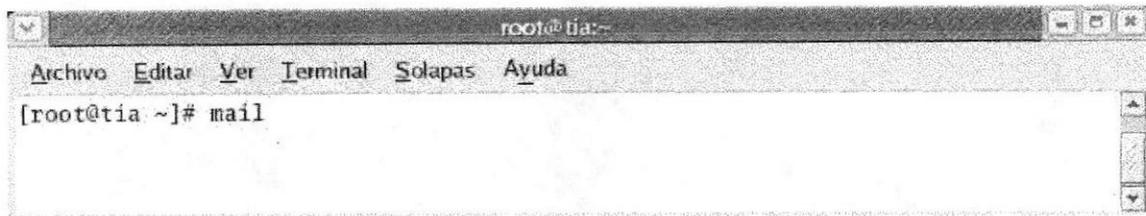


Figura 7-192: Mail

Luego de haber digitado el comando mail, aparecerá una lista de mensajes de los cuales debe estar el enviado por el cliente en Windows.

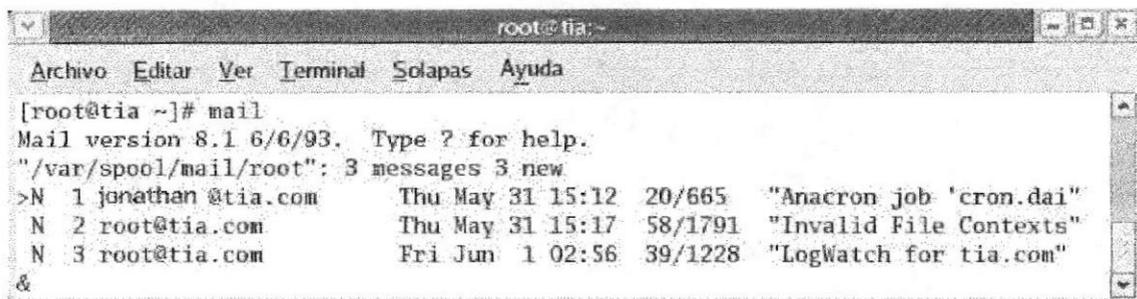


Figura 7-182: Lista de mensajes

Después proceder a digitar el número de mensaje que desee leer en este caso es el 1.

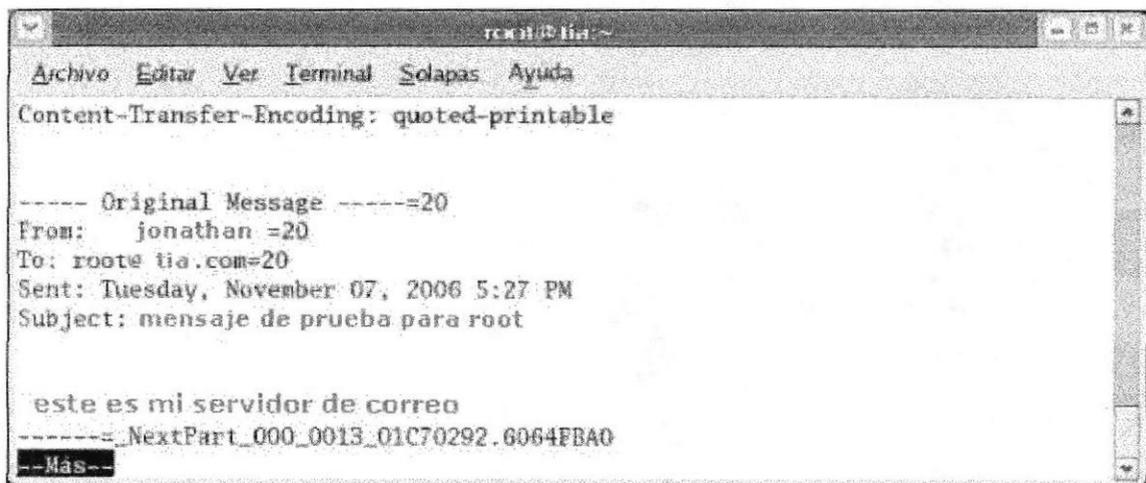


Figura 7-183: Mensaje recibido



7.8.6 CONFIGURACIÓN DEL SERVIDOR DHCP

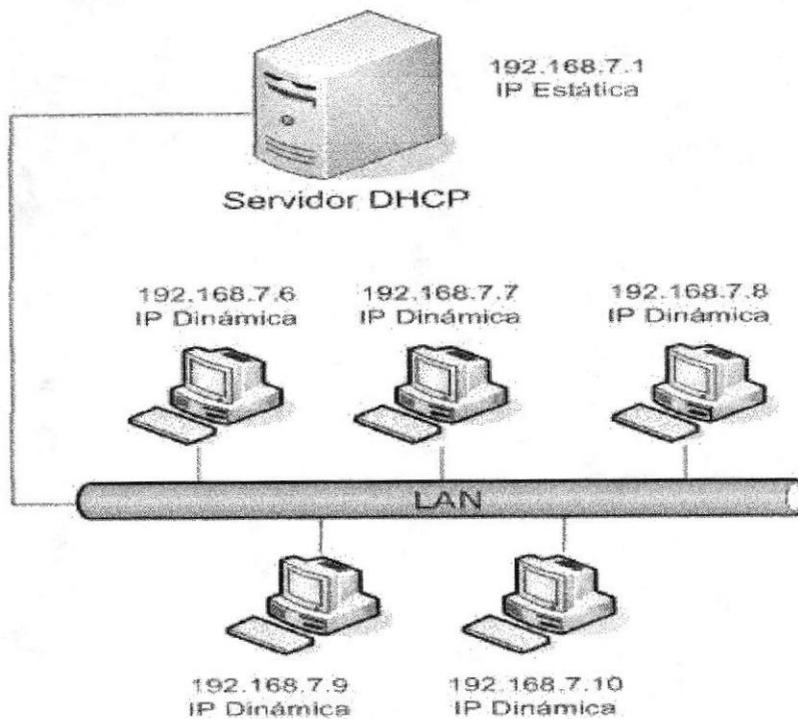


Figura 7-184: Esquema DHCP

DHCP son las siglas que identifican a un protocolo, empleado para que los hosts (clientes), en una red, puedan obtener su configuración de forma dinámica a través de un servidor del protocolo. Los datos así obtenidos pueden ser: la dirección IP, la máscara de red, la dirección de broadcast, las características del DNS, entre otros. El servicio DHCP permite acelerar y facilitar la configuración de muchos ordenadores en una red, evitando en gran medida los posibles errores humanos.

Características

Provee los parámetros de configuración a las computadoras conectadas a la red informática que lo requieran (Máscara de red, puerta de enlace y otros) y también incluyen mecanismo de asignación de direcciones de IP.

Asignación de direcciones IP

Sin DHCP, cada dirección IP debe configurarse manualmente en cada ordenador y, si el ordenador se mueve a otro lugar en otra parte de la red, se debe de configurar otra dirección IP diferente. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si el ordenador es conectado en un lugar diferente de la red.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- **Asignación manual o estática:** Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.

- **Asignación automática:** Asigna una dirección IP de forma permanente a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.
- **Asignación dinámica:** el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

Algunas implementaciones de DHCP pueden actualizar el DNS asociado con los servidores para reflejar las nuevas direcciones IP mediante el protocolo de actualización de DNS establecido en RFC 2136 (Inglés).

El DHCP es una alternativa a otros protocolos de gestión de direcciones IP de red, como el BOOTP (Bootstrap Protocol). DHCP es un protocolo más avanzado, pero ambos son los usados normalmente.

Cuando el DHCP es incapaz de asignar una dirección IP, se utiliza un proceso llamado "Automatic Private Internet Protocol Addressing".

Anatomía del protocolo

DHCP usa los mismos puertos asignados por el IANA (Autoridad de Números Asignados en Internet según siglas en inglés) en BOOTP: 67/UDP para las computadoras servidor y 68/UDP para los clientes.

DHCP Release

Los clientes envían una petición al servidor DHCP para liberar su dirección DHCP. Como los clientes generalmente no saben cuándo los usuarios pueden desconectarles de la red, el protocolo no define el envío del DHCP Release como obligatorio.

DHCP Discover

Los clientes emiten peticiones masivamente en la subred local para encontrar un servidor disponible, mediante un paquete de broadcast. El router puede ser configurado para redireccionar los paquetes DHCP a un servidor DHCP en una subred diferente. La implementación cliente crea un paquete UDP (Protocolo de Datagramas de Usuario según siglas en inglés) con destino 255.255.255.255 y requiere también su última dirección IP conocida, aunque esto no es necesario y puede llegar a ser ignorado por el servidor.

DHCP Offer

El servidor determina la configuración basándose en la dirección del soporte físico de la computadora cliente especificada en el registro CHADDRvbnv. El servidor especifica la dirección IP en el registro YIADDR. Como la cual se ha dado en los demás parámetros.

DHCP Request

El cliente selecciona la configuración de los paquetes recibidos de DHCP Offer. Una vez más, el cliente solicita una dirección IP específica que indicó el servidor.

DHCP Acknowledge

El servidor confirma el pedido y lo publica masivamente en la subred. Se espera que el cliente configure su interface de red con las opciones que se le han otorgado.

DHCP Nack

El servidor envía al cliente un mensaje indicando que el contrato ha terminado o que la dirección IP asignada no es válida.

DHCP Inform

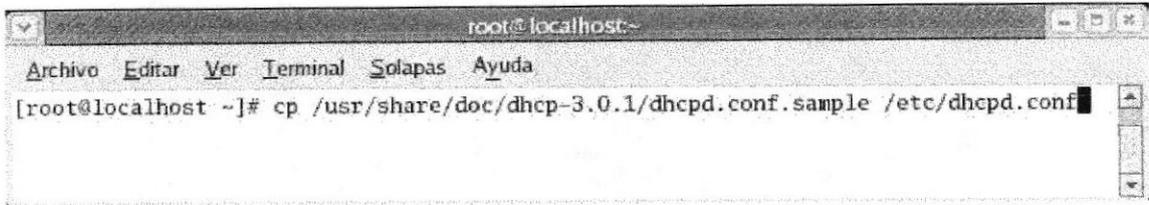
El cliente envía una petición al servidor de DHCP: para solicitar más información que la que el servidor ha enviado con el DHCPACK original; o para repetir los datos para un uso particular - por ejemplo, los browsers usan DHCP Inform para obtener la configuración de los proxies a través de WPAD. Dichas peticiones no hacen que el servidor de DHCP refresque el tiempo de vencimiento de IP en su base de datos.

REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR DHCP

- 1 Pc con Linux Fedora Core 3
- 1 Tarjeta de Red
- Tener una IP Estática
- Tener habilitado los servicios necesarios (dhcpd).

7.8.6.1 CONFIGURACIÓN EN LINUX

Crear el archivo `dhcpd.conf` en el directorio `/etc/` de la siguiente manera.



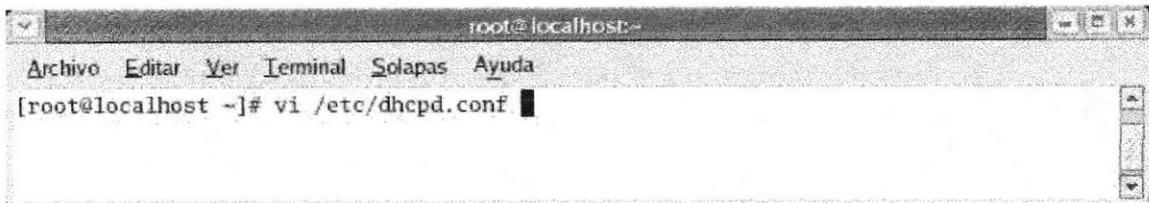
```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# cp /usr/share/doc/dhcp-3.0.1/dhcpd.conf.sample /etc/dhcpd.conf

```

Figura 7-185: Ruta dhcp

Luego de haber creado el archivo de configuración `dhcpd.conf`, proceder a editar con el comando `vi`.



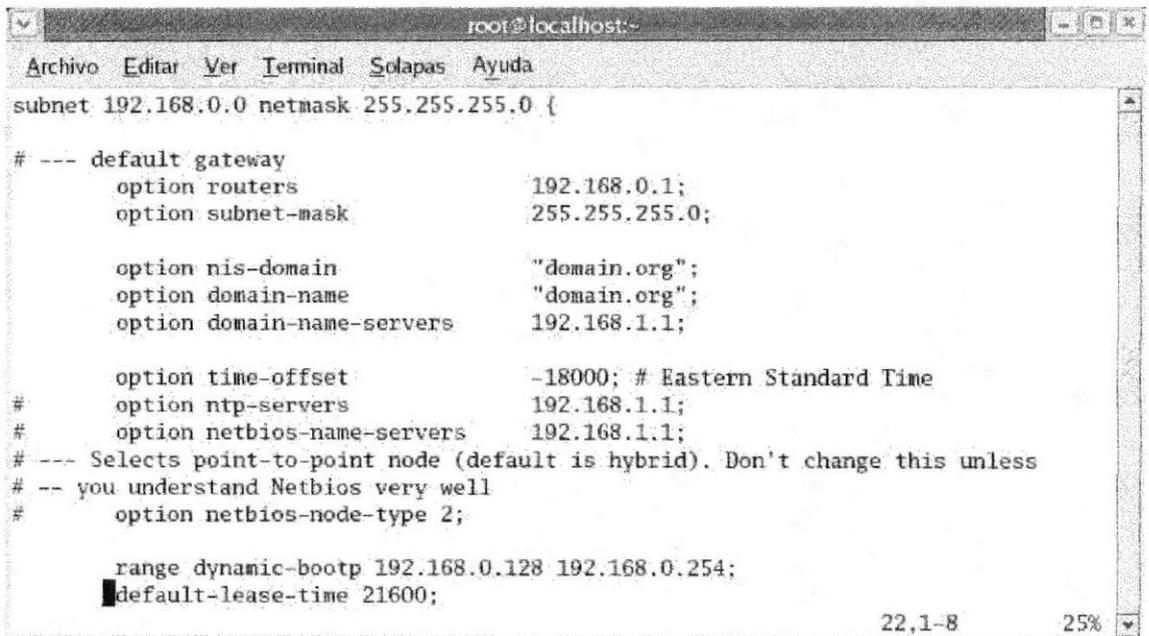
```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# vi /etc/dhcpd.conf

```

Figura 7-186: Editar dhcp

Una pantalla muy parecida a esta aparecerá al momento de haber ingresado al archivo de configuración `dhcpd.conf`.



```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
subnet 192.168.0.0 netmask 255.255.255.0 {
# --- default gateway
    option routers          192.168.0.1;
    option subnet-mask     255.255.255.0;

    option nis-domain      "domain.org";
    option domain-name     "domain.org";
    option domain-name-servers 192.168.1.1;

    option time-offset     -18000; # Eastern Standard Time
#   option ntp-servers     192.168.1.1;
#   option netbios-name-servers 192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#   option netbios-node-type 2;

    range dynamic-bootp 192.168.0.128 192.168.0.254;
    default-lease-time 21600;

```

Figura 7-187: Archivo dhcp

Luego de haber ingresado proceder a editar este archivo agregando las siguientes líneas necesarias para habilitar dhcp, debe especificar en la parte final el rango de direcciones IP que van a ser asignadas automáticamente por dhcp.

option routers 192.168.7.1: Es donde se define los gateway de la red.

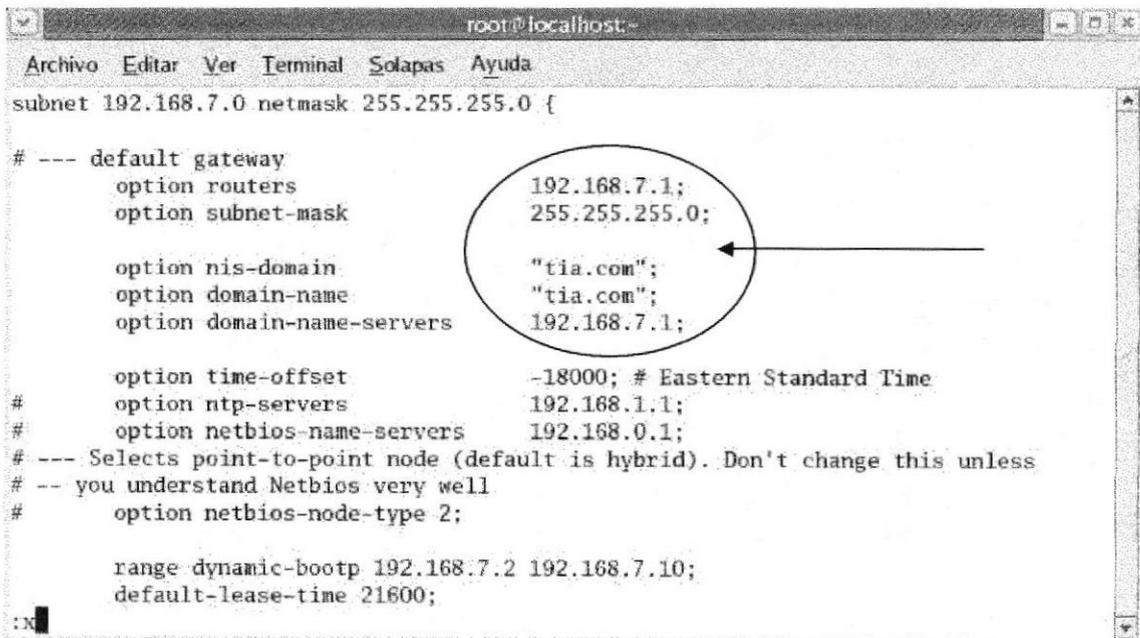
option subnet-mask 255.255.255.0: Es donde se define la máscara general de la red.

option nis-domain "tia.com": Es donde define el nombre del dominio DNS.

option domain-name "tia.com": Es donde define el nombre del dominio DNS que se añade a los nombres de host.

option domain-name-servers 192.168.7.1: Es donde se define la dirección del Servidor DNS en la red.

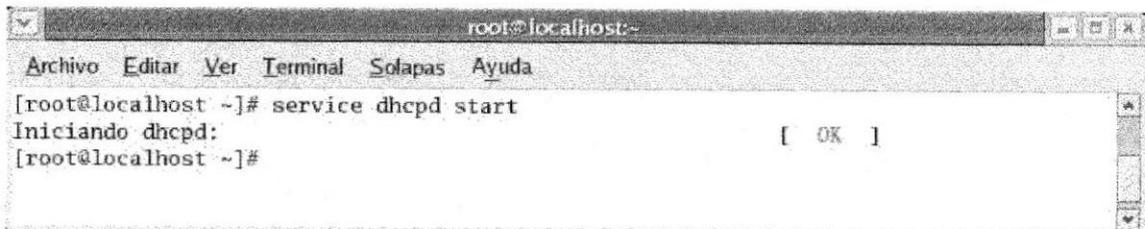
range dynamic-bootp 192.168.7.2 192.168.7.10: Es donde se designará el rango de Ips disponibles.



```
root@localhost:~#
Archivo Editar Ver Terminal Solapas Ayuda
subnet 192.168.7.0 netmask 255.255.255.0 {
# --- default gateway
  option routers                192.168.7.1;
  option subnet-mask            255.255.255.0;
#
  option nis-domain             "tia.com";
  option domain-name            "tia.com";
  option domain-name-servers    192.168.7.1;
#
  option time-offset             -18000; # Eastern Standard Time
#
  option ntp-servers            192.168.1.1;
#
  option netbios-name-servers   192.168.0.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#
  option netbios-node-type 2;
#
  range dynamic-bootp 192.168.7.2 192.168.7.10;
  default-lease-time 21600;
}
:~#
```

Figura 7-188: Archivo dhcp modificado

Luego de haber guardado los cambios del archivo de configuración, proceder a levantar el servicio dhcpd como lo muestra a continuación.



```
root@localhost:~#
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# service dhcpd start
Iniciando dhcpd: [ OK ]
[root@localhost ~]#
```

Figura 7-189: Restauración dhcp



CONFIGURACIÓN Y VERIFICACIÓN DEL CLIENTE POR DHCP

En el cliente Windows debe asignar su respectiva dirección IP, para esto dar clic derecho en el icono de mis sitios de red y elegir la opción propiedades.

