ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

REDISEÑO DE LA RED DEL INSTITUTO TECNOLÓGICO SUPERIOR "CENTRAL TÉCNICO"

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

JUAN DAVID BAZURTO LEONES

juanbazurto@gmail.com

DIEGO ALBERTO MENA AMORES

diegos.99@hotmail.es

DIRECTORA: ING. MÓNICA VINUEZA R. MSc.

monica.vinueza@epn.edu.ec

Quito, Octubre 2011

DECLARACIÓN

Nosotros, **Juan David Bazurto Leones** y **Diego Alberto Mena Amores**, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Juan David Bazurto Leones Diego Alberto Mena Amores

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por, **Juan David Bazurto Leones y Diego Alberto Mena Amores**, bajo mi supervisión.

_____

Ing. Mónica Vinueza R. MSc.

DIRECTORA DEL PROYECTO

AGRADECIMIENTO

Primeramente a mi familia, mi madre, mi padre y mis hermanos los cuales siempre han sido un apoyo constante durante toda mi vida, cuyos ánimos y valores me han acompañado y han sido importantes y me han dado la fuerza necesaria para la realización de este proyecto.

A la Ing. Mónica Vinueza, quien ha sabido guiar este proyecto con sus adecuados consejos, sabiduría y experiencia para poder concretarlo satisfactoriamente.

A mis grandes amigos, que me han acompañado durante el arduo camino universitario. Entre buenos y malos momentos se han convertido en una grata compañía, para concretar los diferentes objetivos propuestos a lo largo de la carrera.

A los buenos amigos que he encontrado en la Facultad de Ciencias, quienes durante el tiempo de realización de este proyecto me han brindado desinteresadamente su apoyo y amistad y se han convertido en una parte importante de mi vida.

A la Escuela Politécnica Nacional, prestigiosa Institución, que me dio la oportunidad de realizar mis estudios y de la cual me llevo buenos recuerdos y grandes amigos.

A todos los que de una u otra forma han colaborado directa o indirectamente en la consecución de este proyecto.

Juan David

AGRADECIMIENTO

Existen numerosas personas a quienes debo agradecer este logro profesional, a todas estas personas les estaré eternamente agradecido y siempre atento a brindarles mi apoyo cuando lo necesiten.

Definitivamente en primer lugar agradezco a Dios, por haberme dado el valor y la sabiduría para terminar satisfactoriamente este Proyecto de Titulación.

Agradezco también a mis padres hermanos y hermanas, quienes siempre apoyaron y motivaron mi formación académica en cada uno de los diferentes niveles educativos.

Del mismo modo me gustaría agradecer a la Ing. Mónica Vinueza por su valioso conocimiento, sus orientaciones, y quien inculcó un sentido de responsabilidad y seriedad, además que con su personalidad fue capaz de ganarse mi admiración y lealtad.

A mis amigos quienes me acompañaron en esta trayectoria de aprendizaje, además de tener una constante comunicación que contribuyeron para mejorar mi forma de actuar profesionalmente, y con quienes he compartido momentos gratos.

Y finalmente a la Escuela Politécnica Nacional por haberme permitido realizar mis estudios, formando profesionales íntegros y competitivos y siendo el lugar de enseñanza más calificado para esta carrera.

Diego

DEDICATORIA

Este trabajo se lo dedico a mi familia, que en buenos y malos momentos han estado siempre ahí prestos a brindarme su apoyo.

A mi madre Nancy, que con sus innumerables cualidades han podido inculcar en mi la fuerza y el valor necesarios, para nunca darme por vencido y siempre creer que el cielo es el límite y que todos los sueños se pueden alcanzar si se pone el esfuerzo y corazón necesarios.

A mi padre Eddye, que a pesar de los obstáculos presentados durante el camino siempre está de frente hacia los retos. Que en el día a día me enseña lo que verdaderamente significa el esfuerzo y la tenacidad en todos los aspectos de la vida.

A mis hermanos, Viviana y Eddye, que a pesar de ser menores me enseñan a diario lo importante que es la vida con sus ocurrencias y siempre han sido una de mis motivaciones para superarme cada vez más.

Juan David

DEDICATORIA

La concepción de este proyecto de titulación quisiera dedicárselo en primer lugar:
A Dios quién en todo el transcurso de la vida, me brindó fortaleza, dedicación, templanza, y que con su bendición siempre me acompaño en momentos de alegrías, tristezas y reveses.

A mis padres que con su amor, cariño y tenacidad, siempre han velado por mi bienestar, guiándome a enfrentar las adversidades y enseñándome a no desfallecer en cada uno de los intentos, y quienes con su lucha incansable han logrado ser el ejemplo a seguir y destacar. Además mis padres me brindaron la confianza en cada reto que se me presentaba, sin dudar de mi capacidad y responsabilidad.

A mi mamá Cruz María a quien tengo la suerte de siempre haber contado con su compresión, y que con una dosis de amor y ternura supo entender mis problemas.

A mi papá Carlos, que el tiempo que me dedicó me enseñó a valorar los pequeños detalles de la vida, y fortaleció mis valores y principios.

A mi sobrina Dámaris por el ser la persona más dulce, tierna e inocente, y por quien cada día me dedico a ser mejor.

A mi hermano Carlos, que me ofreció su apoyo en todo momento y fomentó en mí el deseo de superación.

A mi familia en general que con sus consejos, su apoyo y comprensión me ayudaron a perseverar en cada uno de mis objetivos.

A mi novia Diana por su paciencia, comprensión y amor, y por contar con su valioso apoyo, sincero e incondicional.

Diego

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

CAPÍTULO 1 FUNDAMENTOS TEÓRICOS

CAPÍTULO 2 ANÁLISIS DE LA INFRAESTRUCTURA DE RED ACTUAL

CAPÍTULO 3 REDISEÑO DE LA RED MULTISERVICIOS

CAPÍTULO 4 ALTERNATIVAS TECNOLÓGICAS Y ANÁLISIS DE COSTOS PARA EL REDISEÑO DE LA RED

ÌNDICE DE FIGURAS

CAPÍTULO 1 FUNDAMENTOS TEÓRICOS

CAPÍTULO 2 ANÁLISIS DE LA INFRAESTRUCTURA DE LA RED ACTUAL

CAPÍTULO 3 REDISEÑO DE LA RED MULTISERVICIOS

CAPÍTULO 4 ALTERNATIVAS TECNOLÓGICAS Y ANÁLISIS DE COSTOS PARA EL REDISEÑO DE LA RED.

RESUMEN

El Instituto Tecnológico Superior Central Técnico es un centro de enseñanza media y superior, de carácter público. El presente proyecto se enfoca en el rediseño de la red de datos del Instituto, enfocándose en una base teórica, un análisis de requerimientos, el rediseño, el análisis de alternativas tecnológicas y las conclusiones del proyecto.

En el primer capítulo se realiza una introducción teórica general de los conceptos de las redes de información multiservicios sobre los que se basa el proyecto. Se presenta los fundamentos teóricos para sistemas de voz y datos, abarcando temas como: elementos pasivos de red, normas de cableado estructurado, tecnologías, topologías de redes LAN, funciones de servidores de una intranet, estándares de telefonía IP, videoconferencia y videovigilancia.

En el segundo capítulo se documenta la situación actual de la red de la Institución. Se realiza un listado con toda la información referente a las instalaciones, equipamiento, cableado estructurado, manejo de servicios y datos de usuarios. Además se realiza el análisis del número de usuarios segmentados por grupos, número y tráfico generado por las aplicaciones y el estado actual de los servicios presentes en la Institución.

En el tercer capítulo se realiza el rediseño de la red para soportar datos, telefonía IP y video. En el rediseño de la red pasiva se especifican los subsistemas de cableado estructurado, los elementos activos y pasivos, aquellos que podrán ser reutilizados y los que sean necesarios añadir.

Se considera además el direccionamiento lógico para los dispositivos de red, el diagrama, y la segmentación de la red mediante VLAN´s. Finalmente se contempla el dimensionamiento de los servidores necesarios para cumplir los requerimientos actuales y futuros.

En el capítulo cuatro se presentan las diferentes alternativas tecnológicas (marcas y características técnicas) a disposición, para realizar la reingeniería de la red actual tanto en la parte activa como pasiva. Se presentan los costos

de la implementación de la red y se escoge la más conveniente desde el punto de vista técnico económico.

Y finalmente en el último capítulo se presentan las conclusiones recogidas durante la realización del proyecto; además de las recomendaciones más adecuadas para el proyecto.

PRESENTACIÓN

En la actualidad los establecimientos educativos, tienen como objetivo fomentar y participar en el desarrollo de nuevas habilidades mediante la utilización de herramientas tecnológicas modernas. Debido al avance vertiginoso impulsado y por la curiosidad de aprovechar las TIC, las instituciones educativas buscan alternativas para mejorar sus procesos administrativos, logísticos y pedagógicos.

Siempre con al afán de modernizar los sistemas, es indiscutible el rol que desempeña una red multiservicios que brinde las facilidades para la comunicación entre estudiantes, autoridades y padres de familia. En esta misión el Instituto debe enfrentarse a situaciones y escenarios cada vez más diversos, la cual con una infraestructura desorganizada y sin prevalecer ninguna norma internacional impide que desarrollen sus laborees con satisfactorios resultados.

En un mundo tan desarrollado como el actual los recursos de información son tan amplios que van más allá de lo que podemos imaginar. El desarrollo tecnológico en el país ha cobrado gran importancia, sobre todo en el área de las comunicaciones, lo que se ve reflejado en los modernos sistemas que han implementado las diferentes organizaciones públicas y privadas para este fin. Es importante mencionar que las comunicaciones juegan un papel indispensable en el desarrollo de todas las instituciones educativas y por consiguiente en el desarrollo de un país.

El Instituto Tecnológico Superior Central Técnico debe enfrentar el gran desafío de avanzar en la búsqueda e incorporación de mayores niveles de modernización de su estructura y organización actual para así incrementar la productividad en sus actividades de organización, planificación y control a nivel general. Esto se conseguirá poniendo en funcionamiento soluciones tecnológicas integradas y modernas que permitan dar una atención oportuna y eficiente a la comunidad educativa.

En virtud de lo expuesto, la Institución debe planificar una estrategia que deberá contemplar como elemento indispensable disponer de una red activa que permita la interconexión de las diversas áreas que la conforman como parte de un proyecto diseñado para contribuir a la formación de profesionales que respondan a las necesidades laborales, productivas, sociales y de colaboración con el desarrollo tecnológico industrial del país.

Además el sistema facilitará el acceso de la comunidad educativa a los diferentes servicios que residirán en la Intranet de la Institución, a través del cual podrán tener un fácil manejo de información y recursos compartidos. El mayor beneficio de tener un sistema centralizado, será el de proveer opciones tecnológicas que busquen el desarrollo integral de todos los usuarios que utilicen la red de comunicaciones.

Generar una cultura para utilizar adecuadamente y con responsabilidad las tecnologías de la información. Será responsabilidad de las personas que administren las comunicaciones así como también de los usuarios que accedan a los servicios.

CAPÍTULO 1.

FUNDAMENTOS TEÓRICOS.

1.1 SISTEMA DE CABLEADO ESTRUCTURADO.[F2][P1]

Un Sistema de Cableado Estructurado se define como el conjunto de cables, canalizaciones, conectores y demás dispositivos instalados a fin de proveer una infraestructura de comunicaciones con el propósito de implementar una red de Área Local. Un Sistema de Cableado Estructurado, en función de su extensión puede llegar a ser muy complejo dependiendo de varios factores, por lo que se debe ajustar a parámetros como distancias máximas, interferencia, rutas, entre otras, para cumplir con los objetivos planteados.

Es el fundamento de una red de comunicación de datos, sin embargo muchas veces personas sin la calificación adecuada no lo toman en cuenta lo que conlleva problemas en el funcionamiento de la red e insatisfacción en los usuarios de la misma. Entre las ventajas principales de poseer un Sistema de Cableado Estructurado se pueden anotar:

- Estandarización de materiales, elementos e interfaces de conexión.
- Sistema de arquitectura abierta.
- Consideraciones y diseño uniforme.
- Consistencia, flexibilidad y modularidad en crecimiento, movimiento o conectividad.
- Cumplimiento de estándares y normas internacionales.

1.1.1 MEDIOS DE TRANSMISIÓN [F1]

En un Sistema de Cableado Estructurado, uno de los factores que determina las limitaciones que este pueda tener es el medio de transmisión utilizado. A continuación se mencionan algunos de ellos.

1.1.1.1 Par trenzado

Es el medio de transmisión más ampliamente utilizado debido a su bajo costo, facilidad de conexión y mantenimiento. Un par trenzado está constituido por dos alambres de cobre, recubiertos cada uno por su respectivo aislante, enrollados entre sí a fin de evitar la interferencia. Típicamente se encuentran agrupados varios pares trenzados envueltos por una chaqueta y son usados tanto para transmisiones digitales como analógicas.

Dentro de esta categoría se encuentran los cables blindados o *STP* (*Shielded Twisted Pair*), estos cables además de las características descritas anteriormente poseen una malla protectora para reducir más la interferencia, generalmente son utilizados en ambientes ruidosos donde esta interferencia puede afectar a las comunicaciones.

Figura 1.1 Cable *STP*[W1]

El cable *UTP* (*Unshielded Twisted Pair*) es otro tipo de cable de par trenzado, este no posee la malla protectora que tiene el cable *STP,* sin embargo es el más utilizado por su bajo costo, reducido peso y facilidad de instalación.

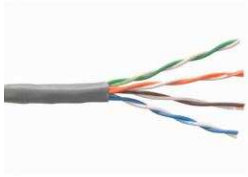


Figura 1.2 Cable *UTP*[W1]

1.1.1.2 Fibra óptica

Es un medio en el que la información es transmitida mediante pulsos de luz que viajan a través de ella, a diferencia de los cables de cobre donde la información

viaja a través de impulsos eléctricos, por lo que no es susceptible a la interferencia electromagnética ni a la estática.

Se pueden distinguir tres componentes, el núcleo que puede ser de plástico o vidrio, el plástico es más flexible pero no propaga la luz con la eficiencia con la que lo hace la fibra de vidrio, sobre este núcleo se monta una cubierta de plástico o vidrio con un menor índice de refracción[1] llamada manto, a la que a su vez cubre una chaqueta protectora.

Por el tipo de propagación de la luz se pueden encontrar dos tipos de fibra óptica, multimodo y monomodo. La fibra óptica multimodo es aquella en la que varios rayos con diferente modo de propagación son transmitidos; mientras que una fibra óptica monomodo es en la que se transmite únicamente un rayo de luz a través de ella.

Su numeración viene determinada por el tamaño del diámetro del núcleo y del manto, por ejemplo si se menciona una fibra óptica multimodo 50/125 micras esto significa que el núcleo tiene un diámetro de 50 micras y el manto tiene un diámetro de 125 micras.

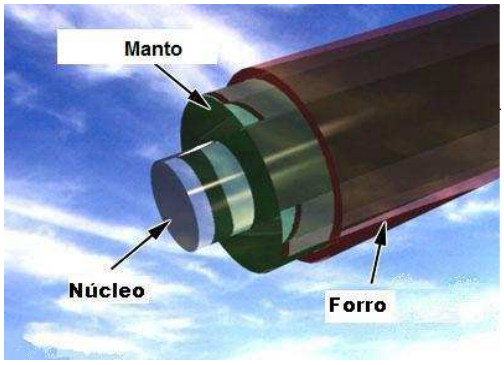


Figura 1.3 Fibra Óptica[W2]

En la fibra óptica multimodo, viajan varios rayos ópticos simultáneamente. Estos se reflejan con diferentes ángulos sobre las paredes del núcleo, por lo que recorren diferentes distancias, y se desfasan en su viaje a través de la fibra, resulta más económica que la fibra monomodo razón por la cual es más utilizada.

[1] Índice de refracción de un medio es el cociente entre la velocidad de la luz en el vacío y la velocidad de la luz en dicho medio

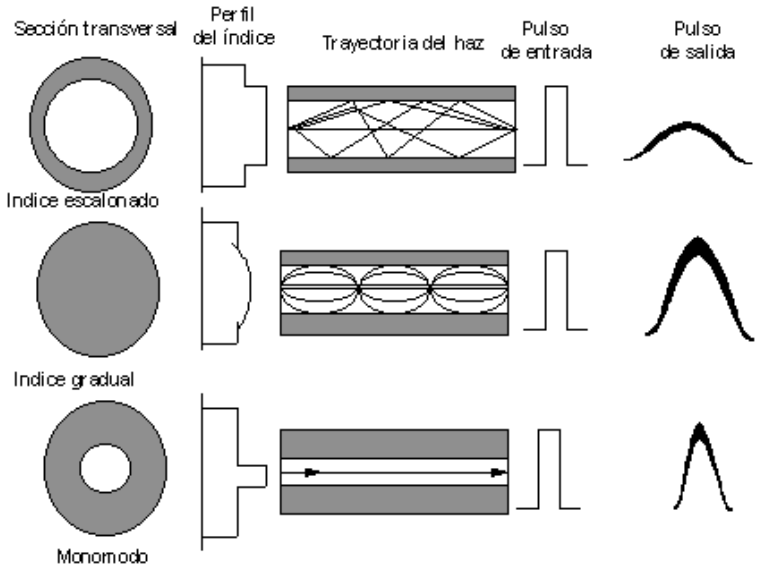


Figura 1.4 Comparación entre los tipos de fibra óptica[W3]

1.1.2 SUBSISTEMAS DEL CABLEADO ESTRUCTURADO[F2]

Un Sistema de Cableado Estructurado está compuesto de seis subsistemas:

1.1.2.1 Cableado Horizontal

El cableado horizontal se encuentra definido desde el conector ubicado en el área de trabajo hasta el cuarto de telecomunicaciones. En el cableado horizontal se incluyen elementos como el cable, el conector en el área de trabajo, las terminaciones mecánicas, los *patch cords* en el closet de telecomunicaciones y elementos multiusuarios ó puntos de consolidación en caso de existir.

Un *patch cord es* un cable usado para los conectores *RJ45* que se usa en una red para conectar un dispositivo electrónico con otro a través de cable *UTP* o sus variedades, estos son usados para la conexión del equipo de usuario hacia el conector del cableado horizontal.

El cableado horizontal debe estar en la capacidad de soportar diferentes tipos de servicios entre los cuales se pueden citar voz, datos, video, señalización tanto de comunicaciones como de automatización. Su diseño debe además contemplar la reducción en el mantenimiento, reubicación, la integración de futuros equipos y

cambios de los servicios de usuario que atraviesan a través de este; sin necesidad de cambios en el cableado.

La topología debe ser en estrella y cada salida deberá estar conectada al cuarto de telecomunicaciones del mismo piso del área a la que está sirviendo, la distancia máxima permitida es de 90 metros. La longitud total de los *patch cords* y los cables de conexión en el cuarto de telecomunicaciones no deben exceder los 10 metros.

Los cables reconocidos para el cableado horizontal son:

- Cable *UTP o ScTP*[2] de 4 pares impedancia 100 ohmios
- Dos o más cables de fibra óptica multimodo de 62.5/125 ó 50/125 micras

En caso de usar cable *ScTP* se debe conectar apropiadamente el apantallamiento a tierra para evitar problemas de interferencia que afecten a la comunicación.

1.1.2.2 Cableado Vertical

La función principal del cableado vertical es la de dar interconectividad entre los cuartos de telecomunicaciones, los cuartos de equipos y la entrada de servicios en el Sistema de Cableado Estructurado. El cableado vertical comprende los cables de *backbone,* que es la infraestructura principal de la red, los cables de interconexión, terminaciones mecánicas y *patch cords* o *jumpers,* usados para la interconexión entre cuartos de telecomunicaciones en un mismo edificio o la interconexión entre edificios.

El cableado vertical debe estar orientado a soportar todas las necesidades de los usuarios para uno o varios períodos, los cuales pueden variar entre tres y diez años. Durante este período el cableado deberá estar lo suficientemente dimensionado para ser capaz de soportar el número máximo de usuarios y aplicaciones simultáneas, por lo que deberá proveer estabilidad frente al crecimiento de las necesidades de los usuarios del sistema.

Es recomendable utilizar un cableado vertical conectado con topología en estrella; sin embargo con los conectores y equipos adecuados en los cuartos de

[2] *ScTP (Screened Twisted Pair, Par Trenzado Apantallado)* Variedad del cable STP posee un blindaje de papel metálico.

telecomunicaciones y dependiendo de las necesidades del usuario final pueden existir sistemas conectados en otras topologías tales como anillo, bus o árbol.

La topología en estrella es recomendada debido a su flexibilidad. En una conexión en estrella no se puede tener más de dos niveles jerárquicos, es decir solo se permite un dispositivo intermedio de conexión, para evitar la degradación de la señal y simplificar los movimientos, cambios y adiciones al sistema.

Los cables reconocidos para el cableado vertical son:

- Cable de Par Trenzado impedancia 100 ohmios
- Fibra óptica multimodo de 62.5/125 ó 50/125 micras
- Fibra óptica monomodo

Las distancias máximas para los diferentes tipos de cables están relacionadas directamente con el tipo de aplicaciones a ser soportadas por lo que resulta apropiado encontrar un punto para el cual las distancias sean las menores hacia el punto central. Incluso se puede observar la posibilidad de dividir el cableado en algunos sitios para trabajar con áreas más pequeñas si así es requerido.

1.1.2.3 Área de Trabajo

El Área de Trabajo está comprendida desde el terminal de salida en la terminación del cableado horizontal hasta el equipo en la estación de trabajo del usuario final, por lo que debe ser de fácil cambio debido a que generalmente no es permanente, se recomienda un área de trabajo de 10 m^2 para propósitos de diseño.

Los conectores deberán estar sujetos a las normas establecidas según el tipo de medio de transmisión utilizado (ANSI/EIA/TIA 568-C.1 para UTP y ANSI/EIA/TIA 568-C.3 para fibra óptica). Un *faceplate* es un accesorio de metal o plástico donde se coloca el conector y que permite la conexión a un dispositivo final de usuario.

1.1.2.4 Cuarto de Telecomunicaciones

La función primaria de un Cuarto de Telecomunicaciones es la terminación del cableado tanto horizontal como vertical a fin de hacer compatible el hardware de conexión. El uso de *jumpers* y *patch cords* permite una conectividad flexible a fin

de proveer un mayor número de servicios a las salidas de telecomunicaciones en el área de trabajo.

Un Cuarto de Telecomunicaciones además provee un ambiente controlado para alojar equipos, hardware de conectividad y empalmes que puedan servir a una cierta porción de las instalaciones servidas. Su superficie estará dada en función del área a la que brinda servicios.

En los Cuartos de Telecomunicaciones se utilizan los racks, que son armazones metálicos destinados a alojar los dispositivos electrónicos, informáticos y de telecomunicaciones. Estos tienen un ancho predeterminado de 19 pulgadas. Los gabinetes son las cajas donde se guardan los rack, estos elementos pueden ser montados en pared o en piso dependiendo de los dispositivos que van a alojar. Además de las regletas para la alimentación eléctrica de los equipos, en los racks se montan dispositivos como:

- *Patch panels*: Son paneles donde se ubican los puertos de telecomunicaciones, donde terminan todos los cables de red. En los *patch panels* se puede tener conectores RJ45 para los cables *UTP* o conectores *LC, FC o SC* en el caso de la fibra. En la figura 1.5 se pueden observar estos conectores.

Los conectores *LC y SC* son utilizados generalmente para la interconexión con los equipos de red, mientras que los conectores *FC* se utilizan para la conexión entre *patch panels*

Figura 1.5 Conectores RJ45, LC, SC y FC[W4]

- Organizadores: Son elementos que protegen y enrutan los cables y facilitan la realización de cambios o adiciones.

Cabe anotar que se pueden tener cuartos de telecomunicaciones secundarios ó *IDF (Intermediate Distribution Frame*) secundarios, utilizados principalmente en el caso de la interconexión entre varios edificios, o cuando existen tantos usuarios en un mismo piso que el cuarto principal de telecomunicaciones o *MDF (Main Distribution Frame)*. Es un rack de cables que sirve como punto intermedio y permite administrar de mejor manera la interconexión entre el *MDF* y los dispositivos de red. En el caso de la distribución de Cableado Estructurado para áreas dispersas, como es el caso de un campus, todos los *IDF´S* deben terminar conectados al *MDF*, donde se encuentran todas las conexiones además de la entrada de servicios de la red. La utilización de estos permite además facilidad cuando sean necesarios cambios o expansión en el Sistema de Cableado.

1.1.2.5 Sala de Equipos

La Sala de Equipos es considerada de manera distinta al Cuarto de Telecomunicaciones, a pesar de tener similares funcionalidades, por la complejidad del equipo contenido en este sitio. Debido a esta complejidad el costo de los equipos albergados en aquel sitio es mayor por lo que deben ser considerados equipos para facilitar la puesta a tierra, vinculación y protección donde sea pertinente. La Sala de Equipos es el punto central de la red donde se alojan los diferentes servidores; además de los equipos considerados de núcleo y la entrada de los servicios desde el exterior.

1.1.2.6 Entrada de Servicios

La entrada de servicios consiste en los cables, hardware de conectividad, dispositivos de protección y otros equipos necesarios para conectar los servicios exteriores a las instalaciones del cableado. Estos componentes pueden ser usados tanto por los proveedores de los servicios así como por los usuarios de la red interna.

El punto de demarcación, es decir el límite entre la red externa y la interna, puede ser constituido como parte de la entrada de servicios. Este punto es determinado por regulaciones vigentes para una locación en particular. Aloja además las protecciones eléctricas regidas por los códigos eléctricos correspondientes.

1.1.3 ESTÁNDARES PARA UN SISTEMA DE CABLEADO ESTRUCTURADO

[F2] [P1] [P14]

1.1.3.1 ANSI/TIA/EIA-568-C

Esta norma reemplaza a la ANSI/EIA/TIA-568-B publicada en 2001. El propósito de la norma ANSI/EIA/TIA-568-C. se describe en el documento de la siguiente forma: “Estándar para el Cableado de Telecomunicaciones Genérico para Instalaciones de Clientes.”

Este nuevo estándar fue desarrollado para que se convirtiera en el documento genérico de uso cuando un estándar específico no estuviera disponible. Se escogió la nomenclatura ANSI/EIA/TIA-568-C, debido a que ya era familiar para el ambiente industrial. Se recalca que el estándar anterior 568 B.1 se dividió en los estándares 568 C.0 y 568 C.1.

- **ANSI/EIA/TIA-568-C.0:** Facilita el diseño e instalación de sistemas de cableado de telecomunicaciones en cualquier tipo de entorno del cliente. El documento aborda la estructura, topologías, distancias, métodos de prueba, rendimiento, polaridad e instalación del sistema, sentando las bases para los estándares de cableado.
- **ANSI/TIA/EIA-568-C.1:** El estándar permanece igual a ANSI/EIA/TIA-568-B.1 en términos de estructura y cobertura. El estándar ahora recomienda fibra multimodo optimizada para láser de 50 µm y 850 nm e incluye pautas para gabinetes de telecomunicaciones (TE). El estándar continúa especificando una longitud de cable horizontal máxima de 100 m. La 568-C.1 es la revisión del estándar existente 568B.1.

Las guías y los requerimientos de la 568-C.0 se aplican a edificios comerciales sujetos a las excepciones y los aspectos permitidos definidos en la 568-C.1. Esto le permite a la 568-C.1 ser un documento que se enfoca hacia las oficinas en edificios comerciales. La nomenclatura en la norma 568-C.1 no modifica la definida por la 568-B.1.

La 568-C.1 también sufrió algunos cambios técnicos incluyendo:

- La Categoría 6 Aumentada (Categoría 6A) fue incluida como un medio reconocido (por referencia a la 568-C.0).
- Fue incluida la recomendación de seleccionar la fibra óptica 50/125um optimizada para láser a 850nm, como la fibra multimodo para edificios comerciales.
- El cableado 150W-STP, Categoría 5 y coaxial de 50-W y 75-W ya no son medios reconocidos.

Este estándar es el que se encuentra actualmente en vigencia para el cableado de telecomunicaciones en edificios comerciales, su propósito es el de establecer criterios técnicos genéricos tanto en implementación como en funcionamiento para un Sistema de Cableado Estructurado.

- **ANSI/TIA/EIA-568-C.2:** Especifica los componentes del par trenzado balanceado, así como los requisitos mecánicos y de transmisión que deben cumplir.

- **ANSI/TIA/EIA-568-C.3:** Dentro el estándar 568-C.3 se reunieron los estándares anteriores del ANSI/EIA/TIA-568-B y B.3, el estándar 568-C.3 fue completado y aprobado para publicación; el proceso de revisión permitió la incorporación de varios cambios:

  La nomenclatura de la ISO 11801 (OM-1, OM-2, etc.), fue incluida como la nomenclatura madre para la tabla de tipos de fibras reconocidas.

  La codificación de colores del conector, la envoltura y el color del adaptador, han sido redefinidos para situaciones donde el conector se utiliza para identificar el tipo de fibra; sin embargo, los códigos de colores no son obligatorios de manera que se pueden utilizar con otros fines.

  El ancho de banda mínimo para la fibra 62.5/125um fue aumentado de 160/500 [MHz/km] a 200/500 [MHz/km]. Esto también aplica para la fibra óptica de los *patch cord*.

Categorías de ANSI/TIA/EIA para cables UTP:

- Categoría 3 16MHz (10Mbps).
- Categoría 4 20MHz (16Mbps).
- Categoría 5 100MHz (100Mbps).
- Categoría 5e 100MHz. Puede llegar hasta 125MHz (250Mbps).
- Categoría 6 250MHz (600Mbps).
- Categoría 7 600MHz.

A continuación en la figura 1.6 se muestra la distribución par/pin de acuerdo se define en la norma para un *jack* de 8 posiciones.

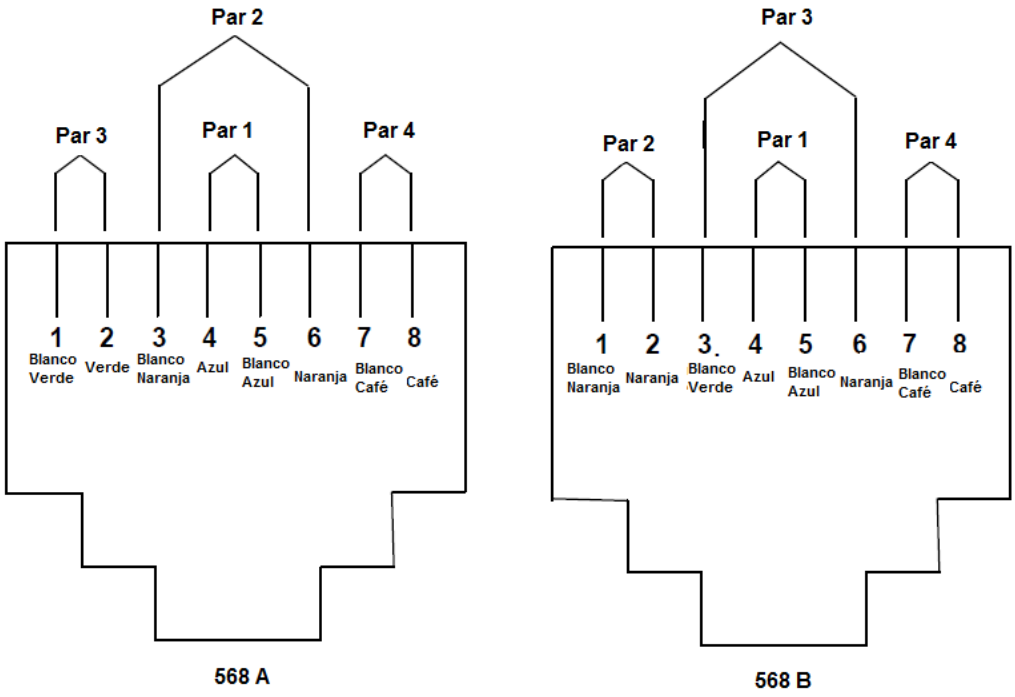


Figura 1.6 Configuración de pines en el terminal para un conector RJ-45 de 8 posiciones según 568A y 568 B[P1]

1.1.3.2 ANSI/TIA/EIA 569-A

Estándar para edificios comerciales-rutas y espacios para telecomunicaciones este estándar reconoce tres conceptos fundamentales relacionados con las telecomunicaciones y los edificios:

- Los edificios son dinámicos
- Las remodelaciones son mas la regla que la excepción
- Las telecomunicaciones son más que voz y datos

Como se define en el documento, el propósito de este estándar es uniformizar específicas prácticas de construcción y diseño, especialmente dentro y entre edificios comerciales. Los estándares son dados para espacios y rutas por las cuales los equipos y medios de telecomunicaciones son instalados.

1.1.3.3 ANSI/TIA/EIA - 606

Estándar de administración para telecomunicaciones en edificios comerciales, provee un esquema de administración uniforme, independiente de las aplicaciones, las áreas a ser administradas según el estándar son:

- Terminaciones.
- Medios de transmisión.
- Enrutamientos.
- Espacios.
- Puestas a tierra.

Entre las características que define se puede encontrar parámetros como codificación de colores, etiquetado, y documentación de un sistema de cableado instalado. Seguir esta norma, permite una mejor administración de una red, creando un método de seguimiento de los traslados, cambios y adiciones.

Facilita además la localización de fallas, detallando cada cable tendido por características tales como tipo, función, aplicación, usuario, y disposición.

1.1.3.4 ANSI/TIA/EIA-607

Estándar de requerimientos para uniones, puestas a tierra para telecomunicaciones en edificios comerciales, permite la planeación, diseño e instalación de sistemas de tierra para telecomunicaciones en un edificio con o sin conocimiento previo de los sistemas de telecomunicaciones subsecuentemente instalados.

1.1.3.5 Pruebas del Sistema de Cableado Estructurado.

Posterior a la instalación total del cableado para comprobar su correcto funcionamiento y desempeño se realiza la certificación por medio de un equipo especializado. Es necesario efectuar algunas pruebas básicas y otras opcionales como son: prueba de funcionamiento de las conexiones, atenuación, niveles de interferencias entre otras, las que son conocidas como pruebas de certificación.

De manera general el indicador describe las características de aprobado o fallido o también dudoso de los puntos del Sistema de Cableado Estructurado. Dependiendo del equipo y del nivel del mismo se pueden efectuar pruebas muy detalladas, las cuales pueden ser impresas para posterior revisión y calificación del sistema. Entre los factores que influyen en la certificación de un cableado estructurado son:

- Calidad y garantía del producto.
- Calidad de productos de cables.
- Calidad de la mano de obras del contratista.
- Calidad de la instalación.

1.2 REDES DE INFORMACIÓN[L1][L2]

El intercambio de información es fundamental para el desarrollo de las actividades cotidianas, para ello se han desarrollado las redes de información. Es así como se define a una red como un conjunto de dispositivos interconectados para el intercambio de información a través de una subred de comunicaciones.

Este proceso puede resultar complejo en la medida en que los servicios involucrados se diversifican. Para simplificar el diseño de las redes, se ha optado por dividirlas en capas que se encarguen de funciones independientes, y que a su vez se comuniquen por medio de protocolos.

Al conjunto de capas y protocolos se lo denomina arquitectura. Tal como lo define W. Stallings, “hay dos arquitecturas que han sido determinantes y básicas en el desarrollo de los estándares de comunicación: el conjunto de protocolos TCP/IP y el modelo de referencia ISO/OSI. TCP/IP es la arquitectura más adoptada para la interconexión de sistemas, mientras que OSI se ha convertido en el modelo

estándar para clasificar las funciones de comunicación.” A continuación se detalla cada uno de ellos.

1.3 MODELO DE REFERENCIA *ISO/OSI*[F4]

Este modelo se constituye como referencia para el desarrollo de protocolos y estándares para la comunicación de computadoras. Posee siete capas descritas a continuación.

1.3.1 CAPA APLICACIÓN

Es la que se encuentra directamente relacionada al usuario, y le proporciona los servicios necesarios para acceder a una red de información, es decir, se convierte en la interfaz final entre el usuario y la red.

1.3.2 CAPA PRESENTACIÓN

Se encarga de proporcionar la independencia necesaria a las aplicaciones con respecto a la representación y formato de los datos transmitidos de tal forma que estos sean tanto legibles para la capa aplicación como capaces de ser transmitidos por la red. Se encarga del formato de los datos pero no de su significado.

1.3.3 CAPA SESIÓN

Establece, gestiona y cierra las conexiones entre las aplicaciones que forman parte de la comunicación, estas conexiones son conocidas como sesiones.

1.3.4 CAPA TRANSPORTE

Brinda servicios de confiabilidad y transferencia transparente de los datos entre los extremos de la comunicación. Provee además mecanismos de control de errores, que permiten la verificación de la información enviada, y control de flujo entre dispositivo origen y dispositivo destino. Divide de ser necesario los paquetes y los pasa a la capa de red asegurando su correcta llegada al destino; además de aislar a la capa sesión de cambios en el hardware.

1.3.5 CAPA RED

Provee independencia a capas superiores respecto de enrutamiento, conmutación e interconexión en redes heterogéneas además de controlar los procesos propios de la subred de comunicaciones. Su unidad de información es el paquete.

1.3.6 CAPA ENLACE DE DATOS

Se encarga de ofrecer a la capa superior un canal libre de errores para la transmisión de datos, ofrece servicios de control de flujo y de errores a la capa de red. Resuelve problemas de daño, pérdida, secuenciamiento y direccionamiento de tramas, su unidad de transmisión.

1.3.7 CAPA FÍSICA

Se encarga de la transmisión y recepción de los bits por medio del canal de comunicaciones, provee características mecánicas, eléctricas y físicas para la activación y mantenimiento del enlace físico entre sistemas. Su unidad de transmisión es el bit.

1.4 ARQUITECTURA *TCP/IP*[F3]

El modelo *ISO/OSI* es un sistema de referencia que únicamente define funciones para cada una de las capas. La arquitectura *TCP/IP* es una familia de protocolos que se han convertido en estándares especialmente a nivel de Internet sin que exista un modelo oficial de *TCP/IP*. El número de capas que se definen es de cuatro a diferencia de las siete del modelo *ISO/OSI.*

1.4.1 CAPA APLICACIÓN

Al igual que en el modelo *ISO/OSI* es la que se relaciona directamente con el usuario. Utiliza los protocolos de nivel más alto con su respectivo número de *RFC*[3] *(Request for comments).*

1.4.2 CAPA TRANSPORTE

Usa dos protocolos para el intercambio de información de extremo a extremo, *TCP (Transfer Control Protocol)* y *UDP (User Datagram Protocol). TCP* es un protocolo de transmisión confiable orientado a conexión, el cual provee servicios

[3] *Request for comments:* Son documentos cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet, que en caso de ser aprobado puede ser implementado.

de control de errores y retransmisión, utilizados en aplicaciones en que los datos deben ser exactos tanto en el origen como en el destino. Por otro lado *UDP* es un protocolo no confiable, no orientado a conexión el cual es utilizado en aplicaciones donde la entrega debe ser más rápida que precisa. En la tabla 1.1 se listan algunos protocolos de capa aplicación, y el protocolo que utilizan en la capa transporte.

PROTOCOLO	FUNCIÓN	RFC	UDP/TCP
TELNET (TELetype NETwork)	Permite el acceso remoto a un equipo a través de la red.	*854*	*TCP*
SMTP (Simple Mail Transfer Protocol)	Permite el intercambio de correo electrónico basado en texto	*2821*	*TCP*
FTP (File Transfer Protocol)	Permite la transferencia de archivos basado en una arquitectura cliente - servidor	*2428*	*TCP*
TFTP (Trivial file transfer Protocol)	Es una versión reducida de *FTP,* permite el intercambio de archivos relativamente pequeños, por lo general asociado a la administración de dispositivos de red.	*1350*	*UDP*
DNS (Domain Name System)	Es un sistema de nomenclatura jerárquica de computadoras, que permite traducir nombres de dominio a direcciones IP.	*1034*	*TCP/UDP*
HTTP (HyperText Transfer Protocol)	Define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, *proxies*) para comunicarse.	*1945*	*TCP*
DHCP (Dynamic Host Configuration Protocol)	Permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente	*2131*	*UDP*

Tabla 1.1 Protocolos de capa aplicación[L4][F3]

1.4.3 CAPA INTERNET

En la capa Internet se utiliza el protocolo *IP* (*Internet Protocol*). Es un protocolo no confiable, se encarga del enrutamiento de mensajes entre redes, segmentación y transporte de los datagramas y deja funciones como control de flujo y control de errores a capas superiores.

En la capa Internet también se utilizan protocolos como *ICMP* (*Internet Control Message Protocol*) que se encarga de proveer mensajes de control a capas superiores, por ejemplo notificaciones de si un determinado host se encuentra o no disponible.

También son utilizados protocolos como, *ARP* (*Address Resolution Protocol*) y *RARP* (*Reverse Address Resolution Protocol*), entre otros que basan su funcionamiento en *IP*. Estos protocolos sirven para determinar direcciones *IP* a través de las direcciones físicas y viceversa

1.4.3.1 Direccionamiento IP

Una dirección IP permite la identificación de cualquier dispositivo en una red *IP,* un equipo puede dispone de tantas direcciones *IP* como interfaces tenga, que pueden ser asignada estática o dinámicamente.

Una dirección IP está formada por 32 bits, representada como cuatro números decimales separados cada uno por un punto. Ésta se divide en dos segmentos que representan, la dirección de la red y la dirección del dispositivo al que pertenece.

Los prefijos de red o máscaras, indican cuales son los números utilizados para uno u otro fin, se rellena con una serie de unos de izquierda a derecha hasta llegar al último bit, que identifique a la red, mientras que los bits restantes se rellenan con ceros e identifican a los *host*.

Existen las direcciones *IP* con clase, *classfull,* o sin clase, *classless.* Una dirección IP sin clase es la que usa una dirección de máscara no predeterminada. Dentro de las redes con clase se diferencian 5 tipos, desde A hasta E, las clases A, B y C son utilizadas para la identificación de redes, mientras que la clase D es utilizada para transmisión *multicast* y la clase E para propósitos experimentales.

Los primeros bits del número de red indican la clase de dirección IP, si se aplica la regla del primer octeto. Dentro de cada clase además se especifican un rango de direcciones reservadas para ser utilizadas en una intranet, las direcciones en este rango son conocidas como direcciones privadas, estas son de acceso restringido,

a diferencia de una dirección pública la cual es única en cualquier parte del mundo. En la tabla 1.2 se presenta un resumen de estas características.

Tipo	Función	Primer octeto	Dirección de máscara predeterminada	Rango de direcciones IP privadas	
				Desde	Hasta
Red clase A	Redes grandes	1 – 126	255.0.0.0	10.0.0.0	10.255.255.255
Red clase B	Redes medianas	128 - 191	255.255.0.0	172.16.0.0	172.31.255.255
Red clase C	Redes pequeñas	192 - 223	255.255.255.0	192.168.0.0	192.168.255.255
Red clase D	Multicast	224 - 239			
Red clase E	Experimental	240 - 255			

Tabla 1.2 Características del direccionamiento IP.[F3]

La falta de direcciones IP públicas, para que un determinado equipo sea identificado en cualquier sitio del mundo, se puede resolver mediante diferentes técnicas, una de ellas es *VLSM (Variable Lenght Subnet Mask),* que permite la optimización de las direcciones *IP,* al dividir cada una de ellas en tantas subredes como sea necesario, cada una con un diferente número de host según sea el caso.

1.4.4 CAPA ACCESO A RED

En la arquitectura *TCP/IP* no se define un protocolo específico para esta capa, lo único que asegura es que los paquetes *IP* sean transmitidos a través de la red.

Debido al avance de Internet en los últimos años los protocolos se han ido adaptando a esta arquitectura sin embargo el modelo *ISO/OSI* sigue siendo la referencia en el diseño de capas. En la figura 1.7 se presenta una comparación entre el modelo de referencia ISO/OSI y la arquitectura *TCP/IP.*

Figura 1.7 Comparación entre *TCP/IP* e *ISO/OSI*

1.5 REDES DE ÁREA LOCAL [L1][L3] [F4]

Una Red de Área Local o por sus siglas en inglés *LAN* (*Local Area Network*), se puede definir como un conjunto de hardware y software interconectados entre sí para compartir información dentro de un área geográfica relativamente reducida, varios cientos de metros.

1.5.1 TOPOLOGÍAS DE RED

Una topología de red es la forma en que los dispositivos se interconectan entre sí para compartir información a través de un medio físico. Esta interconexión puede ser abordada desde dos puntos de vista, físicamente (la disposición real de los equipos dentro de la red) ó lógicamente (la manera en que se comunican en el medio).

Existen diferentes métodos de topologías entre las que podemos anotar estrella, bus, anillo que se han convertido en las más utilizadas. Dependiendo de las necesidades de implementación de la red se puede escoger una o implementar

una combinación de varias de estas. A continuación se presenta una descripción de cada una de ellas:

- Topología Estrella: Es la más común dispone de un concentrador por el que fluye toda la información, es relativamente fácil de administrar e implementar. Su desventaja es que si el concentrador falla toda la red colapsa.

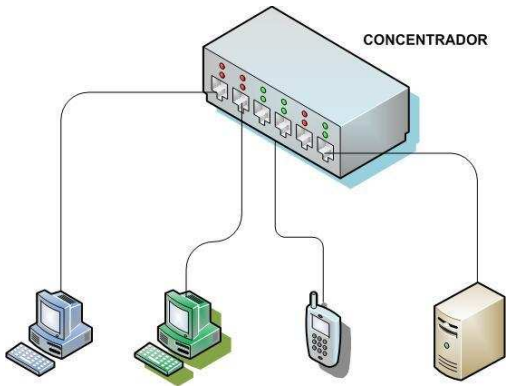


Figura 1.8 Topología Estrella

- Topología Bus: Todos los dispositivos se conectan al medio de transmisión generalmente un cable coaxial con terminaciones en sus extremos a fin de evitar ondas reflejadas. Su desventaja es que cualquier rotura en el cable provocaría la falla de toda la red.

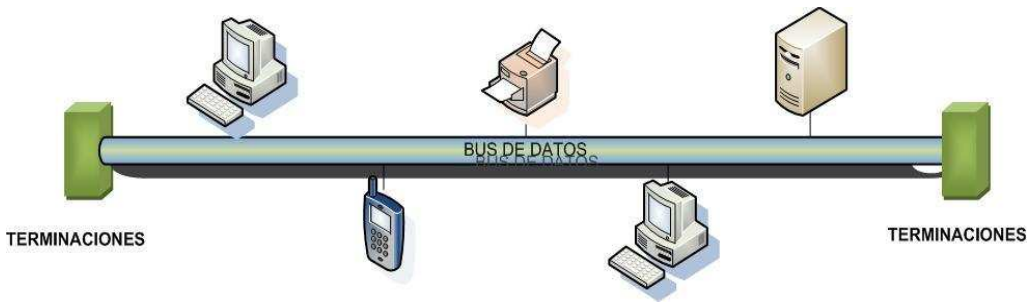


Figura 1.9 Topología Bus

- Topología Anillo: Los dispositivos se encuentran conectados generalmente en estrella sin embargo para la transmisión de datos utilizan un permiso denominado *token*, es muy resistente a fallas debido a que si una estación falla las demás pueden seguir transmitiendo datos; sin embargo no se encuentra difundida debido que resulta costosa.

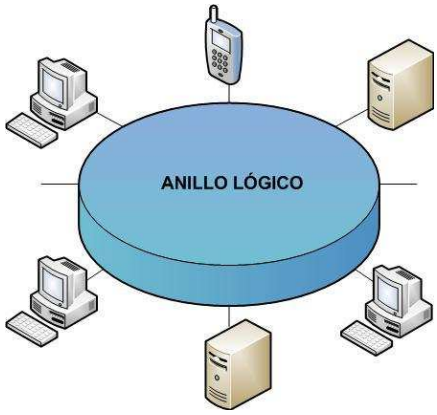


Figura 1.10 Topología Anillo

1.5.2 SISTEMAS *LAN*[F4]

El modelo *ISO/OSI* posee diferentes funcionalidades especialmente en capas superiores que son independientes de la arquitectura a través de la cual va a ser transmitida la información. Es así como en el estudio de Redes *LAN* este modelo se reduce únicamente a las dos primeras capas, la capa física y la capa enlace.

La capa enlace esta subdivida en dos capas las cuales son la subcapa de control lógico del enlace *LLC* y la subcapa de control de acceso al medio *MAC*. La primera se encarga de funciones como el direccionamiento lógico, el control de errores y control de flujo mientras que la segunda determina el procedimiento de acceso a un canal de comunicaciones compartido.

La labor de estandarización para redes de área local fue tomada a cargo por el *IEEE* (*Institute of Electrical anda Electronics Engineers*), mediante el grupo 802 es así como se establecieron los parámetros anteriormente definidos para las diferentes LAN.

Varios estándares fueron definidos sin embargo el más utilizado y desarrollado hasta la actualidad ha sido el 802.3, comúnmente conocida como *Ethernet.* El estándar define diferentes capas físicas lo que permite tener velocidades variadas sobre diversos medios de transmisión identificados mediante los parámetros mostrados en la figura 1.11 donde el método de señalización implica el uso de banda base o banda ancha para la comunicación.

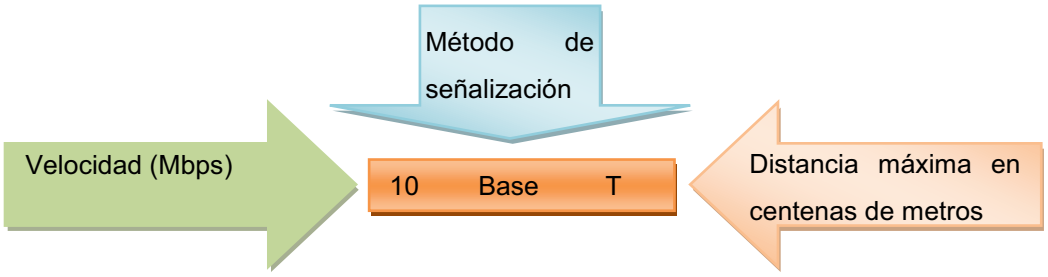


Figura 1.11 Parámetros para identificadores de capa física en IEEE 802.3

La más común de estas redes es 10BaseT (*Ethernet* de pares trenzados, red en estrella de 10 Mbps), donde las estaciones se conectan a la red por medio de un concentrador de cableado a través de las interfaces *RJ45* lo que implica que el medio es compartido por todos los dispositivos conectados, cubre una distancia máxima de 100 metros utiliza cables categoría 3 aunque puede ser utilizados con categorías superiores.

Su mecanismo de acceso al medio es por medio de *CSMA/CD* (*Carrier Sense Multiple Access/ Colission Detection*), lo que implica que para que no existan colisiones una estación que va a transmitir primero detecta si el canal está libre para la transmisión y durante ese intervalo de tiempo ninguna otra estación puede transmitir.

En el desarrollo de Ethernet una de las tecnologías actualmente más utilizadas y ampliamente difundidas es *Fast Ethernet* (Ethernet Rápida), conocida también como 100BaseT, que conserva las características de 10BaseT como el sistema de cableado, el modo de acceso al medio y los formatos de trama.

Esta tecnología implementa un esquema de conmutación lo cual implica transmitir los paquetes únicamente a su destinatario y no a todos como ocurría en sus antecesoras. Tiene una distancia entre estaciones de 250 metros y posee una topología física en estrella y lógica tipo bus.

Fast Ethernet cuenta con diferentes alternativas para diferentes medios físicos y diferentes tecnologías de transmisión para cada uno de ellos, su estándar es 802.3u.

Finalmente se considera también la tecnología *Gigabit Ethernet,* que es compatible con 10BaseT y 100 Base T, lo que permite una fácil migración y soporta diferentes alternativas para capa física.

Para esta tecnología se utilizan los siguientes estándares:

- 802.3z Ethernet conmutada a 1 Gbps.
  - 1000 Base SX: Fibra multimodo a 62.5 ó 50 um, distancia de hasta 550 metros.
  - 1000 Base LX: Puede alcanzar hasta 5 Km con fibra monomodo de 10um.
  - 1000 Base CX: Utiliza cable STP de 2 pares, distancia máxima 25 metros debido a que el medio utilizado es cobre.

- 802.3ab Ethernet conmutada a 1 Gbps.
  - 1000 Base T: Utiliza cuatro pares UTP para conectar dispositivos separados hasta 1000 metros.

En la figura 1.12 se presenta un resumen de las tecnologías presentadas.

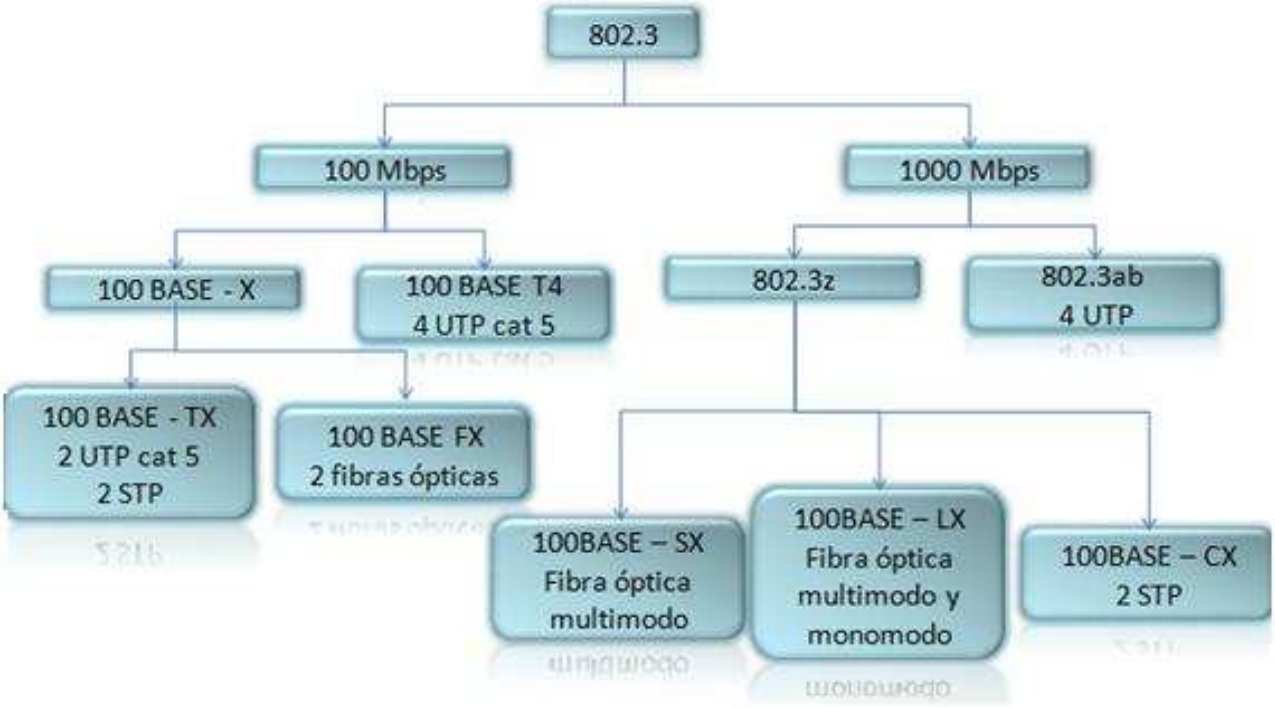


Figura 1.12 Opciones para IEEE 802.3[L1]

1.5.3 EQUIPOS ACTIVOS EN REDES *LAN*[F3][P2][P3]

En redes *LAN* se encuentran varios dispositivos que implementan la tecnología necesaria para la interconexión de los diferentes dispositivos, de acuerdo a las necesidades de la Institución donde se requiera la comunicación se pueden escoger uno o varios de los dispositivos descritos a continuación.

1.5.3.1 Conmutador o *switch*

Un conmutador o más comúnmente llamado *switch,* es un dispositivo que ofrece un mayor ancho de banda y un nivel de procesamiento mayor que el de un *hub*[4]. Como se mencionó anteriormente, un *switch* retransmite los datos de un paquete a un puerto específico basado en información propia de la trama, es decir, analizan las tramas y toman la decisión de enviarla a un determinado puerto en función de la información contenida en ella. Específicamente esta operación la realiza mediante las direcciones físicas[5] de los dispositivos, el *switch* almacena las direcciones físicas de los dispositivos conectados y las asocia con un puerto específico para la entrega de paquetes.

Entre los beneficios más importantes del uso de *switches* se puede anotar que se tiene un medio de comunicación dedicado para una transferencia de manera bidireccional, lo que significa que cada puerto constituye un dominio de colisión; además de tener varias transferencias activas en un mismo instante de tiempo y su velocidad es adaptable al medio.

Para el reenvío de tramas, también conocido como formas de conmutación, existen tres métodos que son:

- ***Cut & Through*:** La velocidad de conmutación es mayor debido a que el *switch* solo toma los campos referentes a la dirección y reenvía la trama al puerto correspondiente sin analizar la integridad de la misma.
- ***Store & Fordward*:** El *switch* almacena la trama completa, comprueba la integridad de la misma y la reenvía.

[4] *Hub:* El concentrador conocido también como *hub* es un dispositivo que en una red opera como repetidor, retransmite la señal que recibe a todos los puertos

[5] Dirección física es una dirección de 48 bits en hexadecimal que identifica a un dispositivo de red, esta dirección es controlada por la *IEEE* y donde los primeros 24 bits corresponden a la identificación del fabricante y los restantes a la identificación del producto.

- ***Fragment Free*:** Se almacenan los primeros 64 bits de la trama para asegurar que no existen colisiones y no transmitir fragmentos con errores.

Existen *switches* que analizan el tráfico de la red y en función de esto escogen un método dependiendo del tiempo y la cantidad de errores.

Con respecto al ancho de banda se puede considerar dos tipos de *switches* los simétricos, en los cuales el ancho de banda es el mismo para todos los puertos que lo constituyen y los asimétricos en los cuales algunos puertos poseen velocidades mayores. Estos puertos son utilizados generalmente cuando se requieren capacidades más altas de transmisión como por ejemplo el caso de conexiones con servidores o con otros *switches*. También se pueden agrupar diferentes puertos con el fin de crear una conexión con un gran ancho de banda equivalente a la suma de estos, esta técnica es conocida como *trunking.*

Un dispositivo que funciona a nivel de capa de enlace necesita un adecuado control de flujo de la transmisión de datos, mediante mensajes de pausa cuando la memoria del *switch* está a punto de llenarse, lo que previene la saturación del *buffer* y por lo tanto una mayor velocidad con la menor cantidad de paquetes perdidos posible. Esto se encuentra estandarizado en la norma IEEE 802.3x que establece transmisión y recepción simultáneos *full duplex* y control de flujo.

1.5.3.1.1 *Redes LAN virtuales VLAN´s*

El concepto de *LAN* virtuales (*VLAN*) se refiere a grupos lógicos dentro de una misma red *LAN,* mejora el rendimiento debido a que reduce los dominios de *broadcast*[6] lo que descongestiona la red y previene el acceso a usuarios no autorizados, colabora con la seguridad pues permite crear grupos de trabajo virtuales sin necesidad de reubicación física, estos grupos son especialmente útiles cuando cumplen la regla del 80/20, es decir que el 80% del tráfico es local al grupo de trabajo y solo el 20% es externo a éste.

En la figura 1.13 se muestran los beneficios de utilizar *VLAN´s* frente a una red sin ella, se puede apreciar que los dominios de *broadcast* se reducen lo que hace que los diferentes grupos de trabajo sean independientes entre sí a diferencia de

[6] Transmisión de paquetes de datos a todos los dispositivos conectados en una red

una solución tradicional donde todos los dispositivos conectados se encuentran un mismo dominio. La comunicación entre *VLAN´S* se realiza mediante *switches* capa 3 o enrutadores y se encuentran estandarizados en IEEE802.1q.

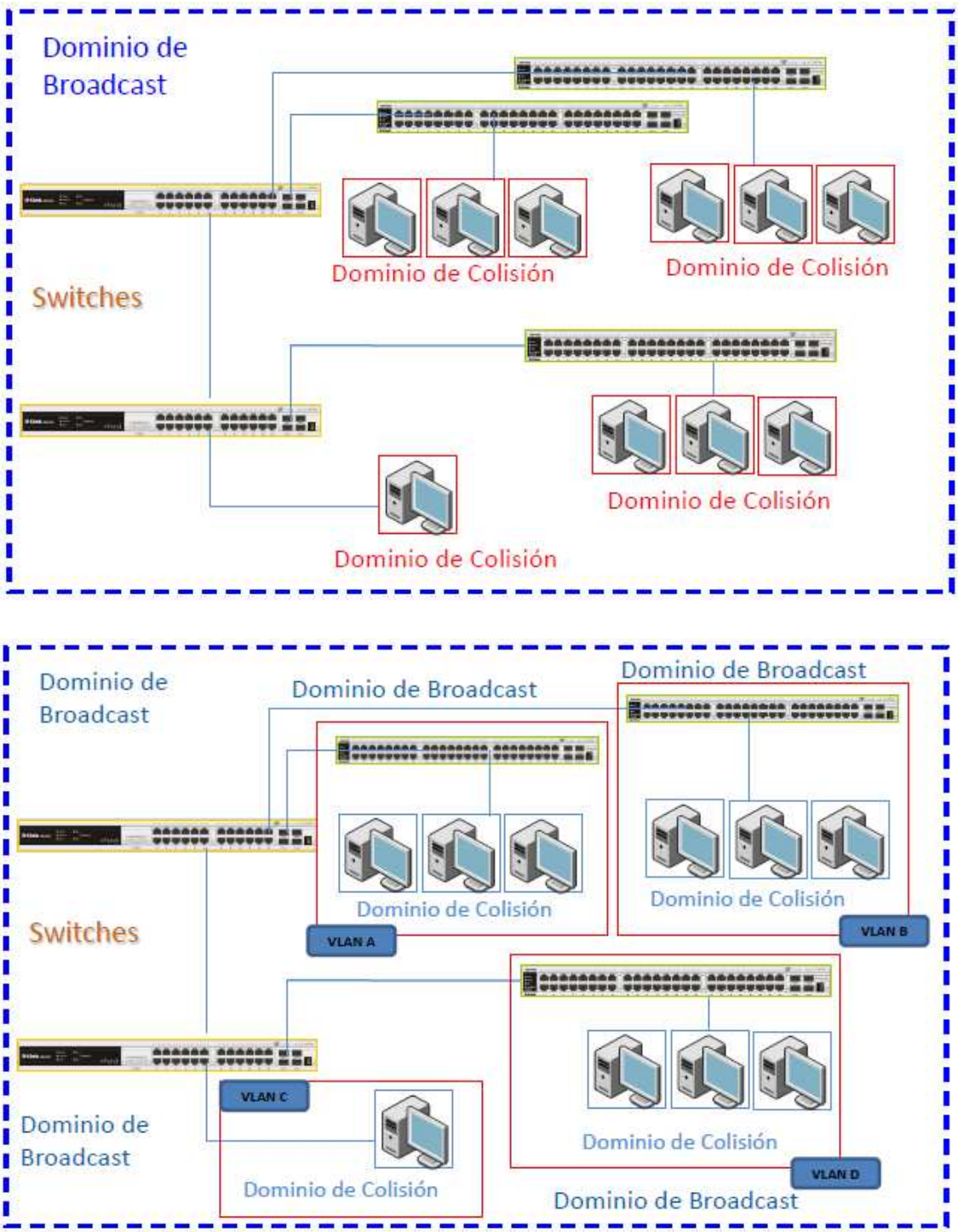


Figura 1.13 Red con uso de *switches* frente a red dividida en *VLAN´s*[P2]

Una *VLAN* se puede implementar de diferentes maneras:

- Por puerto, cada puerto en el *switch* pertenece a una *VLAN* específica, es la de más fácil configuración sin embargo es necesaria su reconfiguración cuando un usuario cambia de ubicación.
- Por dirección física, un dispositivo se puede conectar a cualquier puerto y por medio de su dirección física se asociará automáticamente a la *VLAN* específica, su desventaja es que para conectar cualquier dispositivo se debe conocer su dirección física para asociarla a determinada *VLAN.*
- Por protocolo, como su nombre lo indica cada *VLAN* manejará un tipo de protocolo, su tiempo de retardo es mayor debido a que es más complejo el procesamiento de direcciones lógicas que físicas.
- Por *IP Multicast,* se establece un grupo mediante una dirección *multicast*, un paquete es enviado a un *proxy* que maneja un grupo de direcciones IP específicas donde todas las estaciones son visibles.
- Por capas superiores, se basa principalmente por aplicaciones o servicios.

1.5.3.1.2 *Protocolos utilizados en los switches*

Es necesario también el uso de *Spanning Tree Protocol* el cual permite tener topologías redundantes en caso de falla de los enlaces activos de la red, los enlaces redundantes se colocan en estado de bloqueo para evitar lazos en la red, está estandarizado en IEEE 802.3d. Una mejora a este protocolo es IEEE 802.3w *Rapid Spanning Tree Protocol* el cual incorpora nuevas características que permiten un tiempo de convergencia menor después de un cambio de topología.

Para aplicaciones donde se requiere un gran consumo de ancho de banda la solución no es aumentar este sino optimizarlo para lo cual necesitamos implementar políticas de calidad de servicio. Lo que permiten estos mecanismos es clasificar y dar prioridades a los diferentes paquetes que cursan por la red de tal manera que el ancho de banda sea correctamente utilizado por las aplicaciones que lo necesiten. Se puede brindar calidad de servicio en diferentes capas según sea necesario, estos casos serán analizados posteriormente.

Entre otros estándares de importancia para los *switches* se pueden anotar los siguientes:

- IEEE 802.3af Alimentación sobre *Ethernet PoE*, permite proveer la energía eléctrica necesaria para el funcionamiento del dispositivo a través de la red de datos.
- IEEE 802.1x Define un modelo de control de acceso basado en una arquitectura cliente/servidor y un protocolo de autenticación que restringe el acceso a una red por medio de puertos accesibles de forma pública. El servidor de autenticación autentica a cada cliente conectado a un *switch* antes de permitirle el acceso a cualquier servicio.
- IEEE 802.1q Desarrolla un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (*Trunking*). En uno de sus apartados se especifica el uso de *VLAN´s* y el uso de las *vlan´s* nativas para dispositivos anteriores.
- IEEE 802.1p Permite la priorización de tráfico lo que proporciona calidad de servicio a nivel de capa 2, que se encuentra integrado en los estándares 802.1P y 802.1D, y es altamente difundido en redes *LAN* donde es completamente aplicable.

1.5.3.2 Ruteador y Conmutador Capa 3

Ruteo es la capacidad de transmitir los paquetes a través de diferentes sub redes mediante direcciones de capa de red, en este proceso se pueden atravesar varios nodos intermedios. Cuando una red crece su administración y funcionamiento es cada vez más complejo y es necesario establecer segmentarla en redes específicas. La comunicación entre estas redes se realiza a través de los dispositivos de capa 3, sean estos ruteadores ó conmutadores de capa 3.

Además de conocer la ruta que deberán seguir los paquetes que están conectados a través de este elemento hay protocolos específicos que permiten el intercambio de información de rutas para estos dispositivos como por ejemplo:

- *RIP Routing Information Protocol.* Es un protocolo de puerta de enlace interna o *IGP (Internal Gateway Protocol*) utilizado por los *routers*, aunque también pueden actuar en equipos, para intercambiar información acerca de redes *IP*.

- *OSPF* *Open Short Path First* es un protocolo de enrutamiento *IGP*, que usa un algoritmo enlace-estado (*LSA - Link State Algorithm*) para calcular la ruta más corta posible. Construye una base de datos enlace-estado (*link-state database*, *LSDB*) idéntica en todos los *routers* de la zona.

La elección entre un *router* y un *switch capa 3* dependerá de los requerimientos específicos de uso de la red, una solución con *routers* puede ser mucho más costosa sin embargo es probable que algunas características puedan ser solo implementadas a través de éstos.

1.6 REDES DE ÁREA LOCAL INALÁMBRICAS[F6][W44]

Las Redes de Área Local Inalámbrica se han fortalecido desde la consolidación del estándar IEEE 802.11 en junio 1997, el estándar se enfoca en explicar las dos capas del modelo *ISO/OSI* que son la capa física y la capa de enlace de datos. Las redes inalámbricas o denominadas también (*WLAN*) brindan a los usuarios de una red movilidad, escalabilidad, flexibilidad y reduce el tiempo de instalación además que actualmente este tipo de tecnología está alcanzando a transmitir a velocidades similares a la de una red cableada.

Las redes inalámbricas utilizan un medio de transmisión no guiado, que se propagan a través de ondas electromagnéticas que utilizan dos técnicas luz infrarroja o radiofrecuencia, aquellas que permiten acoplar a los dispositivos finales.

1.6.1 COMPONENTES DE IEEE 802.11

1.6.1.1 Estaciones *STAs*.

Son elementos fundamentales en una red inalámbrica y que deben contener una capa de control de acceso al medio (*MAC*) y una capa fisica (*PHY)*, estos elementos pueden ser móviles, estacionarios o portátiles.

1.6.1.2 Medio de transmisión.

Es el canal por el cual viajará la información, este canal es el espectro radioeléctrico y utiliza dos técnicas infrarrojo y microondas.

La tecnología *WLAN* trabaja en las bandas de frecuencias de 2.4 GHz (100 *Mhz*) y 5 GHz (150 *Mhz*) de las asignadas por la Unión Internacional de Telecomunicaciones (*UIT*) para aplicaciones industriales, científicas y médicas (*ISM*).

1.6.1.3 Puntos de Acceso.

El punto de acceso (*AP*) es una entidad *STA* pero con una funcionalidad añadida, que permite la conexión entre una red cableada y una inalámbrica. El punto de acceso es el eje principal de una red inalámbrica que coordina la comunicación entre *STA´s* mediante una antena externa que es transmisor-receptor. Las áreas de cobertura de estos equipos cuentan con un alcance máximo para diferentes ambientes, siendo estos internos o externos.

1.6.1.4 Sistema de Distribución.

Sistema de distribución o en sus siglas en inglés *WDS* (*Wireless Distribution System*), es aquel que permite la interconexion inalámbrica de un conjunto de *Access Points* (APs), con el propósito de obtener una mayor área de cobertura siempre y cuando los *AP´s* utilicen el mismo identificador, canal de radio y claves en caso de utilizarlas.

“La ventaja de *WDS* sobre otras soluciones es que conserva las direcciones *MAC* de los paquetes de los clientes a través de los distintos puntos de acceso”. Los dispositivos móviles que se trasladan de una zona de cobertura de un *AP* a otro lo realizan si perder la conectividad.

1.6.2 MODOS DE OPERACIÓN DE REDES 802.11

Tomando en consideración todos los elementos que constituyen una red 802.11 se precisan dos conjuntos, Conjunto de Servicios Básicos y el Conjunto de Servicios Extendidos.

1.6.2.1 Conjunto de Servicios Básicos.

Un conjunto de Servicos Básicos (BSS) es la unidad fundamental del estandar IEEE 802.11, el cual esta formado por dos o más dispositivos inalámbricos que se comunican mediante un solo punto de acceso y además que comparten el medio

de transmisión. Toda comunicación que realicen las estaciones estará dentro un zona denominada Area de Servicios Básicos (BSA).

1.6.2.1.1 *Redes Independientes ó Redes Ad Hoc*

En las redes IEEE 802.11 el modo de operación *Ad Hoc* es conocido como Conjunto Básico de Servicos Independientes, son redes inalámbricas que están formados por un pequeño grupo de estaciones las cuales se comunican directamente entre ellas sin la necesidad de un dispositivo de administración centralizada.

Las redes *Ad hoc* pueden expandirse de una forma autónoma, para prestar servicios de enrutamiento, para aquellas estaciones que no tiene una conexión inalámbrica directa retransmitiendo los paquetes.

Las redes *Ad Hoc* son redes temporales que se crean con un propósito específico para compartir información en ese momento, se caracterizan porque cada una de las estaciones puede ser el origen, el destino o el encaminador.

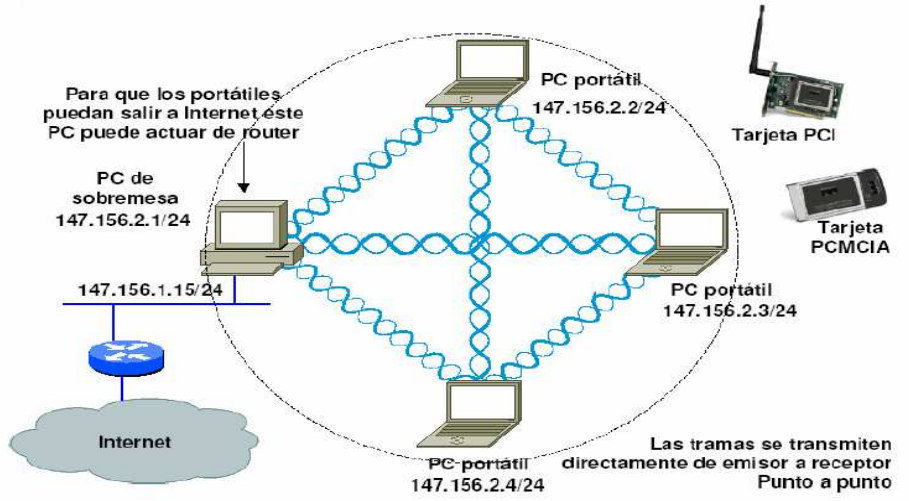


Figura 1.14 Red Ad – Hoc [T13]

1.6.2.1.2 *Redes de Infraestructura*

Una red de infraetsructura se diferencia con la *Ad Hoc* ya que existe una dispositivo de coordinación centralizado (Punto de acceso), que es el encargado de transferir las tramas desde la estación origen al punto de acceso y éste a su

vez se comunica con la estación destino. El punto de acceso administra todas la comunicaciones dentro de la zona de cobertura, por lo cual las estaciones solamente deben estar dentro del rango de cobertura del *AP*.

Para poder comunicarse en una red de infraestructura, las estaciones necesitan estar asociados a un punto de acceso, para la asociación se utliza un *SSID*[7]. Si es necesario un mayor rango de cobertura en una zona, se deben ubicar más *AP´s* con sus áreas sobrelapadas para garantizar la comunicación.

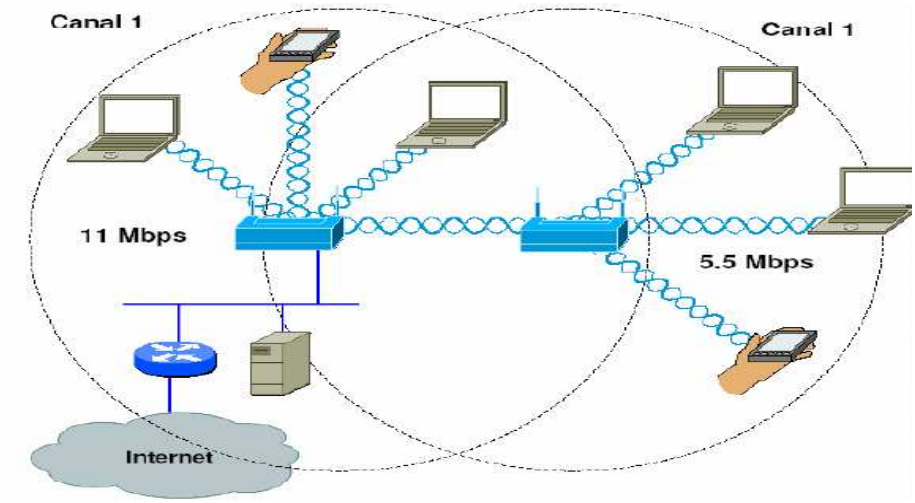


Figura 1.15 Red de Infraestructura.[T13]

1.6.2.2 Conjunto de Sevicios Extendidos (*ESS*)

Es el conjunto de varios *BSS*s y redes de área local integrada con el fin de tener una mayor área de cobertura.

1.6.3 ESTÁNDARES IEEE 802.11[W45][W46]

Desde sus inicios el estándar IEEE 802.11 ha trabajado con velocidades de transmisión de 1 y 2 Mbps, pero desde su creación han existido varias enmiendas a este estándar mejorando las características, así se tienen algunas extensiones al mismo que son 802.11 a, 802.11b, 802.11g, 802.11n.

[7] *Service Set identifier,* es un nombre incluído en todos los paquetes de una red inalámbrica (*Wi-Fi*) para identificarlos como parte de esa red

1.6.3.1 IEEE 802.11a.

Este protocolo es una enmienda al estándar IEEE 802.11 ratificado en 1999. IEEE 802.1a trabaja en la banda de frecuencia de 5 GHz una banda no licenciada, utiliza la modulación *OFDM* (*Orthogonal Frequency Division Multiplexing*) que permite transmitir a velocidades que van desde los 6 Mbps hasta los 54 Mbps.

Este protocolo tiene 12 canales cada uno de 20 MHz, cada canal posee 52 subportadoras, de las cuales 48 se utilizan para transmitir datos y 4 portadoras piloto para monitoreo, la separación entre cada subportadora es de 0.3125 MHZ.

Una de las deficiencias de este estándar es que no es compatible con IEEE 802.11g.

1.6.3.2 IEEE 802.11b.

Este estándar también es una enmienda del estándar original IEEE 802.11 definido en 1999. Opera en el rango de frecuencia de 2.4 GHz, soporta velocidades de 5,5 y 11 Mbps utilizando una modulación DSSS (*Direct Sequence Spread Spectrum*) con CCK (*Complementary Code Keying*) obteniendo así velocidades superiores. CCK ofrece una ventaja de ser más robusta frente a distorsión multi trayectoria.

IEEE 802.11b utiliza 14 canales cada uno de 22 MHz, de los cuales se pueden utilizar 3 canales sin obtener interferencia entre ellos.

1.6.3.3 IEEE 802.11g.

Debido a los grandes problemas de incompatibilidad entre los estándares anteriores, en el año 2003 se ratifica una nueva enmienda sobre IEEE 802.11 y se crea el estándar IEE 802.11g que permite trabajar en la banda de 2.4 GHz utilizando la modulación OFDM para así alcanzar un velocidad máxima de 54 Mbps. Con esto se brinda compatibilidad con el estándar IEE 802.11b (5,5 y 11 Mbps) y el IEEE 802.11 (DSSS).

El estándar mantiene el mismo número de canales y modulación (CCK) que 802.11b. 802.11g es el estándar más difundido hoy en día, mantiene una aceptación muy buena en el mercado por su compatibilidad.

1.6.3.4 IEEE 802.11n.

Estándar aprobado en 2009 y desarrollado en 2007, se afirma que teóricamente pueda llegar alcanzar 540 Mbps, ya que utiliza la técnica MIMO *(Multiple Input, Multiple Output). MIMO* utiliza múltiples receptores como transmisores para elevar el rango de cobertura.

En la tabla 1.2 se observa las principales características de los estándares IEEE 802.11a, b, g y n.

Estándar	802.11 a	802.11 b	802.11 g	802.11 n
DESCRIPCIÓN	Estándar WLAN de alta velocidad	Estándar WLAN de velocidad media	Establece una técnica de modulación adicional	Estándar WLAN mejora el rendimiento
FRECUENCIA [GHz]	5	2,4	2,4	2,4 y 5
VELOCIDAD [Mbps]	54	5 a 11	54	600
USUARIOS SIMULTÁNEOS	64	32	50	
MODULACIÓN	OFDM	DSSS	OFDM	OFDM

Tabla 1.3 Estándares IEEE 802.11[W36]

1.6.4 SEGURIDAD EN REDES INALÁMBRICAS.[T14][T15][W44]

La seguridad en redes inalámbricas debe tomar en consideración los parámetros básicos para cualquier red, es decir se debe proteger la información que se transmite por el medio. En un esquema de seguridad se considerará la confidencialidad, autenticación, integridad y disponibilidad.

- Confidencialidad, protege que la información sea irradiada a usuarios no autorizados.
- Autenticación, permite que antes de acceder a cualquier recurso de la red, los usuarios, se registren y se verifique sus permisos.
- Integridad, busca el mecanismo para que la información no sea modificada por usuarios no autorizados.

- Disponibilidad, se refiere a que el recurso y la información se encuentren siempre accesibles para cualquier usuario que los necesite.

1.6.4.1 *WEP.*

Uno de los primeros métodos de seguridad implementado para el entorno inalámbrico fue la utilización del protocolo *WEP* (*Wired Equivalent Privacy*), este algoritmo de seguridad para el estándar IEEE 802.11 se fundamenta en utilizar una clave compartida para cifrar la comunicación, esta llave la conocerán tanto la estación como el *access point*. *WEP* para cifrar la comunicación se emplea el algoritmo *RC4* con longitud de llaves de 64 ó 128 bits, de los cuales 24 bits de estos son para el vector de inicialización. Además para verificar la información se utiliza el algoritmo *CRC* 32.

Como debilidad de este estándar se observa que el vector inicialización es muy pequeño causando que después de cierto tiempo se pueda repetir y sea factible para un atacante descubrir los datos, además que este estándar no indica la forma en que a clave compartida será distribuido. Otra desventaja radica en que las claves compartidas no se actualizan periódicamente manteniendo las mismas por mucho tiempo y crenado riegos de seguridad, finalmente se puede anotar que *WEP* no realiza autenticación.