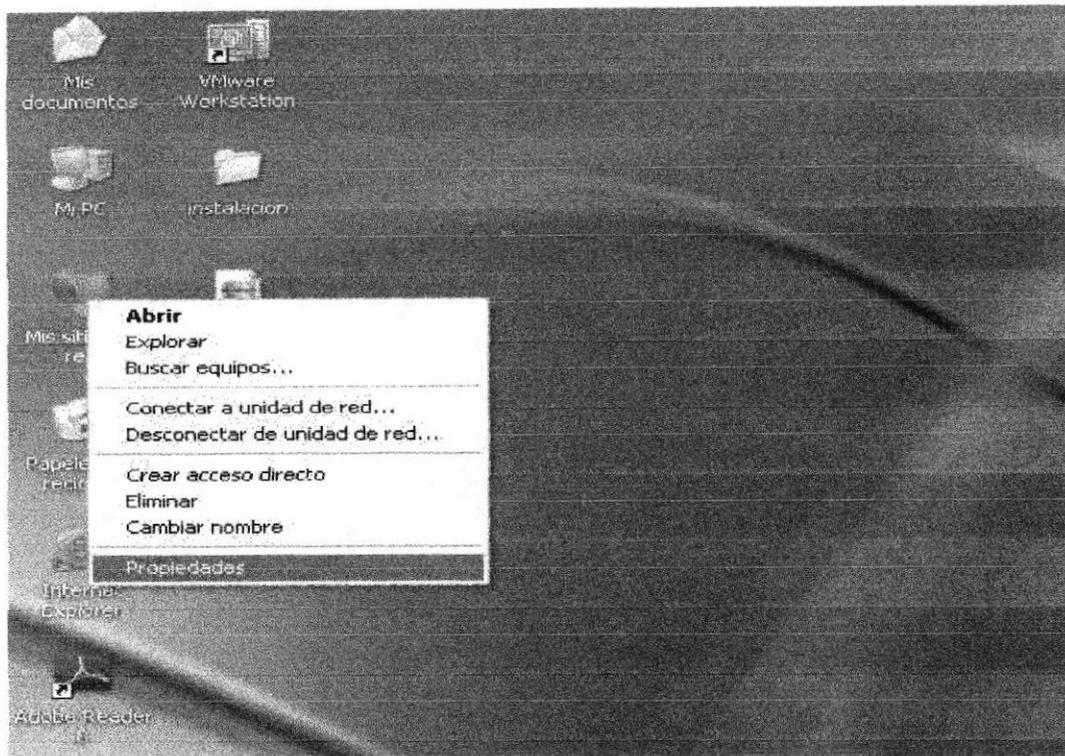


Figura 7-190: Propiedades de mis sitios de red

Una vez ingresado en las propiedades de mis sitios de red, dar clic derecho sobre el icono de conexión de área local y seleccionar propiedades.

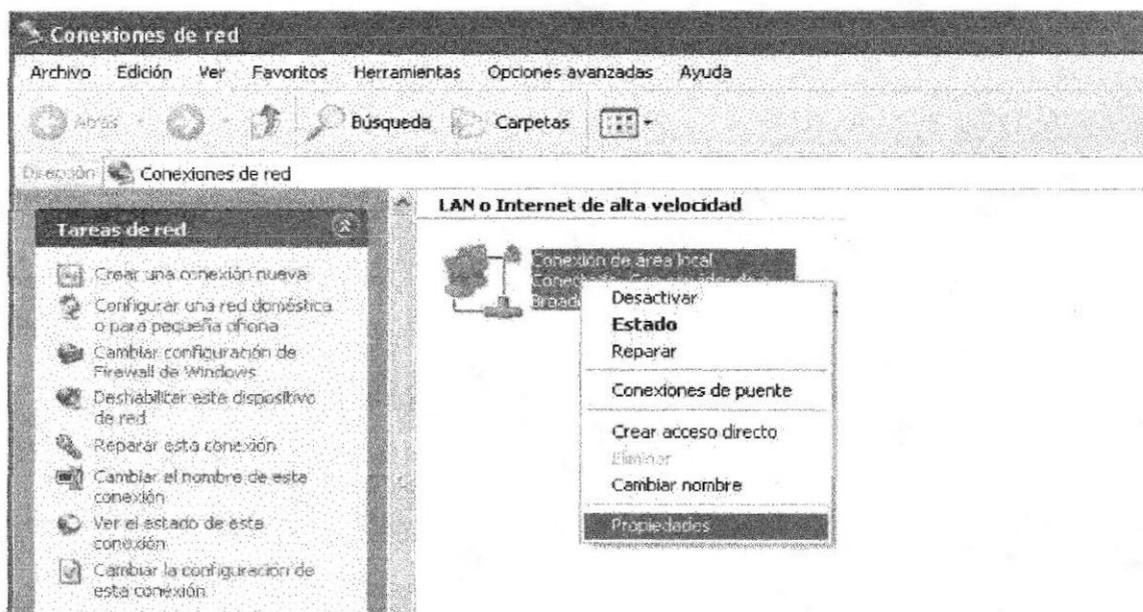


Figura 7-191: Propiedades de conexiones de área local

Luego de esto aparecerá un recuadro de propiedades de Conexión de área local en el cual ubicarse en la opción de protocolos de Internet tcp/ip y dar clic en propiedades.

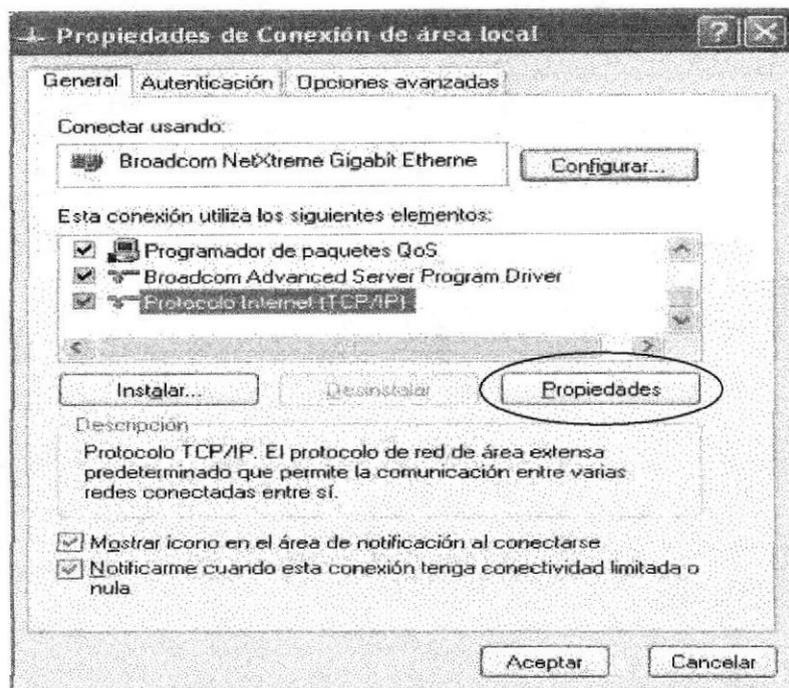


Figura 7-192: Propiedades de TCP/IP

Luego seleccionar en obtener una dirección IP automática, de esta manera podrá demostrar y verificar que la dirección IP es designada por el Servidor dhcp, para continuar debe aceptar los cambios realizados.

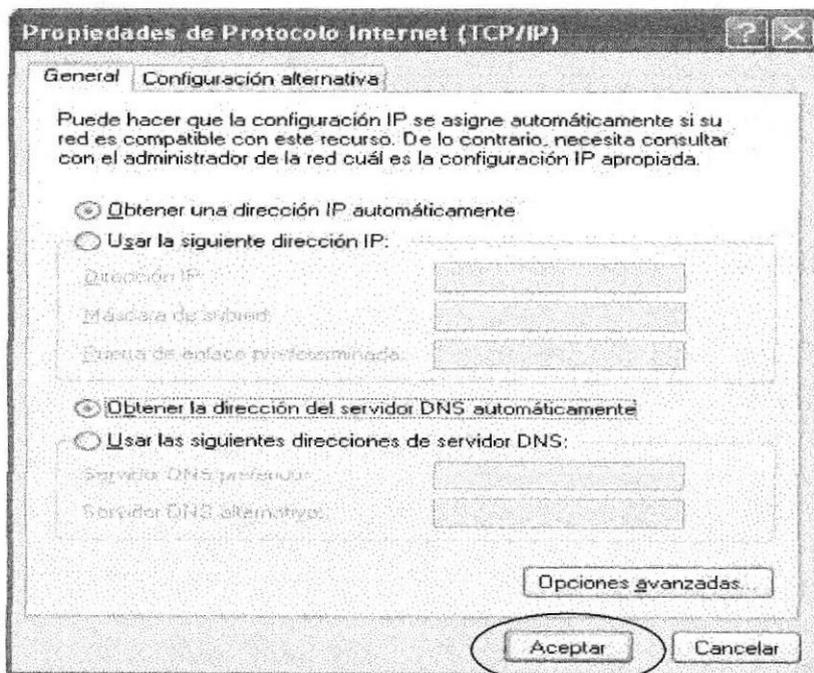


Figura 7-193: Propiedades opción Aceptar

Para poder realizar la verificación del estado de la conexión de área local, dar clic en estado como lo indica la imagen.