1.6.4.2 WPA

Wi-Fi Protected Access, se desarrolla con el objetivo de fortalecer la seguridad y solucionar algunas vulnerabilidades del protocolo *WEP*. De esta forma el protocolo de encriptación es *TKIP* basado en *RC4* pero se emplea dos vectores de inicialización de 48 bits cada uno. Para la distribución de las claves ahora se genera de forma automática*, WPA* incluye parte del protocolo IEE 802.11i y como política de integridad sustituye el algoritmo *CRC* 32 por el *MIC* (*Mesaage Integrity Code).*

Para el proceso de autenticación se mejora empleando dos mecanismos de autenticación con *EAP* y *IEEE 802.1 x,* mediante un protocolo *RADIUS* para que el *AP* se autentique con un servidor. *EAP* es un método es una clave compartida que solamente se utiliza para el inicio de la autenticación, mas no para el cifrado de datos.

1.6.4.3 *TKIP* (*Temporal Key Integrity Protocol*).

Este protocolo brinda integridad a la comunicación aumentando el tamaño de la clave a 128 bits y el tamaño del vector de inicialización a 48 bits, de esta forma se protege que las claves puedan ser reutilizadas. *TKIP* para mantener la integridad y privacidad genera dos etapas, en la primera con la dirección *MAC* de un usuario que desea transmitir, un contador (*TKIP secuence counter*) y la llave temporal se crea una llave de sesión de usuario, la misma que tiene una longitud de 128 bits. El contador se crea a partir de la dirección de destino, de la dirección fuente, la prioridad, y los datos.

Una vez generada la llave de sesión, y con el vector de inicialización se crea una llave para encriptar todos los datos, mediante le algoritmo *RC4.* De esta manera se mejora la integridad de los datos.

1.6.4.4 *EAP*.

La función que especifica *EAP* (Protocolo de autenticación extensible), es la de adicionar nuevos métodos de autenticación. EAP se desarrolló con el objetivo de mejorar a protocolos como *PAP*[8] *y CHAP*[9]*.*

EAP surge como la necesidad de tener un protocolo que transporte el método de autenticación, designando la autenticación a un servidor de acceso. Este servidor determinará el método de autenticación ya sea por certificados digitales o contraseñas, y el protocolo de autenticación. Siendo una ventaja puesto que los *AP´s* no manipularían estas características.

Dentro de EAP se contemplan varios métodos de autenticación, tanto para el uso de certificados digitales como para el uso de contraseñas, que son los siguientes:

- ***EAP TLS*:** Los certificados digitales los deben poseer tanto el cliente como el servidor, su autenticación es de dos vías, utiliza claves dinámicas *WEP*, y el cifrado de los datos se realiza mediante le protocolo *TLS* (Seguridad en capa la capa Transporte). Una de las desventajas es que al enviar la identificación la misma se envía sin cifrar lo cual produce un riesgo se seguridad, además que la distribución de los certificados puede resultar difícil y costosa considerando el número de equipos clientes.

[8] *PAP Pasword authentication protocol*
[9] *CHAP Challenge Handshake Authentication Protocol*

- ***EAP TTLS**:* Es similar a *EAP TLS*, diseñada por *Certicom y Funk*. Este método se caracteriza por tener solamente el certificado en el servidor con lo cual la autenticación del cliente por parte del servidor se procede cuando la sesión *TLS* se establezca.
- ***PEAP*:** Desarrollada por *RSA Security, Microsoft y Cisco*. Este mecanismo también utiliza un certificado en el lado del servidor, crea un túnel cifrado para el intercambia de información mediante *TLS*, el *AP* realiza la función de autenticador. La ventaja de este método es que una vez validado el certificado del servidor se genera un túnel seguro y el cliente envié su identificación, luego de lo cual ambos pueden generar una llave de sesión.

Ahora se detallan los métodos de autenticación basados en contraseñas:

- *EAP-Algoritmos de Hash*: Este tipo de autenticación se realiza con algoritmos de hash sean estos *MD5 o SHA,* se utiliza un nombre de usuario y *password*. La contraseña se cifra con *MD5 o SHA*, las debilidades de estos algoritmos son que generan bajos niveles de seguridad y es susceptible a un ataque de diccionario. La principal desventaja de este método es que no se puede realizar ninguna autenticación al servidor.
- *LEAP*: Esta variante es propietaria de *Cisco.* Emplea un esquema de nombre de usuario y contraseña. Al ser propietaria, exige que todos los puntos de acceso sean marca *Cisco,* y que el servidor *RADIUS* sea compatible con *LEAP*.

1.6.4.5 Estándar IEEE 802.1x[T15]

El protocolo IEEE 802.1x se desarrolló para permitir a los dispositivos finales acceder de forma segura a la red. Este estándar no describe el tipo de encripción o autenticación, el protocolo es quien toma control de todo el proceso. En el proceso de autenticación 802.1x se utiliza el protocolo *EAP* con algún mecanismo de autenticación, una vez realizado esto, se procede con el cifrado de datos utilizando las opciones *WEP, TKIP, AES*, etc.

El proceso de autenticación IEE 802.1x se explica en la figura 1.24, donde intervienen dos protocolos el *EAP* y el *RADIUS,* desde el suplicante[10] se envía la petición mediante *EAP* hacia el Autenticador[11] (AP), desde el AP hacia el servidor se utiliza el protocolo *RADIUS*, una vez que el servidor procesa la información permite o deniega el acceso a la red, el protocolo IEEE 802,1x es quien se encarga de llevar las peticiones desde el suplicante hasta el servidor.

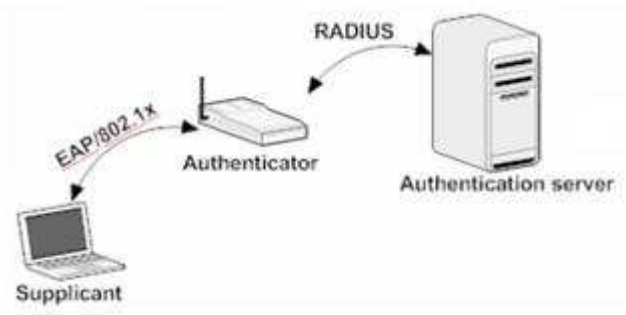


Figura 1.16 Autenticación IEEE 802.1x [T15]

1.6.4.6 RADIUS

Remote Authentication Dial in User Service, es el protocolo que realiza autorización, autenticación y registro en una red, desarrollado por *Livingston Enterprises Inc*. Su misión es crear una conexión segura entre los equipos finales y el servidor *RADIUS*. El servidor permite validar la identidad del usuario, asignarle permisos, y acceder a recursos. Además el servidor trabaja con una base de datos donde se guardan los perfiles de usuarios con sus respectivas contraseñas, las bases de datos con las que es compatible *RADIUS son: Microsoft Active Directory, Novell Network Directory System, MySQL,PostgreSQL, Lightweight Directory Access Protocol (LDAP)*, entre otras.

El servidor *RADIUS* se ejecuta sobre equipos con sistemas operativos, *LINUX* o *Windows*, utiliza el puerto *UDP* 3128 para establecer las conexiones. El protocolo RADIUS utiliza cuatro paquetes para su autenticación que son:

- *Access-Request*: Este paquete consiste en una petición para ser atendido, dando inicio a la secuencia RADIUS.

[10] Dispositivo de acceso a la red que realiza la petición de los servicios de la LAN
[11] Es el punto de acceso a la red que posibilita la autentificación 802.1X.

- *Access-Accept*: Este paquete informa al cliente RADIUS (punto de acceso) que la autenticación es correcta.
- *Access-Reject*: Este paquete informa al cliente RADIUS que la autenticación es incorrecto.
- *Acces-Challenge*: Este paquete es usado para hacer un pedido de credenciales de usuario al cliente RADIUS.

Un servidor *RADIUS* se implementa para mejorar la eficiencia, uso y seguridad de la red, al *RADIUS* se lo denomina con un servidor AAA puesto que brinda los siguientes servicios:

- **Autenticación:** Realiza la identificación de los usuarios de la red validando las credenciales que enviaron. El servidor compara la información enviada con la información almacenada en la base de datos si es correcta permite el acceso la red caso contrario se le deniega.
- **Autorización:** Una vez autenticado el usuario se deben asignar los recursos correspondientes, estos recursos se otorgan dependiendo de las políticas de administración y seguridad implementadas en la red.
- **Registro:** Esta funcionalidad permite revisar y tener un reporte de los eventos y recursos asignados a cada usuario en la red, para analizar o modificar las políticas de seguridad.

1.6.5 EQUIPOS DE COMUNICACIÓN INALÁMBRICA.

1.6.5.1 *Router* Inalámbrico.

Es un dispositivo de conectividad utilizado en redes inalámbricas (*WLAN*), el equipo permitirá realizar la interconexión con la red cableada y la de dirigir los paquetes para que la información se direccione a la red correcta, estableciendo las rutas para llegar al destino. El *router* es considerado dispositivo de capa 3.

1.6.5.2 *Access Point.*

Dispositivo que enlaza a clientes inalámbricos a la red cableada, este equipos centralizan todas la comunicaciones en rede ad-hoc o de infraestructura, estos equipos permiten conectarse a otros APs. Este dispositivo trabaja en modo repetidor y se puede considerar como el equivalente inalámbrico de un *switch*.

1.6.5.3 *Bridge*.

Es el equipo que permite la funcionalidad de conectar dos o más segmentos de red, que físicamente y lógicamente están separados, esta función se la puede implementar mediante *hardware o software*. Para trabajar en modo *bridge* los dos extremos debe configurarse o tener activada esta función.

1.7 SERVICIOS. [W51]

1.7.1 SERVICIOS EN UNA INTRANET

La estructura interna de la red facilita el intercambio de información de los usuarios, mediante el acceso a diversos recursos. Los servicios que brinde la intranet a la comunidad educativa deberán satisfacer las necesidades de la misma.

La cantidad de servicios que la intranet puede ofrece depende de las necesidades, no existe un límite, se debe dimensionar y seleccionar el software adecuado para que las aplicaciones funcionen correctamente y alcance un rendimiento óptimo.

Los servicios que una institución educativa debe tener para manejar la información adecuadamente son los siguientes:

- Correo Electrónico.
- Servicios Web
- *FTP*
- *DNS*
- *DHCP*
- Servicios de autenticación, autorización. y contabilidad.
- Antivirus

Para la selección de un servidor se deben considerar algunos parámetros, como son: el número de usuarios que accederán al servicio, que tipo de *software* a ser utilizado, los requerimientos de *hardware;* además se debe tomar en cuenta la facilidad de administración, configuración, costo de licencias y el costo de soporte técnico de los servidores a implementarse.

En cuanto al *software,* actualmente se utilizan dos sistemas operativos para implementar una solución de servidor, que son *Windows Server* en sus versiones 2003 ó 2008, y *UNIX*.

"Los sistemas operativos UNIX están disponibles en versiones comerciales, por ejemplo: Solaris de la Sun Microsystem, AIX de IBM, HP-UX de Hewlett- Packard, SuSE, Red Hat, etc. También se tiene versiones gratuitas como FreeBSD, o la gran gama de distribuciones Linux, por ejemplo: Fedora, Ubuntu, Centos, Debian, etc."

1.7.1.1 Servidor DNS.

Este servicio está formado por una base de datos jerárquica, distribuida que realiza la traducción de un nombre de un dominio a una dirección IP y viceversa. *DNS* se compone de tres elementos el cliente, el servidor *DNS* y las zonas de autoridad.

Un cliente DNS es el usuario final que realiza la petición de traducción de un nombre de dominio, a un servidor *DNS*.

Existen tres servidores básicos *DNS*:

- **Servidor maestro:** Almacena los registros de las zonas originales y de autoridad.
- **Servidor esclavo:** Responde a la peticiones de un usuario *DNS* pero obtiene información acerca de los nombres de dominio desde un servidor maestro.
- **Servidor caché:** Almacena la resolución de nombres de dominio cierto tiempo, para poder acceder a esta información rápidamente y responder a un cliente *DNS*.

El servidor *DNS* necesita realizar consultas, las mismas que pueden ser iterativas o recursivas.

- **Recursiva:** Obliga al servidor DNS a que responda aunque tenga que consultar a otros servidores.

- **Iterativa:** El servidor contesta si tiene la información y si no, le remite la dirección de otro servidor capaz de resolver. De esta forma el cliente tiene mayor control sobre el proceso de búsqueda.
- **Inversa:** Permite dada una IP, consultar el nombre. Para ello se ha creado un dominio especial llamada "*in-addr.arpa*"

Finalmente las zonas de autoridad, "contienen las características sobre las cuales el dominio actuará, en ella se configuran aspectos como las opciones especificas de cada zona, estas configuraciones hechas a las zonas son cargadas desde el servidor maestro".[W50]

1.7.1.1.1 *Software para Servidor DNS.*

- ***BIND (Berkeley Internet Name Domain)***[W49]***:*** Es una de las aplicaciones más utilizadas en Internet. BIND ofrece un servidor de nombres de dominio a través de una biblioteca llamada *named* que se ejecuta como proceso demonio y realiza la resolución de sistemas de nombres de dominio además de contar con un paquete de herramientas para monitorizar el correcto funcionamiento de todo el sistema. Este servicio escucha en el puerto 53 de *TCP y UDP*. Este *software* puede funcionar correctamente sobre sistemas *UNIX o Linux*.
- ***Djbdns***[W52]: Es una herramienta para implementar *DNS* que está conformada por pequeños programas englobando más de un tipo de servidor *DNS*. *Djbdns* incluye características adicionales para brindar mayor seguridad.
- ***PowerDNs***[W53]***:*** Es un servidor de nombres de alto rendimiento con una serie de *backends*[12]. Trabaja en sistemas operativos *UNIX* como *Windows* y es compatible con base de datos *MySQL, Oracle, PostgreSQL* etc.
- ***MyDNS***[W54]: Es un servidor DNS que utiliza una base de datos MySQL como *backend* en vez de los archivos de configuración como, por ejemplo, *Bind* o *djbdns*. Añade características como gestión de usuarios y privilegios de acceso.

[12] **Servidor *Back-End*:** Parte del *software* que procesa la entrada desde el *Front-End,* que interactúa directamente con los usuarios.

1.7.1.2 Servidor de correo electrónico.

Este servicio ayuda a mantener una comunicación permanente con todos los miembros de una Institución, al enviar y recibir notificaciones electrónicas y de la misma forma poder almacenar en los buzones del correo la información requerida por cada uno de los usuarios.

El servidor de correo permitirá acceder a los usuarios de la red, siempre y cuando obtengan una cuenta de correo; además que a este servicio se podrá acceder tanto de la red interna como desde el exterior.

- ***Postfix***[W55]*:* Es un *software* para correo electrónico que está formado por pequeños programas, cada uno de los cuales lleva a cabo una función especializada. Utiliza el protocolo *SMTP*, es fácil de administración y es compatible con *Sendamail, y Squirremail*. Ambos son aplicaciones web escritos en *PHP*[13]. Se debe considerar también que junto con *Postfix* se debe tener el programa *Dovecot,* este permite tener un servidor *POP3*[14] (Protocolo de la oficina de correo *v3*) *e IMAP*[15]*(Internet Message Access Protocol*).
- **Exim**[W55]**:** Es un servidor de correo electrónico (*MTA, Mail Transport Agent*, agente de transporte de correo). *Exim* es un servidor con grandes características ofrece configuraciones de *ACL´s* (Listas de control de acceso) y soporte para base de datos desde *MySQL y PostgreSQL y Oracle.*
- ***Qmail***[W56]: Es un servidor de correo electrónico (*SMTP)* pensado para Unix. Los mensajes recibidos en cada casilla pueden ser filtrados a voluntad por medio de archivos. *Qmail* tiene una gran modularidad del mismo modo los mensaje pueden ser encolados.

[13] *PHP*, es un lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas.
[14] *POP3,* es un protocolo estándar para recibir mensajes de *e-mail*, y en el cual el usuario puede descargar los archivos desde el servidor.
[15] *IMAP,* es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor.

1.7.1.3 Servidor Web

El servidor Web es un programa que atiende y responde demandas de información de los navegantes en protocolo *HTTP*, por lo que es necesario que este servidor esté ubicado dentro del domino local para que pueda ser administrador por personal de la Institución. En cuanto a soluciones Web se pueden utilizar:

- ***Apache***[P9]**:** Es un servidor web basado en *HTTP*, se caracteriza por ser fácil de configurar, bases de datos de autenticación y negociado de contenido. Además de ser modular pues permite incrementar funcionalidades, es de código abierto, multiplataforma y extensible; además tiene un soporte técnico muy amplio.

- ***Cherokee***: Es un servidor web multiplataforma , es rápido y funcional. Soporta la configuración de servidores virtuales. Se puede utilizar para balancear carga y dispone de un panel de administración desde la web.

- ***Lighttpd (tiny/turbo/throttling HTTP server)***[W58]: Desarrollado para entornos donde la velocidad es muy importante, razón por la cual consume menos recursos de CPU y memoria RAM que otros servidores. Por todo lo que ofrece, *lighttpd* es apropiado para cualquier servidor que tenga problemas de carga, es de distribución libre.
- ***thttpd (tiny/turbo/throttling* HTTP server)***[W59]:* Es un servidor web de código libre disponible para la mayoría de las variantes de *Unix*. Se caracteriza por ser simple, pequeño, portátil, rápido, y seguro, ya que utiliza los requerimientos mínimos de un servidor *HTTP*. Esto lo hace ideal para servir grandes volúmenes de información estática.

1.7.1.4 Servidor *FTP*.

Servicio utilizado para realizar descargas y almacenar información, de tal forma que se pueda tener disponibilidad de la información. Siempre es adecuado tener una base de datos donde se guarde información primordial. Entre las plataformas de software más utilizadas se tiene:

- ***Vsftpd (Very secureFTP Daemon)***[W23]: El servidor *vsftpd* es de rápida configuración, estable y seguro. *Vsftpd* está diseñado para ejecutarse bajo UNIX o sistemas relacionados como puede ser Linux. Ofrece seguridad a partir de las ventajas ofrecidas por *UNIX*. Soporta encripción sobre *SSL*.

- ***ProFtpd***[W24]**:** Es seguro, sumamente flexible, modular y fácil de configurar, permite autenticar usuarios y utilizar servidores virtuales de *FTP*. Se pueden tener múltiples servidores brindando servicio de *FTP* anónimo. No está basado en ningún otro servidor, su código fuente fue escrito totalmente desde cero.
- ***Pure-FTPd***[P10]: Es un servidor *FTP* libre basado en *Troll-FTPd*, Controla el ancho de banda y el espacio de disco duro por usuario, indica estadísticas en tiempo real en texto o HTML, provee autenticación de usuarios mediante *MySQL, PostgreSQL, LDAP*, y tiene opciones avanzadas de seguridad.

1.7.1.5 Servidor *DHCP*[W62].

Este servicio administra de manera centralizada toda la información de configuración de IP. De esta forma se elimina la necesidad de configurar manualmente los parámetros de la conexión *IP* de los clientes. Además, los clientes obtienen la configuración exacta y en poco tiempo sin ninguna intervención. Ofrece flexibilidad en caso de ser necesarios cambios en la infraestructura. En general en las distribuciones para servidor de *Windows y Linux* esta función está presente por defecto, lo único que se necesita es activarla o configurarla.

1.7.1.6 Servidor AAA y base de datos[T5].

El servidor AAA y el servidor de base de datos trabajan de forma conjunta para brindar el servicio a la red. Al considerar los sistemas de bases de datos se debe tomar en cuenta la facilidad de migrar la información, para que esta labor no se convierta en una tarea complicada en caso de ser necesaria

Las bases de datos almacenan la información de los usuarios, estos datos son accedidos por el servidor para verificar la identidad del usuario que desea el acceso a la red, la diferencia entre las diferentes bases de datos radica en la

utilización o no de licencias para su funcionamiento y la plataforma sobre la que pueden ser instalados, *Windows o Unix.* En la tabla 1.3 se presentan algunas opciones para la base de datos.

Base de datos	Windows	Unix	Licencia
MySQL	✓	✓	Gratuita
MS Access	✓	No	Pagada, incluida en el paquete Microsoft Office
MS SQL	✓	No	Pagada, es propiedad de Microsoft
mSQL	No	✓	Gratuita para uso no comercial
PostgreSQL	✓	✓	Gratuita
Oracle	✓	✓	Pagada

Tabla 1.4 Características de las opciones para base de datos del servidor AAA.[T5]

Para la implementación del software para la autenticación, autorización y registro se tienen las siguientes opciones en *software*:

- ***FreeRadius*:** Incluye servidor, clientes, y desarrollo de múltiples librerías. Este servicio puede manipular un gran número de cuentas de usuario, es de distribución gratuita compatible con diferentes plataformas informáticas. Opera con bases de datos *MySQL, PostgreSQL*, *Oracle,* donde se almacenará toda la información de los usuarios. La autorización la realiza mediante protocolos tales como: *EAP-MD5, EAP-TLS, EAP-PEAP, EAP-TTLS, LEAP.*
- ***OpenRadius*:** Permite conseguir la información de los perfiles de usuario de cualquier fuente externa. Soporta autenticación con directorios *LDAP* y base de datos *SQL*. Utiliza esquemas de autenticación y política de red modificables, la interfaz es muy sencilla y ampliamente documentada, puede ser modificado y se redistribuye bajo términos de la licencia pública *GNU*.

1.7.1.7 Servidor de Antivirus.

Una solución de antivirus brinda la posibilidad de proteger a los equipos como la información detectando y eliminando los virus informáticos. La principal característica de este servicio es de controlar de manera centralizada mediante

una consola todos los equipos de red, de esta forma se puede monitoreará de forma proactiva, para conocer si existen virus informáticos en la estaciones y poder desinfectarlos; además permite actualizar la base de datos.

- ***Kaspersky:*** Antivirus compatible con plataformas informáticas *Windows y Linux,* protege en tiempo real contra virus y programas espía, analiza los sitios *web* y mensajes de correo electrónico en busca de código malicioso, protege la identidad del usuario, analiza las vulnerabilidades, y actualiza automáticamente la base de datos del antivirus cuando se conecta a Internet. Facilita funcionalidades de *antispyware*[16]*, y antispam*[17]. Ofrece consola de administración centralizada y para el monitoreo utiliza un agente en cada equipo. Esta solución tiene un costo de licencia dependiendo del número de usuarios en el dominio de red.

- ***ESET NOD32:*** está disponible para *Windows, Linux, FreeBSD, Solaris, Novell y Mac OS X*. Permite la detección en tiempo real de nuevas amenazas, *ESET NOD32* es capaz de detectar códigos maliciosos, como virus, troyanos[18]*,* gusanos[19] *y* spyware[20], entre otros. Utiliza menos recursos de hardware. Este *software* también tiene un costo por licencia dependiendo el número de estaciones.

- ***Symantec Norton Antivirus:*** Es uno de los antivirus más utilizados, está diseñado para el uso dentro de cualquier ambiente de trabajo. Esta solución tiene una consola de administración para control centralizado de los virus y la actualización de base de datos. *Norton* brinda seguridad para todo tipo de amenazas. Al igual que las anteriores esta solución requiere un pago por la licencia.

[16] Tipo de aplicación que se encarga de buscar detectar y eliminar espías en el sistema
[17] Método para prevenir el correo basura
[18] Código malicioso que se ejecuta ocultándose dentro de una aplicación registrada.
[19] Es un código malicioso que se reproduce así mismo en paquetes de varios archivos
[20] Código malicioso que trata de tomar de control de un host para obtener información.

1.7.2 SERVICIOS EN TIEMPO REAL

Las redes de datos se encuentran cada vez más relacionadas con cada uno de los aspectos de la vida cotidiana, las redes ya no son simplemente para transmitir información entre computadoras que son utilizadas únicamente por expertos en ellas. El auge del Internet ha hecho que cada vez más servicios que antes eran provistos por medios tradicionales ahora sean brindados a través de este medio. Un claro ejemplo es el de la telefonía que se ha trasladado desde la tradicional red conmutada pública hacia el Internet.

1.7.2.1 Telefonía IP[F5][W9]

La telefonía IP ha tomado mucha fuerza especialmente dentro del ámbito empresarial debido a la utilización de las redes de datos también para la transmisión de voz. Estos sistemas basan su funcionamiento en el protocolo IP, ampliamente expandido por el mundo porque es el estándar de Internet.

La telefonía IP ha ido reemplazando a la telefonía tradicional a pesar de que todavía resulte costosa en su inversión; sin embargo los beneficios a mediano plazo como por ejemplo ahorro en nuevas instalaciones y reducción de costos de mantenimiento, además de la capacidad de incluir nuevas y mejores funcionalidades, hacen que estos sistemas sean altamente cotizados en la actualidad.

La telefonía IP es una tecnología basada en conmutación de paquetes, la voz analógica se digitaliza mediante un proceso de codificación y luego es comprimida en paquetes de datos. Estos paquetes son transmitidos en las redes de comunicación mediante protocolo IP, hasta llegar a su destino donde se realiza el proceso inverso a fin de obtener la señal de voz original.

1.7.2.1.1 *Estándar H.323*

El estándar H.323 es una pila de protocolos que regulan la transmisión de datos a través de redes LAN que no provean calidad de servicio. En este estándar se encuentran definidas las entidades que forman parte del sistema así como los protocolos adecuados para su funcionamiento.

- **Terminales:** Son los dispositivos finales de usuario, estos pueden ser equipos específicos de telefonía o sistemas adaptados mediante software. Son capaces de soportar comunicaciones en tiempo real con otro dispositivo H.323 por lo que manejan tanto los protocolos para voz como los de señalización.
- ***Gateway:*** Son los dispositivos que permiten la conectividad de la LAN con los medios externos, por ejemplo un *Gateway* utilizado para conectar a la red telefónica pública con una red empresarial es conocido como *IP/PSTN Gateway*.
- ***Gatekeeper:*** Realiza las funciones de procesamiento de llamadas en lo referente a traducción de direcciones, control de admisiones, requerimientos de ancho de banda y manejo de una determinada zona o conjunto de dispositivos H.323.
- ***MCU (Multipoint Control Unit)*:** Controla la multidifusión cuando se realizan conferencias entre más de dos puntos, controla la señalización mediante un *multipoint controller MC* y se encarga de las tramas de los participantes a través del *multipoint processor MP.*

El estándar H.323 define distintos tipos de protocolos entre los que se encuentran protocolos de señalización, direccionamiento, compresión, codificación que al final serán transportados por medio del protocolo IP como se muestra en la figura 1.19. En la tabla 1.4 se presenta una breve descripción de los protocolos soportados en esta arquitectura.

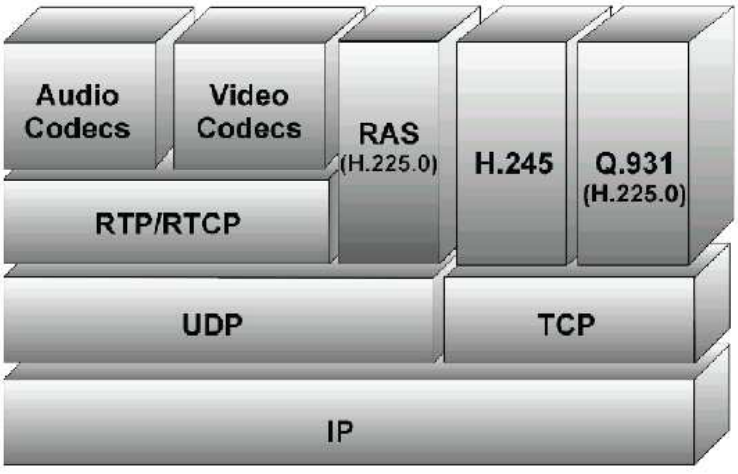


Figura 1.17 Protocolos de H.323[F5]

PROTOCOLO	FUNCIÓN	CARACTERÍSTICAS
RAS (Registration, Admision and Status).	Direccionamiento	Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través del Gatekeeper.
DNS (Domain Name Service).		Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.
Q.931	Señalización	Señalización inicial de llamada
H.225		Control de llamada: señalización, registro y admisión, y paquetización / sincronización del flujo de voz.
H.245		Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz.
Requeridos: G.711 y G.723. Opcionales: G.728, G.729 y G.722.	Compresión de Voz	Códecs
RTP (Real Time Protocol).	Transmisión de voz	Maneja los aspectos relativos a la temporización, marcando los paquetes *UDP* con la información necesaria para la correcta entrega de los mismos en recepción
RTCP (Real Time Control Protocol).	Control de la Transmisión	Se utiliza principalmente para detectar situaciones de congestión de la red y tomar acciones correctoras.

Tabla 1.5 Protocolos utilizados en H.323[F5]

1.7.2.1.2 *Estándar SIP*

SIP es un protocolo de señalización usado para crear, administrar y terminar sesiones de telefonía en redes basadas específicamente en IP. Desarrollado por el *IETF,* es uno de los estándares más utilizados para la señalización en *VoIP. SIP* puede ser utilizado tanto para llamadas de voz como de video, debido a que es sumamente flexible, debido a su arquitectura, permite además la iniciación de sesiones de texto y de multimedia, como mensajería instantanea, vídeo, juegos en línea y otros servicios. Este protocolo es utilizado únicamente para el establecimiento y la terminación de las llamadas, todos los mensajes *SIP* son encapsulados sobre *RTP.*

SIP fue creado para ser utilizado como un estándar de Internet, por lo que se basa en una estructura cliente – servidor. Además que utiliza las características de éste como son el uso de *DNS, URL (Uniform Resource Locator/ Localizador Uniforme de Recursos), proxies etc.* Permite el reuso de la codificación de *HTTP,* que permite basarse en texto para la comunicación entre los componentes de la comunicación. Los mensajes consisten de encabezados y un cuerpo de mensaje. Los cuerpos de mensaje de *SIP* para las llamadas telefónicas se definen en *SDP* (*Session Description Protocol*/ Protocolo de descripción de la sesión). Las aplicaciones *SIP* pueden ser transportadas en *UDP y TCP*, además que pueden utilizar otros transportes. En la figura 1.18 se muestra la ubicación de *SIP* dentro del *stack* de protocolos de una red *IP.*

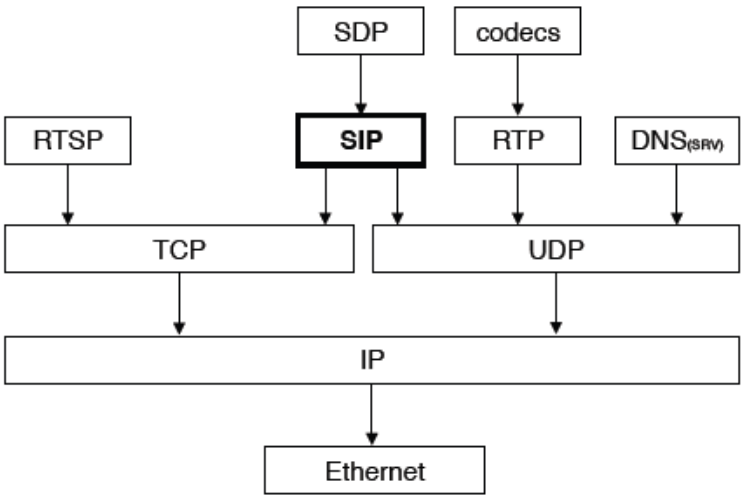


Figura 1.18 Ubicación de *SIP* en el *stack* de protocolos *TCP/IP*[F5]

Su arquitectura está conformada de dos componentes básicos:

- Agente de usuario (*UA, User Agent*) El agente de usuario establece las llamadas bajo una estructura Cliente/Servidor, estableciendo sesiones *peer to peer,* comprende un elemento cliente (*UAC, User Agent Client*) que inicia las llamadas y un elemento servidor (*UAS, User Agent Server*) que responde las peticiones.
- Servidor de red (*NS, Network Server*). Los servidores registran a los clientes y deciden hacia donde enviar las peticiones del cliente y le informan a éste donde dirigir su siguiente petición. Pueden guardar o no información de estado, dando lugar a dos modos de funcionamiento, *statefull o stateless*. Los servidores sin estado constituirían lo que se podría denominar el 'backbone' de una infraestructura *SIP*, mientras que los servidores con estado serían los dispositivos más cercanos a los agentes de usuario, que se encargarían del control de los dominios de usuarios.

En la figura 1.19, se muestra un ejemplo de una conexión con *SIP.*

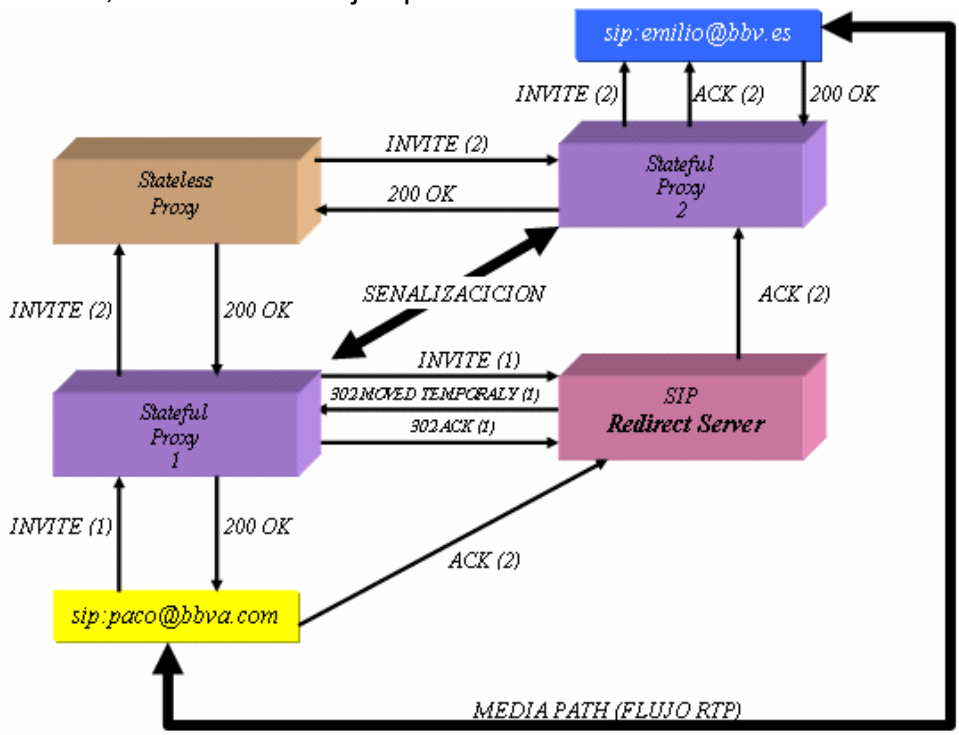


Figura 1.19 Comunicación *SIP*[F5]

Finalmente bajo esta estructura se puede obtener la gama de servicios anteriormente descritos, implementándolo en la aplicación donde va a ser utilizado el protocolo.

1.7.2.2 Video Seguridad IP[P4]

El video en red ofrece todo lo que el video analógico proporciona, además de una amplia gama de funciones y características innovadoras que sólo son posibles con la tecnología digital. Si a esta facilidad añadimos además la ventaja de efectuar la transmisión imágenes a través de la red de datos, proporciona una plataforma flexible en términos de vigilancia y seguridad con prestaciones sumamente altas, sin tener que gastar en infraestructura adicional.

1.7.2.2.1 *Elementos*

Un sistema de video en red, está compuesto por dos elementos principales: cámaras de red y *software* de gestión. La cámara de red y el codificador de video cuentan con capacidades que superan ampliamente a los sistemas de video analógico, debido a que su arquitectura es basada en sistemas computacionales.

Otros componentes de un sistema de video en red incluyen accesorios, codificadores de video para cámaras analógicas, carcasas para cámaras, micrófonos adicionales, *splitters* activos que sirven para la alimentación de las cámaras en el caso que no manejen *PoE*. Algunos de los principales protocolos necesarios para la implementación de este sistema son:

- ✓ **Cámaras:** Las cámaras *IP* incorporan dos dispositivos a la vez, una cámara y un computador. Este dispositivo puede conectarse a cualquier punto de la red de datos, característica que la diferencia respecto a una cámara Web, que únicamente puede ejecutarse cuando está conectada a una computadora. Una cámara de red proporciona servidor *web*, *FTP* y funciones de correo electrónico. También incluye gran variedad de protocolos de red IP y de seguridad. Las imágenes capturadas pueden secuenciarse como *Motion JPEG, MPEG-4 o H.264* utilizando distintos protocolos de red. Asimismo, pueden subirse como imágenes *JPEG* individuales usando FTP, correo electrónico o *HTTP*.

Motion JPEG comprime cada fotograma del video como una imagen *JPEG* separada, a pesar de que tiene pérdida en la capacidad de compresión, pero facilita la edición de video, dado que se pueden realizar ediciones simples en cualquier cuadro.

MPEG-4 es el nombre de un grupo de estándares de codificación de audio y video así como su tecnología relacionada normalizada por el grupo *MPEG (Moving Picture Experts Group*) de *ISO/IEC*. *H.264 o MPEG4* parte *10* permite tener funcionalidades específicas para sistemas que utilizan aplicaciones a través de Internet, debido a que maneja compresiones mayores que sus antecesores lo que reduce el consumo de ancho de banda.

- ✓ **Software de gestión**: Un sistema de gestión de video puede admitir muchas características diferentes. A continuación, se enumeran algunas las más comunes:
  - Visualización simultánea de video desde varias cámaras.
  - Grabación de video y audio.
  - Funciones de gestión de eventos con video inteligente, como detección de movimiento de video.
  - Administración y gestión de cámaras.
  - Opciones de búsqueda y reproducción.
  - Control de acceso de usuarios y registro de actividades (auditoría) existen dos tipos.

El software de gestión puede ser instalado en un servidor donde se pueden instalar diferentes características o en un dispositivo especializado para tal labor conocido como *NVR (Network Video Recorder),* que por lo general viene con un software propietario de los fabricantes y que permite aprovechar al máximo las funcionalidades del sistema.

Además para esta gestión se puede utilizar simplemente el software que viene por defecto instalado en una cámara y que por lo general es accesible vía navegador *web*.

1.7.2.2.2 *Ventajas*

Entre las ventajas se incluyen la accesibilidad remota, alta calidad de imagen, la gestión de eventos y las capacidades de video inteligente, así como las posibilidades de una integración sencilla y una escalabilidad, flexibilidad y rentabilidad mejoradas.

• **Accesibilidad remota:** Se pueden configurar las cámaras de red y los codificadores y acceder a ellos de forma remota, ventaja que permite a través del *software* de gestión almacenar directamente los datos de la grabación en el disco duro que aloja el servidor, el que de la misma manera puede ser configurado para acceder desde cualquier sitio a través de Internet.

• **Alta calidad de imagen:** En una aplicación de videovigilancia, uno de los factores que puede influir en su éxito es la calidad de la imagen, la cual va a depender de la necesidad de identificar un incidente en curso o a las personas u objetos implicados. Con respecto a un sistema analógico, existe menor número de conversiones, que deterioran la calidad de la imagen. En un sistema integrado *IP* la imagen digitalizada se almacena directamente.

• **Gestión de eventos y video inteligente:** Se pueden programar respuestas de grabación para los servidores, por ejemplo realizar el monitoreo de determinada área en un determinada hora del día. También se pueden integrar funciones como la detección de movimiento por video, alarma de detección para conexiones de entrada y salida (E/S) y funcionalidades de gestión de alarmas y eventos.

Estas funciones permiten que las cámaras de red y los codificadores de video analicen de manera constante las entradas para detectar un evento y responder automáticamente a éste con acciones como la grabación de video y el envío de notificaciones de alarma.

• **Escalabilidad y flexibilidad:** Un sistema de video en red puede crecer a la vez que las necesidades del usuario. Los sistemas basados en IP ofrecen la facilidad de integrar cámaras a la red, sin que ello suponga cambios significativos o costosos para la infraestructura de red. En el caso

de sistemas analógicos, por ejemplo, se debe extender un cable coaxial directamente desde cada cámara a un puesto de visualización o grabación.

1.7.2.3 Calidad de Servicio *QoS*[P2][P3]

Los parámetros de calidad de servicio son fundamentales dentro de las nuevas redes que pretenden converger en una sola infraestructura varios servicios, en especial, para incluir servicios en tiempo real que incluyen la transmisión de audio y/o video.

QoS puede ser aplicado en tres diferentes niveles:

- **Mejor esfuerzo:** Es el comportamiento predeterminado de la red sin especificar ningún tipo de nivel de calidad de servicio.
- **Modelo de servicios integrados:** El nivel de calidad de servicio es requerido por la aplicación a través del protocolo *RSVP (ReServation Protocol).* Dentro de la arquitectura de servicios integrados, podrían distinguirse las siguientes funciones principales:
  - **Control de admisión**: Se reservan los recursos mediante *RSVP* en función de la caracterización del tráfico y la negociación de parámetros como tasa de transmisión y niveles de pérdida de paquetes.
  - **Enrutamiento:** los dispositivos se basarán en la calidad de servicio para enrutar los paquetes. Los paquetes serán enviados a una de las colas de calidad de servicio según la clasificación dada para su envío.
  - **Disciplina del servicio:** Se refiere al comportamiento de la cola.
  - **Descarte de paquetes** a fin de realizar control de congestión, descartando los paquetes recién llegados, los que tengan menos calidad de servicio o aleatoriamente según sea la configuración
- **Modelo de servicios diferenciados:** Los Servicios Diferenciados (*DiffServ*) proporcionan un método que intenta garantizar la calidad de servicio en redes de gran tamaño, como puede ser Internet.

Servicios Diferenciados, analiza varios flujos de datos en vez de conexiones únicas o reservas de recursos. Esto significa que una negociación será

hecha para todos los paquetes en función de los Acuerdos de Nivel de Servicio *(SLA, Service Level Agreement)*, que especifican que clases de tráfico serán provistos, qué garantías se dan para cada clase y cuántos datos se consideran para cada clase.

A nivel de capa 2 se clasifican los paquetes utilizando los encabezados de 802.1p, mientras que en capa 3 se realiza esta operación de dos formas, a través de ToS (Tipo de servicio) también conocido como IP precedente. ToS utiliza banderas o marcas, que pueden ser configuradas para darle prioridad a un paquete sobre el resto o *DSCP* (*Differentiated Services Code Point*) una extensión de ToS que se utiliza para diferenciar la calidad en la comunicación que requieren los datos a ser transportados.

1.7.2.4 Videoconferencia[W63].

Los sistema de video conferencia permite establecer una comunicación en tiempo real entre diferentes personas en lugares geográficos distantes. Todo sistema de videoconferencia está formado por la sala de videoconferencia, la red de comunicaciones y el *códec* a utilizarse.

- **Sala de videoconferencia:** Es el espacio físico adecuado donde los se situaran todos los equipos de video así como los participantes. De acuerdo a los equipos que se utilicen y el espacio físico existen varios tipos de video conferencia las cuales son: habitación preparada o sala específica para videoconferencia, *Rollabout* espacio para la videoconferencia dentro de otra sala y de escritorio donde interviene un computador personal conectado a otro.
- **El códec:** Se encarga de comprimir y multiplexar las señales de audio y video para transformarlas a señal digital.

1.7.2.4.1 *Configuraciones*

Existen dos configuraciones básicas entre equipos terminales en la videoconferencia y esta son punto a punto y punto multipunto.

- **Punto a Punto:** Solamente interviene dos terminales audiovisuales los cuales intercambian simultáneamente la información.

- **Punto Multipunto:** Utiliza un equipo multipuerto denominado *MCU* (Unidad de control multipunto) el cual es capaz de conmutar entre los participantes.

Para un sistema de videoconferencia se tiene tres tipos de comunicaciones

- **Radiodifusión:** Tipo televisión, dónde la transmisión es en tiempo real para uno o más receptores.
- ***Streaming:*** El material audiovisual se encuentra almacenado en un dispositivo al cual los usuarios pueden acceder y revisarlos directamente.
- **Conferencia:** Las conversaciones son bidireccionales y multipunto.

1.8 SEGURIDAD EN LA RED[P5][W35][W66].

Una de las principales preocupaciones al implementar una red de datos es el asunto de seguridad de la misma. Una red al ser un medio para la interconexión de diferentes dispositivos por su naturaleza es vulnerable de sufrir ataques que pueden comprometer recursos que pueden llegar a ser críticos en el correcto desenvolvimiento de una organización.

En un sistema los puntos fundamentales a asegurar con respecto a la información deben ser:

- **Autenticidad**: La información debe ser accedida solo por las personas con los permisos adecuados
- **Confidencialidad:** Prevenir la divulgación de información a personas o sistemas no autorizados
- **Integridad:** La información debe estar libre de modificaciones no autorizadas
- **Disponibilidad:** La información debe estar a disposición cada vez que se necesite sea por personas o por aplicaciones.

Para poder cumplir estas características se deben crear las estrategias más adecuadas, basadas en el desarrollo organizacional del lugar donde se encuentre la red. Se debe realizar un análisis previo de riesgos, que comprende el inventario de activos y la identificación de amenazas y vulnerabilidades. Posterior a este

análisis se realiza el diseño. Es importante la realización de una encuesta que permita cuantificar situaciones como:

- Cómo debe ser protegida la información
- Donde se encuentra más vulnerable la información
- Y a qué nivel de protección debe llegar el sistema.

Las estrategias a implementarse deben considerar tres aspectos fundamentales que son el personal, la tecnología y la operación involucrada en el sistema.

1.8.1 PERSONAL

Con respecto al personal, se deben definir procedimientos acerca de cuál debe ser el comportamiento del personal con respecto al uso de las redes. Generar políticas de uso de la red que permitan uniformizar el manejo de la información dentro de la organización y que cuenten con el total apoyo de los directivos encargados de la toma de decisiones. Estas políticas deben estar adecuadamente documentadas en un lenguaje claro, conciso y estructurado adecuadamente a fin de ser entendidas claramente por todo el personal involucrado.

Una necesidad fundamental con respecto al personal es prevenir los ataques denominados de ingeniería social o de abuso de confianza. El movimiento o cambio del personal hace que las estrategias de seguridad tengan que contemplar, por ejemplo, el cambio de los permisos de acceso hacia los recursos de la red.

La seguridad física del personal también debe ser precautelada por la organización, para evitar la pérdida de recursos tanto humanos como tecnológicos o económicos.

1.8.2 TECNOLOGÍA

Con respecto a la tecnología se debe especificar un modelo de seguridad adecuado que permita equilibrar tanto la seguridad de los usuarios como la productividad de la organización, por lo cual este modelo debe estar completamente adaptado al funcionamiento de la organización y no ésta adaptarse al modelo. Así mismo debe ser completamente flexible de tal manera

que pueda adaptarse a los cambios en la misma. A continuación se presentan los tipos de modelos para su funcionamiento, según la tecnología utilizada.

1.8.2.1 Abiertos

Los usuarios son confiables, el acceso a la red es por lo general a través de contraseñas de acceso y por lo general no se encuentra conectada a Internet. Existe poca cantidad de activos que proteger y todos los usuarios tienen acceso a todas las áreas, por lo que una brecha de seguridad en un sistema así, produce grandes daños.

1.8.2.2 Restrictivos

Existe la posibilidad de que existan algunos usuarios no confiables por lo que existen amenazas más constantes. Suben los costos de implementación y se reduce la facilidad de uso y configuración debido al uso de:

- ***DMZ (Desmilitarized Zone)***[W66]***:*** Es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. Su objetivo es que las conexiones tanto internas como externas estén permitidas, de acuerdo a los permisos establecidos. Mientras que los equipos locales en la *DMZ* no pueden conectar con la red interna.

  Esto permite que los equipos de la *DMZ* puedan dar servicios a usuarios remotos, a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada. La *DMZ* se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de e-mail, Web y DNS.

- ***Firewalls:*** Un firewall es un sistema o un grupo de sistemas que controlan el acceso entre dos o más redes. Hay tres tecnologías que son las más comunes que son:
  - **Filtrado de paquetes**: Se define un conjunto de reglas para el acceso o restricción de paquetes. Trabaja generalmente a nivel de

capa Transporte del modelo *IOS/OSI.* Un ejemplo clásico de filtrado de paquetes son las llamadas *ACL o Access List.*

- ***Proxy***: Se examina el contenido del paquete en capas superiores del modelo *ISO/OSI.* Intercepta las conexiones a nombre del cliente y en caso de ser válida la redirecciona hacia él evitando el contacto directo entre cliente y servidor. Su inconveniente es que el procesamiento aumenta y añadir nuevos servicios es complejo debido a que debe ser capaz de interpretar todos los protocolos.
- **Inspección y análisis de estado***:* Se utilizan listas de acceso simples, se genera una tabla con el estado de las conexiones y así se determina que paquetes pueden pasar de acuerdo a las peticiones realizadas.

Existen dos formas básicas de implementar una *DMZ* a través de firewall tal como se especifica en la figura 1.20. Con un *firewall* denominada también en trípode o *three legged firewall* o con dos *firewall*.

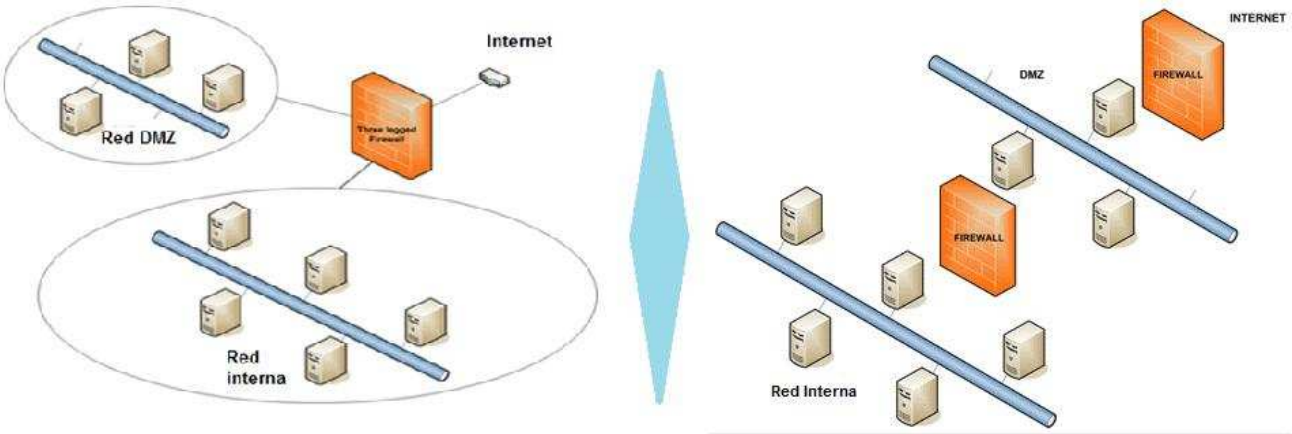


Figura 1.20 *DMZ* implementada con uno o dos *firewall*[W35]

Un firewall a su vez puede brindar servicios adicionales a la red como por ejemplo:

- *NAT (Network Address Translation*) que permite el uso de direcciones IP privadas para el acceso a Internet, a través de la traducción de éstas a direcciones públicas.
- *DHCP*
- Administración de ancho de banda

- Inspección de contenidos
- Alta disponibilidad y balanceo de carga
- *IDS (Intrusion Detection System)* que permite la detección de comportamiento de acceso sospechoso en la red para tomar acciones al respecto de ser necesario.

1.8.2.3 Cerrados

Un sistema cerrado es el más difícil de implementar, tanto el *hardware* como el *software* son configurados al máximo de seguridades debido a que no se considera a ningún usuario confiable dentro de la red. El acceso a la red debe ser considerado como difícil debido a que las amenazas son frecuentes y es necesaria la intervención de administradores de alto nivel a tiempo completo. Este tipo de sistemas es utilizado en redes corporativas grandes con manejo crítico de información.

1.8.3 OPERACIÓN

La operación se refiere a la gestión de los eventos que ocurren en la red. Se deben establecer los mecanismos más adecuados tanto para la administración de los equipos como para la definición de procedimientos para el uso de la red.

Por ejemplo, determinar claramente los encargados de los equipos en los diferentes niveles de la red, establecer procesos para cambios, readecuaciones, ingreso o salida de equipos. Establecer las políticas necesarias para el acceso de los usuarios a los recursos y prácticas tanto de mantenimiento como de solución de incidentes.

CAPÍTULO 2.

ANÁLISIS DE LA INFRAESTRUCTURA DE RED ACTUAL.

2.1 ANÁLISIS DE LA INFRAESTRUCTURA DE LA RED

2.1.1 INTRODUCCIÓN

El Instituto Tecnológico Superior Central Técnico es una Institución de enseñanza media y superior con una trayectoria de 139 años al servicio de la población de la ciudad de Quito y del país. En los últimos años se ha logrado un avance en la infraestructura fruto de la gestión institucional y representantes de los alumnos.

En la actualidad se busca implementar un sistema que permita acceder y sistematizar la información razón por la cual el personal administrativo, profesores, padres de familia y alumnos ven la necesidad de contar con una infraestructura de red para permitir la gestión y la comunicación de los diferentes actores que forman parte de la Institución educativa.

2.1.2 IDENTIFICACIÓN, DESCRIPCIÓN Y DIAGNÓSTICO DEL PROBLEMA

El Instituto Tecnológico Superior Central Técnico es una Institución educativa pública, laica, dedicada a la formación humana y profesional, sustentada en las áreas de ciencia, técnica, tecnología, cultura y sociedad, con énfasis en el sector técnico – industrial.

Satisface las demandas sociales del país con formación de ciudadanos, líderes y libres, con pensamiento crítico, creativo, con espíritu solidario, ético, cívico y conciencia social que aporten al mejoramiento de la calidad de vida de los

ecuatorianos y hagan posible la consecución de la justicia social; se distingue por su calidad profesional y académica de su personal, en la prestación de servicios a los sectores populares de la población ecuatoriana.

En esta misión el Instituto debe enfrentarse a situaciones y escenarios cada vez más diversos, con integración desde el ámbito administrativo hasta el organizativo sin dejar de lado el aspecto académico base fundamental del trabajo de la Institución, lo que hace fundamental e indiscutible la modernización del Instituto, que actualmente no cuenta con los recursos tecnológicos necesarios para estar a la par de estos nuevos retos y desarrollar adecuadamente su labor.

En un mundo tan desarrollado como el actual los recursos de información son tan amplios que van más allá de lo que podemos imaginar. El desarrollo tecnológico en el país ha cobrado gran importancia, sobre todo en el área de las comunicaciones, lo que se ve reflejado en los modernos sistemas que han implementado las diferentes organizaciones públicas y privadas para este fin. Es importante mencionar que las comunicaciones juegan un papel indispensable en el desarrollo de todas las instituciones educativas y por consiguiente en el desarrollo de un país.

El Instituto Tecnológico Superior Central Técnico debe enfrentar el gran desafío de avanzar en la búsqueda e incorporación de mayores niveles de modernización de su estructura y organización actual para así incrementar la productividad en sus actividades de organización, planificación y control a nivel general. Esto se conseguirá poniendo en funcionamiento soluciones tecnológicas integradas y modernas que permitan dar una atención oportuna y eficiente a la comunidad educativa.

En virtud de lo expuesto, una estrategia exitosa de la Institución es que deberá contemplar como elemento indispensable, disponer de una red de datos convergente que permita la interconexión de las diversas áreas que la conforman como parte de un proyecto diseñado para contribuir a la formación de profesionales que respondan a las necesidades laborales, productivas, sociales y de colaboración con el desarrollo tecnológico industrial del país. Además el sistema eventualmente facilitará el acceso de la comunidad

educativa a los diferentes servicios que residirán en la intranet de la Institución, a través del cual podrán tener un fácil manejo de información y recursos compartidos.

2.1.3 INSTALACIONES

El Instituto Tecnológico Superior "Central Técnico" posee un campus de 5.48 Hectáreas, ubicado en la avenida Gaspar de Villaroel N E6 – 125 de la ciudad de Quito. Dentro del cual se encuentran distribuidas diferentes áreas a fin de cumplir con su misión dentro de la sociedad. Las mismas que se señalan a continuación:

- Bar y Asociaciones
- Biblioteca
- Bloque de aulas
- Bodegas Generales
- Canchas Deportivas
- Centro Médico
- Educación Física
- Electricidad
- Electrónica
- Física y Química
- Inspección General
- Inspecciones de Cursos
- Laboratorios de Informática
- Nivel Superior
- Oficinas Administrativas
- Parqueaderos
- Salón de actos
- Talleres de Opciones Prácticas
- Talleres Mecánica Automotriz
- Talleres Mecánica Industrial
- Talleres Opciones Prácticas
- Tecnicentro Automotriz

Si bien su distribución dentro del campus es diversa, estas pueden ser agrupadas en áreas funcionales las cuales poseen una relación directa en su trabajo, tal como se especifica en la tabla 2.1.

Área Administrativa:	• Oficinas Administrativas: Secretarías, Rectorado, Vicerrectorado • Inspección General • Inspecciones de Cursos
Área Educativa:	• Laboratorios de Informática: Aulas de laboratorio, Sala de Internet • Electricidad: Aulas, laboratorio y bodegas • Electrónica: Aulas, laboratorio y bodegas • Nivel Superior • Laboratorios de Física y Química • Bloque de aulas
Área de Talleres:	• Talleres Mecánica Automotriz • Talleres Mecánica Industrial • Talleres de Opciones Prácticas • Tecnicentro Automotriz
Otras áreas:	• Bar y Asociaciones • Biblioteca • Bodegas Generales y Centro Médico • Educación Física • Parqueaderos • Salón de actos

Tabla 2.1 Áreas de la Institución

2.1.4 ANÁLISIS DE LA TOPOLOGÍA DE LA RED DE DATOS

La red de la Institución, durante este tiempo de funcionamiento, ha crecido de manera desordenada sin la documentación ni administración adecuadas debido

a lo cual los equipos no se encuentran conectados apropiadamente. Entre los problemas encontrados se pueden destacar los siguientes:

En base a los requerimientos instantáneos de la Institución se instalan nuevos puntos de red o equipos que muchas veces no cumplen las normas establecidas para el efecto y peor aún tienen la debida etiquetación, estos puntos son conectados simplemente a cualquier puerto que se encuentre disponible en ese instante.

Los equipos detallados en el punto 2.1.4.1 están interconectados mediante una topología física en estrella con tecnología *Fast Ethernet* mediante cables categoría 5e. Sin embargo los equipos presentan múltiples conexiones entre sí por lo que no se puede definir una topología específica debido al desorden de la red. Tampoco se encuentra basada en algún tipo de modelo donde por ejemplo se puedan definir niveles como acceso, distribución o núcleo, por lo que no se encuentran definidas funciones de red como *VLAN´s*, seguridad entre otros.

El enlace hacia el Internet se encuentra contratado mediante un plan PYMES de la empresa Telmex de 3 Mbps y es el único enlace WAN que posee actualmente la Institución. Esta conexión llega al *router* 1 ubicado en la Sala de Internet, este se encuentra conectado al *switch* 1, en la misma sala, al que a su vez están conectados los computadores que cumplen la función de servidores. El servidor 2 que actúa como proxy recibe las conexiones de todos los equipos de la red a través del *switch* 2. Este *switch* está conectado en cascada con los *switches* 3 y 4 (Laboratorio de computación) a los que a su vez también se encuentran conectadas los demás usuarios que tiene servicio en otros puntos como colecturía, departamento técnico pedagógico, autoridades y bodega general. Al *switch* 2 también se encuentran conectados los *switches* 5 y 6 que dan el servicio a Secretaría. En la figura 2.1 se presenta un diagrama de la red de datos y como funciona actualmente la misma.

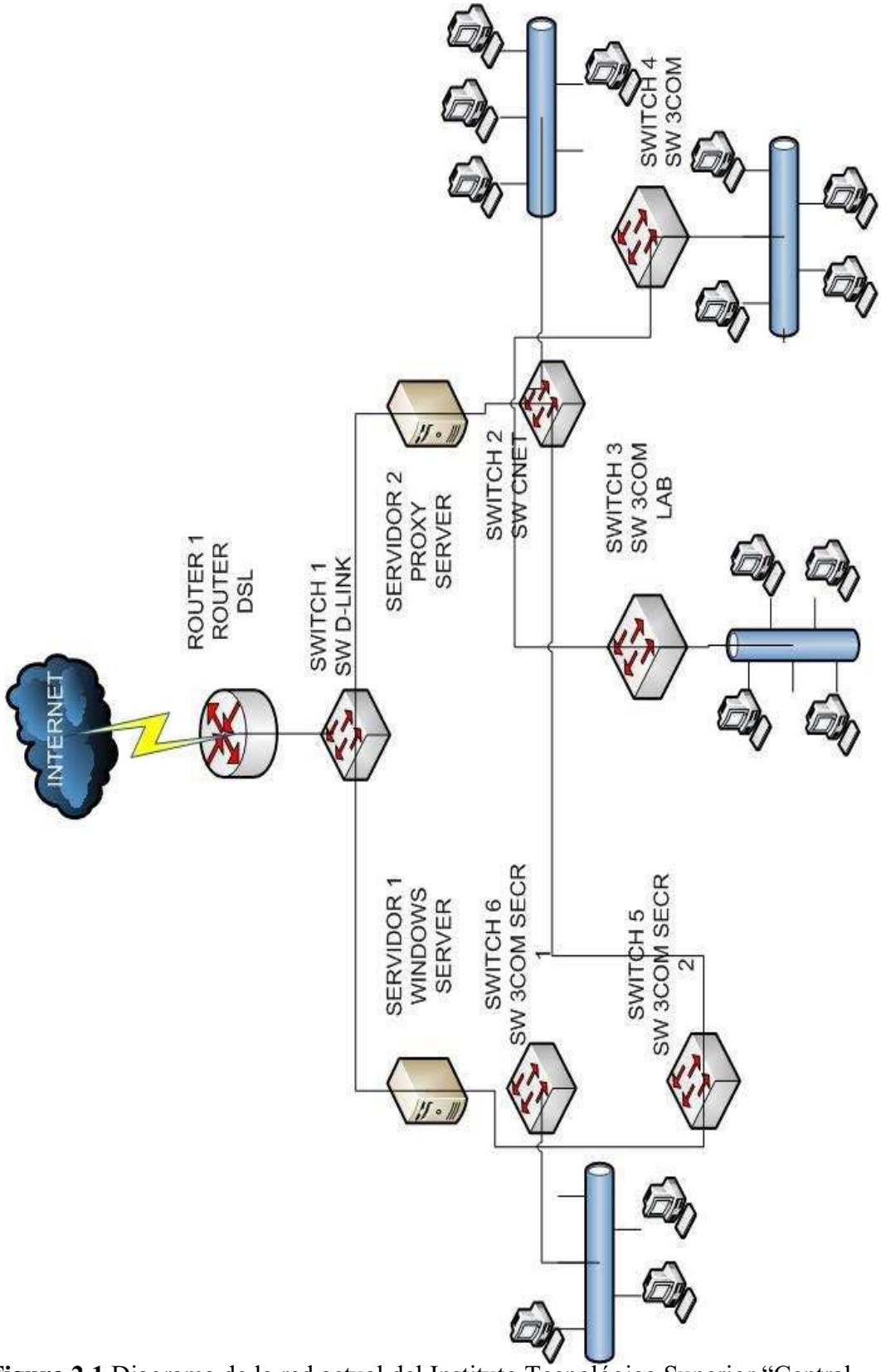


Figura 2.1 Diagrama de la red actual del Instituto Tecnológico Superior "Central Técnico"

2.1.5 EQUIPAMIENTO

Con el propósito de brindar una idea general acerca de la situación actual de la red de comunicaciones de la Institución se realiza el inventario de los equipos con los que actualmente cuenta la Institución. La red de datos se encuentra funcionando de manera independiente de la red de voz en la Institución, por lo que su análisis se realiza de la misma manera.

Dentro del área administrativa del campus, se encuentran dos sitios donde actualmente residen los equipos de comunicación: la sala de Internet y la Secretaría que son sectores de trabajo no apropiados para el alojamiento de equipos, ya que no cuentan con la infraestructura adecuada de una Sala de equipos o un cuarto de telecomunicaciones (*rack* para equipos, ambientes de acceso restringidos, control de temperatura, etc.).

El acceso a estas áreas es libre lo que también resulta una falla de seguridad debido a que cualquier persona puede ingresar y sustraer cualquiera de ellos. Además que no se encuentra adecuadamente documentada la situación actual del equipo, así como la función que desempeña dentro de la red lo que dificulta la administración de la misma.

Como equipos activos se definen los equipos destinados a la interconexión de la red. Equipos tales como *switches, routers, access points*, así como equipos con los que los usuarios interactúan directamente como son las estaciones de trabajo e impresoras y los servidores de la Institución.

2.1.5.1 Equipos para la comunicación de datos

Los equipos de red corresponden a diversos fabricantes: 3Com, DLink, Cisco, CNet de los cuales la marca preponderante es la marca 3Com sin embargo esta amalgama de marcas no se encuentra debidamente especificada. A continuación, en la tabla 2.2, se presenta una descripción de los equipos que actualmente brindan servicios a los usuarios de la red.

	MARCA	FUNCIÓN	UBICACIÓN	PUERTOS	EQUIPO
Router 1	*Cable Modem Motorola SBV5121*	Enlace del Servicio de Internet PYMES (4:1) Telmex	Sala de Internet	• 1 puerto *Fast Ethernet* • 1 puerto USB	[W12]
Router 2	*Router Cisco 2600*	Conexión hacia el Ministerio de Educación Proyecto "AMIE" Conexión hacia el Access Point para conexión de Internet a los profesores del laboratorio de informática	Sala de Internet	• 2 puertos *Fast Ethernet* 100 BaseT, Fa0/0 al *Access Point* 1, Fa0/1 al convertidor de fibra • 1 Puerto de consola • 1 Puerto Auxiliar	[W13]
Switch 1	*Switch D-Link DES1008 D Fast Ethernet*	Switch de core Interconecta los switches de otras áreas hacia los servidores y hacia el Internet	Sala de Internet	• 8 puertos *Fast Ethernet* 3 puertos utilizados: • Puerto 1 conexión hacia el *router1* • Puerto 3 conexión hacia el servidor1 • Puerto 5 conexión hacia el servidor2 5 puertos disponibles	[W14]

Tabla 2.2 Equipos de interconectividad en funcionamiento actualmente en la Institución

	MARCA	FUNCIÓN	UBICACIÓN	PUERTOS	EQUIPO
Switch 2	*Switch CNet CNSH–1600 Power Switch*	Interconexión de switches	Sala de Internet	• 16 puertos *Fast Ethernet* 4 puertos utilizados: • Puerto 6 conexión hacia el *Switch3* • Puerto 8 conexión hacia el *Switch4* • Puerto 9 conexión hacia el *Switch5* • Puerto 16 conexión hacia el servidor 2 12 puertos disponibles	[W15]
Switch 3	*Switch 3Com Baseline 2024*	Conexión hacia la red la de la Sala de Internet	Sala de Internet	• 24 puertos *Fast Ethernet* 19 puertos utilizados: • Puertos 10-11-13-14-22 disponibles • Puerto 24 conexión hacia el *Switch2*.	[W16]
Switch 5	*Switch 3Com 3CFSU08*	Conexión de puntos de Secretaria hacia el *switch2*	Secretaria	• 8 puertos *Fast Ethernet* 3 puertos utilizados: • Puerto 1 conexión hacia Switch 2 • Puerto 4 conexión hacia el Switch 6 • Puerto 5 conexión a Vicerrector2 5 puertos disponibles	[W17]

Tabla 2.2 Equipos de interconectividad en funcionamiento actualmente en la Institución

	MARCA	FUNCIÓN	UBICACIÓN	PUERTOS	EQUIPO
Switch 4	*Switch 3Com Baseline 2024*	Interconexión hacia: • Computador de Administrador • Bodega • Vicerrectorado • Departamento Técnico Pedagógico	Sala de Internet	• 24 puertos *Fast Ethernet* 7 puertos utilizados: • Puerto 4 conexión hacia Bodega General • Puerto 6 conexión hacia computador Vicerrector1 • Puerto 8 conexión hacia el DTP • Puerto 9 conexión computador Administrador • Puerto 11 conexión computador Secretaria • Puerto 12 conexión computador Administrador 2 • Puerto 24 conexión hacia el *Switch2* 17 puertos disponibles	[W16]

Tabla 2.2 Equipos de interconectividad en funcionamiento actualmente en la Institución

	MARCA	FUNCIÓN	UBICACIÓN	PUERTOS	EQUIPO
Switch 6	*Switch 3Com Baseline 2024*	Interconexión en Secretaria	Secretaria	• 24 puertos *Fast Ethernet* 2 puertos utilizados • Puerto 13 conexión hacia el *Switch5* • Puerto 15 conexión hacia el Servidor1 22 puertos disponibles	[W16]
Access Point 1	*Access Point D-Link DWL 2100AP*	Conexión de Internet para profesores del laboratorio de informática	Sala de Internet	1 puerto para enlace WAN	[W18]

Tabla 2.2 Equipos de interconectividad en funcionamiento actualmente en la Institución

A pesar de que los equipos *router 1 y router 2* son enlaces hacia Internet, se puede establecer que el único que puede ser aprovechado por toda la Institución es aquel a través del cable modem Motorola (*router 1*). Este equipo es proporcionado por la compañía Telmex, con esta empresa la Institución tiene un contrato del tipo Pymes de 3 Mbps con un nivel de compartición de 4:1, el otro puede ser utilizado únicamente por los delegados del Ministerio de Educación que trabajan en la Institución, sin embargo inalámbricamente es utilizado por los profesores que dictan la materia de informática en las aulas situadas frente a la Sala de Internet.

También se puede establecer que los equipos que se encuentran funcionando en la Institución no cumplen con requisitos mínimos, como por ejemplo ser administrables. El *switch1* que cumple la función de *switch* de *core* es de muy baja capacidad lo que reduce el nivel de optimización de las conexiones y no permite utilizar funciones propias de un equipo de este nivel, por lo que resulta erróneo afirmar que esta red este completamente estructurada.

2.1.5.2 Servidores

En la red de la Institución actualmente se encuentran operando dos computadores que realizan funciones de servidores, sin embargo estos equipos no cumplen con las características para un adecuado funcionamiento dentro de una red convergente como la que se planea diseñar para la Institución debido a que poseen similares prestaciones a las de las estaciones de trabajo y no resultan adecuadas para el alojamiento de servicios.

Los actuales equipos que funcionan como servidores son estaciones de trabajo normales adaptadas con los programas necesarios para su funcionamiento, que a pesar de encontrarse funcionando actualmente no son la opción más recomendable, en cualquier momento estos pueden dejar de funcionar dejando a la Institución sin los servicios que prestan. Además estos equipos no poseen características como redundancia de fuente, o protecciones adicionales que brindan confiabilidad en un equipo dedicado exclusivamente como servidor.

2.1.5.2.1 Servidor 1

Marca: Clon

Ubicación Secretaría

Procesador: *Intel Core 2 Quad @ 2.4 Ghz*

Memoria: 4 GB

Tarjetas de red: *Realtek* RTL 8139 PCI

- *Realtek* RTL 8168/8111 PCI-E *Gigabit*
- Via Rhine III Compatible *Fast Ethern*

Plataforma: Windows Server 2003 R2 SP2

Función: Aloja el servidor del sistema de información académica de la Institución que básicamente sirve para la asignación de notas mensualmente a los estudiantes.

2.1.5.2.2 Servidor 2

Marca: Clon

Ubicación Sala de Internet

Procesador: *Intel Pentium 4 @ 3.4 GHz*

Memoria: 3 GB

Tarjetas de red: NIC Fast Ethernet PCI Familia RTL8139 de Realtek

Intel 82562ET/EZ/GT/GZ PRO/100 VE Ethernet Controller

Plataforma: *CentOS* [21]*release* 4.4 (Final)

Función: Servidor *Proxy* ubicado en la Sala de internet por el medio del cual se controla el acceso a Internet en la Institución. Por medio de este se realiza filtrado de página web además de control del acceso a la red.

[21] CentOS (Community ENTerprise Operating System) es un clon a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat.

2.1.5.3 Estaciones de Trabajo

Las estaciones de trabajo de la Institución poseen diferentes características de acuerdo al área a la que sirven. De los laboratorios de computación en la Institución solo uno de ellos tiene acceso a la red, la llamada Sala de Internet donde se presta este servicio a la comunidad educativa, mientras en las otras salas los equipos son utilizados para la utilización de aplicaciones de escritorio entre las que podemos mencionar paquetes ofimáticos y *Autocad*.

De igual manera en las secretarías, en su gran mayoría, también se trabaja con equipos que no tienen acceso a la red de la Institución, sin embargo estos equipos deben ser tomados en cuenta debido a que se espera tener una interconexión de todas las estaciones de trabajo a la red de datos, no tienen creados cuentas de usuario, todos poseen una cuenta con privilegios de administrador, además no existe ningún control sobre el software que posee cada usuario. A través del campus se encuentran además diferentes equipos para el trabajo de los departamentos de la Institución que en su gran mayoría no se encuentran conectados a la red, por lo que su solicitud para poder ingresar a la misma es una constante. En la tabla 2.3 se encuentran especificadas las máquinas, de uso permanente, por cada área de la Institución y en la tabla 2.4 las características de las mismas.

Áreas	Número de equipos por áreas de la Institución
Administración	18
Electrónica	8
Automotriz	1
Industrial	1
Electricidad	9
Bodegas	5
Inspecciones	4
Superior	6
Aulas	14
Cámaras	13
Total	**77**

Tabla 2.3 Resumen de equipos en la Institución.

Cantidad	Sistema Operativo	Procesador		Memoria RAM	Tarjeta de Red/(Acceso a la red)	Ubicación
		Marca	Velocidad			
1	Microsoft Windows XP Colossus	Intel Celeron E1200	1.6 GHz	256 MB	No tiene / (No)	Laboratorio de Informática Electrónica
5	Microsoft Windows XP Professional SP2	Intel Pentium III	2.4 GHz	1 GB	nVIDIA nFORCE Network Adapater / (No)	Laboratorio de Informática y Sala de Audiovisuales de Electrónica
1	Microsoft Windows 7	Intel Celeron E1200	1.6 GHz	1 GB	No tiene / (No)	Laboratorio de Informática Electrónica
3	Microsoft Windows XP Professional SP2	Intel Celeron E1200	1.6 GHz	512 MB	Adaptador Fast Ethernet Compatible VIA / (No)	Laboratorio de Informática Electrónica
12	Microsoft Windows XP Professional SP3	Intel Pentium 4	2 GHz	512 MB	Intel 82562 PRO/100 VE Network Connection / (Si)	Sala de Internet, Centro médico, Mecatrónica
1	Microsoft Windows XP Professional SP3	Intel Pentium 4	3 GHz	512 MB	NIC Fast Ethernet PCI Familia RTL8139 de Realtek / (Si)	Sala de Internet, Mecánica Industrial
4	Microsoft Windows XP Professional SP3	Intel Pentium 4	3 GHz	1 GB	NIC Fast Ethernet PCI Familia RTL8139 de Realtek / (Si)	Sala de Internet
12	Microsoft Windows XP Professional SP3	Intel Core 2 Duo CPU 6320	1,86 GHz	2 GB	Intel PRO/100 VE Network Connection / (Si)	Sala de Internet, Laboratorios de Física y Química, Inspecciones, Nivel Superior
1	Microsoft Windows XP Professional SP3	Intel Pentium 4	3 GHz	512 MB	Intel PRO/100 VE Network Connection / (Si)	Sala de Internet

Tabla 2.4 Características de los equipos de la Institución

Cantidad	Sistema Operativo	Procesador		Memoria RAM	Tarjeta de Red/(Acceso a la red)	Ubicación
		Marca	Velocidad			
2	Microsoft Windows XP Professional SP2	Intel Core 2 Duo CPU 6320	1,86 GHz	1 GB	D-Link Wireless 108G DWA-520 Desktop Adapter / (Si)	Laboratorios Informática 1 y 2
37	Microsoft Windows XP Professional SP2	Intel Core 2 Duo CPU 6320	1,86 GHz	1 GB	Intel PRO/100 VE Network Connection / (No)	Laboratorios Informática 1 y 2
5	Microsoft Windows 7	Intel Core 2 Quad	2,4 GHz	4 GB	Intel PRO/100 VE Network Connection / (Si)	Contabilidad, Biblioteca, Jefatura de Talleres
10	Microsoft Windows XP Professional SP2	Intel Core 2 Duo CPU 6320	1,86 GHz	2 GB	Intel PRO/100 VE Network Connection / (Si)	Secretaria, Sala de audiovisuales, Bodega General
11	Microsoft Windows XP Professional SP3	Intel Pentium 4	1 GHz	512 MB	Intel PRO/100 VE Network Connection / (No)	Biblioteca, Bodegas, Inspecciones, Oficinas, DOBE
31	Linux Ubuntu 10.4	AMD Athlon(tm) II X2 215 Processor	2,4 GHz	2 GB	NetXtreme BCM5761 Gigabit Ethernet PCIe / Wireless Interface RT2860 / RaLink / (No)	Laboratorio 3 Ministerio de Educación
136						**TOTAL**

Tabla 2.4 Características de los equipos de la Institución

2.1.5.4 Equipos de impresión

La Institución cuenta con impresoras para el uso administrativo en las diferentes oficinas del área. Todas estas están conectadas directamente a una estación de trabajo a pesar de que algunas de ellas tienen funciones de red estás no son aprovechadas lo que hace que sean ineficientes en términos de optimización. A continuación en la Tabla 2.5 se presenta una lista de los equipos de impresión existentes.

Equipo	Marca	Soporte para conexión a la red	Cantidad
 [W19]	*Lexmark E260dn*	Sí	1
 [W20]	*HP LaserJet MI522nf*	Sí	1
 [W21]	*HP Laserjet 1320n*	Sí	3
 [W22]	*HP Laserjet 1300*	No	1
 [W23]	*HP Color LaserJet CP3525dn*	Sí	1
 [W24]	*Epson LX-300+*	No	1

Tabla 2.5 Características de las impresoras de la Institución

La única impresora destinada al uso de estudiantes y profesores, a pesar de que no se encuentra compartida dentro de la red, es la HP *LaserJet* MI522nf que se encuentra conectada a la computadora del administrador de red. Esta impresora puede ser utilizada previo al pago de la impresión sin embargo al igual que las demás está conectada únicamente a un computador desde el cual se accede a los documentos compartidos en la red para su posterior impresión.

Este servicio puede ser optimizado de gran manera mediante la red de datos por medio de la cual una impresora puede ser compartida para el uso de la misma por varios usuarios, lo cual además de optimizar el tiempo de acceso a ellas representa un significativo ahorro de recursos.

2.1.5.5 EQUIPOS PARA LA COMUNICACIÓN DE VOZ

Como se anotó anteriormente la red de datos es independiente de la de voz. La red de voz de la Institución está compuesta por una central telefónica y un sistema de procesamiento de voz ambos de marca Panasonic para las funciones internas de telefonía. Cabe precisar que posee además un número de líneas telefónicas troncales contratadas con la Corporación Nacional De Telecomunicaciones CNT para poder comunicarse con la red telefónica pública. Estos equipos se encuentran ubicados en la Secretaría general de la Institución. A continuación se presenta un resumen de las características de los mismos.

2.1.5.5.1 Central Telefónica Híbrida IP:

Marca: Panasonic KX-TDA200

Ubicación: Secretaría

Características: Se trata de una central telefónica híbrida la cual puede ser conectada a la red IP a través de un módulo que le permite manejar un número de llamadas simultáneas IP, posee además funciones como red privada virtual, red QSIG y funciones de correo de voz. Está diseñada para el uso de pequeñas y medianas empresas sin embargo la mayoría de características

no se encuentras programadas y están en desuso. Actualmente se encuentra en servicio tanto para teléfonos analógicos como digitales.

Figura 2.2 Central Telefónica Panasonic KX-TDA200[W25]

2.1.5.5.2 Sistema de procesamiento de voz:

Marca: Panasonic KX - TVM50

Ubicación: Secretaría

Características: Es el complemento a la central telefónica funciona tanto para teléfonos analógicos como digitales, posee configuración automática y monitoreo de llamadas, integra correo electrónico y permite transferencia de llamadas distribuciones a grupos, servicios de llamada automática, transferencia automática de fax, enrutamiento de llamada por medio de identificadores de usuarios y 64 niveles de clase de servicio. Cabe anotar que estas funciones son solo para teléfonos digitales de los cuales existen 2 en la Institución

Figura 2.3 Sistema de procesamiento de voz Panasonic KX - TVM50[W26]

2.1.5.5.3 Teléfonos:

MARCA	CANTIDAD	EQUIPO
Panasonic KX TS500MXW	**30**	 [W27]
Teléfono analógico que presenta funciones básicas De telefonía como control de volumen electrónico, flash temporizador y ajustes de tono / impulso programables.		
Panasonic KX – T7730	**2**	 [W28]
Teléfono analógico con pantalla LCD, teclas de gestión de llamada, manos libres, integra funciones programables para conocer si las extensiones se encuentran ocupadas mediante luces indicadoras y acceso al directorio a través de *JOG DIAL*[22]. Este teléfono se encuentra en secretaría y posee estas funciones debido a que en este sitio son necesarias estas.		
Panasonic KX – T7436	**1**	 [W29]
Teléfono digital ubicado en el rectorado que además de las características expuestas para teléfonos analógicos, cuenta con una pantalla LCD para ayuda, directorio telefónico.		
Panasonic KY –FHD351	**1**	 [W30]
Fax Copiadora ubicado en rectorado con contestador, Velocidad del modem (Kbps) 14.4 y Pantalla LCD. Entre otras características se pueden anotar Identificador de llamadas, altavoz. Respecto a las funciones telefónicas presenta transferencia de llamadas, directorio telefónico 110 memorias. Mensajería de voz con un tiempo de grabación de hasta 18 minutos.		

Tabla 2.6 Características de los teléfonos de la Institución

[22] Es una rueda que al momento de girar permite la navegación a través del directorio

2.1.6 DIRECCIONAMIENTO IP

Las direcciones IP son asignadas de forma manual utilizando una dirección clase C (192.168.100.0/24), como se mencionó anteriormente otra falencia dentro de esta red es el hecho de que no se encuentra segmentada, es decir, no existen *VLAN´s* o subredes. Todos los usuarios se encuentran dentro de la misma red, lo cual es una falla tanto en el aspecto administrativo como de seguridad. En la tabla 2.7 se presenta la actual distribución de direcciones IP.