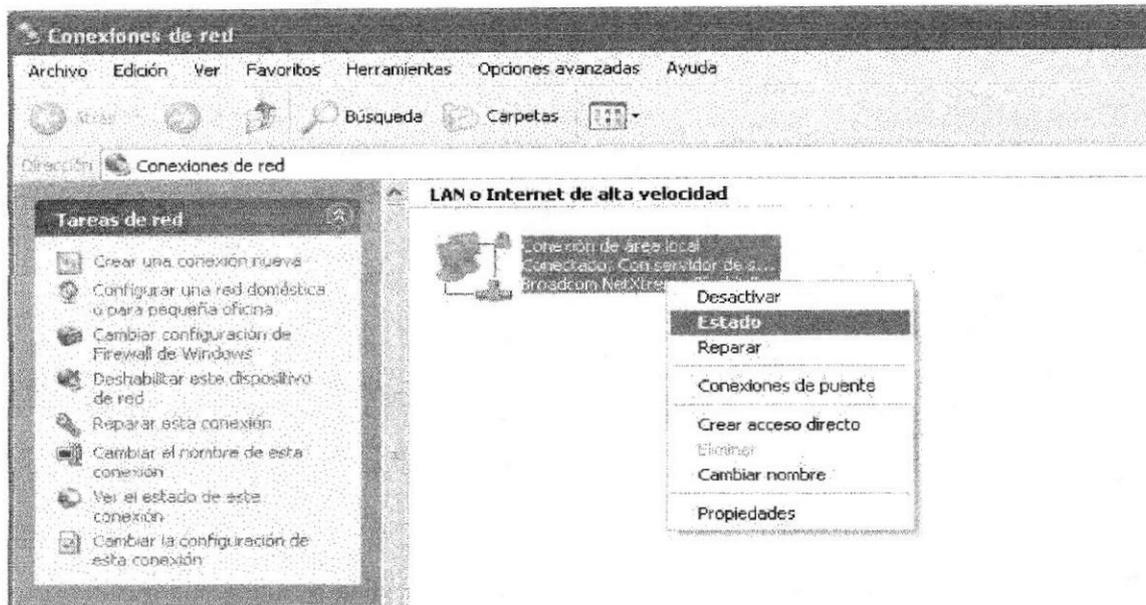


Figura 7-194: Estado de conexión de area local

En esta parte aparecerá una ventana como esta, en la cual colocarse en la pestaña Soporte.

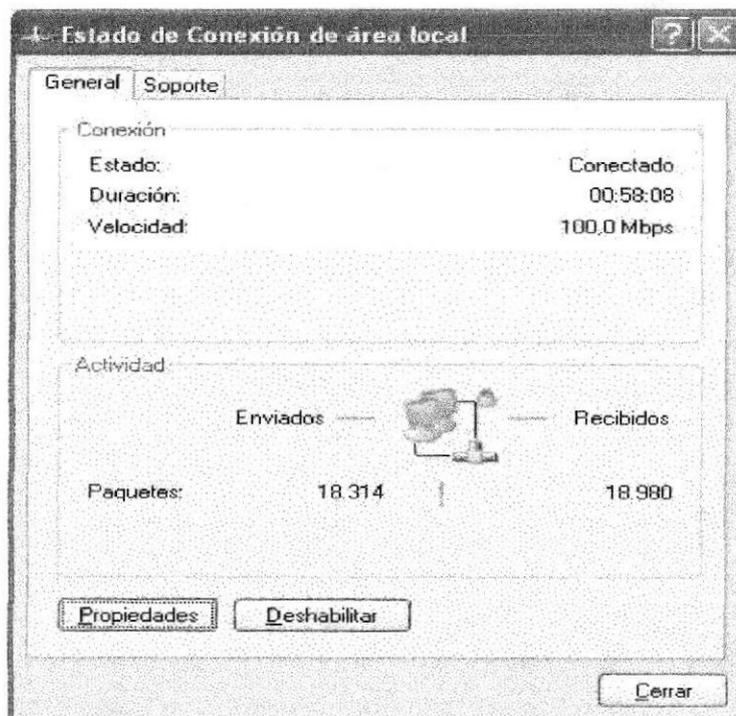


Figura 7-195: Conexión opción General



Aquí verificar que la dirección IP con su respectiva subred y puerta de enlace es asignada por DHCP.

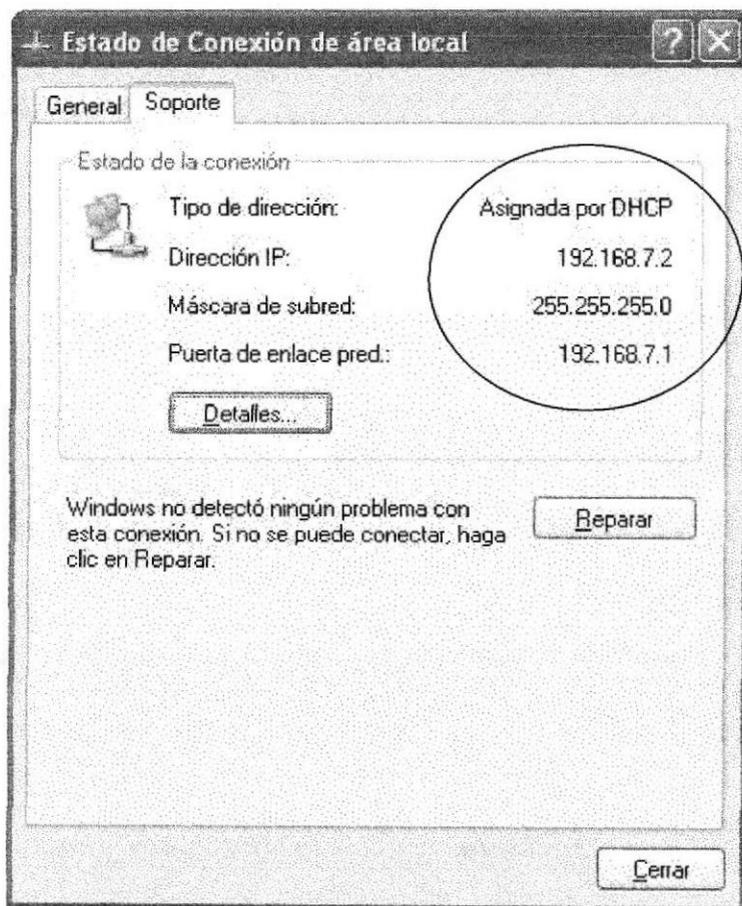


Figura 7-196: Conexión de DHCP

7.8.7 CONFIGURACIÓN DEL SERVIDOR FIREWALL

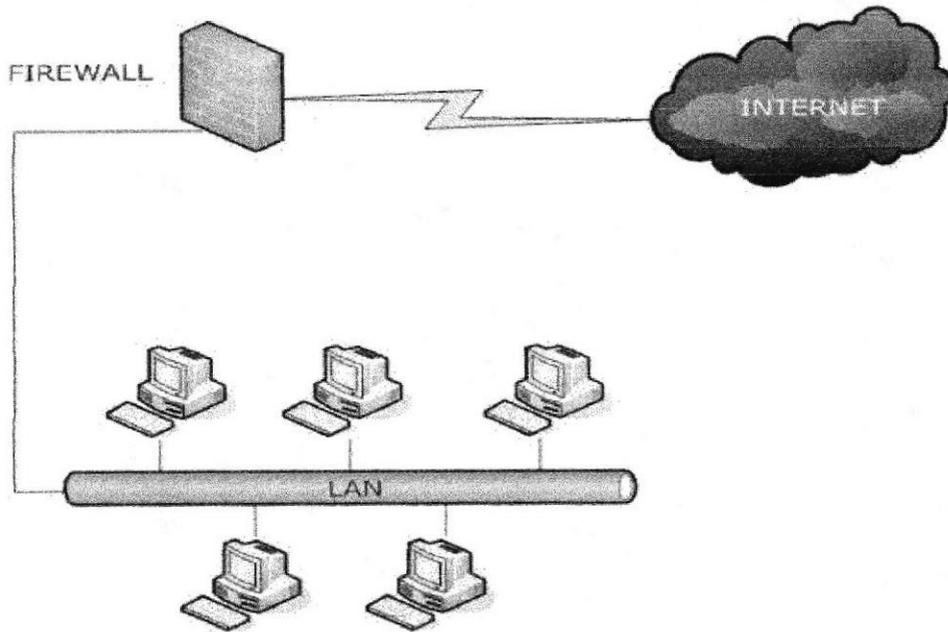


Figura 7-197: Pantalla esquema firewalle

Un firewall se utiliza primariamente para separar y controlar la actividad entre redes, como por ejemplo entre su red interna e Internet.

Puede querer tener control sobre los servicios de su red que pueden ser vistos desde afuera, así como también ser notificado si alguna máquina de su red local empieza a enviar paquetes innecesarios al exterior.

Por otro lado, con un firewall Linux entre dos redes tiene la posibilidad de gerenciar el ancho de banda de una forma eficiente en una etapa posterior, mejorando los tiempos de respuesta de sus servicios.

Por último vale aclarar que si bien muchos ataques a su servidor pueden ser originados en Internet, la estadística demuestra que muchos de estos ataques provienen de la red interna de la empresa. Un firewall ayuda minimizar estos riesgos.

Características de un Firewall Linux

Filtrado a nivel de Núcleo

El filtrado de paquetes en Linux se hace a nivel de núcleo. No es una aplicación corriendo sobre él como en otras plataformas. Esto de por sí ya le da una cualidad de seguridad sobresaliente respecto a otras opciones, así como un elevado rendimiento.

Requerimientos de Hardware

Los requerimientos de hardware para realizar esta tarea son mínimos. El límite está en el *throughput* del bus.

Flexibilidad

Los firewalls comerciales, denominados "por hardware", usualmente son vistos como cajas negras por sus propietarios. Un firewall Linux es totalmente flexible y adaptable a las necesidades particulares de cada situación.

Economía

No hay forma más económica y confiable para filtrar paquetes. El costo de instalar un firewall Linux puede ser hasta 10 veces más económico que comprar un firewall por hardware o paquetes de software comerciales.

Herramientas de Administración

El filtrado de paquetes del kernel Linux es realizado mediante el código NetFilter del mismo. Como herramienta de administración se puede utilizar la herramienta IPTables de línea de comandos, o algún front-end gráfico como FWBuilder.

Logic no sólo asesora en la instalación y personalización del firewall, sino que además capacita al cliente en las herramientas necesarias (consola o entorno gráfico, según elección) para su posterior administración.

REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR FIREWALL

- 1 Pc con Linux Fedora Core 3
- 1 Tarjeta de Red
- Tener una IP Estática
- Tener habilitado los servicios necesarios (iptables).