Direcciones IP asignadas		
Departamento	**Computador**	**Dirección IP**
Rectorado	Dr. Jhony Rodríguez	192.168.100.47
Vicerrectorado	Msc. Manuel Miño	192.168.100.46
Vicerrectorado	Dr. José Bermúdez	192.168.100.49
Secretaría	Lda. Carmen Paillacho	192.168.100.42
Técnico Pedagógico	Lcdo. Hernando Abad	192.168.100.40
Bodega General	Sra. Nancy Grijalva	192.168.100.43
Inpección General	Sra. Elena Hidalgo	192.168.100.44
Sala de Internet	Tlga. Ana Guerra	192.168.100.5……..(.13)
Sala de Internet	Tlga. Ana Guerra	192.168.100.16……..(.21)

Tabla 2.7 Direccionamiento IP actual

Todos los equipos en el Instituto acceden a Internet por medio del *servidor 1* el cual como ya se explicó cumple la función de servidor proxy con la dirección IP 192.168.100.1. Este servidor se configura manualmente, de la misma forma que las direcciones IP, como default Gateway en todos los equipos que tienen acceso a la red, tal como se muestra en la figura 2.4 donde se presenta un ejemplo de la configuración de los equipos. Actualmente las direcciones IP son asignadas por el administrador de la red, sin embargo estas no tienen ningún orden específico o alguna diferenciación entre las áreas o lugares en donde se encuentran los equipos a las que son dadas, además que estas direcciones no se encuentran debidamente documentadas sino que solo el administrador tiene conocimiento de ellas.

Se emplean dos direcciones IP públicas proporcionadas por el proveedor de servicios de Internet TELMEX para el acceso a Internet así como para el uso del servidor de notas, las direcciones son mostradas en la Tabla 2.8.

Figura 2.4 Configuración de las propiedades de IPv4 para la conexión de Internet

Direcciones IP asignadas		
Departamento	**Servidor**	**Dirección ip**
Sala de internet	Proxy Linux	200.124.229.124
Secretaría	Windows 2003 server	200.124.230.69

Tabla 2.8 Direcciones IP públicas

2.1.7 ANÁLISIS DE LA TOPOLOGÍA DE LA RED DE VOZ

Con respecto a la red de voz actual de la Institución se encuentra funcionando a través de un sistema conformado por una central telefónica y un sistema de

manejo de funciones de voz como correo, agenda telefónica entre otras. Esta central telefónica maneja extensiones internas, troncales y líneas directas contratadas con la Corporación Nacional de Telecomunicaciones CNT.

Los teléfonos se encuentran conectados mediante una topología tipo estrella, cuyo nodo central es la central telefónica (PBX), la cual se encarga de distribuir el tráfico de voz en la red según su configuración y permite conectarse a la *PSTN (Public Switched Telephone Network).* La figura 2.5 muestra un esquema de la conexión de los equipos en la red de voz actual.

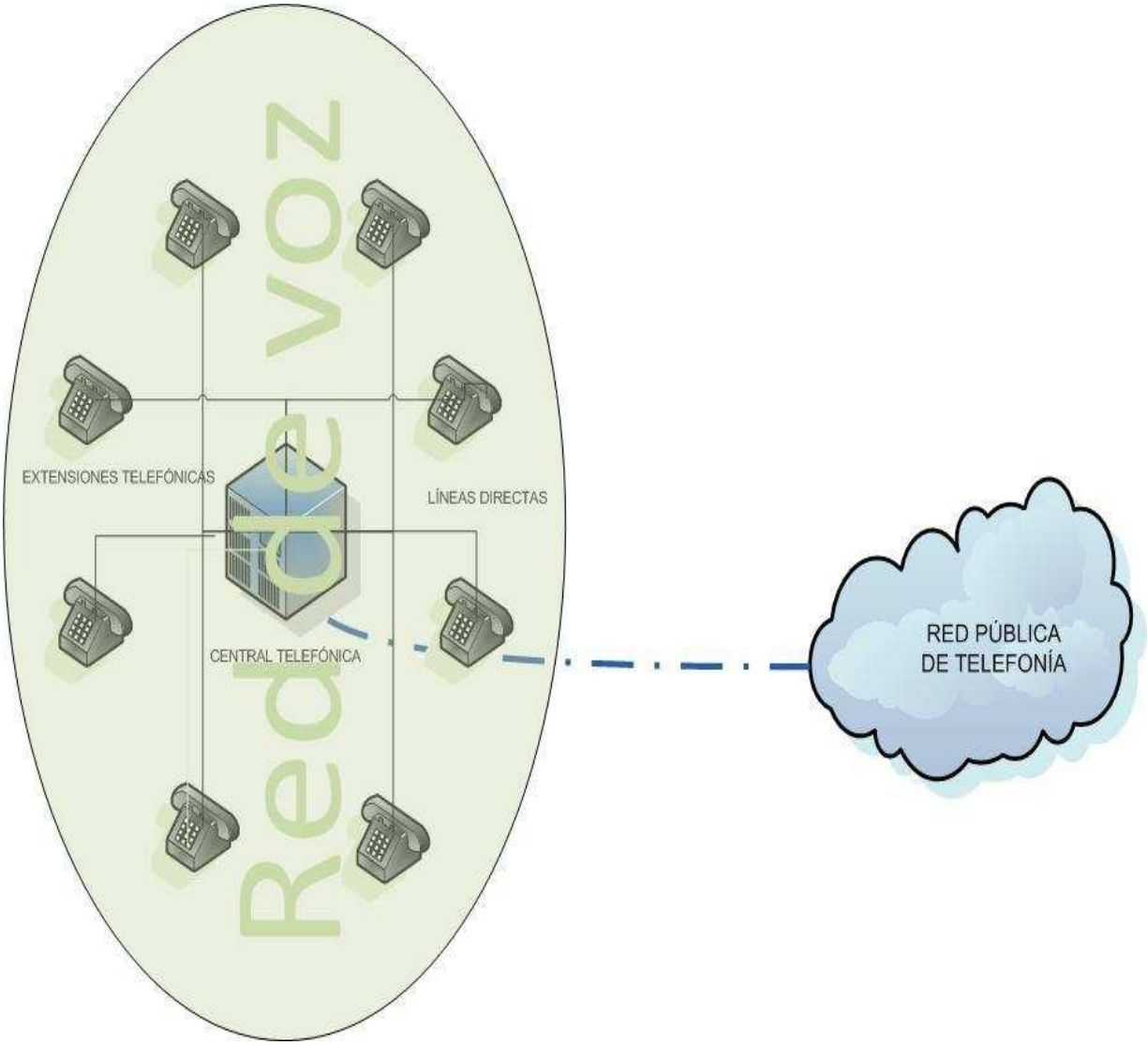


Figura 2.5 Diagrama esquemático de la red de voz actual

2.2 ANÁLISIS DEL SISTEMA DE CABLEADO ESTRUCTURADO.

El Sistema de Cableado Estructurado brinda una perspectiva para crear un sistema organizado que el Administrador, usuario, técnicos y cualquier persona pueda fácilmente identificar, comprender o modificar cuando lo desee. El cableado garantiza eficiencia, efectividad, escalabilidad, ya que cuando se realiza el diseño se toma en cuenta que el modelo dura alrededor de 15 años. Uno de los objetivos que se persigue con esto es encontrar una solución óptima que permita interconectar todos los dispositivos, y al mismo tiempo cumplir con las normas y estándares internacionales que permitan admitir tecnologías actuales y futuras.

Además con el cableado estructurado se planifica y se proyecta para dar conectividad teniendo en cuenta el crecimiento de usuarios en la intranet. La infraestructura de cableado conserva la libertad de elegir múltiples proveedores ofreciendo así la posibilidad de realizar modificaciones fácilmente y a bajo costo. Todo cambio que se quiera implementar será independiente de tipo de aplicación así como de los equipos de conectividad utilizados. Las salidas (*outlets*) garantizarán que cualquier movimiento se lo pueda hacer sin modificar el cableado existente.

Actualmente el Instituto Tecnológico Superior Central Técnico no goza de los estándares internacionales ANSI/TIA/EIA para el Sistema de Cableado Estructurado. Es un cableado de topología en estrella jerárquica. La Institución cuenta con una Sala de Equipos que no brinda las comodidades necesarias para un buen funcionamiento, los equipos activos no poseen ninguna protección eléctrica, no hay una adecuada conexión a tierra, tampoco utiliza *UPS*. En base a lo expuesto se puede concluir que ninguna parte del sistema se encuentra apropiadamente certificada.

Se realizó una inspección visual de todas las instalaciones, aéreas de trabajo y laboratorios para conocer exactamente donde existe cableado estructurado y donde resulta primordial implementarlo, así como prever el lugar donde se pueden ubicar la de Equipos y el Cuarto de Telecomunicaciones.

2.2.1 ÁREA DE TRABAJO

Se compone de todos los equipos, terminales, *jacks* que se conectan a la toma de información. Se analizó las estaciones de trabajo dentro de la intranet, las cuales se detallaron anteriormente indicando sus características técnicas. En el análisis de las estaciones se comprobó que todos los equipos eran computadores, y que no existían teléfonos IP, ni impresoras IP conectadas actualmente a la red. Además únicamente en Secretaría General ubicada en la planta baja, se encuentran terminales *(Faceplates)* como se observa en la figura 2.6 para conectar directamente los dispositivos al sistema.

Figura 2.6 *Faceplate* Secretaría

En los laboratorios de informática existe un cableado que recorre por ductos en las paredes pero que no se conectan a ningún *faceplate*. Estos cables directamente se conectan al computador y no utilizan *patch cords* con lo cual están violando la norma 568C.1 del cableado estructurado.

Cada una de las secretarias disfruta de un espacio de trabajo separado por vidrios y por madera como se presenta en la figura 2.7.

Figura 2.7 Área de trabajo Secretaria.

Los *patch cords* utilizados en Secretaría General cumplen con la norma EIA/TIA 568 B. Ninguna de los restantes computadores del Instituto Tecnológico Superior Central Técnico cuenta con *patch cords* certificados.

2.2.2 CABLEADO HORIZONTAL.

Comprende la conexión desde el Cuarto de Telecomunicaciones hasta los *faceplates*. En este caso como no se cuenta con *faceplates* el cable viaja directamente a conectarse con los computadores utilizando un cable UTP categoría 5e. En los laboratorios de Informática, los cables atraviesan ductos en las paredes como se observa en la figura 2.8 y llegan directamente a los computadores. En Secretaría es el único lugar donde el cable viaja por canaletas y llega a los *faceplates* para acoplarse a los equipos. Ninguno de los *faceplates* instalados tiene un etiquetado por lo que se hace difícil administrar y poder detectar fallas, con lo que se confirma que no se está cumpliendo con la norma TIA/EIA 606.

Figura 2.8 Cableado horizontal. Cable UTP directo a equipo.

Los equipos activos que se están utilizando se enumeran a continuación en la tabla 2.9 donde están indicados los puertos disponibles y los ocupados.

EQUIPOS ACTIVOS		
	Puertos Ocupados	**Puertos Disponibles.**
Router Cable Modem SBV5121	1	1
Switch D-Link DES – 1008 D Fast Ethernet	3	5
Switch C-Net CNSH – 1600 Power Switch	4	12
Switch 3Com Baseline 2024	19	5
Switch 3Com Baseline 2024	7	17
Switch 3Com 3CFSU08	3	5
Switch 3Com Baseline 2024	2	22

Tabla 2.9 Disponibilidad de puertos de los equipos activos

De la tabla anterior se determina que los *Switches* 3COM y C-NET CNSH pueden ser reutilizados para el diseño de la red de área local, como *switches* de acceso ya que sus especificaciones indican que no son administrables y servirán para conectar a los usuarios finales.

2.2.3 CABLEADO VERTICAL.

En el cableado vertical no cumple con el estándar ANSI/ TIA/EIA 568 B.2 para conectar el *backbone* de la red. Este subsistema tiene una interconexión en estrella, se toma como referencia que la altura del edifico es de 3 metros, puesto que en la planta baja se encuentra dos *switches* y un servidor. Únicamente este subsistema se conecta a los equipos de comunicaciones mediante un cable UTP categoría 5e, de cuatro pares. La distancia entre los equipos activos desde la planta baja al Cuarto de Telecomunicaciones en la sala de internet es de aproximadamente 10 metros.

2.2.4 CUARTO DE TELECOMUNICACIONES, SALA DE EQUIPOS Y ACOMETIDA.

El cuarto de telecomunicaciones se ubica en el segundo piso, dentro de la Sala de Internet sin embargo en la planta baja en Secretaria General también existe otro Cuarto de Telecomunicaciones el cual alberga dos *switches* 3COM, el servidor *Windows Server* 2003, y la Central telefónica Híbrida IP que se visualiza en la figura 2.9. Los dos Cuartos de Telecomunicaciones tienen un área aproximadamente de unos 10 metros cuadrados. Solamente existe una persona autorizada para la administración del mismo. Esta instalación no cumple con la norma ANSI/TIA/EIA 569 para un Cuarto de Telecomunicaciones.

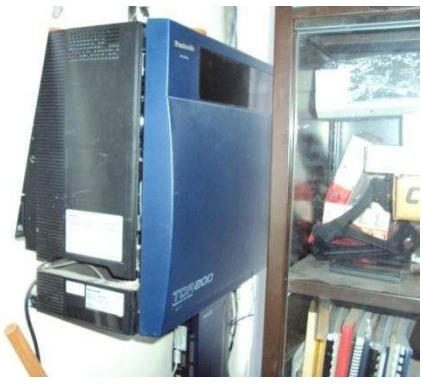


Figura 2.9 Ubicación de la Central telefónica Híbrida Panasonic en el Cuarto de Telecomunicaciones.

En el Cuarto de Telecomunicaciones de la Sala de Internet existe un *patch panel* de 24 puertos como se observa en la figura 2.10 que se ubica en un bastidor el cual se utiliza principalmente para alojar a los *switches* 3COM, el resto de quipos de interconectividad se ubican sobre una mesa. Ninguno de los equipos de *networking* está conectado a un equipo *UPS (Uninterruptíble Power Supply)*, todos ellos se conectan directamente a la red pública de energía por lo que si existe una descarga eléctrica los mismos podrían arruinarse. Adicionalmente el cuarto utilizado no posee un adecuado sistema de aire acondicionado que brinde el nivel de humedad adecuado y que evite cualquier problema de calentamiento. Incluso no tiene una conexión de puesta a tierra.

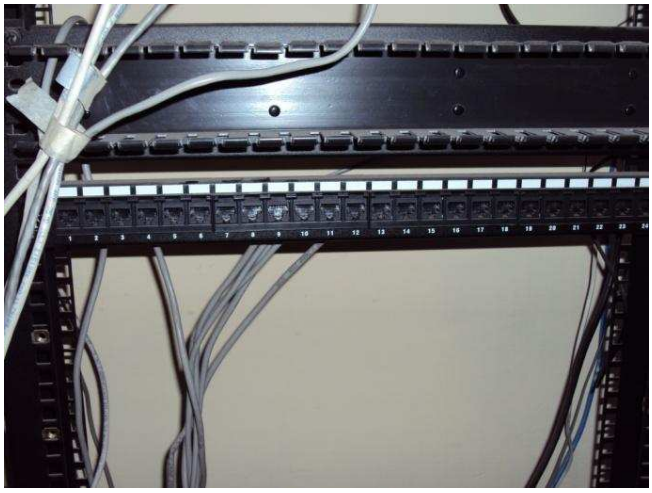


Figura 2.10 *Patch Panel* 24 puertos ubicado en el Cuarto de Telecomunicaciones.

No se puede hablar de una acometida o entrada de servicios hacia la Institución debido a que esta no se encuentra especificada. Los servicios llegan a través de cables sueltos según el proveedor de servicios ha supuesto conveniente el momento de la instalación.

2.2.5 REQUERIMIENTOS DE PUESTA A TIERRA

El sistema de conexión a tierra para el diseño del cableado estructurado es fundamental para proteger la vida útil de los equipos así como preservar la vida del personal que manipula el mismo. La mayoría de casos los daños a los equipos de telecomunicaciones se debe a variaciones de voltaje debido a malas conexiones de puesta a tierra o en su defecto defectuosas conexiones.

Por este motivo un sistema de puesta a tierra es fundamental para la infraestructura del Instituto y el cuarto de telecomunicaciones debe necesariamente contar con una Barra de tierra principal de telecomunicaciones (*TMGB*) como lo indica la norma de cableado estructurado correspondiente a los sistemas de puesta a tierra.

2.2.6 CANALIZACIONES.

Las canaletas que se emplean en el cableado del Instituto son de plástico PVC lisas normales de un vía de dimensiones 60mm x 40mm (base x alto) ver figura 2.11, se debe acotar que no están instaladas cajas ni terminaciones.

Para toda la Institución se tiene una independencia entre el cableado eléctrico y los espacios que ofrecen cableado estructurado, lo cual disminuye interferencias eléctricas.

No se utiliza techo falso en ninguna de las instalaciones de Secretaria, Vicerrectorado, Contabilidad, y Laboratorios. El cableado únicamente viaja a través de la loza o a su vez esta direccionado por las paredes laterales de los edificios y llega directamente a un *switch* o a un computador según sea el caso.

Figura 2.11 Canaletas Plásticas PVC que recorren por la pared.

2.2.7 RESUMEN DE LOS PUNTOS DE CABLEADO DE LA INSTITUCIÓN

Como se indicó anteriormente, en el Instituto la conexión actual de la red no cumple con las normas de cableado estructurado, una de las razones es que las salidas de telecomunicaciones en las áreas de trabajo no se encuentran debidamente terminadas en *faceplates*, debido a que el sistema de cableado no se encuentra certificado, el servicio llega las estaciones simplemente a través de cables directamente conectados a los *switches*, sin embargo en la tabla 2.10 se indica un resumen de las salidas de datos que actualmente brindan servicio en la Institución y su ubicación.

DEPARTAMENTO	NÚMERO DE PUNTOS DE DATOS
Rectorado	1
Vicerrectorado	2
Secretaría	1
Departamento Técnico Pedagógico	1
Bodega general	1
Inspección genreal	1
Sala de Internet	21
TOTAL	**29**

Tabla 2.10 Resumen de puntos de cableado actuales en la Institución

Como se explica más adelante, en el literal 2.3, los usuarios potenciales de la red superan ampliamente al número total de puntos actuales en servicio, además que a excepción de Bodega General e Inspección General, todos los demás sitios se encuentran exclusivamente en el edificio administrativo. Esto implica que las demás áreas del colegio no tienen acceso a la red en la Institución por lo que resulta imperiosa la necesidad de la implementación de la red de datos.

2.3 ANÁLISIS DE LOS USUARIOS DE LA RED

Para el análisis de los usuarios de la red se ha considerado conveniente el dividirlos por grupos de usuarios para una fácil clasificación de los mismos. Los grupos considerados en este análisis solo los siguientes:

- Administrativos
- Profesores
- Estudiantes
- Periféricos

2.3.1 USUARIOS ADMINISTRATIVOS

En el sector administrativo cuenta con 55 personas que entre los que se encuentran los siguientes usuarios:

- Autoridades
- Secretarias y Personal Contable
- Personal de bodega y biblioteca
- Inspecciones

Las autoridades y secretarias se encuentran en su mayoría trabajando en el área administrativa en este sector a cada usuario se le asigna una computadora, sin embargo cabe resaltar que no todos los usuarios tienen acceso a la red. Una gran cantidad de usuarios no poseen este acceso por lo que su documentación es manejada únicamente de manera local.

De este grupo solo poseen acceso a Internet, la Secretaria General, el Rector y los vicerrectores por lo que resulta indispensable el que todos ellos puedan tener acceso tanto a la Intranet como a Internet. Los usuarios conectados a la red se conectan al *switch 6* que a su vez se encuentra conectado al *switch 5,* ambos ubicados en Secretaría General, por medio de este se logra la conexión con el servidor *Proxy* para acceso a Internet.

Los usuarios que tiene acceso a Internet si bien están conectadas a través del servidor *Proxy* no poseen restricciones de uso para la red lo cual es una falla muy grave respecto de la seguridad. De los mencionados dentro de usuarios administrativos existen algunos que tiene acceso a la red y otros que no debido a que se encuentran distribuidos en diferentes sitios del campus por lo que no poseen puntos de red razón por la cual no acceden a la misma.

2.3.2 ESTUDIANTES

Los estudiantes se encuentran divididos en los siguientes grupos:

- Sección Diurna
  - Ciclo Básico (Vespertino)
  - Ciclo Diversificado (Diurno)
- Sección Nocturna
- Nivel Superior

Casi la totalidad de los estudiantes que accede a la red lo hace por medio de las computadoras ubicadas en la sala de Internet que tienen instaladas el sistema operativo (*Windows XP*), para su acceso los estudiantes compran un ticket en colecturía lo cual les permite el uso del Internet por una hora, controlados por el administrador de la red a través del proxy instalado. El número de computadores ubicados para este fin en la sala es de 17, además de dos computadoras para uso del administrador de red. En la tabla 2.11 se muestra el número de estudiantes de la Institución que vendrían a ser potenciales usuarios de la red.

Sección Diurna		**Sección Nocturna**	**Nivel Superior**	**TOTAL**
Ciclo Básico	**Ciclo Diversificado**			
1271	1153	1143	998	**4565**

Tabla 2.11 Número de estudiantes totales del Instituto Tecnológico Superior "Central Técnico"*Fuente:* Secretaría

Los estudiantes no acceden a servicios dentro de la Intranet directamente, además el uso de Internet en la sala correspondiente es limitado en comparación al número total de estudiantes. El acceso a ciertas aplicaciones y páginas web se encuentra restringido por el administrador.

Esta realidad es la que se intenta cambiar y masificar el uso de la red no tan solo para el Internet sino también para los servicios planificados a ser incluidos en la intranet de la Institución.

2.3.3 PROFESORES

El Instituto cuenta con 246 profesores, no poseen puntos de red exclusivos, sin embargo acceden a la red desde la Sala de Internet y los laboratorios de informática los cuales poseen acceso a la red por medio de un *Access Point* al cual se conectan a través de una conexión inalámbrica. Al igual que los estudiantes poseen restricciones en el acceso de ciertas aplicaciones y páginas web y su uso no es masivo. Además cabe resaltar que el uso de los profesores de la red es mayormente para el registro de calificaciones mensuales a través de un sistema instalado en el servidor Windows ubicado en secretaría y conectado a Internet a través de una dirección pública, y casi todos lo realizan desde sitios de Internet externos a la Institución. El acceso de los profesores a los recursos es indispensable para poder darles herramientas adecuadas para realizar su labor educativa.

Finalmente como periféricos se toman en cuenta las impresoras para el uso administrativo en cada uno de las oficinas, estas suman ocho en total. Únicamente, la impresora localizada en la Sala de Internet es de uso estudiantil como impresora compartida. No existe otro tipo de periféricos conectados a la red de la Institución. Sin embargo el uso de estos dispositivos a través de la red significaría el aprovechamiento de recursos y la inclusión de otros servicios como almacenamiento compartido, video seguridad entre otros.

2.3.4 RESUMEN DE LOS USUARIOS POTENCIALES DE LA RED

A continuación en la tabla 2.12 se presenta un resumen con los usuarios potenciales de la red y el grupo al que pertenecen, es decir todos aquellos que hipotéticamente harían uso de la red de datos de la Institución, para indicar la relación existente entre los usuarios actuales.

ADMINISTRATIVOS	PROFESORES	ESTUDIANTES	TOTAL
55	246	4565	**4866**

Tabla 2.12 Número de usuarios potenciales de la red

2.4 ANÁLISIS DE TRÁFICO Y ANCHO DE BANDA GENERADO POR LAS APLICACIONES

A fin de realizar un completo análisis de la situación actual de la red resulta conveniente el tener una visión del tráfico actual que generan las aplicaciones instaladas, así como las que podrían cursar tráfico en la implementación futura de la red de datos multiservicios. Estas harán uso de la red para sus actualizaciones así como para un uso compartido mediante un servidor de aplicaciones.

2.4.1 ANÁLISIS DE LAS APLICACIONES INSTALADAS EN LOS EQUIPOS DE LA RED

Dentro del análisis de la situación actual de la red es conveniente realizar un reconocimiento de las aplicaciones que comúnmente se están utilizando en las estaciones de trabajo y en los servidores. En base a esta recopilación de información se puede determinar cuál es la vida útil de las computadoras y sus componentes para un adecuado funcionamiento de las aplicaciones utilizadas.

Las aplicaciones de software, con las que se trabaja en la Institución, cuentan con su respectiva licencia y es responsabilidad únicamente del personal de Sistemas la instalación de las mismas. Todas las estaciones de trabajo se encuentran funcionando bajo la plataforma de Windows. En la tabla 2.13 se muestra un resumen de las aplicaciones encontradas en los equipos de la Institución.

	Descripción	**Fabricante**	**Observaciones**
Microsoft Office Professional 2007	Suite de oficina (Word, Excel, PowerPoint)	Microsoft	
Reproductor de Windows Media	Reproductor de música y video de Windows	Microsoft	
WinRar archiver	Software de compresión de datos	RAR Lab	
J2SE Runtime Enviroment 5.0 Update 6	Desarrollo de software y acceso a aplicaciones Java.	Sun Microsystems	
Acrobat Reader 8.0 Professional	Visualización e impresión de archivos PDF	Adobe	
Adobe Flash Player 9 ActiveX	Reproductor multimedia	Adobe	
TuneUp Utilities 2008	Mejorar rendimiento del sistema	Tune Up software	
Windows Live Messenger	Mensajería Instantánea	Microsoft	
Autocad 2007 Spanish	Programa de diseño asistido por computadora	Autodesk	Instalado en los laboratorios de informática
Microsoft Internet Explorer	Navegador web	Microsoft	
Mozilla Firefox	Navegador web	Mozilla	
PRTG Traffic Grapher	Monitoreo de red y uso de ancho de banda	Paessler	Instalado para la medición de tráfico en este proyecto, en el equipo del administrador
Avira Antivir Personal	Antivirus	GmbH	

Tabla 2.13 Aplicaciones instaladas en las estaciones de trabajo

2.4.2 ESTUDIO DE TRÁFICO UTILIZADO EN LA RED

Posteriormente se realiza el estudio del tráfico utilizado por la red en el enlace al ISP, a fin de determinar que tan aprovechada está la capacidad de dicho enlace, en función de las aplicaciones que son requeridas por la empresa para el desarrollo de sus actividades. Para este propósito se utilizó un software conocido como *Paessler Router Traffic Grapher* (*PRTG)*.

En el manual de la herramienta seleccionada para el monitoreo del tráfico de enlaces de Internet se recomienda varias opciones que pueden ser utilizadas para este propósito, entre una de ellas se indica que se puede monitorear el tráfico total de la red usando un *switch* configurando un puerto de monitoreo, conocido como puerto "*mirror* o espejo" al cual se replica toda la información que fluye por el del enlace con el *router* al cual se desea monitorear.

Con la finalidad de determinar el flujo de información que atraviesa el enlace hacia el ISP se incorporó un computador destinado a realizar el monitoreo del tráfico en el cual se instaló la aplicación antes mencionada en la forma especificada, como se muestra en la figura 2.12.

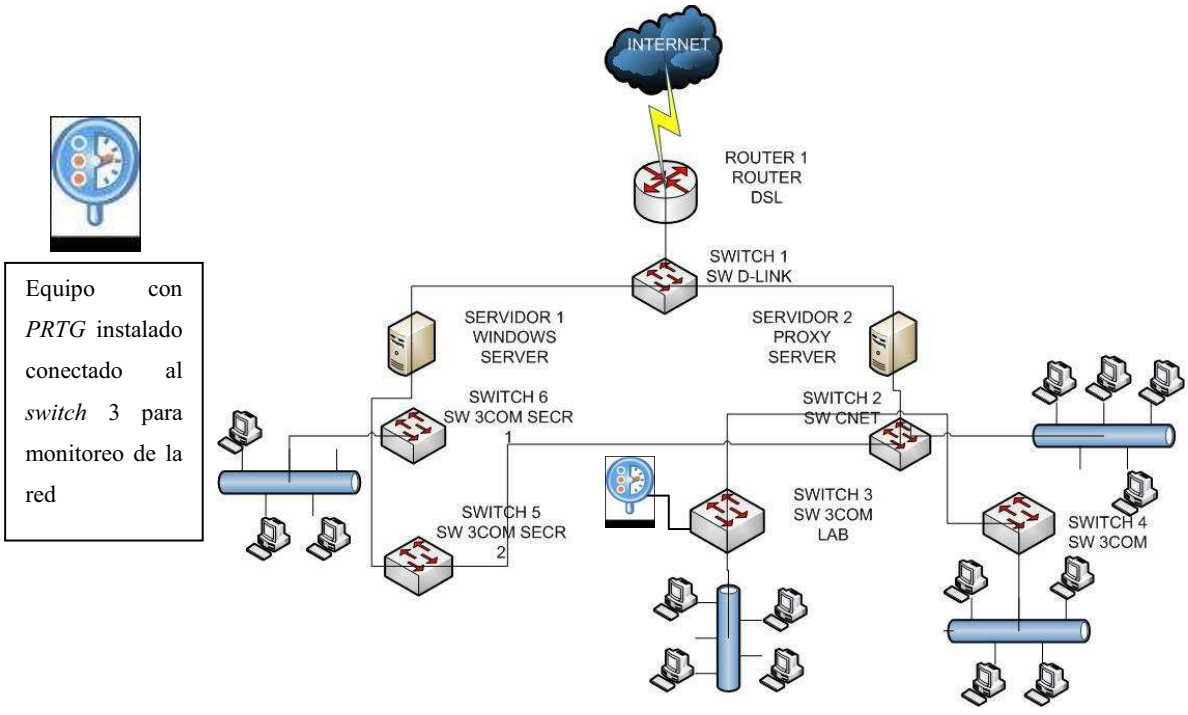


Figura 2.12 Ubicación del equipo para monitoreo de la red.

Debido a que no existe ningún tipo de restricción o segmentación, todos los equipos que tienen acceso a la red pudieron ser monitoreados desde este punto, el cual corresponde a uno de los computadores de administrador puesto que se encuentran conectados al proxy por medio del cual se puede realizar el escaneo completo de los equipos conectados a la red para determinar la cantidad de tráfico que cursa por la red, como se puede observar en la información del anexo A.

Adicionalmente el proveedor de servicios de Internet proporcionó información acerca del tráfico que cursa a través del enlace correspondiente a la Institución en un determinado intervalo de tiempo. En la figura 2.13 se muestra el resultado obtenido, el cual es analizado en el punto 2.4.3.

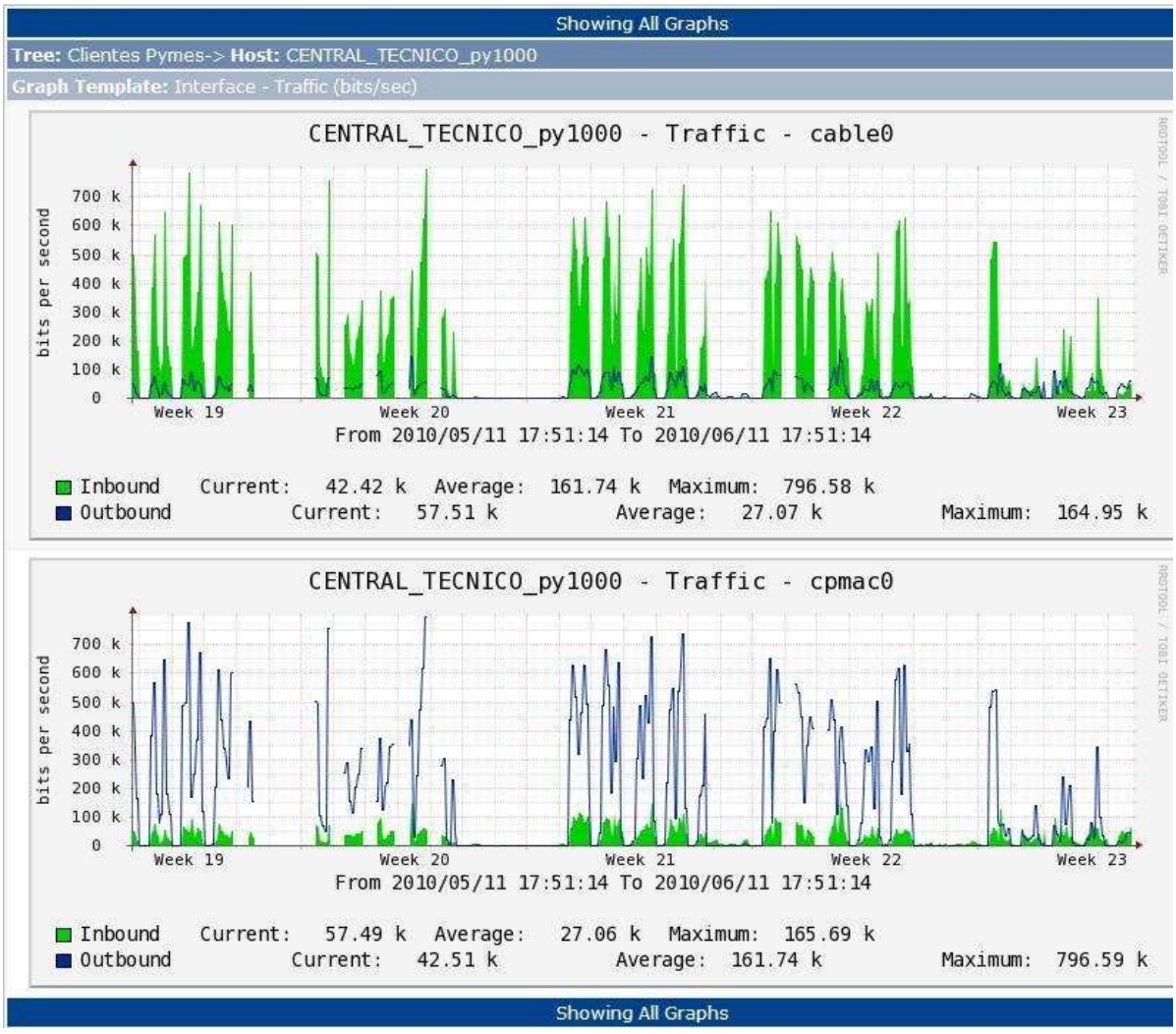


Figura 2.13 Monitoreo del enlace "Central Técnico" a través del proveedor de servicios de Internet.[Telmex]

2.4.3 ANÁLISIS DE RESULTADOS DEL ESTUDIO DE TRÁFICO

Para la salida a Internet la Institución cuenta con un plan Professional Pack *PYMES*[23] compartido 4:1, tipo *ADSL* (*Línea de Suscriptor Digital Asimétrica*) de 3072 Kbps (3Mbps) asimétrico provisto por Telmex.

El hecho que el enlace sea asimétrico, significa que se tiene diferente ancho de banda en el canal hacia el Internet como en el canal desde el Internet, la velocidad de *upstream* (subida) es diferente a la *downstream* (bajada), siendo esta última la mayor.

Para el análisis de este enlace, se utiliza el servicio *CACTI* para la medición de tráfico, en el cual se facilita información de tráfico entrante, saliente, entrante pico y saliente pico en períodos diarios, semanales, mensuales y anuales así como el grado de utilización del enlace.

Este servicio permite monitorizar en tiempo real las redes, dispositivos de red, servidores y servicios implementados en los servidores de las mismas. *CACTI* está escrito en *PHP* y genera gráficas utilizando herramientas propias del sistema.

El tráfico máximo hace referencia al valor más significativo del tráfico medido durante un día, una semana, un mes o un año dependiendo del período, en este caso se realizó el monitoreo por un mes entre el 11 de mayo y el 11 de Junio, un mes de gran cantidad de tráfico debido a la culminación del año lectivo, donde los valores máximos en el equipo instalado en la Institución son de 796,58 Kbps de entrada y 164,95 Kbps de salida.

El tráfico promedio como su palabra lo indica, es el promedio del tráfico durante el período de tiempo, se puede tomar este tráfico como referencia para conocer el grado de utilización del enlace, en este caso el valor es fue de 161,74 Kbps de entrada y de 27,07 Kbps de salida.

El tráfico actual es el tráfico que circula por la red en el momento mismo en que se solicita los datos, los valores medidos fueron 42,42 Kbps de entrada y 57,87 Kbps de salida.

[23] PYMES: Pequeña y mediana empresa

Para el monitoreo del tráfico de la intranet se utilizó el protocolo *SNMP,* habilitando el servicio en cada uno de los equipos monitoreados, mediante el software PRTG se empezó a analizar desde el 15 de Noviembre hasta el 30 del mismo mes, para obtener los valores de ancho de y los volúmenes de datos tanto de entrada como de salida.

Como se muestra en el anexo A, se puede observar que el tipo de tráfico generado en la intranet es del tipo ráfaga teniendo en cuenta que el único servicio que presta la Institución es el Internet y su uso no es permanente. Los valores de volumen de tráfico oscilan entre 12.624 y 1.276.023 Kbytes, todos los dispositivos en total generaron 412 Kbps con lo que se concluye que la infraestructura actual no soportará aplicaciones IP que requieran mayor ancho de banda. .

Lo que se puede concluir es que el enlace de Internet contratado actualmente se encuentra subutilizado es decir no es aprovechado en su máxima capacidad. Sin embargo por parte de los usuarios se percibe cierta sensación de lentitud del servicio debido a que los equipos utilizados para el acceso al servicio son poseen las características necesarias para procesar de una manera adecuada las aplicaciones.

Esta subutilización se debe además al número reducido de usuarios que tienen acceso, razón por la cual se pretende incrementar el acceso a este servicio para evitar este problema a través de una nueva red de datos, que además permita incluir una mayor cantidad de servicios.

2.5 ANÁLISIS DE SERVICIOS.

El Instituto Tecnológico Superior “Central Técnico” posee dos servidores, uno utilizado para filtrar el tráfico que se genera tanto internamente como hacia Internet y otro que es un servidor de notas en línea. En este caso se hace el análisis del servidor *proxy* debido a que el servidor de notas es manejado por una empresa privada con la cual la Institución presenta un convenio de prestación de servicios.

2.5.1 SERVIDOR *PROXY*

En el servidor que es utilizado como *Proxy* se encuentra funcionando con *DansGuardian* que es una aplicación de filtrado de contenido *WEB* que funciona sobre la plataforma Linux, es de distribución libre y actualmente opera sobre el sistema operativo *CentOS*. Como se mencionó anteriormente *DansGuardian* es de código abierto y desarrollada en el leguaje de programación C++. Este servicio es muy flexible pues permite o niega el acceso a ciertas aplicaciones de acuerdo a las necesidades del administrador. En la figura 2.14 se muestra la pantalla de ingreso al sistema que como se puede observar en la barra de direcciones se encuentra en la dirección 192.68.100.1 la cual como se explicó en el apartado 2.1.6 se encuentra configurada como *default Gateway* en la configuración del protocolo TCP-IPv4 de los equipos de la Institución.

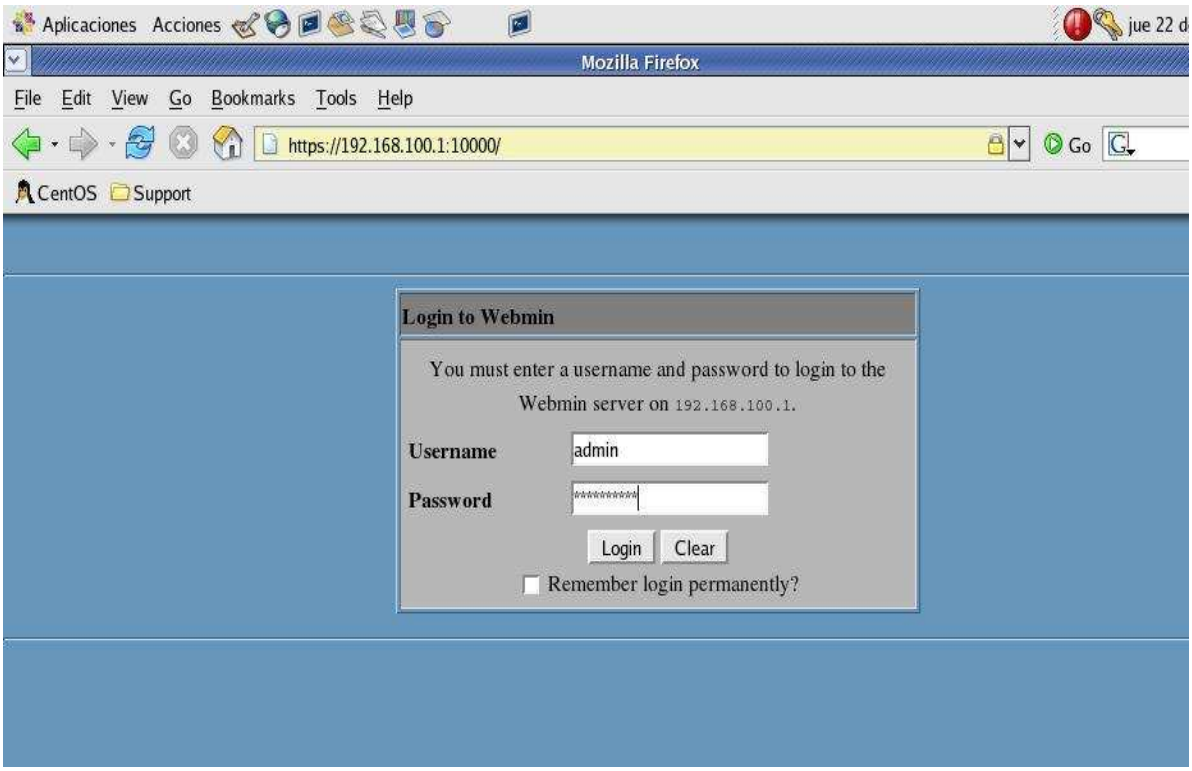


Figura 2.14 Pantalla de login para el administrador de *DansGuardian*

Todas las peticiones que los usuarios realicen *DansGuardian* las recibe y solamente redirecciona aquellas que superan la fase de filtrado. *DansGuardian*

recibe la información en el puerto 8080 y redirecciona al *SQUID,* que es el que actúa como *proxy* propiamente dicho, que escucha en otro puerto diferente, por lo tanto la función de *DansGuardian* es filtrar y pasar al *proxy SQUID*. Este servidor permite el acceso a Internet a los usuarios en la intranet.