7.8.7.1 CONFIGURACIÓN DE FIREWALL EN LINUX

DENEGAR PING PARA USUARIOS

Para verificar si esta habilitado el ping para los usuarios se lo hará a continuación:

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\redes>ping 192.168.7.1

Haciendo ping a 192.168.7.1 con 32 bytes de datos:

Respuesta desde 192.168.7.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.7.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
  
```

Figura 7-198: Verificación del ping

Esta línea de comando es para denegar ping, para que los usuarios que tienen el mismo segmento de red no puedan acceder a un Servidor determinado.

(protocolo)(acción aplicar)

```

Iptables -A INPUT -s 192.168.7.0/24 -d 192.168.7.1 -p icmp -j DROP
  
```

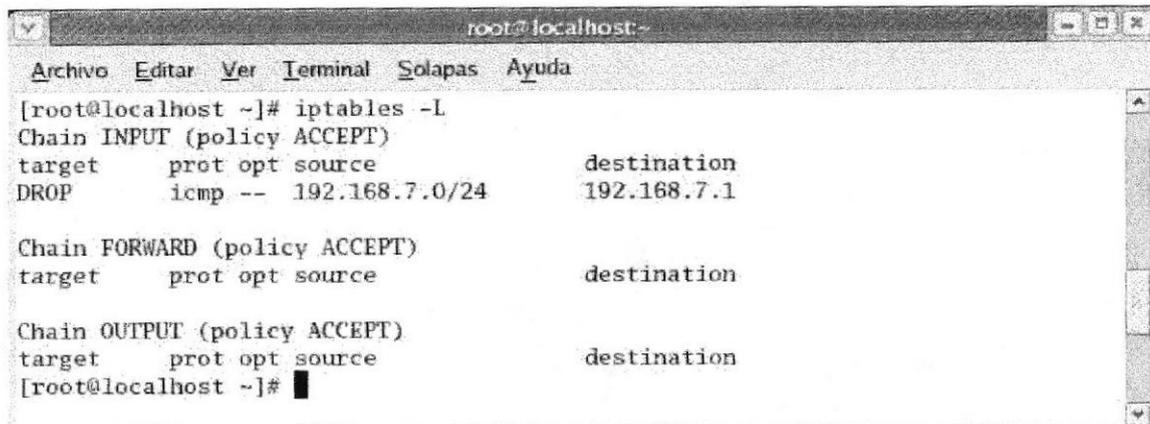
(Palabra Reservada) (ADD)(origen)(red origen)(destino)(IPServidor) (Denegar)

```

root@localhost:~# iptables -A INPUT -s 192.168.7.0/24 -d 192.168.7.1 -p icmp -j DROP
  
```

Figura 7-199: Denegar ping

En esta parte observar que esta denegando el ping para cualquier usuario que intente acceder al servidor dentro del mismo segmento.



```

root@localhost:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      icmp -- 192.168.7.0/24         192.168.7.1

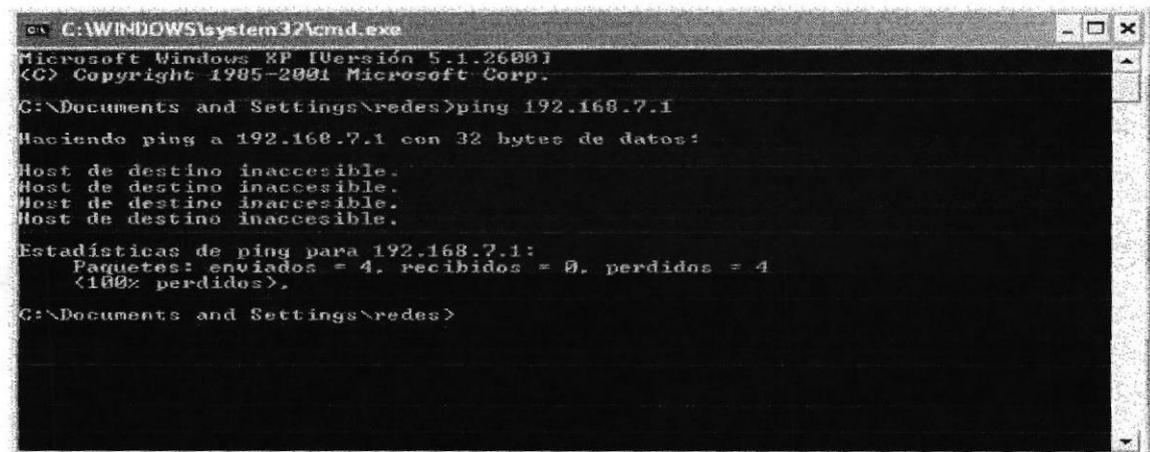
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
[root@localhost ~]#

```

Figura 7-200: Comprobación del ping

Aquí se realiza la comprobación en el cliente, como se observa hacer ping al servidor y como respuesta da Host de destino inaccesible.



```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\redes>ping 192.168.7.1

Haciendo ping a 192.168.7.1 con 32 bytes de datos:

Host de destino inaccesible.
Host de destino inaccesible.
Host de destino inaccesible.
Host de destino inaccesible.

Estadísticas de ping para 192.168.7.1:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos).

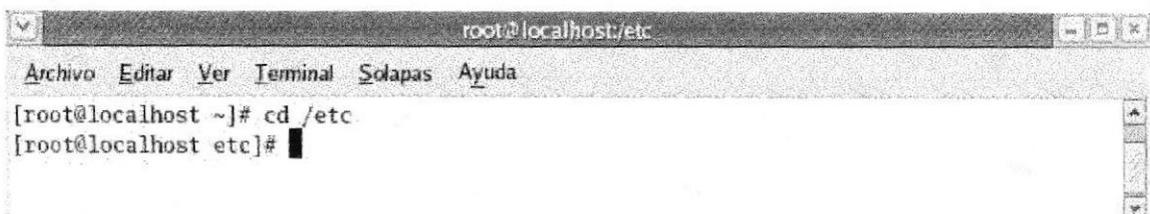
C:\Documents and Settings\redes>

```

Figura 7-201: Ping denegado

HABILITAR TELNET

Para poder habilitar el telnet, entrar al directorio /etc/ de la siguiente manera.



```

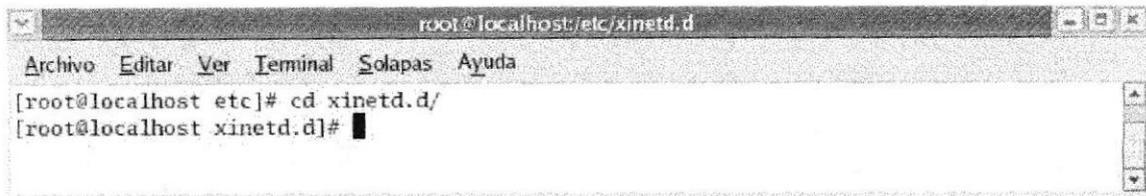
root@localhost/etc
Archivo Editar Ver Terminal Solapas Ayuda

[root@localhost ~]# cd /etc
[root@localhost etc]#

```

Figura 7-202: Ingreso al etc

Luego dentro del directorio etc, proceder a ingresar al directorio xinetd.d para editar el archivo krb5-telnet.

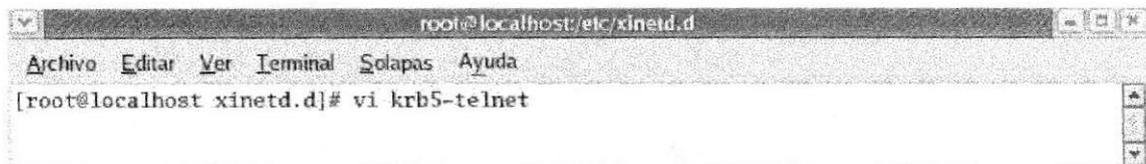


```

root@localhost:/etc/xinetd.d
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost etc]# cd xinetd.d/
[root@localhost xinetd.d]#
  
```

Figura 7-203: Ingreso xinetd.d

En este caso editar el archivo krb5-telnet con el comando vi.

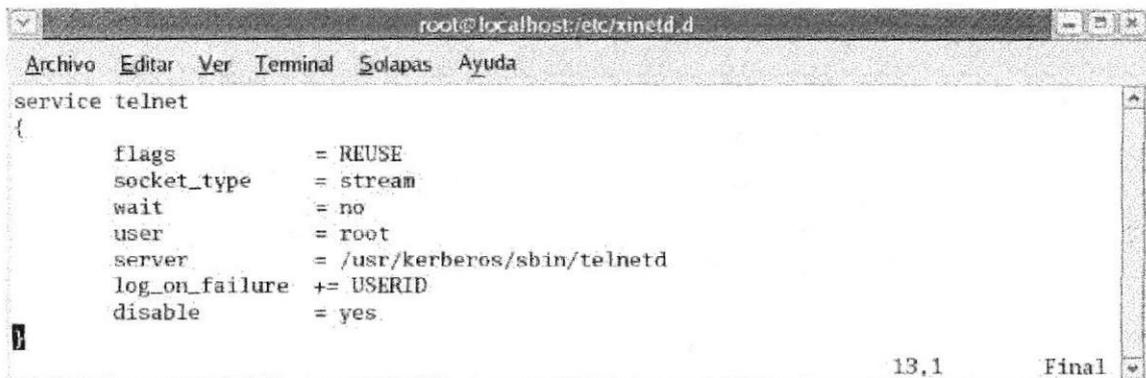


```

root@localhost:/etc/xinetd.d
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost xinetd.d]# vi krb5-telnet
  
```

Figura 7-204: Editar krb5-telnet

Después de haber ingresado al archivo de configuración de telnet proceder a editar este archivo.

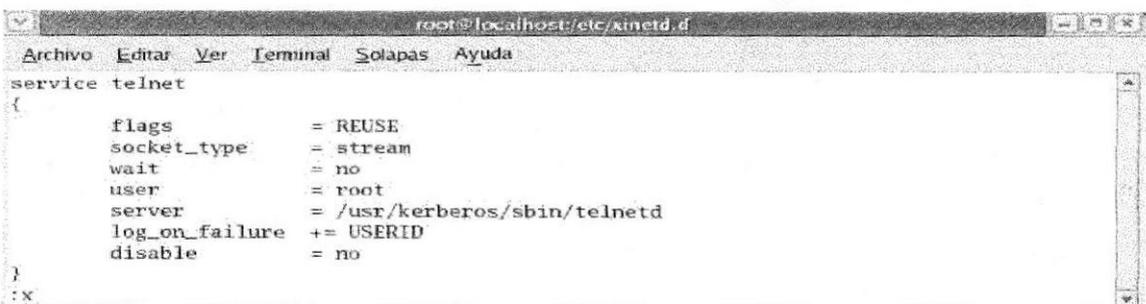