La ventaja de este servidor es que permite bloquear el contenido por URL, dirección IP, por frase etc. En la figura 2.15 se presenta la configuración de la dirección IP del servidor.

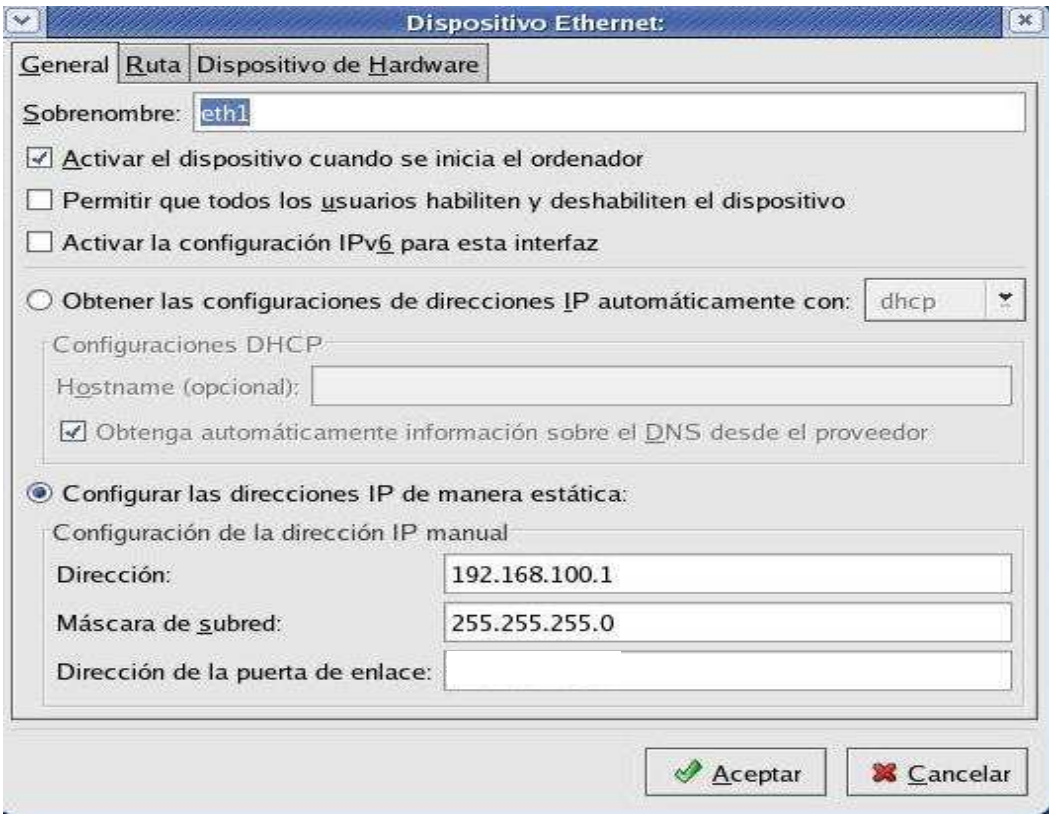


Figura 2.15 Configuración IP del servidor *proxy*

En la figura 2.16 se muestra un esquema del funcionamiento de este servidor dentro de la red, el mismo que se encuentra como intermediario entre los usuarios finales de la red y el Internet, este servidor cumple la función de redireccionar el tráfico que llega a él, hacia la tarjeta que se encuentra conectada a la red *WAN*, luego del filtrado.

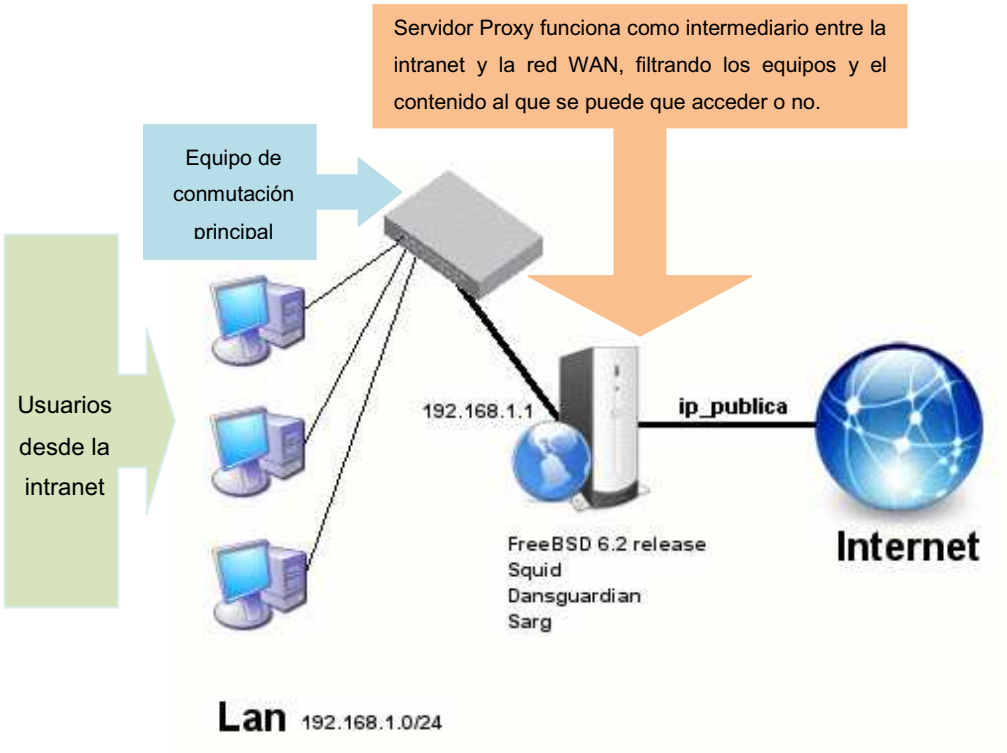


Figura 2.16 Esquema de funcionamiento del proxy

Además de lo ya mencionado en dicho equipo se tienen levantados servicios para instalar base de datos, servicios FTP, servicios Web y muchos más propios del paquete de instalación.

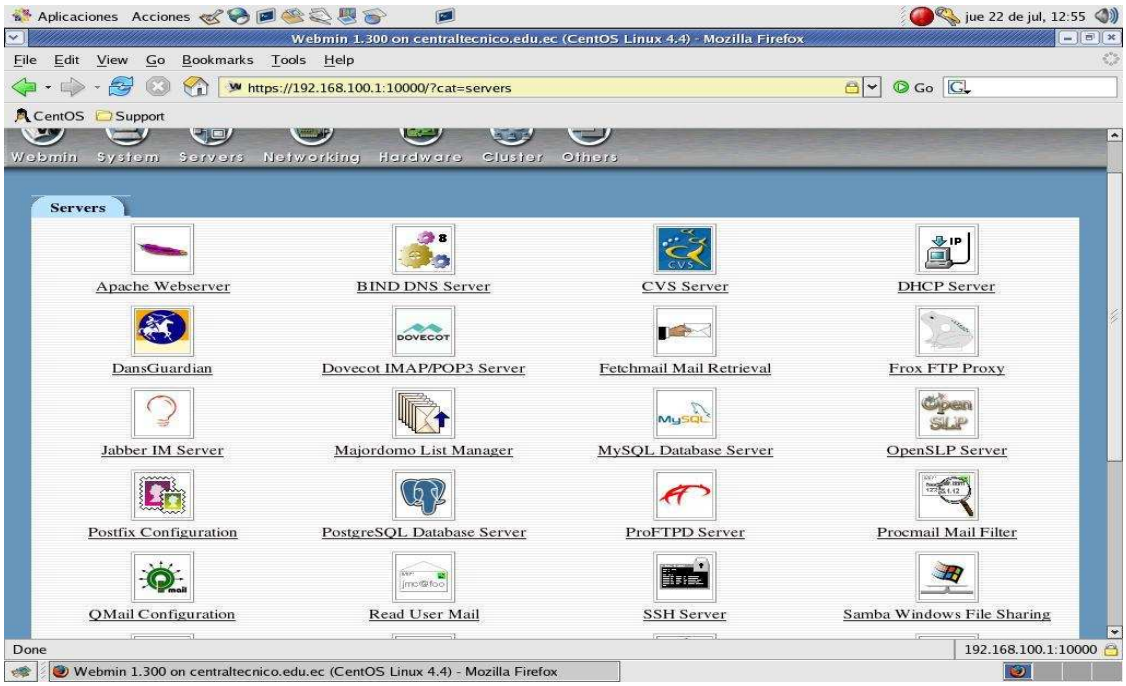


Figura 2.17 Servicios en funcionamiento

En la figura 2.17 se muestra un ejemplo de los diferentes servicios, sin embargo es importante que debido al desconocimiento de sus uso estos no se encuentran funcionando lo que puede resultar beneficioso debido a que las características del equipo no permitirían un adecuado funcionamiento de ellos.El filtrado *Web* que realiza se basa en editar uno de los archivos de configuración del servidor *proxy* en la tabla *exception list,* el administrador ha detallado todas las direcciones que tienen acceso total a cualquier contenido como se puede ver en la figura 2.18.

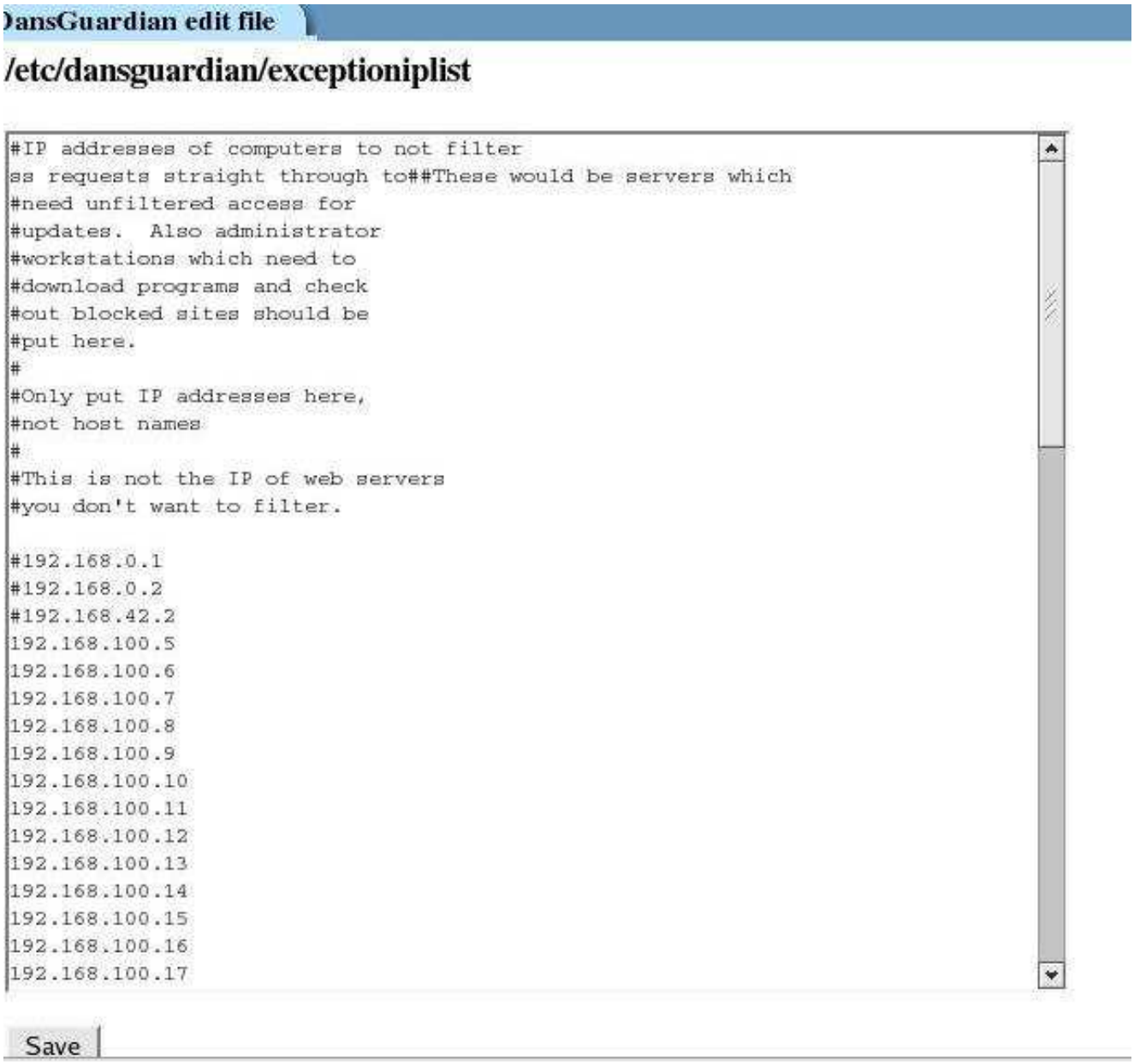


Figura 2.18 Exception List : Usuarios autorizados

En la lista *exception site list* se escriben las direcciones *web* que los usuarios pueden visitar de esta forma se niega el acceso a los usuarios a paginas prohibidas, como se muestra en la figura 2.19.

Figura 2.19 Exception Site List: Sitios *web* no autorizados

2.5.2 SERVICIOS DE RED REQUERIDOS.

En una infraestructura de comunicaciones es imprescindible contar con servicios de intranet para los usuarios de las diferentes Áreas. El Instituto Tecnológico Superior Central Técnico requiere de servicios de intranet e Internet para satisfacer las necesidades de los usuarios. A continuación se hace referencia a los servicios requeridos por los usuarios obtenidos tanto de las encuestas realizadas al personal administrativo, profesores y alumnos de la Institución así como de las necesidades propias de una entidad educativa.

2.5.2.1 Servicios *WEB*

Conforme lo investigado de los recursos de la Institución se detalla que tiene un Servidor *Web* que se utiliza para el ingreso y consulta de notas por parte de los profesores y estudiantes respectivamente. Es por esto que El Instituto Central Técnico tiene la disposición de tener su propio sitio *WEB* para publicar la información relevante como congresos, autoridades, cronograma de actividades para inscripciones y matriculas, etc. Además el sitio *Web* servirá para educación virtual, *e-learning*, para que estudiantes profesores o las diferentes áreas de la Institución diseñen su propio blog para informar a sus alumnos del horarios de prácticas en talleres, pruebas teóricas y prácticas, y enlaces educativos a diversos dependencias.

2.5.2.2 Servicios de Nombre de Dominio (DNS)

Actualmente en la red del Colegio Central Técnico no existe una gran cantidad de computadores, servidores y periféricos por lo que un servidor de *DNS (Domain Name System) local* no fue estimado. Pero para facilitar referirse a los dispositivos y otros periféricos se considera el dimensionamiento de un servidor *DNS* local para resolver los nombres de servicios internos así como para la administración de las computadoras. Se toma en cuenta este servicio ya que el direccionamiento es estático y que para los usuarios es más sencillo aprender un nombre que una dirección IP. El servidor local ayudará a resolver inconvenientes con las aplicaciones que se manejen en la intranet. El dominio de la Institución será @centraltecnico.edu.ec

2.5.2.3 Servicio de Correo Electrónico

El correo electrónico es una herramienta imprescindible tanto para el trabajo como para la comunicación más aún en una Institución educativa como esta que trabaja con una gran número de estudiantes profesores y personal administrativo. Por lo cual se requiere disponer de una herramienta flexible, y accesible desde cualquier lugar que se encuentre. Este servicio proporcionará la creación de cuentas para los profesores y personal administrativo así como su adecuado seguimiento. Al referirse a seguimiento se toma en cuenta que es responsabilidad del administrador que no exista encolamiento, aumentar la capacidad de la cuenta de usuario si lo necesitan entre otras acciones.

2.5.2.4 Servicio de Archivos Compartidos.

Es necesario un servidor donde pueda compartir información entre los diferentes miembros de la Institución (profesores, alumnos y empleados) y asegurar que la información esté disponible. El servicio mantendrá los archivos en un lugar específico todos los documentos como formularios, normativas, notificaciones, formato de prácticas, de solicitudes de reinscripciones etc., para que los usuarios los descarguen o realicen una copia de seguridad.

2.5.2.5 Servicio de Impresión.

Existe una gran cantidad de impresoras conectadas a cada una de las máquinas en los diferentes áreas ya sean estas administrativas como laboratorios de informática lo cual genera un gasto innecesario. Se dispondrá de un servidor de impresión con capacidad de almacenamiento que gestionará los archivos en colas para ser impresos. Así se logrará asignar una impresora a un grupo de usuarios que la podrán utilizar optimizando el uso de recursos.

2.5.2.6 Servicio de Antivirus.

Las aplicaciones que los usuarios manejarán para acceder a recursos hacia el Internet o a la intranet deberán ser escaneados por un servidor de antivirus. Así toda la información sea texto o multimedia no se verá afectada a posibles ataques maliciosos que perjudiquen las comunicaciones y los demás servicios a ser implementados.

2.6 ANÁLISIS DE LA RED DE VOZ

En el análisis de la topología de la red de voz se identificó que el sistema telefónico se encuentra conformado por la central telefónica y un sistema de procesamiento de voz, a continuación se presenta un análisis detallado de esta red.

2.6.1 DESCRIPCIÓN DE LOS EQUIPOS[P6]

A continuación se presenta una descripción de las funcionalidades de los equipos que se encuentran actualmente formando parte de la red de voz de la Institución. Esta descripción brindará una visión general acerca de los equipos, como funcionan en el sistema actual y aquellos que pueden ser reutilizados en la futura implementación de una red multiservicios que soporte Telefonía IP.

2.6.1.1 Panasonic KX-TDA200

Este equipo es una central telefónica IP híbrida, es decir maneja funciones de telefonía tanto analógica como IP, si con anterioridad son instaladas tarjetas de servicios específicos mediante las cuales podemos agregar funciones a la central. Actualmente estas tarjetas no se encuentran instaladas en la central lo que limita su capacidad de reuso en la nueva red.

En las tablas 2.14, 2.15 y la figura 2.20 se encuentran detalladas las características de las capacidades que puede alcanzar esta central como se había explicado anteriormente instalando los módulos adecuados.

TARJETAS DE LÍNEAS Y DE ENLACE	
TIPO DE TARJETA	KX-TDA200
TARJETAS DE ENLACE*	8
TARJETAS DE EXTENSIÓN	
TOTAL	10
***Una tarjeta E1, PRI, IP-GW4 ó IP-GW16 cuenta como 2 tarjetas**	

Tabla 2.14 Capacidad para tarjetas tanto de troncales como extensiones[P6]

CAPACIDAD DEL SISTEMA (EXTERNA)	
TIPO DE TARJETA	KX-TDA200
PUERTOS DE LÍNEA EXTERNA	128
LÍNEA EXTERNA ANALÓGICA	128
ENLACE E&M	64
ENLACE E1	4
ENLACE BÁSICO RDSI (BRI)	64(128 can.)
ENLACE PRIMARIO RDSI (PRI)	4(120 can.)
IP-GATEWAY	4(64 can.)

Tabla 2.15 Capacidad para enlaces externos (troncales) [P6]

Si bien la central se encuentra funcionando, la configuración actual no permite obtener toda su funcionalidad y el mantenimiento de la misma no se puede realizar periódicamente debido a la falta de la consola de administración de la misma

La central permite la conexión a otras centrales a través de una red privada IP. En este caso, las señales de voz se convierten en paquetes IP y se envían a través de esta red. Estas operaciones las puede realizar mediante el módulo IP-GW4 o IP-GW16. Estos módulos permiten tener 4 ó 16 llamadas IP respectivamente de manera simultánea y solo puede ser instalada una debido a que solo existe una ranura para tal efecto.

Esta central-IP híbrida es compatible con Sistemas de procesamiento de voz y actualmente se encuentra funcionando con uno de ellos para adicionar funciones sin embargo no se encuentra totalmente operativo tanto por la falta de configuración como por que los teléfonos instalados actualmente no permite estas funciones.

CAPACIDAD DEL SISTEMA (INTERNA)

Tipo de tarjeta	KX-TDA100*2		KX-TDA200*3	
	SIN MEC*4	CON MEC*4	SIN MEC*4	CON MEC*4
Extensiones fijas	64	128	128	256
Teléfonos Regulares (TR)	64		128	
Teléfonos Específicos Digitales (TED)				
Serie T76	64	128	128	256
Series T72, T74, T75	64		128	
Teléfonos Específicos Analógicos (TEA)	32		64	
Sistema DECT				
Antenas (CS)	16		32	
Portátiles (PS)	128			
Sistemas de Proceso Vocal	2			
Porteros automáticos				
Interfonos	8		16	
Abridores de puerta	8		16	
Pulsadores	8		16	
Módulos de 12 teclas adicionales	64	128	128	256
Módulos USB	64		128	
CTI 1ª Parte				
PC Phone	64		128	
PC Console	8			

*2 Para capacidad máxima podría requerir una fuente de alimentación M
*3 Para capacidad máxima podría requerir una fuente de alimentación L
*4 MEC: Tarjeta de ampliación de memoria KX-TDA0105
Nota: Por favor, consulte la configuración deseada a su distribuidor

Figura 2.20 Capacidad para enlaces internos (extensiones) [P6]

Se puede incrementar el número de teléfonos conectados a la central sin tener que añadir tarjetas de extensión adicionales utilizando funciones de modo paralelo.

Modo Paralelo: Un teléfono regular (TR) se puede conectar a un teléfono específico analógico (TEA) o a un teléfono específico digital (TED) que esté conectado al puerto súper híbrido de la central (puerto que soporta TEA como TED). El teléfono regular funcionará compartiendo el mismo número de extensión que el TEA o él TED.

Modo función doblar puerto (XDP): Un teléfono regular (TR) se puede conectar a un TED que esté conectado al puerto súper híbrido de la central. A diferencia del modo paralelo, el modo XDP, cada TED actúa como una extensión independiente con su propio número de extensión.

XDP digital: Un TED se puede conectar a otro TED que esté conectado al puerto TED o al puerto súper híbrido de la central. Similar al modo XDP, cada TED actúa como una extensión independiente con su propio número de extensión.

Cabe anotar que además puede soportar teléfonos inalámbricos mediante sistema *DECT*[24] de la misma manera que para utilizar las funciones de central IP se necesita el módulo específico de esta funcionalidad

2.6.1.2 Panasonic KX - TVM50

Adicionalmente a la central telefónica se encuentra funcionando un sistema de procesamiento de voz que ofrece enrutamiento automático de llamadas con operadora automática y notificación de mensajes que pueden ser configurados de acuerdo a la necesidad pertinente.

El sistema puede ser configurado para recibir notificaciones por correo electrónico de que se ha recibido nuevos mensajes; se puede conectar a distancia con el buzón y escucharlos. Además de la posibilidad de convertir los mensajes en archivos WAV para ser recibidos como archivos adjuntos de correo electrónico, lo que permite el almacenamiento de respaldos de los mismos.

Puede ampliarse de acuerdo con el mayor tráfico de llamadas. El KX-TVM50 tiene 2 puertos, capaces de recibir 2 llamadas a la vez, según el sistema PBX en uso. Este sistema básico está listo para satisfacer las necesidades de correo de voz de pequeña escala con sólo abrir el paquete y puede ser ampliado a 6 puertos para recibir 6 llamadas a la vez. El tiempo de grabación también puede duplicarse añadiendo una Tarjeta de Expansión de Tiempo de Grabación de 4 Horas KX-TVM524. Posee una capacidad de 64 buzones es decir 64 usuarios pueden tener correo de voz con este sistema.

Es posible colocar un solo equipo KX-TVM en redes de equipos conmutadores de hasta un máximo de 8 enlazados por VoIP para integrarse a una red LAN se debe instalar la tarjeta adicional KX-TVM594.

De lo anotado este sistema resulta inútil en un sistema de VoIP debido a que estas funcionalidades y muchas más se pueden integrar mediante un servido de

[24] ***D**igital **E**nhanced **C**ordless **T**elecommunications*, es un estándar europeo para teléfonos inalámbricos digitales, comúnmente utilizado para propósitos domésticos o corporativos.

telefonía IP lo que reduciría tanto los costos como facilitaría la administración e incluso la capacidad del sistema.

2.6.1.3 Teléfonos

El sistema telefónico puede ser configurado para obtener varias funciones adicionales sin embargo, el sistema actual del Instituto se ve condicionado por los teléfonos utilizados debido a que son teléfonos analógicos en su gran mayoría que al momento no prestan las características necesarias para aprovecharlas, y los teléfonos que tiene las poseen no han sido configurados para el efecto.

2.6.2 DETALLE DE LA ESTRUCTURA DEL SISTEMA [T1]

El armario básico contiene una tarjeta principal, llamada MPR, la cual controla la central-IP híbrida. Para utilizar el sistema, debe estar el armario básico más la tarjeta principal MPR conectada a una unidad de alimentación (PSU) y con las tarjetas de servicio opcional necesarias. En la figura 2.21 se muestra la distribución física de estos componentes.

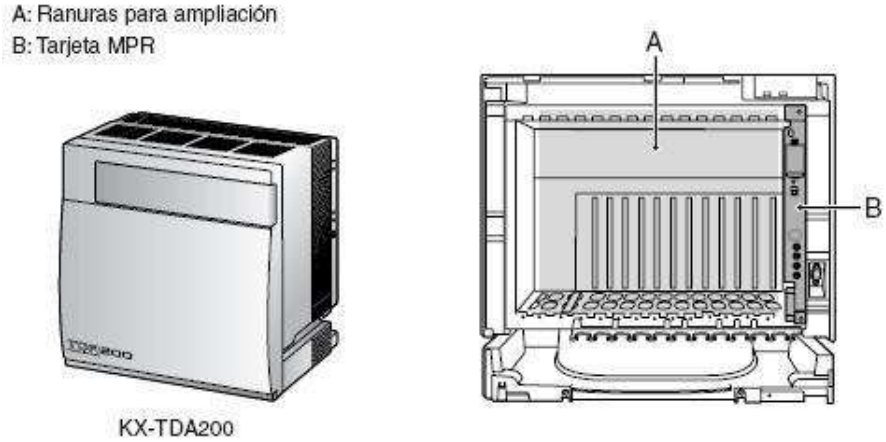


Figura 2.21 Estructura del armario básico

En la figura 2.22 se muestra el diagrama de conexiones generales de los dispositivos que se pueden conectar a la central-IP híbrida y la estructura general de un sistema implementado mediante esta central telefónica, donde se encuentra también ubicado el sistema de procesamiento de voz que actualmente sirve en la Institución.

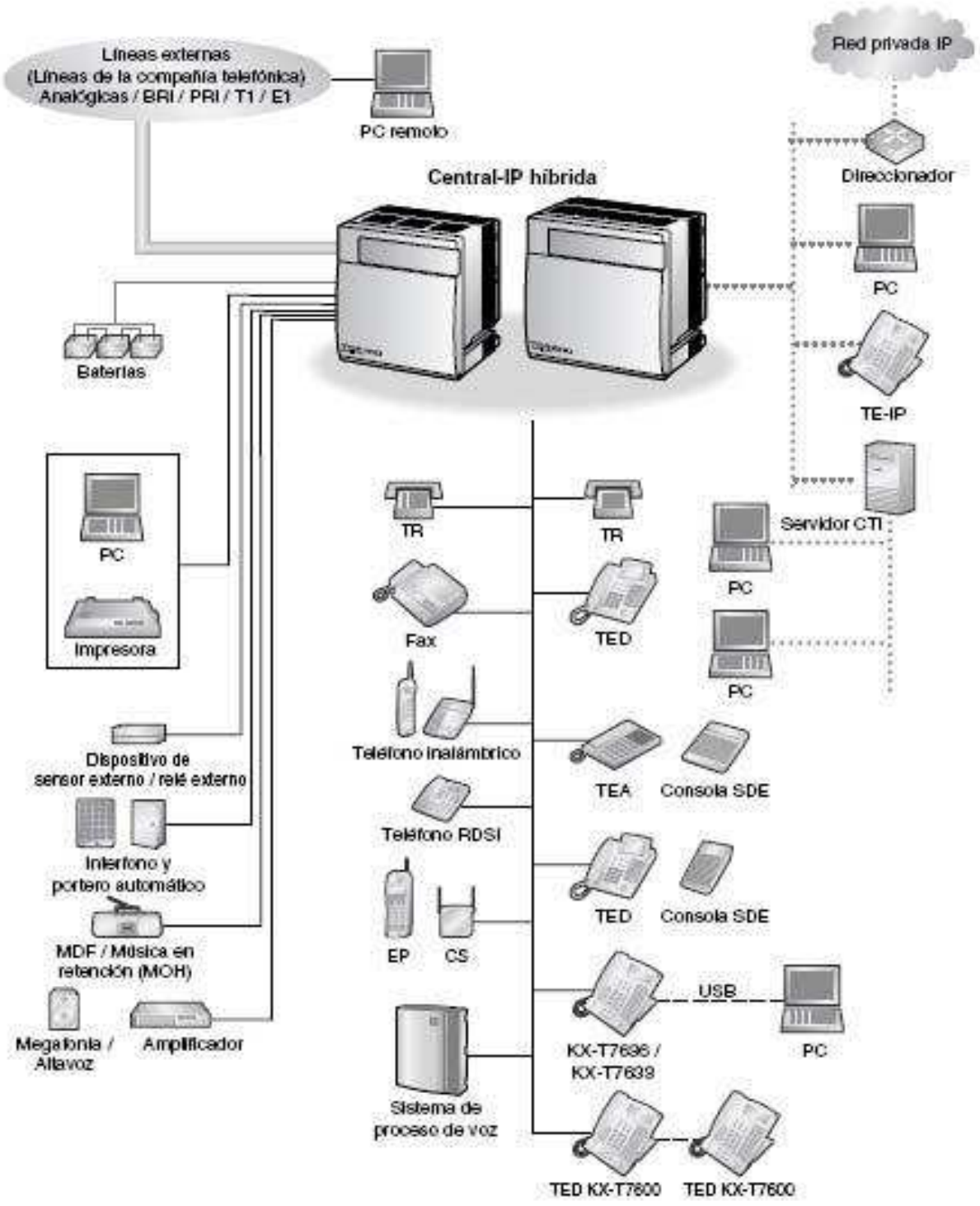


Figura 2.22 Sistema integrado mediante KX-TDA200

Como se puede observar en la figura este sistema bien podría utilizarse para la integración de varios servicios sin embargo presenta capacidades muy reducidas lo que es una limitante, además la integración con la red IP resultaría bastante costosa y compleja.

2.6.3 DETALLE DE USUARIOS ACTUALES

Actualmente en el sistema se encuentran conectadas un total de 35 extensiones telefónicas para servicios internos de la Institución, las cuales se encuentran distribuidas a través del campus de forma dispersa.

Existe una alta demanda de extensiones telefónicas debido a que estas no son suficientes. El sistema de numeración es desordenado y existen puntos de voz que no están actualmente en funcionamiento, debido a fallas de los cables que los conectan con el sistema.

La central telefónica maneja 5 troncales telefónicas conectadas hacia la red telefónica pública por medio de la Corporación Nacional de Telecomunicaciones además de 3 líneas directas contratadas con la misma empresa que son usadas para servicios como envío y recepción de faxes.

Los usuarios que se encuentran conectados a esta central poseen extensiones de 3 dígitos. Para llamar a extensiones de esta central se lo hace de forma directa de igual manera para llamar de extensiones a números convencionales y celulares se requiere de un código de salida.

La distribución del número de extensiones por grupos de usuarios en el campus de detalla en la Tabla 2.16. En resumen, actualmente en la Institución existen 22 personas en el grupo de personal administrativo y 13 docentes que tiene acceso a una extensión telefónica de la red de voz. Todos los teléfonos a excepción de los ubicados en Secretaría y en Rectorado son analógicos.

Número	Oficina	Ext.	Tfno. Directo	Grupo
1	ASOCETEC	128		ADMINISTRATIVO
2	AUDIOVISUALES	138		ADMINISTRATIVO
3	AUXILIAR RECEPCION	109		ADMINISTRATIVO
4	BAR PROFESORES	127		ADMINISTRATIVO
5	BIBLIOTECA	117		ADMINISTRATIVO
6	BODEGA GENERAL	121		ADMINISTRATIVO
7	C.C. PADRES FAMILIA	120		ADMINISTRATIVO

Número	Oficina	Ext.	Tfno. Directo	Grupo
8	CENTRO MÉDICO	123		ADMINISTRATIVO
9	COLECTURÍA	132	2435038	ADMINISTRATIVO
10	D.O.B.E	139		ADMINISTRATIVO
11	D.T.P	137		ADMINISTRATIVO
12	DPTO. SECRETARÍA	141		ADMINISTRATIVO
13	ELECTRICIDAD	136		ADMINISTRATIVO
14	ELECTRÓNICA	122		ADMINISTRATIVO
15	MANTENIMIENTO	129		ADMINISTRATIVO
16	NIVEL TECNOLÓGICO	118	2446540	ADMINISTRATIVO
17	PUERTA OCCIDENTAL	126		ADMINISTRATIVO
18	PUERTA PRINCIPAL	131		ADMINISTRATIVO
19	RECEPCIÓN	101		ADMINISTRATIVO
20	SECRETARÍA GENERAL	105		ADMINISTRATIVO
21	SECRETARIA INSP.GENERAL	107		ADMINISTRATIVO
22	SECRETARÍA VICERRECTORADO	103		ADMINISTRATIVO
23	CULTURA FÍSICA	135		DOCENTE
24	INSPECCIÓN BÁSICO/DIVERSIFICADO	130	2448155	DOCENTE
25	INSPECCIÓN GENERAL	106		DOCENTE
26	JEFATURA TÉCNICA	119		DOCENTE
27	LAB. DIBUJO	143		DOCENTE
28	LAB. FÍSICA	125		DOCENTE
29	LAB. INTERNET	142		DOCENTE
30	LAB. QUÍMICA	124		DOCENTE
31	MEC. AUTOMOTRIZ	134		DOCENTE
32	MEC. INDUSTRIAL	133		DOCENTE
33	RECTORADO	102		DOCENTE
34	SISTEMAS	140		DOCENTE
35	VICERRECTORADO	144		DOCENTE

Tabla 2.16 Extensiones del Instituto Tecnológico Superior “Central Técnico”

2.7 RESUMEN DEL DIAGNÓSTICO DE LA RED

A lo largo de este capítulo se ha analizado el estado actual de la red de datos del Instituto Central Técnico, finalmente se presenta a manera de resumen los puntos principales analizados en este capítulo.

Con respecto a la topología y funcionamiento lógico de la red, ésta se encuentra actualmente desorganizada, no existe una jerarquía para la interconexión de los equipos, no existe ningún tipo de restricción para la comunicación de los diferentes integrantes de la red. El equipamiento de la Institución no es el adecuado, ninguno de los equipos es administrable y no se han tomado en cuenta las características mínimas para su adecuado funcionamiento.

Los servicios que se encuentran el funcionamiento son: el servidor de notas, que es brindado por una empresa externa a la Institución y un servidor proxy que sirve para controlar el acceso a Internet. Los servidores actuales son computadores personales adaptados para su funcionamiento, no están dimensionados en función de la carga que van a soportar, razón por la cual en cualquier momento podría existir una falla del sistema que podría terminar en pérdida de información.

Los equipos finales de usuario encontrados en la Institución son las estaciones de trabajo y las impresoras. Las estaciones de trabajo en su mayoría son demasiado antiguas, lo que hace que su trabajo sea ineficiente y no tienen acceso a la red. Las impresoras son para el uso local lo que representa un desperdicio de recursos al tener que conectar una impresora por cada computador que la necesite.

La red de voz actual está separada de la de datos y se encuentra provista por una central Panasonic híbrida, es analógica en gran parte, sin embargo por sus características podría ser utilizada como digital o incluso IP. A excepción de secretaría y rectorado, todos tienen teléfonos analógicos. La Institución cuenta además con un sistema de procesamiento de voz que no está configurado adecuadamente para proveer las capacidades necesarias. El mantenimiento de este sistema está a cargo de una persona que actualmente no se encuentra en la ciudad y que es la única que posee tanto la información como los equipos

necesarios para el mismo, por lo que si existe alguna falla en el sistema, su reparación resultaría sumamente costosa.

El cableado actual no cumple con las normas de los sistemas de Cableado Estructurado, no existe una Sala de Equipos y el enrutamiento es hecho de manera precaria en función de las necesidades inmediatas de los usuarios de la red, este sistema llega a muy pocos usuarios y no es escalable o flexible. El cableado vertical es inexistente debido a que las estaciones de trabajo se conectan directamente a los equipos ubicados en la sala de Internet donde se encuentran los equipos de interconectividad. No existe una adecuada conexión a tierra ni protecciones para los equipos por lo que una falla en el sistema eléctrico podría dejar sin funcionamiento a todo el sistema.

El número de potenciales usuarios de la red es muy grande con respecto a los usuarios actuales de la red porque en general la mayoría de integrantes de la comunidad educativa no tiene acceso a ésta. Los usuarios que tienen acceso a la red, no tienen una adecuada cultura de uso, a más de que no existen las políticas de uso que regulen el acceso a la red. Los usuarios inalámbricos son prácticamente nulos debido a que solo existe esta conexión para dos computadores de los profesores que dictan clases en los laboratorios de informática.

Las aplicaciones usadas en la Institución son de carácter local, no existe ninguna aplicación instalada para su funcionamiento en red, debido a esto el tráfico local no existe, el único tráfico que circula en la red es el que va hacia el Internet, el cual es subutilizado debido a que las características de los equipos no son las más recomendadas, además que en su gran mayoría no es utilizado con labores acorde a la misión de la comunidad educativa.

CAPÍTULO 3.

REDISEÑO DE LA RED MULTISERVICIOS.

3.1 SISTEMA DE CABLEADO ESTRUCTURADO

3.1.1 INTRODUCCIÓN

La infraestructura actual de la red del Instituto Tecnológico Superior "Central Técnico", no registra una adecuada administración de su Sistema de Cableado Estructurado. Por lo cual el presente diseño se enfocará en brindar todos los servicios necesarios que a largo plazo toda la comunidad educativa utilizará con un rendimiento óptimo.

El Instituto Tecnológico Superior "Central Técnico" cuenta con diferentes áreas entre las que se destacan:

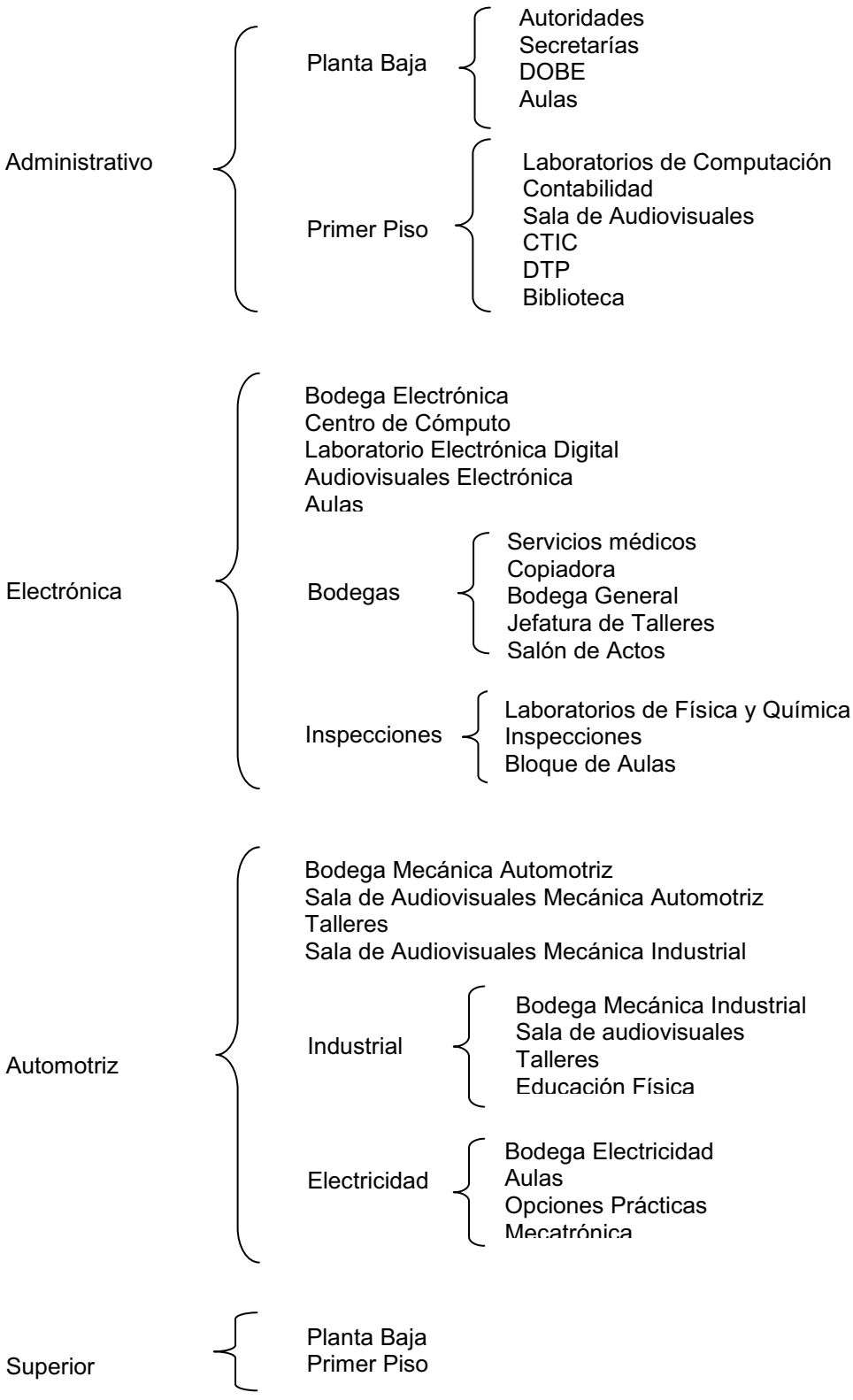
Área Administrativa, Áreas técnicas (Electrónica, Automotriz, Industrial, Electricidad); además de Biblioteca, Bodegas, Inspecciones, Salón de Actos, y bloque de aulas, como se especificó en el capítulo 2.

Todos los edificios en los que funcionan estas dependencias tienen una sola planta, a excepción del área administrativa y del nivel superior, que funcionan en edificios de dos plantas. Cada una de estas áreas y edificios tienen requerimientos para el cableado estructurado, y se describen a continuación para cada uno.

3.1.2 DISTRIBUCIÓN DE LOS PUNTOS DE CABLEADO PARA LAS ÁREAS.

Debido al extenso campus que le corresponde al Instituto, éste ha sido dividido en diferentes áreas para brindar todos los servicios. En cada una de estas áreas se ubicará un cuarto de telecomunicaciones para el acceso a la información.

A continuación, se presenta un resumen de la agrupación de las dependencias, en las diferentes áreas a las que se brindará el servicio.



3.1.2.1 Administrativo.

El edifico Administrativo está conformado por dos plantas, en la planta baja se encuentran las oficinas del Rector, Vicerrector, Secretaria General, Secretarias de Rectorado y Vicerrectorado, Información, Área de matemática, UTE-2, Aulas y

Departamento de Orientación Vocacional. En el primer piso se encuentran cuatro laboratorios de Informática, una sala de Audiovisuales, Departamento de Contabilidad, CTIC y el DTP. Además se incorpora a esta área la biblioteca del Instituto. De lo expuesto anteriormente se resume en la tabla 3.1 los puntos de voz y datos a instalar así como el porcentaje de crecimiento.

Planta	Área Trabajo	Puntos Red	Puntos Voz	Total
Baja	Rectorado	1	2	3
	Vicerrectorado	2	2	4
	Secretaria Rectorado	1	1	2
	Secretaria Vicerrectorado	1	1	2
	Información	1	1	2
	Secretaría General	7	4	11
	DOBE	4	4	8
	Sala Dibujo	1	-	1
	Área Matemática	1	1	2
	UTE-2	1	1	2
	Impresora Secretaría	1	-	1
	Aulas	3	-	3
Primer Piso	Laboratorio de computación 1	1	1	2
	Laboratorio de computación 2	1	1	2
	Laboratorio de computación 3	1	1	2
	Laboratorio de computación 4	1	1	2
	Departamento de Contabilidad	3	3	6
	Sala de Audiovisuales	2	1	3
	CTIC	3	1	4
	DTP	1	1	2
	Biblioteca	2	1	3
	Cámaras	4	-	4
TOTAL		**43**	**28**	**71**
			30% crecimiento	21

Tabla 3.1 Distribución de puntos de red: Edificio Administrativo

Para cada una de las Áreas se proyecta un crecimiento de un 30% en el Sistema de Cableado Estructurado de esta forma se prevee que existan los suficientes

puertos en los equipos y además el suficiente espacio en la ductería, ya que cuando entre en funcionamiento la red tendrá mayor demanda para los usuarios de toda la Institución Educativa. Este valor ha sido determinado a partir de reuniones con las autoridades y profesores sobre las proyecciones de crecimiento esperadas en el Instituto.

En este edificio se tiene en total 71 puntos de red, debido a la proyección se estima que se debe considerar 21 puntos adicionales para esta Área.

3.1.2.2 Electrónica.

Al área de Electrónica, se anexan dos zonas diferentes que son independientes. Estas zonas son el área de bodegas y el de Inspección, esto con el objetivo de distribuir de una manera eficiente los puntos de red. A continuación se detallan cada una de las áreas mencionadas.

El área de Electrónica presenta una bodega, dos laboratorios de informática el primero es un centro de cómputo, y el segundo es un laboratorio de electrónica digital, una sala de audiovisuales y diecinueve aulas. En la tabla 3.2 se observa el total de los puntos para esta área.

Área	Área Trabajo	Puntos Red	Puntos Voz	Total
Electrónica	Bodega	1	1	2
	Centro Cómputo	1	1	2
	Lab. Electrónica Digital	1	1	2
	Sala de Audiovisuales	2	-	2
	Aulas	19	-	19
	Cámaras	1	-	1
TOTAL		**25**	**3**	**28**
			30% crecimiento	8

Tabla 3.2 Distribución de puntos de red: Electrónica

En el área de bodegas, se considera que los departamentos de Bodega General, Jefatura de talleres, Centro Médico, Odontología, Copiadora, aula y Salón de Actos, formen parte de una zona diferente. De esta manera se pretende agrupar

de una manera más eficiente a los usuarios en la red. En la tabla 3.3, se detallan los puntos asociados para el segmento de red correspondiente a Bodegas.

Área	Área Trabajo	Puntos Red	Puntos Voz	Total
Bodegas	Odontología	2	2	4
	Centro Médico	1	1	2
	Copiadora	1	1	2
	Aula	1	-	1
	Jefatura de Talleres	1	1	2
	Bodega General	3	1	4
	Salón de Actos	2	1	3
	Cámara	1	-	1
TOTAL		**12**	**7**	**19**
			30% crecimiento	5

Tabla 3.3 Distribución de puntos de red: Bodegas

Los laboratorios de Física, Química, Inspección, y dos aulas, pertenecerán a una nueva zona para brindar cobertura a los usuarios, al igual que el segmento de bodegas, esta área se conectará a la de electrónica. La tabla 3.4 indica los puntos de voz y datos de esta zona denominada de inspecciones.

Área	Área Trabajo	Puntos Red	Puntos Voz	Total
Inspecciones	Laboratorio de Física	3	1	4
	Laboratorio de Química	3	1	4
	Aulas	2	-	2
	Inspección	4	2	6
	Cámaras	1	-	1
TOTAL		**13**	**4**	**17**
			30% crecimiento	5

Tabla 3.4 Distribución de puntos de red: Inspecciones

Además se considera un bloque aulas, que se encuentra ubicado en la parte posterior de la Institución, al cual también se debe dar acceso. Esta área tendrá

conexión a través del área de Inspecciones, en la tabla 3.5, se detalla el número de punto de voz y datos para este bloque.

	Área de trabajo	Puntos de Red	Puntos de Voz	Total
Aulas	Aulas	27	1	28
	Cámara	1	-	1
TOTAL		**28**	**1**	**29**
			30% Crecimiento	9

Tabla 3.5 Distribución de puntos de red: Bloque de aulas

3.1.2.3 Automotriz.

El área de Mecánica Automotriz comprende un espacio físico amplio con respecto a las demás Áreas. Está formado por una bodega, una Sala de Audiovisuales, y quince talleres dedicados para las prácticas de los estudiantes de esta especialidad, en la tabla 3.6 se resume lo siguiente:

Área	Área Trabajo	Puntos Red	Puntos Voz	Total
Mecánica Automotriz	Bodega	1	1	2
	Sala de Audiovisuales	1	-	1
	Talleres	15	-	15
	Cámaras	2		2
	Audiovisuales industrial	1		1
TOTAL		**20**	**1**	**21**
			30 % Crecimiento	6

Tabla 3.6 Distribución de puntos de red: Mecánica Automotriz

3.1.2.4 Industrial.

La especialidad de Mecánica Industrial consiste de un laboratorio de Mecatrónica, una bodega, talleres, audiovisuales, y el departamento de educación Física. La distribución de los puntos para esta área se encuentra detallada en la tabla 3.7.

Área	Área Trabajo	Puntos Red	Puntos Voz	Total
Mecánica Industrial	Bodega	2	2	4
	Audiovisuales	1	-	1
	Talleres	6	-	6
	Educación Física	1	1	2
	Cámaras	1	-	1
TOTAL		**11**	**3**	**14**
			30 % Crecimiento	4

Tabla 3.7 Distribución de puntos de red: Mecánica Industrial

3.1.2.5 Electricidad.

Esta especialidad es la más alejada del Instituto, cuenta con dos plantas, en la cuales se encuentran ubicadas una Bodega, aulas, y los talleres de opciones prácticas; además que se conecta Mecatrónica que pertenece a Mecánica Industrial por cercanía de ésta. Toda la información se la puede observar en la tabla 3.8.

Área	Área Trabajo	Puntos Red	Puntos Voz	Total
Electricidad	Bodega	1	1	2
	Aulas	16	-	16
	Opciones prácticas	3	-	3
	Mecatrónica	2	-	2
	Cámara	1	-	1
TOTAL		**23**	**1**	**24**
			30 % Crecimiento	7

Tabla 3.8 Distribución de puntos de red: Edificio Electricidad

3.1.2.6 Superior.

El área del Nivel Superior actualmente se encuentra ubicada en un edificio de dos niveles, esta área se encuentra en un estado de transición debido a que se

prevee su reubicación, razón por la cual en base a los requerimientos de la Institución se han considerado los puntos especificados en la tabla 3.9.

Área	Área Trabajo	Puntos Red	Puntos Voz	Total
Tecnológico Superior	Planta Baja	6	3	5
	Primer Piso	5	1	5
	Cámaras	1	-	1
TOTAL		**12**	**4**	**16**
			30 % Crecimiento	7

Tabla 3.9 Distribución de puntos de red: Edificio Superior

La ubicación de los puntos de red con su respectiva etiquetación se los presenta en el ANEXO B.

3.1.3 ASIGNACIÓN DE GRUPOS DE USUARIOS PARA LA RED MULTISERVICIOS.

Para proporcionar todos los servicios a la red del Instituto es necesario y urgente segmentar la red y dividir en grupos de usuarios, con la finalidad de mantener una administración centralizada y brindar prioridades, manteniendo así la independencia y seguridad.

Tomando en consideración los requerimientos de la comunidad educativa se establece los siguientes grupos:

Administrativa.

- Rectorado.
- Vicerrectorado.
- Secretarias.
- Inspección.
- Departamento de Contabilidad.
- DOBE.

Bodegas.

- Jefatura de Talleres.
- Bodega Electrónica.

- Bodega Mecánica Industrial.
- Bodega Mecánica Automotriz.
- Bodega Electricidad.

Servicios.

- Biblioteca
- Centro Médico.
- Bodega general
- Educación Física.

Educación.

- Profesores
- Alumnos.

3.1.4 REDISEÑO DEL SISTEMA DE CABLEADO ESTRUCTURADO

El cableado actual de la Institución, como se analizó en el capítulo 2, no posee ninguna topología, ni se rige a ninguna norma por lo que no se puede identificar adecuadamente los subsistemas que lo componen, en base a estas consideraciones es necesario su rediseño.

3.1.4.1 Cableado Horizontal.

Para realizar el rediseño del Sistema de Cableado Estructurado, primero se debe anotar que no se puede reutilizar la infraestructura actual existente puesto que el cableado no cumple con ninguna de las normas internacionales establecidas.

Partiendo de esto se concluye que para el cableado horizontal se utilizará cable *UTP* CAT 6, que comprenderá el tendido desde el área de trabajo hacia los *switches* de acceso. Esta recomendación se basa, cotejando la información obtenida en el análisis de tráfico del capítulo 2 y el cálculo de ancho de banda por aplicación de la tabla 3.15. A través de esta información, se establece que este medio de transmisión es válido y que además mejorará el rendimiento de la red para soportar voz, datos y video sin ningún inconveniente.

3.1.4.2 Cableado Vertical. *(Backbone)*

Para este subsistema se desarrollará un esquema jerárquico en estrella con dos niveles de interconexión, la fibra recorrerá desde los *switches* en cada una de las áreas hasta los *switches de core* como se puede observar en la figura 3.5 donde se muestra el esquema de la topología de la red.

El cable a utilizarse será fibra óptica multimodo de 50/125 *um*, de 6 hilos. Por cada enlace se debe considerar los siguientes aspectos, cada enlace utiliza 2 hilos, uno para transmisión y otro para recepción; además se considerará el doble de hilos para utilizarlos de redundancia.

Considerando esto, por cada enlace se necesita fibra óptica de 6 hilos de los cuales serán utilizados 4 hilos con lo que los dos hilos restantes estarían disponibles para futuras expansiones del servicio de la red, o algún corte o algún problema con alguno de los hilos.

Se podría utilizar una fibra óptica de 12 hilos; sin embargo el tener enlaces de fibra de 6 hilos brinda independencia de cada uno de los enlaces, lo que brinda un nivel de seguridad adicional en la red, protegiendo el *backbone* de algún tipo de intrusión o daño que se pueda producir de manera intencionada o accidental

Entre los factores para la elección de fibra óptica como medio de transmisión para el *backbone,* se puede mencionar:

- Para proteger el medio de transmisión, debido a que en su mayor parte estos enlaces atraviesan áreas abiertas que están expuestas a condiciones ambientales variantes y que serían puntos vulnerables de la red.
- Debido a las distancias que en algunos casos exceden los 100 metros que se considera para un sistema con un medio de transmisión de cobre. Estas distancias se encuentran detalladas en la figura 3.6, en el apartado de topología de la red de datos.
- El uso de fibra óptica para la interconexión de los *switches*, evitará que se generen cuellos de botella en la red y optimizará el rendimiento; además que en un sistema de *backbone* las velocidades se ajustan al enlace de

menor capacidad por lo que es preferible tener el mismo sistema de transmisión en los enlaces.

El cableado vertical se rige bajo la norma EIA/TIA 568-C.3, que especifica el cableado con fibra óptica. La fibra óptica a utilizarse debe ser protegida para ambientes externos, el enrutamiento de la fibra óptica será a través de tubería, de esta forma se protege que el medio transmisor sea manipulado por personas ajenas o sufra cortes no previstos.

La distancia máxima a cubrir con este medio de transmisión será de 300 metros con lo cual si se observa la tabla 3.10, la fibra deberá tener un diámetro de 50 micrones para soportar un ancho de banda de 1 *Gbps*. Basándose en esta información la fibra óptica deberá ser multimodo 1000 Base SX en la ventana de 850 nm.

Características	**1000 Base – SX**		**1000 Base – LX**		
Longitud de onda	850		1300		
Tipo de FO	62,5	50	62,5	50	Monomodo
Ancho de banda [Mhz/Km]	160-200	400-500	500	400-500	s/d
Distancia [m]	220-275	500-550	550	550	5000
Perdida del *link* [dB]	3,2-3,2	3,4-3,9	4	2,4-3,5	4,7

Tabla 3.10 Parámetros *Giga Ethernet* para ancho de banda fibra óptica.[W67]

3.1.4.3 Cuartos de Telecomunicaciones.

El Instituto Tecnológico Superior Central Técnico cuenta con área física muy extensa por lo es que necesario ubicar varios Cuartos de Telecomunicaciones en cada una de las áreas, puesto que en la Norma EIA/TIA 568-C, se recomienda que la distancia máxima desde los Cuartos de telecomunicaciones hasta la estación de trabajo no debe sobrepasar los 100 metros, incluidos los *patch cords*. Por lo que se deben ubicar Cuartos de Telecomunicaciones para brindar un acceso a todos los usuarios de la red.

La Sala de Equipos se localiza en el primer piso del Edificio Administrativo, siendo este el punto central al cual los diferentes Cuartos de Telecomunicaciones

de todo el campus se conectarán. A continuación, en la tabla 3.11, se detalla la ubicación de los Cuartos de Telecomunicaciones a través del campus.

ÁREA	UBICACIÓN CUARTO DE TELECOMUNICACIONES
Administración	Primer piso
Automotriz	Bodega Automotriz
Electricidad	Bodega Electricidad
Industrial	Bodega Industrial
Electrónica	Bodega Electrónica
Bodegas	Jefatura de talleres
Inspección	Inspección general
Bloque de aulas	Inspección de cursos
Superior	Primer Piso

Tabla 3.11 Ubicación de Salas de Equipos en cada una de las áreas.

El Cuarto de Telecomunicaciones es un espacio centralizado de uso específico para equipo de telecomunicaciones, terminaciones mecánicas y el cableado de interconexión. Las características de un cuarto de telecomunicaciones deben cumplir la norma EIA/TIA 568-C.

En el caso de la Institución donde se necesita tener varios Cuartos de Telecomunicaciones, para los que se recomienda:

- Un Cuarto de Telecomunicaciones por cada 1.000 m^2 de área utilizable.

- La distancia de las canalizaciones de distribución horizontal desde la sala de telecomunicaciones hasta las áreas de trabajo no puede superar en ningún caso los 90 m. Si algún área de trabajo se encuentra a más de esta distancia de la sala de telecomunicaciones, debe preverse otra sala de telecomunicaciones, para cumplir con este requerimiento

- Además se considera el tamaño de los Cuartos de Telecomunicaciones para una área de trabajo de 10 m^2, como se especifica en la norma EISA/TIA 568-C, las dimensiones se especifica en la tabla 3.12.

Espacio Utilizable	Número de Equipos por espacio utilizable	Tamaño recomendado para Cuartos de Telecomunicaciones
500 m^2	50	3m x 2.2 m
800 m^2	80	3m x 2.8 m
1000 m^2	100	3m x 3.4 m

Tabla 3.12 Espacio Físico Cuarto de Telecomunicaciones[P1]

Para las diferentes áreas del Instituto de acuerdo al espacio utilizable y al número de equipos que ésta va a servir, se determina que en el área administrativa existirá un Cuarto de Telecomunicaciones con todas la recomendaciones hechas por el estándar, debido a que el cuarto de telecomunicaciones brindará servicio a 71 equipos se recomienda tener un área de 3m x 2.8m, este espacio será suficiente para albergar los equipos activos, pasivos, central telefónica, servidores y entrada de servicios. Mientras que para las otras áreas simplemente se buscará un espacio donde se pueda situar los racks de telecomunicaciones con su respectiva seguridad y protección ya que el número de usuarios a servir es reducido.

En el caso de los racks el espacio a utilizar se detalla en la tabla 3.13.

Área	Número de equipos	Numero de racks
Electrónica	28	1m x 1m
Bodegas	18	1m x 1m
Inspecciones	17	1m x 1m
Aulas	29	1m x 1m
Superior	16	1m x 1m
Industrial	14	1m x 1m
Automotriz	21	1m x 1m
Electricidad	24	1m x 1m

Tabla 3.13 Recomendación de espacio físico para ubicar los racks.

Siguiendo las recomendaciones de los estándares se sugiere tener un Cuarto de Telecomunicaciones por piso o edificio, para este caso en particular se diseña un Cuarto de Telecomunicaciones por cada una de las Áreas a servir puesto que actualmente solo se cuenta con una Sala de Equipos.

El sistema de distribución secundario permite que se interconecten el cableado horizontal con los respectivos equipos de comunicaciones. Este espacio debe contar con *Patch Panels* RJ45 CAT 6 de 24 puertos, los *patch panel* serán sólidos y estos componentes deberán tener la adecuada identificación y administración. De igual forma se deben utilizar organizadores tanto horizontales como verticales.

Se considera tener *ODF's*, organizadores para fibra óptica, ubicados en estos *Patch Panels* para la conexión del cableado vertical, los *ODF's* deben admitir conectores *SC, LC, FC,* estos son conectores estándares ampliamente utilizados y que soportan la interconectividad con los equipos de conmutación.

Tanto en los Cuartos de Telecomunicaciones como en la Sala de Equipos se debe cumplir con la norma EIA/TIA 569. A continuación se detalla las características que estos deben poseer:

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

- El número y tamaño de los ductos utilizados para acceder al cuarto de telecomunicaciones varía con respecto a la cantidad de áreas de trabajo, sin embargo se recomienda por lo menos tres ductos de 100 milímetros (4 pulgadas) para la distribución del cable del *backbone*.

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

- Se debe el evitar polvo y la electricidad estática utilizando piso de concreto, loza o similar (no utilizar alfombra). De ser posible, aplicar tratamiento

especial a las paredes pisos y cielos para minimizar el polvo y la electricidad estática

- En cuartos que no tienen equipo electrónico la temperatura del Cuarto de Telecomunicaciones debe mantenerse continuamente (24 horas al día, 365 días al año) entre 10 y 35 grados centígrados. La humedad relativa debe mantenerse menor a 85%. Debe de haber un cambio de aire por hora.

- En cuartos que tienen equipo electrónico la temperatura del cuarto de telecomunicaciones debe mantenerse continuamente (24 horas al día, 365 días al año) entre 18 y 24 grados centígrados. La humedad relativa debe mantenerse entre 30% y 55%. Debe de haber un cambio de aire por hora.

- Se debe evitar el uso de cielos falsos en los Cuartos de Telecomunicaciones. Los pisos de los Cuartos de Telecomunicaciones deben soportar una carga de 2.4 kPa[25].

- Los cuartos deben estar bien iluminados, se recomienda que la iluminación debe estar a un mínimo de 2.6 metros del piso terminado, las paredes y el techo deben estar pintadas de preferencia de colores claros para obtener una mejor iluminación.

- También se recomienda tener luces de emergencia por si al foco se daña. Se debe proporcionar un mínimo equivalente a 540 lux[26] medidos a un metro del piso terminado.

- El estándar establece que debe haber un mínimo de dos tomacorrientes dobles de 110V C.A. dedicados de tres hilos. Estos dos tomacorrientes podrían estar dispuestos a 1.8 metros de distancia uno de otro. La

[25] El pascal (símbolo Pa) es la unidad de presión del Sistema Internacional de Unidades
[26] El lux (símbolo lx) es la unidad derivada del Sistema Internacional de Unidades para la iluminancia o nivel de iluminación.

alimentación específica de los dispositivos electrónicos se podrá hacer con UPS[27] y regletas montadas en los andenes.

- El Cuarto de Telecomunicaciones debe contar con una barra de puesta a tierra que a su vez debe estar conectada mediante un cable de mínimo 6 *AWG* con aislamiento verde al sistema de puesta a tierra de telecomunicaciones según las especificaciones de ANSI/TIA/EIA−607.

La disposición de la Sala de Equipos y los Cuartos de Telecomunicaciones se detalla en el ANEXO B, se ha considerado que estos cuartos se ubiquen en las bodegas de cada una de las áreas a brindar servicio puesto que existe un espacio físico seguro y accesible para realizar labores de revisión, mantenimiento o reparación.

3.1.4.3.1 *Rack Principal.*

Simplemente se ubicará un *rack* cerrado de piso de 73,5 pulgadas, 42 UR, para la Sala de Equipos. Un *rack* cerrado significa que posee su correspondiente gabinete. El rack tendrá esta altura puesto que debe albergar los equipos de conectividad, accesorios como organizadores de fibra y de cobre así como también los servidores.

En el numeral 3.3.5.6, se observa cómo se dimensionó el rack principal, ubicado en la Sala de Equipos, tomando en cuenta los diferentes elementos que lo conforman. De la misma forma se realizará el análisis para las Cuartos de telecomunicaciones, ubicados en las diferentes áreas.

Este *rack* tendrá un metro de profundidad, este con el objetivo de poder ubicar servidores de tipo rack y además ubicar un monitor para tener control de los servicios. El diseño del rack mantiene un adecuado espacio, y así el administrador logre manipular los equipos. Como se observa en la figura 3.1 un *rack* cerrado de piso.

[27] Sistema de alimentación ininterrumpida, SAI (en inglés *Uninterruptible Power Supply*, *UPS*), es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados

Figura 3.1 Racks de piso para telecomunicaciones[W64]

3.1.4.3.2 *Gabinetes.*

En cada uno de los Cuartos de Telecomunicaciones, así como en la sala de equipos, se dispondrán de gabinetes cerrados abatibles, como se observa en la figura 3.2, los cuales ayudarán a la administración de los equipos activos y pasivos, impidiendo así el uso inadecuado de los mismos por personas ajenas a estas tecnologías. Los gabinetes cerrados almacenarán los equipos activos como *switches,* y elementos pasivos como organizadores, multitomas de poder, etc. Para disponer los gabinetes en cada una de las zonas, se empotrará a la pared y cada uno de ellos tendrá una adecuada conectorización a tierra.

Los gabinetes tendrán una cerradura para que el administrador de red pueda manipular los equipos, del mismo modo en la parte posterior estará libre para permitir futuras expansiones o movimientos.

Figura 3.2 Gabinete de Telecomunicaciones[W38].

Para el diseño se considera ubicar accesorios como son organizadores horizontales, verticales, *patch panel* de 24 puertos, *switch* de 24 puertos, panel para toma de energía, y para los Cuartos de Telecomunicaciones, donde sea necesario, el organizador para fibra óptica.

Ubicación	Medida del gabinete en (UR)
Electrónica	18
Bodegas	12
Inspecciones	12
Bloque de aulas	18
Superior	12
Industrial	12
Automotriz	18
Electricidad	18

Tabla 3.14 Medidas en UR de los gabinetes para cada Área

En la tabla 3.14 se detalla la altura mínima que debe tener cada gabinete para los *IDFs* a instalarse en las áreas en UR[28], de acuerdo al dimensionamiento del apartado 3.3.5.6 y medidas de racks disponibles en el mercado.

3.1.4.4 Sala de Equipos.

Actualmente el Instituto no cuenta con un espacio dedicado para la Sala de Equipos, los equipos de comunicaciones y de telefonía se encuentran dispersos en la planta baja y primer piso del Edificio Administrativo, como se especificó en el capítulo 2.

En el rediseño del Sistema de Cableado Estructurado se dispone ubicar a los equipos de comunicación, servidores, así como la acometida de entrada de servicios, en el mismo espacio físico. Esta sala de equipos, deberá tomar en consideración todas las recomendaciones hechas por la norma, se encontrará ubicada en el primer piso del edificio de Administración, su ubicación se encuentra detallada en el ANEXO B.

[28] UR unidad de rack 1,75 pulgadas

3.1.4.5 Área de Trabajo.

El área de trabajo comprende el recorrido desde la salida de telecomunicaciones o *Faceplate* hasta llegar al equipo final de usuario. El área de trabajo comprende principalmente computadores, impresoras, teléfonos entre otros.

De acuerdo a la distribución, establecida en el apartado 3.1.2, cada área trabajo constará de una salida doble de telecomunicaciones, una para datos y otra para voz, o una simple para datos de acuerdo a las necesidades del usuario.

En los ambientes como son laboratorios dentro de la Institución se ubicarán puntos dobles, debido a que un punto de datos será para uso exclusivo de los docentes y como requerimiento del Instituto se debe disponer una extensión telefónica. Los *faceplates* deben tener conectores hembras RJ45, y también deben soportar etiquetas individuales para su correcta administración. Los *faceplates* se ubicarán a una distancia de 40 cm medidos desde el suelo, para evitar posibles daños.

La conectorización de los equipos en las áreas de trabajo a un punto de red sea este voz o datos, se la realizará mediante un *patch cord* certificado CAT 6 de tres metros de longitud. La terminación de estos debe ser de acuerdo a la norma T568B.

Ninguno de los *patch cords* existentes en la red del Instituto cumplen con las normas, por lo cual es necesario el cambio de los actuales. De igual forma los *patch cords* para la interconexión entre equipos de *networking*[29] y *patch panels* en los Cuartos de Telecomunicaciones, deberán ser certificados tanto para cable UTP CAT 6, como para la fibra óptica multimodo.

3.1.4.6 Canalizaciones y enrutamiento.

De acuerdo a la inspección de la infraestructura de las oficinas, aulas, y talleres, se establece que las canalizaciones más adecuadas en estos espacios es utilizar canaletas decorativas. Toda la ductería superficial para el cableado vertical y horizontal se debe instalar previamente, siguiendo la norma EIA/TIA 569A.

[29] *Networking:* Equipos de interconectividad que permiten el intercambio de datos sean estos *switches, hubs o routers*.

Las canaletas decorativas deben contener los elementos necesarios para los montajes de curvas, dando cumplimiento así a la norma establecida. Todas las canaletas que bajen desde el tumbado de las aulas, talleres y oficinas serán plásticas y retardantes al fuego. En los planos del cableado estructurado correspondiente la ANEXO B se especifica la ruta a seguir para la conexión, y en el capítulo 4, se detalla la cantidad y características tanto de las canaletas y accesorios a utilizarse.

3.1.4.7 Etiquetado.

Se rige bajo el estándar EIA/TIA 606, que norma la correcta y adecuada identificación de cada uno de los Subsistemas de Cableado Estructurado. El etiquetado será en ambos extremos del cable, en los *faceplates* y en los *patch panels* de los Cuartos de Telecomunicaciones.

Los cables que conectan el subsistema de cableado horizontal y vertical deber ser rotulados con una etiqueta sobre el conductor para conocer a que *patch panel* y área pertenece. Las etiquetas del *faceplate* y del *patch panel* serán adhesivas.

Para diferenciar la salida de datos de la de voz, se recomienda establecer el siguiente formato para reconocer a que *rack* de telecomunicaciones está conectado dependiendo del área en la que se que se encuentra, la tabla 3.15 se lista las áreas con su respectiva denominación.

Área	Identificación
Administrativo	A
Electrónica	E
Mecánica Industrial	I
Mecánica Automotriz	T
Electricidad	L
Bodegas	B
Inspecciones	P
Superior	S

Tabla 3.15 Etiquetado del cableado para las diferentes Áreas.

Luego se procede a identificar al *patch panel* al cual se encuentra conectado el punto de red en el correspondiente *rack* de telecomunicaciones, en forma descendente de arriba hacia abajo.

Después se realiza el etiquetado del puerto al cual está conectado en el *patch panel* y finalmente determinar si se trata de un punto de voz o de datos. En la figura 3.3 se adjunta un ejemplo que explica en detalle la identificación.

Figura 3.3 Ejemplo de identificación de un punto de red.

- **E:** Área Electrónica.
- **01:** Pertenece al *Patch Panel* 1 del Área antes mencionada.
- **07:** Puerto al que se conecta en el *Patch Panel*.
- **D:** Punto de Datos.

Este esquema de etiquetación se propone para los puntos de voz y datos, además que permite al administrador identificar fácilmente y detectar posibles fallas en lo concerniente al cableado.

Una vez terminada la instalación del Sistema de Cableado Estructurado es importante que una empresa certifique todos los puntos de red, a través del equipo diseñado para el efecto. El equipo certificador debe presentar un informe detallado indicando los principales parámetros tomando en consideración los mismos que garantizarán el correcto desempeño de la red multiservicios.

3.2 DIMENSIONAMIENTO DEL TRÁFICO[T4][T2]

La infraestructura actual, según los análisis de tráfico realizado en el capitulo anterior, es exclusivamente para la navegación *web* a través del Internet, debido a que la red no ofrece más servicios para los usuarios. Por esta razón para el nuevo diseño se contempla incluir servicios como son Correo Electrónico, acceso a Internet, descarga de archivos, cámaras IP y *VoIP*.

3.2.1 CÁLCULO DE ANCHO DE BANDA PARA CORREO ELECTRÓNICO.

La mayor parte de la comunidad educativa tiene acceso a una cuenta de correo electrónico, pero el interés de la Institución es contar con un correo electrónico institucional para el manejo de información como avisos, reuniones, comunicados, oficios, etc.

El tamaño promedio de un correo electrónico es de 30KB, esta información se estimó en base a la información la pagina de optimización de sitios web[30], por lo tanto se asume que un usuario revisa 4 mails cada hora con lo cual se procede a calcular lo siguiente:

$$AB = \frac{30KB}{1\ mail} \times \frac{4\ mail}{1\ hora} \times \frac{1\ hora}{3600\ seg} \times \frac{8\ bits}{1\ Byte}$$

$$AB = 0.26\ Kbps$$

3.2.2 CÁLCULO DE ANCHO DE BANDA PARA *WEB*

Este servicio es el más utilizado actualmente por los usuarios de la red, en conclusión se estima que los usuarios acceden a 5 páginas cada hora, con un tamaño promedio de 312 KB, este tamaño es promedio de acuerdo al monitoreo realizado una semana en la Institución donde se determinó que las páginas más solicitas fueron *Facebook, Hotmail, Yahoo, YouTube*, SRI, Ministerio de Educación, IESS; además se comparó con el sitio web antes mencionado para el cálculo promedio de un correo electrónico.

Tomando esto en consideración se realiza el siguiente cálculo:

$$AB = \frac{312\ KBytes}{1\ pagina} \times \frac{8\ bits}{1\ byte} \times \frac{5\ paginas}{1\ hora} \times \frac{1\ hora}{3600\ segundos}$$

$$AB = 3.46Kbps$$

3.2.3 CÁLCULO DE ANCHO DE BANDA PARA DESCARGA DE INTERNET.

Se considera que el peso promedio de un archivo es de 1000 KB y el tiempo aceptable para la descarga es de 1 minuto, estos datos se estimaron tomando en

[30] http://www.websiteoptimization.com/speed/tweak/average-web-page/

promedio la descarga de diferentes tipos de archivos (audio, video, documentos) realizados tanto en la propia Institución así como en diferentes redes actualmente en funcionamiento.

En una hora se estima que un usuario puede alcanzar a descargarse 1000 KB, siendo esta un descarga crítica en promedio por usuario, esto quiere decir que el cálculo se realizará tomando en cuenta un tamaño de archivo de 1000 KB como máximo que el usuario realizará periódicamente con lo cual se estable un valor de descarga aproximado. Sin embargo esto no significa que el usuario deberá esperar toda la hora para descarga esta cantidad de información, esta descarga se estima que debería demorarse en promedio un minuto.

Tomando en cuenta que la latencia de la red actual es alta, que los computadores no ofrecen capacidades mayores para procesar, y las aclaraciones anteriores el ancho de banda para este caso sería:

$$AB = \frac{1000\ KB}{1\ min} x \frac{1 min}{60\ seg} x \frac{8\ bits}{1\ byte}$$

$$AB = 133{,}33\ Kbps$$

3.2.4 CÁLCULO DE ANCHO DE BANDA PARA CÁMARAS IP.

Para calcular el ancho de banda que va a circular a través de la red es necesario tomar en cuenta diversos factores a ser tomados en cuenta en el manejo de transmisión de imágenes en tiempo real tales como el tamaño de la imagen, número de cuadros por segundo y la compresión a ser utilizada.

El ancho de banda se calcula en función de los siguientes parámetros:

- Ancho x altura: Se refiere al tamaño de la imagen en *pixeles*. El tamaño de la imagen debe definirse para proporcionar el número adecuado de detalles a ser visualizados en la imagen.

  De acuerdo a los requerimientos de la Institución y en base a los fabricantes de cámaras IP, para video vigilancia se recomienda un tamaño de imagen de 640 x 480. Este tamaño de imagen proporciona el número de detalles adecuado para este fin, utilizando una profundidad de 24 bits, 3bytes de color para el uso de imágenes JPEG.

- Cuadros por segundo: El número de cuadros por segundo define la cantidad de imágenes que van a ser transmitidas, es la medida de la frecuencia a la cual un reproductor de imágenes genera distintos fotogramas (*frames*).

  La frecuencia de los fotogramas es proporcional al número de píxeles que se deben generar, incidiendo en el rendimiento del equipo que los reproduce.

  Debido a que los datos no van a ser transmitidos por el Internet, se considera el número de fotogramas de acuerdo al estándar *NTSC* (*National Television System Committee*) que es de 30 cuadros por segundo.

- Factor de compresión: El factor de compresión dependerá del algoritmo utilizado para esto y es utilizado generalmente cuando se necesita ahorro en el ancho de banda a utilizarse, especialmente para redes extendidas como Internet donde los costos para una transmisión completa serían muy elevados e ineficientes. Sin embargo a mayor compresión la calidad de la imagen será menor.

  El ancho de banda necesaria sería el siguiente:

$$\frac{640\ x\ 480\quad [pixeles]}{1\quad [cuadro]} \times \frac{3\quad [bytes]}{1\quad [pixel]} \times \frac{8\quad [bits]}{1\quad [byte]} \times \frac{30\quad [cuadros]}{1\quad [segundo]} = 221184000 \text{ bps}$$

Para el cálculo del ancho de banda se debe tomar en cuenta la compresión a ser utilizada por las cámaras. Se pone como ejemplo el estándar MPEG-4, como caso crítico debido a que éste utiliza el mayor ancho de banda para la transmisión de imágenes. El factor de compresión de este estándar varía de acuerdo al movimiento que va a ser registrado por el dispositivo; entre 70 a 1[31] para imágenes con mucho movimiento, y 200 a 1 para imágenes estáticas.

Para el cálculo se toma el menor nivel de compresión (70 a 1), es decir

[31] 70:1. Esto significa que por cada 70 bits utilizados el estándar los reduce 1, por medio de su algoritmo que utiliza técnicas para eliminar redundancia[w64].

$$\frac{221184000 \text{ bps}}{70} = 3159771bps = 3{,}16\ Mbps$$

Si se estima un total de 13 cámaras para la Institución se tendría un tráfico total de 41,08 Mbps, de las cámaras IP para video vigilancia lo que es un ancho de banda que la red puede soportar, sin presentar problemas en la transmisión.

Se debe anotar que este es un valor máximo debido a que la compresión podría variar de acuerdo al algoritmo utilizado por la cámara o incluso el movimiento de las imágenes registradas por éstas.

3.2.5 CÁLCULO DEL ANCHO DE BANDA DE LA INTRANET.

Luego de haber calculado el tráfico promedio que cada usuario necesita para navegar, descargar o utilizar el correo electrónico, se estima un cálculo en función del número de usuarios y de acuerdo a cada área del Instituto.

No todos los usuarios van a utilizar todas las aplicaciones al mismo tiempo, por lo que se debe considerar un nivel de simultaneidad de usuarios que accedan a las servicios a través de la red, este nivel de simultaneidad se considera para conocer cuántos usuarios concurrentemente utilizan los servicios y estimar un valor aproximado para el intercambio de información, estos valores se indican a continuación:

- Correo Electrónico 10%
- Tráfico *Web* 15%
- Descarga de archivos 10%
- Cámaras IP 100% (Transmisión continua de video)

Esto significa que del total de usuarios que hagan uso de los servicios de la red, por ejemplo, el 10 % hará uso de la aplicación de correo electrónico en el mismo instante de tiempo. Para las cámaras se considera un 100 %, debido a que todas las cámaras se encontrarán enviando tráfico ininterrumpidamente durante el día.

Puesto que la red del Instituto Tecnológico Superior no tiene actualmente los suficientes puntos de red, para el cálculo del tráfico generado se debe considerar que los puntos de cableado estructurado a instalarse son los usuarios potenciales, mientras que para este caso en particular los usuarios reales serán todos aquellos

en los que se encuentren conectados dispositivos finales a la salida de telecomunicaciones para mencionar el caso crítico. Esta información se basó en el levantamiento de datos de los equipos finales realizados en el capítulo dos.

A continuación en la tabla 3.16 se presenta el resumen de usuarios tanto potenciales como reales de la red.