```

root@localhost:/etc/xinetd.d
Archivo Editar Ver Terminal Solapas Ayuda
service telnet
{
    flags           = REUSE
    socket_type     = stream
    wait           = no
    user           = root
    server         = /usr/kerberos/sbin/telnetd
    log_on_failure += USERID
    disable       = yes
}
13.1 Final
  
```

Figura 7-205: Archivo krb5-telnet

En este archivo editar la parte final la línea disable, la cual debe cambiarle a no, luego guardar los cambios y salir.

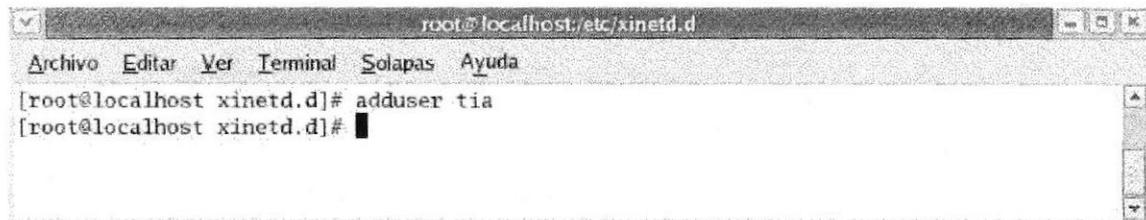


```

root@localhost:/etc/xinetd.d
Archivo Editar Ver Terminal Solapas Ayuda
service telnet
{
    flags           = REUSE
    socket_type     = stream
    wait           = no
    user           = root
    server         = /usr/kerberos/sbin/telnetd
    log_on_failure += USERID
    disable       = no
}
:~
  
```

Figura 7-206: Archivo telnet editado

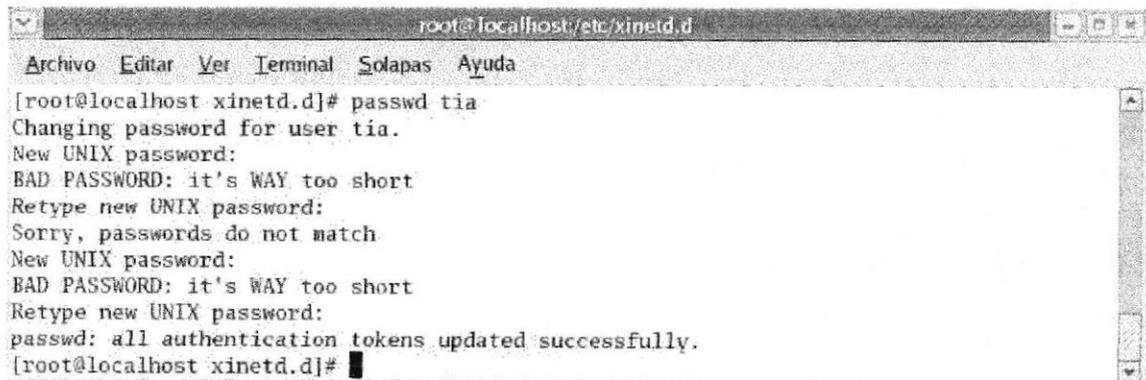
Luego de haber editado el archivo crear un usuario para el momento de hacer telnet poder acceder mediante este usuario y contraseña.



```
root@localhost:/etc/xinetd.d
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost xinetd.d]# adduser tia
[root@localhost xinetd.d]#
```

Figura 7-207: Creación de usuario

Después de haber creado el usuario proceder a asignar una contraseña.



```
root@localhost:/etc/xinetd.d
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost xinetd.d]# passwd tia
Changing password for user tia.
New UNIX password:
BAD PASSWORD: it's WAY too short
Retype new UNIX password:
Sorry, passwords do not match
New UNIX password:
BAD PASSWORD: it's WAY too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@localhost xinetd.d]#
```

Figura 7-208: Asignación de contraseña

7.8.7.1 CONFIGURACIÓN EN EL CLIENTE WINDOWS

HACIENDO TELNET DESDE EQUIPO CLIENTE WINDOWS

Para poder hacer telnet al equipo servidor debe hacer los siguientes pasos, ir a menú inicio del cliente y dar clic en ejecutar.

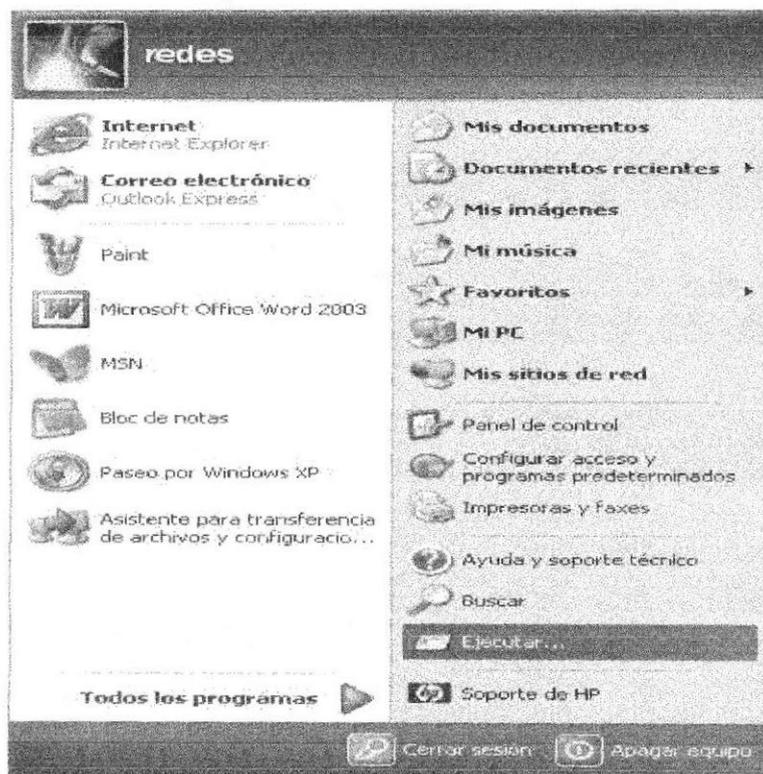


Figura 7-209: Inicio opción ejecutar

Luego aparecerá algo parecido a esta ventana donde debe digitar cmd para que se abra el ambiente texto del cliente.

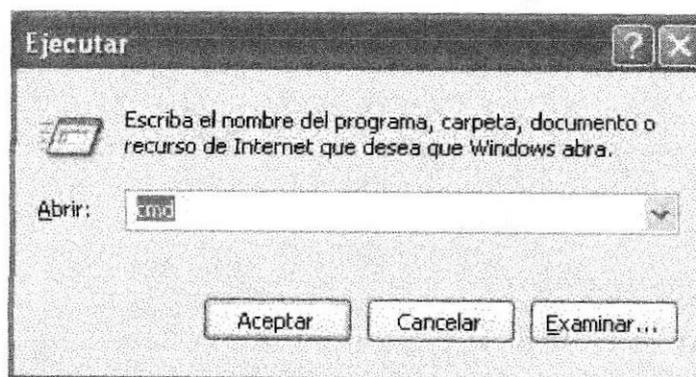


Figura 7-210: Comando cmd

Luego debe digitar la siguiente línea telnet + dirección IP a la que se quiere acceder, en este caso es el Servidor Linux.

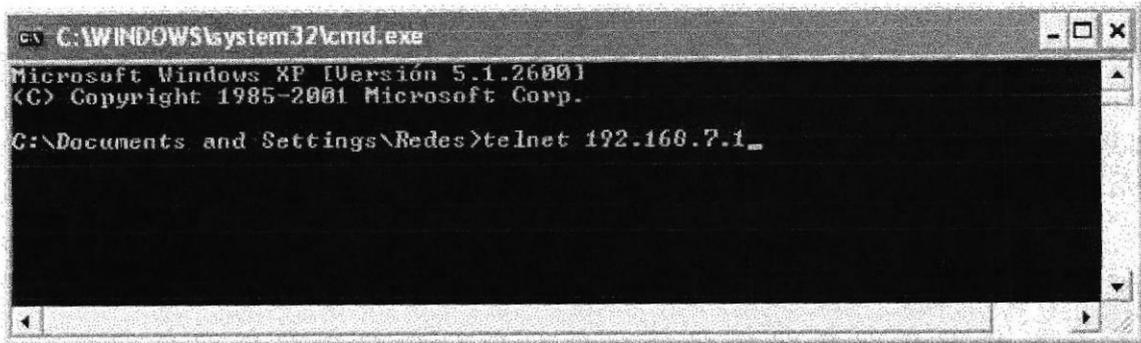


Figura 7-211: Comando telnet

Después de haber hecho el telnet pedirá el usuario y clave creados en el Servidor.

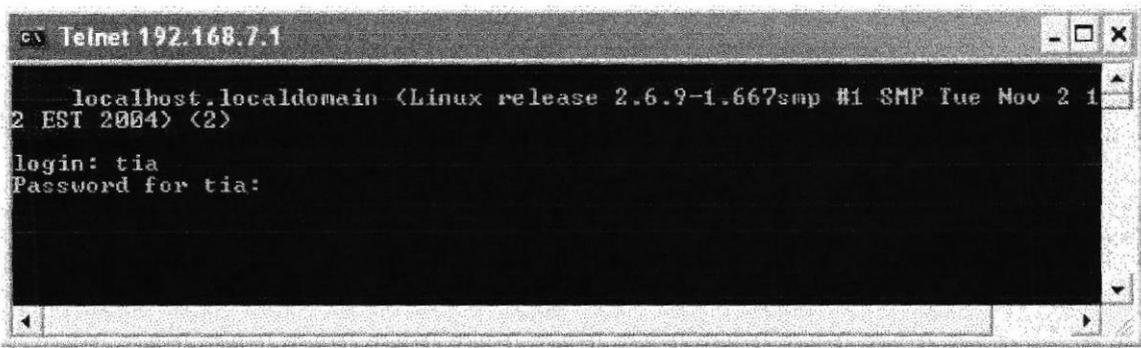


Figura 7-212: Autenticación

En esta parte como se puede observar ya entró a la configuración con el dominio tia.

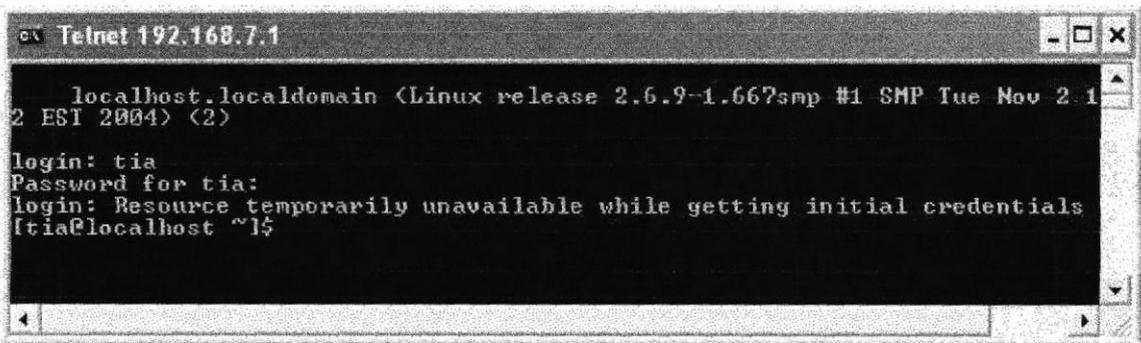
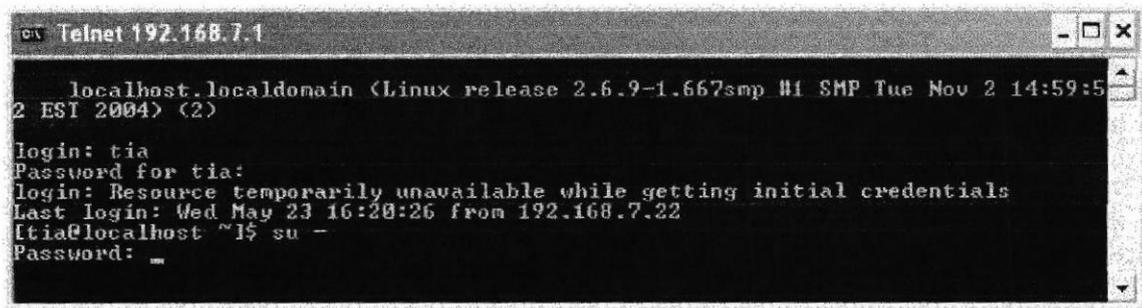


Figura 7-213: Ingreso modo no privilegiado



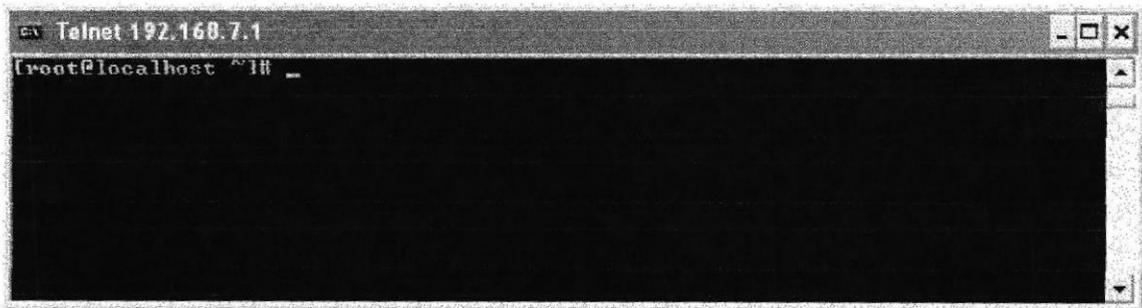
Para poder acceder al ambiente texto del servidor root, se hace con el comando su – el cual pedirá una contraseña, cabe indicar que es la misma contraseña con la que entró al servidor.



```
telnet 192.168.7.1
localhost.localdomain (Linux release 2.6.9-1.667smp #1 SMP Tue Nov 2 14:59:5
2 EST 2004) (2)
login: tia
Password for tia:
login: Resource temporarily unavailable while getting initial credentials
Last login: Wed May 23 16:20:26 from 192.168.7.22
Itia@localhost ~1$ su -
Password: _
```

Figura 7-214: Autenticación modo privilegiado

Como se puede observar aquí ya ha ingresado al ambiente texto del servidor, como lo muestra la gráfica.



```
telnet 192.168.7.1
[root@localhost ~]# _
```

Figura 7-215: Ingreso a modo privilegiado

DENEGAR TELNET

Para poder denegar el telnet se debe digitar esta línea, como lo muestra la gráfica.

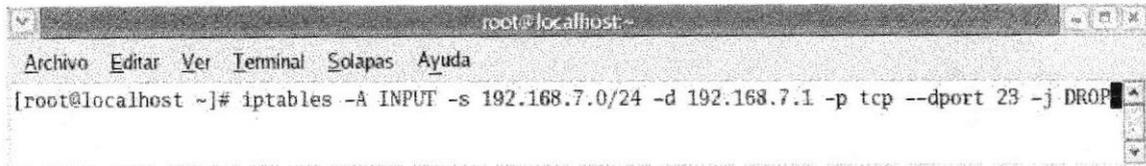


Figura 7-216: Denegar telnet

Para verificar si se denegó el telnet debe hacerlo con el comando iptables -L

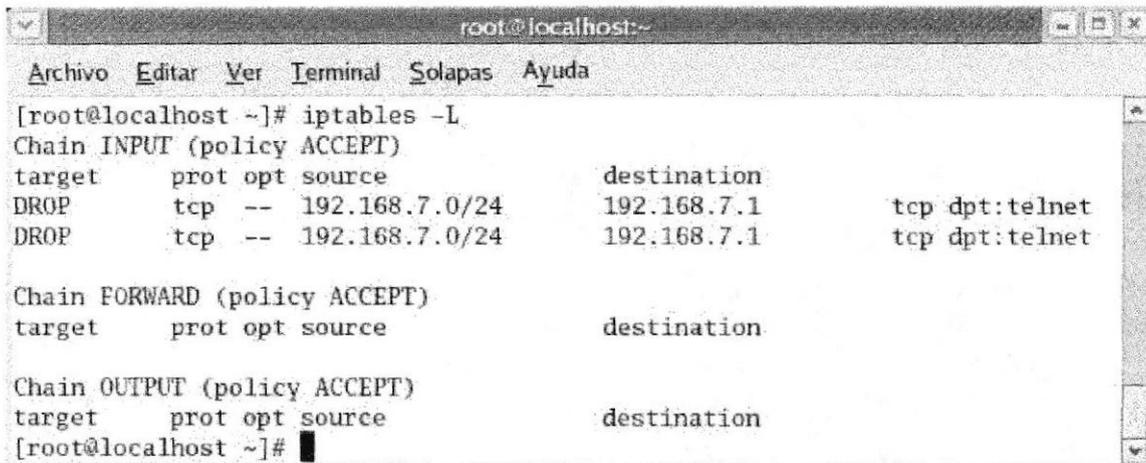


Figura 7-217: Verificación del telnet

Para hacer la comprobación abrir un símbolo del sistema Windows o ambiente texto de Windows.

Hacer telnet a la dirección IP del Servidor, como se puede observar ya está denegado el telnet.

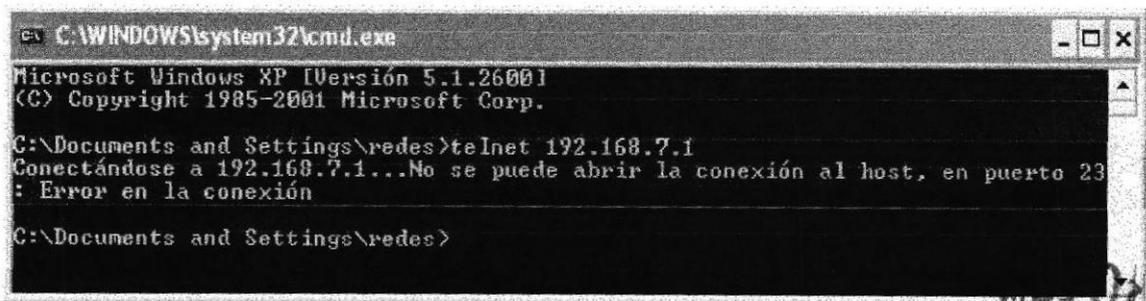
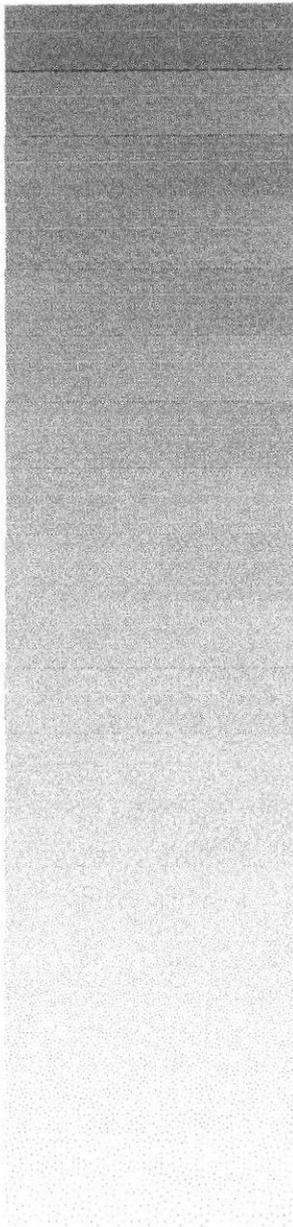


Figura 7-218: Verificación de telnet denegado





ANEXO
GLOSARIO

GLOSARIO

A

ADMINISTRACIÓN:

Proceso por el cual se mantiene un sistema a punto y operativo. Es una tarea de la que se encarga el administrador o root y sus posibles colaboradores. Abarca acciones tales como: configurar nuevos dispositivos, administrar cuentas, seguridad del sistema...

ALOJAMIENTO WEB:

También llamado hosting. Para tener una Web en Internet, disponible para todo el mundo las 24 horas del día, ésta tiene que estar alojada en un servidor permanentemente conectado a la Red, con las mayores garantías. HOSTALIA ofrece a sus clientes sus servidores para tal fin.

APACHE:

Servidor de páginas Web. Hoy por hoy líder del mercado de servidores, por delante de soluciones propietarias.

B

BRIDGENO: Número de puente si hay.

BIND:

Berkeley Internet Name Domain. Servidor de nombres de dominio.

BOOT:

Proceso de arranque en un sistema informático.

C

CONSOLA:

Una consola la forman el teclado y el monitor del equipo donde se tiene instalado GNU/Linux. No confundir con Terminal.

CUENTA:

Una cuenta en un sistema Unix/Linux puede ser algo así como la llave de un taller comunitario. Es decir, e tiene una llave personal que permite acceder a ese taller y utilizar algunas de las herramientas del mismo. Donde además se tiene que atender a las normas que rijan en ese taller.

CP:

Comando que se utiliza para copiar ficheros.



D

DATAGRAMA:

Un datagrama es un paquete discreto de datos y cabeceras que contiene direcciones, que es la unidad básica de transmisión a través de una red IP. Puede que lo haya oído llamar paquete.

DEMONIO:

Aparte del significado que todos conocen, en Unix/Linux se conoce como un programa que permanece en segundo plano ejecutándose continuamente para dar algún tipo de servicio. Ejemplos de demonio, son los servidores de correo, impresora, sistemas de conexión con redes etc.

DOMINIO:

Un dominio es tu dirección de Internet, tu nombre. Adquirir un dominio es tener el derecho a utilizar esa dirección, en exclusiva y para todo el mundo. Un dominio es, por ejemplo, tia.com, o hotmail.com.

DNS:

Domain Name Server. Servidor de nombres de dominio. Servicio de red que facilita la búsqueda de ordenadores por su nombre de dominio.

E

ENLACES:

Los enlaces o links permiten tener "copias" de un mismo archivo, ocupando solo el espacio del archivo real. Es decir, el enlace no es mas que otro archivo que apunta a el original.

ETHERNET:

Son redes que permiten distribuir datos a través de un solo cable por lo que necesitan de un protocolo especial que evite la colisión de los paquetes de datos, ya que solo se permite el envío de un solo paquete al mismo tiempo, encargándose el protocolo de su reenvío en caso de la colisión de ambos.

F

FTP:

File Transfer Protocol. Servicio de Internet que permite el envío y la recepción de ficheros. Para su uso se necesita disponer de una cuenta en la maquina que va a recibir o enviar los ficheros. Si bien hay multitud de maquinas en Internet que permiten el uso de sus sistemas utilizando una cuenta anónima y validando el password con la dirección de correo.

FIND:

find, comando que se utiliza para buscar archivos:



G

GNOME:

GNU Network Object Model Environment. Entorno de escritorio basado en las librerías GTK diseñadas para el programa de retoque fotográfico GIMP. Ofrece un entorno amigable y la posibilidad de que las aplicaciones intercambien datos entre si.

GNU:

Gnu is Not Unix. Proyecto de la FSF para crear un sistema UNIX libre.

GNU/LINUX:

Sistema operativo compuesto de las herramientas GNU de la FSF y el núcleo desarrollado por Linus Torvalds y sus colaboradores.

H

HOST:

Nombre de un ordenador en una red.

HTTP:

HyperText Transfer Protocol. Protocolo de red para la transferencia de páginas de hipertexto, o lo que es lo mismo, páginas Web.

I

IP:

Es un número que identifica unívocamente una máquina TCP/IP en la red. La dirección es de 4 bytes de longitud y normalmente se la representa en notación decimal puntuada, donde cada byte es representado en decimal con puntos . entre ellos.

ISP:

Es un acrónimo de Proveedor de Servicios de Internet (ISP - Internet Service Provider). Son organizaciones y compañías que proporcionan conectividad con Internet.

INETD:

Demonio encargado de mantener en escucha determinados puertos y de llamar a determinados programas en función de las señales recibidas. Por ejemplo, atiende a las llamadas de telnet, finger o ftp.

IDE:

El sistema de velocidad e intercambio del disco.

J

JOB:

Orden interna de bash que muestra los trabajos pendientes que se tiene en segundo o primer plano.

K

KDE:

K Desktop Environment. Entorno de escritorio que integra gestor de ventanas propio y una barra de tareas y que al igual que GNOME permite la interacción entre sus aplicaciones. Programado en C++ y con la base de librerías QT+ ha sido víctima de críticas por parte de la comunidad GNU/Linux, ya que estas librerías eran propiedad de una empresa comercial.

L

LINUX:

Núcleo del sistema operativo GNU/Linux

LOGIN:

Programa encargado de la validación de un usuario a la entrada al sistema. Primero pide el nombre del usuario y después comprueba que el password sea el asignado a este.

LOOPBACK:

Sistema de trabajo en red en modo local. Con este sistema se puede trabajar en red con su propio ordenador, su utilidad radica en probar programas de seguridad, leer las noticias o el correo de los servidores instalados en el ordenador o simplemente poder ejecutar Xwindow.

LS:

Comando para listar los ficheros y directorios.

M

MTU:

Tamaño máximo de los paquetes transmitidos por el puerto expresado en bytes.

MODULOS:

Porciones de código que se añaden en tiempo de ejecución al kernel para el manejo de dispositivos o añadir funciones al núcleo.

MONTAR:

Poner un dispositivo o un sistema de ficheros en disposición de ser usado por el sistema.

MKDIR:

Comando utilizado para crear directorios.



MV:

Comando utilizado para MOVER y RENOMBRAR tanto ficheros como directorios, no debe utilizarse desde "/", y si eso ocurriera, procura no hacerlo como ROOT.

N**NAME:**

Nombre de vlan.

NUCLEO:

Parte principal de un sistema operativo, encargado del manejo de los dispositivos, la gestión de la memoria, del acceso a disco y en general de casi todas las operaciones del sistema que permanecen invisibles para el resto.

O**O.S.:**

Operativo Sistema

P**PARENT:**

Parentela.

PORTS:

Puertos asignados a la vlan.

PASSWORD:

Palabra clave personal, que nos permite el acceso al sistema una vez autenticada con la que posee el sistema en el fichero passwd.

PATH:

Variable del entorno, cuyo valor contiene los directorios donde el sistema buscara cuando intente encontrar un comando o aplicación. Viene definida en los ficheros .bashrc o .bash_profile de el directorio home.

PARTICIÓN:

La partición de un disco, como su propio nombre indica es un fraccionamiento lógico (que se utilizan programas para hacerlo, no físico) donde se puede guardar información, o son requeridas dependiendo del S.O. utilizado.

PERMISOS:

Todos los archivos en UNIX/Linux tienen definido un set de permisos que permiten establecer los derechos de lectura, escritura o ejecución para el dueño del archivo, el grupo al que pertenece y los demás usuarios.

POP3 (CUENTAS DE CORREO):

Son los buzones de email a las que puedes acceder para ver tus mensajes mediante programas de correo como Outlook, Fedora o similares, y también vía Web mediante el

panel correspondiente. Cada cuenta POP3 tienes su propia contraseña para mantener la privacidad del correo.

PROCESO:

Programa en ejecución en un sistema informático.

Q

R

RINGNO: Número de anillo si hay.

REDIRECCIÓN

Con los operadores de redirección se puede dirigir la salida de un proceso hacia un dispositivo diferente al estándar o a un fichero.

ROOT:

Persona o personas encargadas de la administración del sistema Tiene TODO el privilegio para hacer y deshacer, por lo que su uso para tareas que no sean absolutamente necesarias es muy peligroso.

RM:

Comando utilizado para BORRAR FICHEROS. Usalo con precaución, en Linux no hay UNDELETES (Recuperación de ficheros)

RMDIR:

Comando utilizado para borrar directorios.

RUTA:

La ruta es el camino que siguen los datagramas a través de la red para alcanzar su destino. Servidor

S

STP:

STP usado

SIAD:

Encabezado para identificar vlan.

STATUS:

Estado de la Vlan.

SCSI:

El sistema de velocidad e intercambio del disco.



BIBLIOTECA
CAMPUS
PEÑAS

S.O.:

Son las siglas de Sistema Operativo, que también te lo puedes encontrar en inglés como

SEÑALES:

Las señales son eventos que se hacen llegar a un proceso en ejecución para su tratamiento por este. Las señales se las pueden mandar otros programas a otros programas. Tienen diferentes valores, y en función a esos valores el proceso que las recibe actúa de una manera u otra.

SHELL:

Traducido del inglés concha o caparazón. El shell es el intérprete de comandos que se establece entre nosotros y el kernel. Hay muchos tipos de shell cada uno con sus propias características, sin embargo el estándar en GNU/Linux es el shell bash ya que es el que forma parte del proyecto GNU.

SMTP:

Siglas de Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Email). Es un protocolo que permite transferir mensajes de correo electrónico de un servidor a otro. Se utiliza para enviar mensajes, y para recibirlos, el protocolo POP3. Es por ello que son dos parámetros habituales al configurar el email en un programa de correo.

SWAP:

Memoria virtual. Espacio de disco duro que utiliza el kernel en caso de necesitar mas memoria de la que se pueda instalar en el ordenador.

T**TRANS:**

TRANS, o si es una VLAN que cambia de topología Token Ring / FDDI a Ethernet.

TYPE:

Tipo de interfaces.

TELNET:

Servicio que nos permite la conexión a otro ordenador de la red, pasando el sistema a ser una Terminal de ese ordenador.

TERMINAL:

Una Terminal es un teclado y una pantalla conectados por cable u otro medio a un sistema UNIX/Linux, haciendo uso de los recursos del sistema conectado.

U**UNIX:**

Sistema operativo creado por AT&T a mediados de los 70

V

VLAN:

Identificación vlan.

VI:

Editor de texto muy potente aunque algo complejo al principio. Es el editor por defecto en casi todas las distribuciones. Hay versiones mejoradas (vim) o versiones para X Xvim. Debería ser obligado su aprendizaje 8-).

W

XWINDOW:

Es aquel que tiene la facultad de visualizar programas que están siendo ejecutados en otro ordenador de la red.

X

X Ó XWINDOW:

Entorno gráfico. Es el programa que se encarga de dibujar en pantalla todo lo que le solicitan los procesos que corren bajo este entorno.