Áreas	Usuarios Potenciales	Usuarios Reales
Administración	33	18
Electrónica	16	8
Automotriz	18	1
Industrial	10	1
Electricidad	22	9
Bodegas	11	5
Inspecciones	10	4
Superior	12	6
Aulas	27	14
Cámaras	-	13
Total	**159**	**77**

Tabla 3.16 Resumen de usuarios potenciales y reales de la red.

Del mismo modo, se consideran los usuarios que se conectarán mediante la red inalámbrica. En el área administrativa, no se consideraron los laboratorios de Computación para el cálculo hecho anteriormente, puesto que estos se conectarán mediante un dispositivo inalámbrico.

Se elige este medio de transmisión ya que treinta y nueve computadores poseen tarjetas inalámbricas y que estás áreas están sujetas constantemente a cambios de acuerdo a las necesidades de aulas de la Institución. Los equipos de estos laboratorios se obtuvieron de forma directa por parte del Ministerio de Educación que proporcionó las tarjetas de red inalámbricas.

Se debe recalcar que por solicitud de las autoridades del Instituto se decide utilizar dispositivos inalámbricos para todos los laboratorios ya que la inversión de adquirir una interfaz de red inalámbrica es mucho menor que implementar un punto de cableado estructurado, inclusive estos laboratorios no tienen un grado

de utilización muy alto, puesto que únicamente se genera información en horas de clase y que por supuesto el uso de los recursos serán únicamente a nivel educativo.

La estimación de los usuarios potenciales de la red inalámbrica se realizó en base a la utilización de cada una de las áreas la cuales se explica a continuación:

- En el área administrativa se promedia un total de 10 usuarios potenciales, los cuales se establecieron ya que la red inalámbrica servirá para reuniones o conferencias a realizarse en las oficinas administrativas.

- En los laboratorios de computación uno, dos, y cuatro se determina que los mismos, solamente se activarán durante el período de clases. En un día existe aproximadamente ocho horas de prácticas informáticas; además el tráfico a generarse será del tipo ráfaga únicamente en las horas a utilizarse.

- En el laboratorio tres o Sala de Internet, se atienden como máximo ocho horas a partir de las ocho de la mañana hasta cuatro de la tarde, por consiguiente este horario impide que los alumnos lo utilicen regularmente ya que se encuentran estudiando.

- En el área de Biblioteca, actualmente los estudiantes no poseen equipos portátiles para realizar consultas, considerando esto se dimensiona el número de usuarios potenciales para treinta usuarios.

- En Electrónica y Electricidad existen laboratorios con ocho computadores según los requerimientos se debe conectar mediante una equipo inalámbrico, pero además este equipo puede ayudar a brindar cobertura a una mayor cantidad de usuarios.

- En el bloque de aulas y salón de actos por ser espacios físicos grandes se estima brindar servicio a veinte usuarios potenciales.

- Para cada una de esta áreas, lo usuarios reales serán el cincuenta por ciento (50%) del los usuario potenciales, debido a que la red no está funcionando a su máxima capacidad, se calcula para la mitad de los usuarios ya que el trafico a generarse no será constante y la red inalámbrica podrá solventar cualquier problema de conexión física.

En la tabla 3.17 se presenta el resumen de los usuarios que harán uso de la red inalámbrica.

Áreas	Usuarios Potenciales	Usuarios Reales
Administrativo	10	5
Laboratorios de Computación 1	20	10
Laboratorios de Computación 2	19	10
Laboratorios de Computación 3	17	9
Laboratorios de Computación 4	31	16
Biblioteca	30	15
Electrónica	12	6
Electricidad	10	5
Aulas	20	10
Salón de actos	20	10
Total	**189**	**96**

Tabla 3.17 Resumen de usuarios potenciales y reales de la red inalámbrica.

El ancho de banda calculado se detalla a continuación en la tabla 3.18, considerando el número de usuarios reales de cada área, la aplicación de acuerdo al promedio calculado anteriormente y la simultaneidad del uso.

A continuación se presenta como ejemplo el cálculo del ancho de banda de la aplicación de correo electrónico para los usuarios del área administrativa.

$$Ancho\ de\ banda\ correo\ electrónico\ para\ el\ área\ administrativa$$

$$= 18\ usuarios\ reales\ \times 3.16\ Kbps\ promedio\ de\ la\ aplicación$$
$$\times 0.15\ de\ simultaneidad\ =\ 0{,}468\ Kbps$$

Aplicación	Áreas	Ancho de Banda promedio por usuario [Kbps]	Porcentaje de simultaneidad [%]	Usuarios Reales	Ancho de Banda [Kbps]
Correo Electrónico	Administración	**0,26**	**10**	18	0,468
	Electrónica			9	0,234
	Automotriz			1	0,026
	Industrial			1	0,026
	Electricidad			9	0,234
	Bodegas			5	0,13
	Inspecciones			4	0,104
	Superior			6	0,156
	Aulas			14	0,364
Total Correo Electrónico				**67**	**1,742**
Web	Administración	**3,46**	**15**	18	9,342
	Electrónica			9	4,671
	Automotriz			1	0,519
	Industrial			1	0,519
	Electricidad			9	4,671
	Bodegas			5	2,595
	Inspecciones			4	2,076
	Superior			6	3,114
	Aulas			14	21,519
Total Tráfico WEB				**67**	**34,773**
Descarga	Administración	**133,33**	**10**	18	240
	Electrónica			9	120
	Automotriz			1	13,33
	Industrial			1	13,33
	Electricidad			9	120
	Bodegas			5	66,66
	Inspecciones			4	53,33
	Superior			6	80
	Aulas			14	186,66
Total Descargas				**67**	**893.311**
Cámaras			**100**	11	41080

Tabla 3.18 Ancho de Banda por aplicación en cada área

Se consideró que las cámaras IP funcionarán simultáneamente como vigilancia de la Institución. El detalle del cálculo de tráfico para *VoIP* se detalla en el apartado 3.5.3.

En la siguiente tabla se observa el cálculo de las aplicaciones web, correo electrónico, y descarga para los usuarios inalámbricos. De la misma manera que para los usuarios de la red cableada.

Aplicación	Usuarios Reales	Ancho de Banda promedio por usuario [Kbps]	Porcentaje de simultaneidad [%]	Ancho de Banda [Kbps]
Correo Electrónico	96	0,26	10	2,496
Web	96	3,46	15	49,824
Descarga	96	133,33	10	1280
Total				**1332,32**

Tabla 3.19 Ancho de Banda usuarios red inalámbrica

Una vez que se tiene los valores parciales por aplicación en las diferentes áreas se procede a sumar estos datos obteniendo así la tabla 3.20, con lo cual se obtiene los valores totales que se generarán en la intranet.

Aplicación	Ancho de Banda (Kbps)	Ancho de Banda (Mbps)
Correo Electrónico	1,742	0,001742
Web	34,773	0,034773
Descarga	893,31	0,893
VoIp	1360.32	1,36032
Cámaras IP	41080	41,08
Red inalámbrica	1332,32	1,332

Tabla 3.20 Ancho de Banda Total para todas las Áreas

3.2.6 ANCHO DE BANDA DE LA CONEXIÓN A INTERNET.

El cálculo de acceso a Internet para el uso compartido de todos los usuarios, se toma en cuenta las descargas que realizan desde el Internet, el acceso *Web* así como el uso del correo electrónico. A continuación se detalla los valores de cada una de las áreas:

$$Capacidad\ ISP = \text{Capacidad}_{\text{web}} + \text{capacidad}_{\text{e-mail}} + \text{Capacidad}_{\text{descarga}} + \text{Capacidad}_{\text{wlan}}$$

$$Capacidad\ ISP = 1{,}742\ Kbps + 34{,}773 Kbps + 893{,}31 Kbps + 1{,}332 Kbps$$

$$Capacidad\ ISP = 2262{,}145\ Kbps$$

De acuerdo al cálculo anterior se establece que el enlace hacia Internet debe ser de mínimo 2262,145 Kbps, por lo que se recomienda a la Institución Educativa contratar un enlace dedicado de 3072 Kbps. Este valor se considera debido a que se debe sobredimensionar este enlace porque en un futuro tanto el número de usuarios como de aplicaciones se incrementará, y por ende el ancho de banda deberá satisfacer las necesidades inmediatas de la Institución.

3.3 DISEÑO DE LA RED ACTIVA

Es fundamental diseñar la red del Instituto Tecnológico Superior Central Técnico de acuerdo con un esquema jerárquico, este esquema es necesario en una red convergente que soporte la transmisión de voz, datos y video. La ventaja de este modelo es que permite distinguir funciones para cada una de las capas de red, surgiendo así la posibilidad de que la red sea mucho más predecible, flexible y escalable.

El diseño para el Instituto Tecnológico Superior Central Técnico contempla utilizar dos niveles, siendo estos el de acceso - distribución y el de núcleo. Al separar la red en dos niveles lógicos se puede implementar seguridad, escalabilidad, redundancia y mejorar el desempeño, con una relación costo beneficio acorde a los requerimientos de la Institución.

El diseño jerárquico de la red en dos niveles lógicos permite asignar a cada uno de estas funciones específicas y "*se puede tener distintos dispositivos en una sola capa o un dispositivo haciendo las funciones de más de una de las capas. En la figura se observa la jerarquía*" [W65].

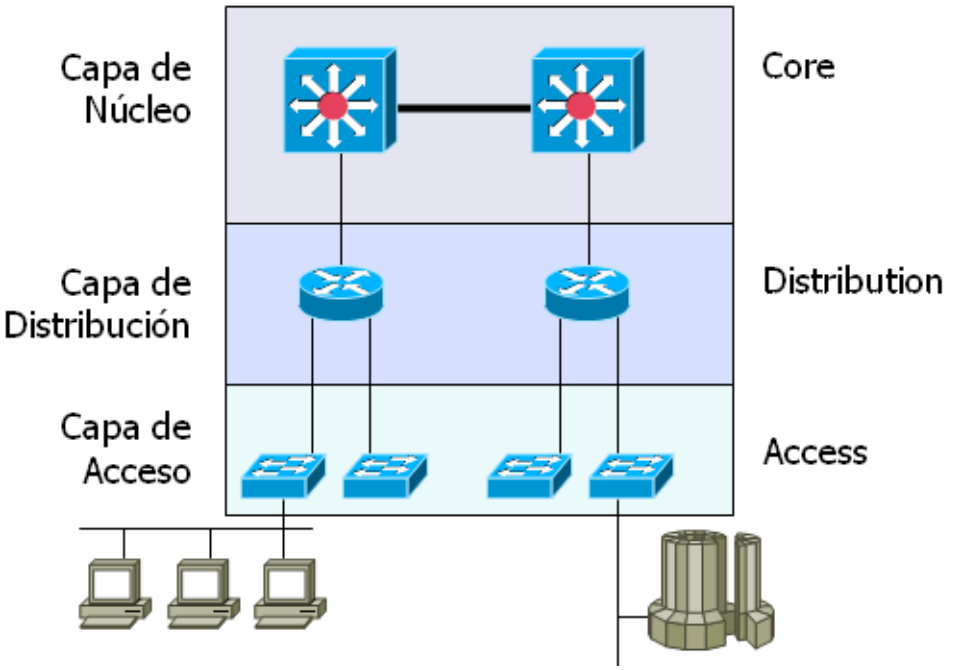


Figura 3.4 Modelo Jerárquico[W65]

3.3.1 ACCESO Y DISTRIBUCIÓN DE RED.

La capa de acceso comprende el segmento de la red donde se conectan los dispositivos finales de usuario, y la capa de distribución permite la conectividad hacia los diferentes servicios de la red. En el diseño de la red del Instituto los equipos se conectan directamente a los *switches* capa 2 a los cuales se conectará cada *host*, teléfono *IP* o punto de acceso inalámbrico. En este dispositivo se realizará configuraciones de *VLANs*, seguridad a nivel de puerto, a nivel de dirección *MAC, Spanning Tree Protocol* entre otras configuraciones, por lo que estos equipos cumplen las funciones de las dos capas tal como se señaló anteriormente.

3.3.2 NÚCLEO DE RED.

El núcleo de red comprende el *switch* multicapa modular que será el encargado de las funciones de conmutación de paquetes y enrutamiento entre *VLANs*. Este equipo debe tener alto desempeño, un nivel de *troughput* elevado y alta disponibilidad, para esto se prevé redundancia a nivel de fuente de poder, En esta capa comúnmente se contempla la instalación de equipos como controladora de red inalámbrica*, PBX*, etc.

3.3.3 GRANJA DE SERVIDORES Y CENTRO DE DATOS.

La capa granja de servidores y centro de datos comprende el conjunto de servidores de aplicaciones de la Unidad Educativa. Estos servicios se especificarán en el dimensionamiento de servidores.

3.3.4 DISEÑO LOGICO DE LA RED.

El alcance propuesto para la red de comunicaciones del Instituto Central Técnico, es utilizar tecnología tipo *Giga Ethernet* para el *backbone* en la topología en estrella, que interconecta las diferentes áreas del campus. Y para los enlaces de acceso a computadores y teléfonos IP se utilizará tecnología tipo *Ethernet* Conmutada a 100 *Mbps.*

Debido a que el Instituto forma un Campus extenso se decidió agrupar en 4 zonas para formar los enlaces de fibra óptica con el *Switch* de *Core*, estas zonas son Electrónica, Automotriz, Superior, Administración.

En la figura 3.5, se muestra un esquema de la topología de Red propuesta.

Como se observa en la figura 3.5, algunas de estas zonas se interconectan con otros equipos de conmutación en otras áreas, permitiendo así evitar los cuellos de botella que pueden generar en la red, como se muestra

El *switch* ubicado en Electrónica brindará acceso a dos áreas cercanas como son Bodegas e Inspección. Desde el *switch* de Inspección se facilitará el acceso hacia el bloque de aulas que es uno de los lugares más alejados del Instituto. Todas estas conexiones serán mediante la tecnología *Gigabit Ethernet*.

En Automotriz, se diseñó un enlace principal hacia el Edificio Administrativo donde se ubicará el *switch* de *Core*, y desde Automotriz se debe tener un enlace de fibra óptica hacia Electricidad, el cual es el punto más alejado de todo el campus. Además para enlazar Automotriz con Industrial debido a la corta distancia conviene utilizar tecnología *Ethernet Conmutada a 100 Mbps,* ya que no supera los cien metros. En la figura 3.6 se presenta un esquema de las distancias a cubrir por los enlaces de datos a fin de brindar una cobertura total de las áreas de la Institución.

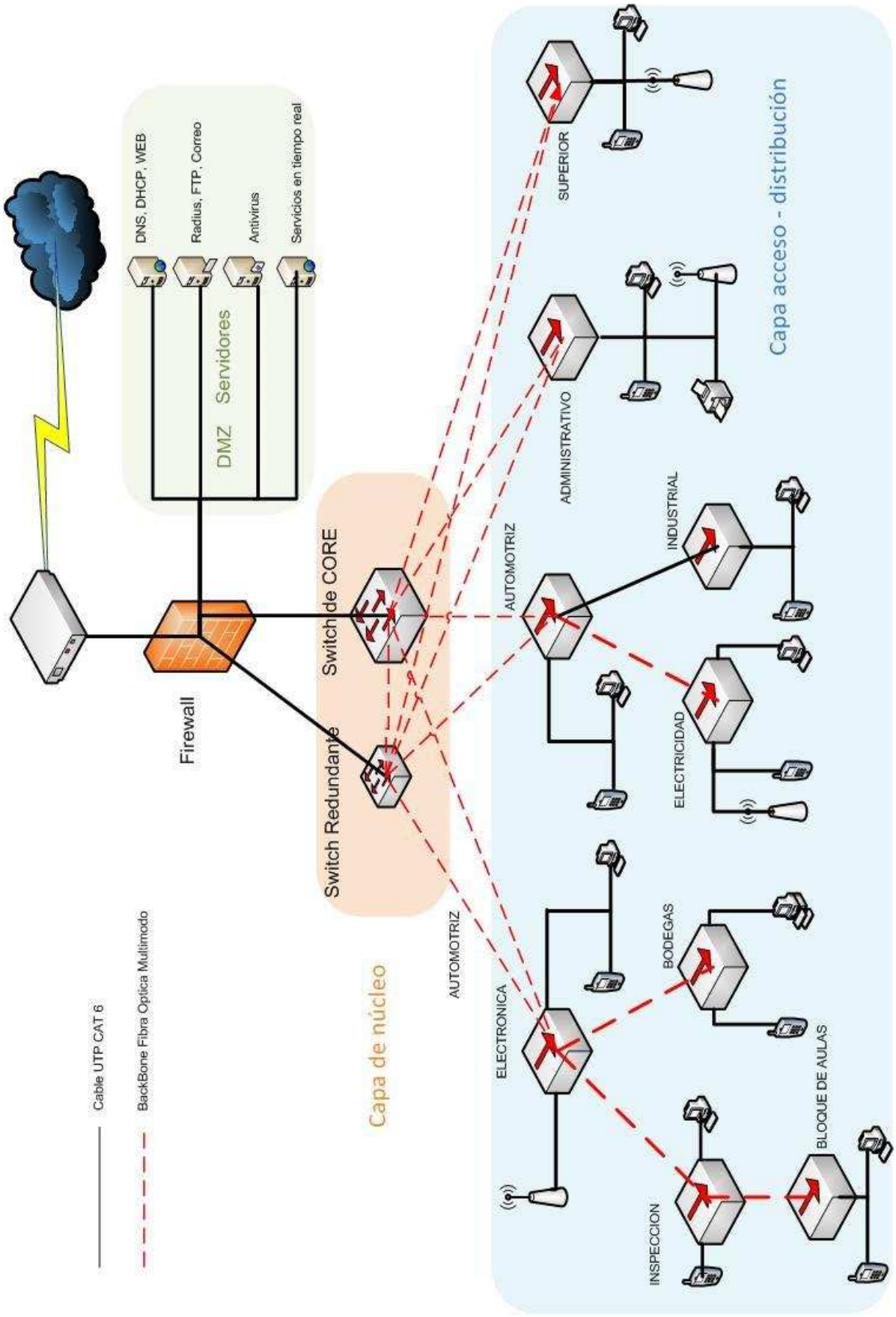


Figura 3.5 Topología de la red de Comunicaciones

En Automotriz, se diseñó un enlace principal hacia el Edificio Administrativo donde se ubicará el *switch* de *Core*, y desde Automotriz se debe tener un enlace de fibra óptica hacia Electricidad, el cual es el punto más alejado de todo el campus. Además para enlazar Automotriz con Industrial debido a la corta distancia conviene utilizar tecnología *Ethernet Conmutada a 100 Mbps,* ya que no supera los cien metros. En la figura 3.6 se presenta un esquema de las distancias a cubrir por los enlaces de datos a fin de brindar una cobertura total de las áreas de la Institución.

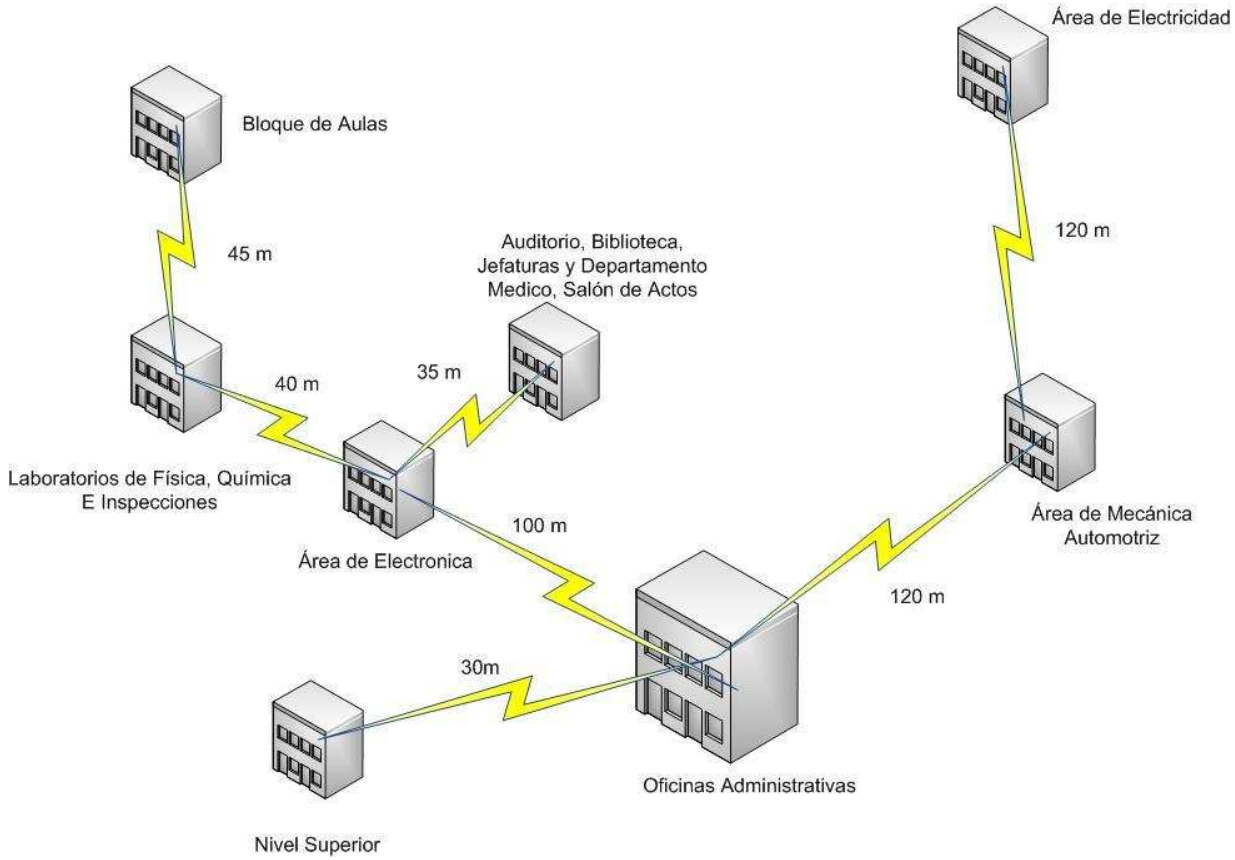


Figura 3.6 Distancias desde el cuarto de equipos a las diferentes áreas de la Institución

Finalmente se necesitará un enlace de fibra para conectar el Edificio Administrativo con el Superior, con esto se obtiene una malla parcial en todo el campus.

Uno de los principales objetivos del diseño propuesto para la red es el brindar seguridad así como redundancia a nivel de los equipos y enlaces, previniendo así la generación de cuellos de botella o en su defecto que los segmentos de red queden aislados.

Mediante este esquema se tienen dos s*witches* de *core* de iguales características, los que proporcionarán balanceo de carga entre los enlaces y redundancia en caso de falla.

Estos equipos serán los encargados de manipular toda la información y direccionarla de una forma adecuada a los dispositivos finales. Estos equipos de conectividad proveerán características de capa 3, además de contar con doble fuente de poder.

3.3.5 *DMZ*[W66]

La zona desmilitarizada permite brindar seguridad a los usuarios de la red, asignándoles niveles de confianza. La *DMZ* para este diseño se considera puesto que los usuarios internos como externos necesitarán acceder a los servicios de la Institución. Con lo cual la granja de servidores (*Web, DNS*, Servidor de Notas, Correo Electrónico, etc.) se les establece en una red separada para no comprometer la seguridad de la información y de los equipos internos.

3.3.5.1 Características de la DMZ.

La seguridad de la red estará complementada con la defensa en capas asociadas a una *DMZ*, las cuales se detallan a continuación:

- Red Interna, gestión y control de los servicios por parte de la Institución Educativa.
- Red externa sin ningún tipo de protección, no es gestionada.
- *DMZ*, se ubican los servicios para que los usuarios puedan acceder de forma interna o externa.
- En caso de existir algún posible ataque a la red, y de que sus vulnerabilidades sean explotadas, es obligación de la *DMZ* restringir los daños para no perder información.
- La *DMZ* se encarga de aplicar los mecanismos necesarios para limitar el tráfico entrante como saliente mediante el uso de un *Firewall*.
- El *Firewall* tendrá una configuración en trípode (*Three-legged firewall*). Se elige esta configuración puesto que se puede brindar diferentes zonas de seguridad a los segmentos conectado al firewall. El filtrado se realizará de

una forma más ordenada para la DMZ y la LAN. Esta configuración permitirá conectarse a un puerto diferente en el firewall.

- Todos los servicios que se ubiquen en la *DMZ* deberán estar configurados de forma segura, es decir, los servidores de la *DMZ* tendrán una *VLAN* propia, con una red diferente puesto que así se restringe su acceso, que es una vulnerabilidad.

En la figura 3.7 se explica de forma detallada el uso del *firewall* para no comprometer la seguridad física ni lógica de la información. Existe la red interna, la red externa y la *DMZ,* el firewall se ubicará entre el *modem* de acceso al Internet y los *switches de core* de la red.

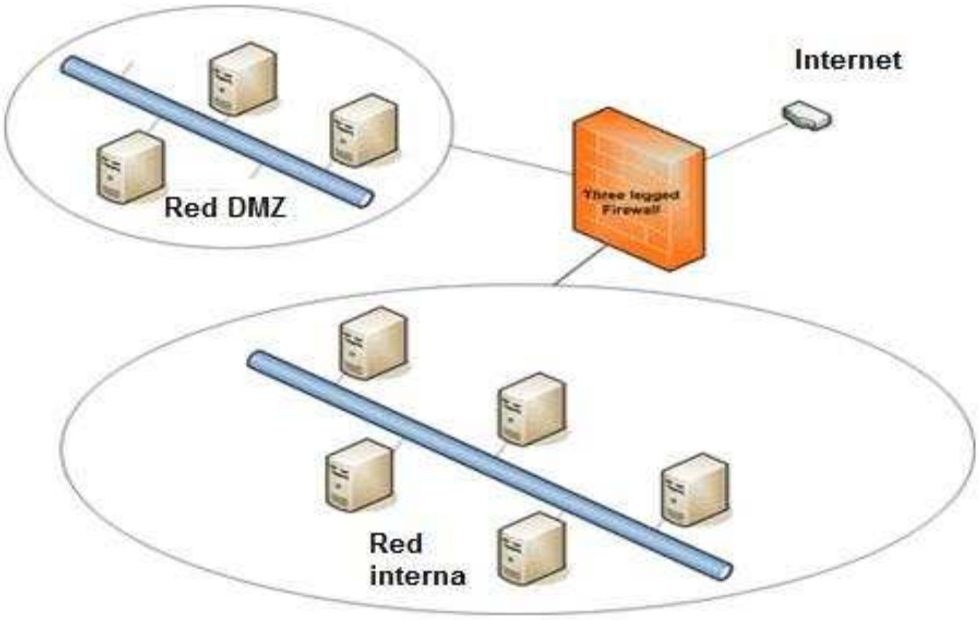


Figura 3.7 Zona desmilitarizada[W66]

Puesto que la *DMZ* contiene los servidores que brindan toda la información a los usuarios, la solución del firewall puede ser implementada tanto en hardware como *software*, sin embargo se decide aplicar una tecnología basada en *hardware,* con un equipo especializado en seguridad, debido a las prestaciones más altas que ofrece un dispositivo de estas características.

Este dispositivo bloqueará y filtrará el tráfico en función de las cabeceras de los paquetes; además filtrará los paquetes por estado de conexión, es decir tomará

en consideración los datos de la capa aplicación, examinando todo el flujo de datos y verificando con las políticas permisivas o restrictivas de seguridad a implementarse. Mediante el uso de este equipo se optimizará el acceso de los usuarios a las aplicaciones que necesiten evitando así posibles riegos de seguridad y los cuellos de botella en la red.

Se contempló utilizar el *firewall* basado en hardware debido a las ventajas que ofrece, teniendo en cuenta los riegos que se pueden generar dentro de la intranet. A continuación se detallan algunas de ellas.

- Un equipo dedicado de seguridad brinda mayor confiabilidad y rendimiento que un *software* instalado en una máquina. Puesto que en el diseño el dispositivo permitirá el ingreso y salida de datos, el rendimiento debe ser alto para que no provoque inestabilidad en la red o generar un cuello de botella en este dispositivo.

- En energía y espacio físico un equipo dedicado, ocupa menor espacio y además consume mucho menos energía que una PC normal en la cual se puede instalar un *software* de seguridad.

- Un firewall basado en hardware en un equipo especializado, con lo cual la lógica de su funcionamiento es a muy bajo nivel y su rendimiento mayor en comparación a un firewall basado en software.

- La administración de un equipo dedicado puede resultar mucho más fácil que la de un software, puesto que firewalls en hardware tienen sus propios sistemas operativos y además que en su gran mayoría poseen una interfaz gráfica que permite al administrador una mejor solución frente a problemas.

- Finalmente estos dispositivos dedicados, uno solo de ellos pueden ofrecer vario servicios a la vez como son: firewall, VPN, IDS, Anti malware, Filtro de contenido, Filtrado Web, Anti spam. Mientras que un firewall por software se debería instalar para cada una de estas aplicaciones por separado, para que ofrezca las mismas características.

En conclusión un equipo dedicado ofrece mayor fiabilidad, rendimiento, menor espacio físico que un *firewall* basado en software, cuya ventaja frente al *firewall* por *hardware* sería que permite mayor flexibilidad. Además se debe tomar en cuenta que un equipo dedicado cumple varias funciones la vez, simplemente como factor adicional en conjunto con el *firewall* se puede instalar en la granja de servidores, un antivirus que permita mantener el correcto funcionamiento de las estaciones de trabajo.

En el diseño de red existen dos *switches* capa 3 que serán los encargados de brindar redundancia y soportar todo el tráfico generado por la red interna. Estos dispositivos entre una de sus funcionalidades pueden limitar el tráfico mediante *ACL´s* que permiten o deniegan solo tráfico especifico, es decir los *switches* principales serán configurados de tal modo que permitan el acceso a subredes predeterminadas o aplicaciones. Inclusive los equipos de comunicación serán un respaldo para el equipo dedicado como *firewall* de la red del Instituto Tecnológico Central Técnico.

3.3.6 DIRECCIONAMIENTO IP

En la Institución Educativa existirán 239 puntos de red divididos en puntos de voz datos y video, los cuales servirán para conectar PCs, teléfonos, cámaras etc. Por lo cual se decide utilizar *VLSM* (Máscaras de subred de longitud variable), además para todo el direccionamiento se establece una dirección clase B privada que es la 172.16.0.0.

Debido a que la zona desmilitarizada (*DMZ*) debe estar en una red diferente, para brindar seguridad en especial a los servidores de *Mail y WEB,* a este segmento se le asigna una dirección clase A 10.10.10.0/24, mediante esto se protege a la información interna de la LAN.

Para la telefonía IP se asigna la subred 192.168.10.0/24, puesto que esta subred transmitirá tráfico etiquetado que tendrá una prioridad más alta. Todas estas direcciones son privadas por lo cual el rango de las mismas se puede utilizar independientemente sin tener ningún problema. En la tabla 3.21, se detallan parámetros del direccionamiento IP, como el segmento, la máscara, las direcciones *IP´*s válidas, la puerta de enlace para cada segmento y el número de

hosts, tanto para cada uno de los grupos de usuarios establecidos así como para los servicios de la red del Instituto.

Segmento	Subred/Mask	Direcciones IPs válidas		Puerta de enlace predeterminada	Dirección de *Broadcast*	Hosts disponibles
		Dirección IP Inicial	Dirección IP Final			
Educativo	172.16.0.0/25	172.16.0.1	172.16.0.125	172.16.0.126	172.16.0.127	126
Administrativo	172.16.0.128/26	172.16.0.129	172.16.0.189	172.16.0.190	172.16.0.191	62
Servicios Generales	172.16.0.192/28	172.16.0.193	172.16.0.205	172.16.0.206	172.16.0.207	14
Cámaras	172.16.0.208/28	172.16.0.209	172.16.0.221	172.16.0.222	172.16.0.223	14
Servidores	172.16.0.224/28	172.16.0.225	172.16.0.237	172.16.0.238	172.16.0.239	14
DMZ	10.10.10.0/28	10.10.10.1	10.10.10.13	10.10.10.14	10.10.10.15	14
Telefonía IP	192.168.10.0/24	192.168.10.1	192.168.10.253.	192.168.10.254	192.168.10.253	252

Tabla 3.21 Direccionamiento Privado para la Red de la Institución.

3.3.7 DISEÑO DE *VLANS*.

Con el objetivo de aprovechar el ancho de banda de la red y mantener la confidencialidad en la información que se intercambia, es necesario separar a los segmentos de la red en *VLANs* (*LAN*s virtuales). En cada uno de los *switches* de *core* se crearán las *VLANs*, estas reducirán la latencia en la red, por medio de un protocolo de enlace troncal se compartirán hacia los demás switches de un mismo dominio.

Las *VLANs* a crearse en los equipos de comunicación serán basadas en puerto. En las VLANs basadas en puerto cada puerto es independiente del usuario o sistema conectado, todos los usuarios que se conecten al puerto estarán en la misma VLAN, este tipo de VLAN es de fácil configuración y administración; además la búsqueda de tablas no es compleja

En resumen, la creación de *VLANS,* hará que la administración de la red sea más eficiente.

Segmento	**Nombre VLAN**	**Subred/*Mask***	**Direcciones IPs validas**		**Puerta de enlace predeterminada**
			Dirección IP Inicial	**Dirección IP Final**	
Educativo	CTEDUC	172.16.0.0/25	172.16.0.1	172.16.0.125	172.16.0.126
Administrativo	CTADM	172.16.0.128/26	172.16.0.129	172.16.0.189	172.16.0.190
Servicios	CTSERV	172.16.0.192/28	172.16.0.193	172.16.0.205	172.16.0.206
Cámaras	CTCIP	172.16.0.208/28	172.16.0.209	172.16.0.221	172.16.0.222
Servidores	CTSERVID	172.16.0.224/28	172.16.0.225	172.16.0.237	172.16.0.238
DMZ		10.10.10.0/28	10.10.10.1	10.10.10.13	10.10.10.14
Telefonía IP	CTTELF	192.168.10.0/24	192.168.10.1	192.168.10.253	192.168.10.254

Tabla 3.22 Identificación de las *VLANs*.

En la tabla 3.22 se establecen los nominativos de las *VLANs* a crearse para los equipos de conectividad, cada una de las *VLANs* se crearon en función de los grupos de usuarios explicado en el numeral 3.1.3.

3.3.8 CARACTERÍSTICAS DE LOS EQUIPOS DE RED ACTIVA.

En las tablas 3.19, 3.20 y 3.21 se detallan las características mínimas para los equipos de conectividad tanto de acceso como de *core,* así como el *switch* para la granja de servidores. Se especifica los protocolos que se deben soportar así como especificaciones técnicas respecto al hardware del equipo.

3.3.5.2 Requerimientos para los *switches* de distribución - acceso

Para los equipos de acceso se debe considerar además que no todos son iguales debido a que van a ser ubicados en áreas diferentes con requisitos de puertos que deben tener para lograr la completa interconectividad según la topología de red especificada en la figura 3.5 y el apartado 3.3.4.

- Tres áreas con *switches* con 1 puerto de fibra óptica *Giga Ethernet*
  - *Bodegas, Electricidad, Granja de servidores*
- Tres áreas con *switches con* 2 puertos de fibra óptica *Giga Ethernet*

  - *Inspección, Administrativo, Nivel Superior*
- Un área con *switches con* 3 puertos de fibra óptica *Giga Ethernet.*
  - *Mecánica Automotriz*
- Un área con *switches con* 4 puertos de fibra óptica *Giga Ethernet.*
  - *Electrónica*

Las características a enumerar son especialmente para que los equipos de conmutación trabajen en capa dos y capa tres. Los puertos de los *switches* deberán ser de tecnología *Ethernet* conmutada a 10/100/1000 Mbps, que permitan que cualquier dispositivo que se conecte al *switch* cense la interfaz y negocie automáticamente el método de intercambio de información. Adicional algunos equipos necesitan de puertos con módulos para fibra óptica.

- Los switches deben trabajar con el protocolo IEEE 802.3x para recepción y transmisión simultáneos (full dúplex), IEEE 802.3u para conexión de los equipos finales mediante tarjetas 10/100 Mbps a través de cable UTP CAT6.

- IEEE 802.3ab para conexión de los equipos finales mediante tarjetas 10/100/1000 Mbps a través de cable UTP CAT6 y el estándar IEEE 802.3z, para la conexión de los enlaces de fibra óptica a 1 Gbps.

- Los *switches* deben soportar el protocolo IEEE 802.1q, que permite tener múltiples redes compartiendo el mismo espacio físico, mediante esta alternativa se generan segmentos de red lógicos en el Instituto. Este protocolo permite crear *VLAN´s*.

- Es necesario garantizar la redundancia de la red, que los enlaces tengan disponibilidad por lo cual se establece utilizar protocolos tales como IEEE 802.1d y 802.1w.
- Para proveer enrutamiento entre diferentes *VLANs* se necesitará tener protocolo de enrutamiento como *RIP*, además de generar rutas estáticas para los servicios de la Intranet, se necesita protocolos de capa 3.

- El *switch* principal debe brindar calidad de servicio y etiquetar el trafico diferenciándolo si son datos o es voz. Para lo cual se necesita tener el protocolo IEEE 802.1p, y diferenciar el tráfico generado por las VLANs. Tanto los *switches* de acceso como los de núcleo deben proveer el servicio dinámico de asignación de hosts.

- A nivel de seguridad se requiere que los puertos de los *switches* soporten el protocolo IEEE 802.1x para autenticación y que mediante listas de acceso se brinde permisos a los usuarios, las listas de acceso deberán ser estándares y extendidas. Inclusive la administración del equipo debe proveer seguridad mediante el protocolo *SSH*, acceso remoto con el protocolo *Telnet*, y que soporte el protocolo de administración *SNMP* en sus versiones actuales.

- Los equipos de conmutación deben soportar administración tanto por interfaz gráfica como por línea de comando.

- Para los *switches* de *core* se necesita poseer redundancia a nivel de fuente de energía, esta fuente debe ser interna.

Para el cálculo de la velocidad de *backplane* se consideró que todas las interfaces del switch estén funcionando a *full dúplex*, con lo cual se calcula para el caso crítico, es decir todas las interfaces de fibra y de cobre trabajen a su capacidad máxima. Para el caso del Instituto Central Técnico se debe considerar que actualmente las interfaces de las estaciones de trabajo no trabajan a la velocidad de 10/100/1000 Mbps; además no todos los *switches* utilizarán sus puertos al mismo tiempo. A continuación se presenta el cálculo para el *switch* con mayor velocidad de *backplane*.

$$Vbackplane = \#\ puertos\ de\ cobre\ x\ 2\ x\ 1000\ +\ número\ de\ puertos\ de\ fibra\ x\ 2\ x\ 1000$$

$$V_{Backplane} = 24x2x1000\ +\ 4x2x1000$$

$$V_{backplane} = 56000\ Mbps$$

A continuación, en la tabla 3.23, se detallan las características mínimas para el *switch* de distribución - acceso, para la granja de servidores se utilizara un *switch* con idénticas características.

CARACTERÍSTICAS DE LOS SWITCHES DE DISTRIBUCIÓN - ACCESO

DETALLES DE HARDWARE	
Capacidad de backplane mínima	54 Gbps
CARACTERISTICAS CAPA 2	
Puertos Ethernet 10/100/1000 Mbps	24
Adicional Puertos de fibra *Gigabit Ethernet* 10/100/1000 Mbps	2,3,4 (según el requerimiento)
SPF conector LC	
Protocolos de Red Soportados	
Protocolo IEEE 802.3 u	
Protocolo IEEE 802.3 z	
Protocolo IEEE 802.3 x	
Protocolo IEEE 802.1 p	
Protocolo IEEE 802.1 q	
Protocolo IEEE 802.1 d	
Protocolo IEEE 802.1 w	
Protocolo IEEE 802.1 x	
Capacidad para troncalización en puertos	
ADMINISTRACIÓN	
Soporte de administración basada en *Web*	
Administración basada en consola CLI	
Soporte de *Telnet*	
Soporte de *SNMP* v1, v2, y v3	

Tabla 3.23 Requerimientos equipo de Distribución - Acceso

3.3.5.4 Requerimientos para los *switches* de *core*

En la tabla 3.24 se detallan las características de los switches de core.

DETALLES DE HARDWARE	
Capacidad de *backplane* mínima	32 Gbps o superior
CARACTERÍSTICAS CAPA 2	
Puertos Ethernet 10/100/1000 Mbps	**Mínino 12**
Adicional Puertos Gigabit Ethernet 10/100/1000 Mbps	**4**
SPF conector LC	
Protocolos de Red Soportados	
Protocolo IEEE 802.3 u	
Protocolo IEEE 802.3 z	
Protocolo IEEE 802.3 x	
Protocolo IEEE 802.1 p	
Protocolo IEEE 802.1 q	
Protocolo IEEE 802.1 w	
Protocolo IEEE 802.1 d	
CARACTERISTICAS CAPA 3	
Soporte *de Routing Information Protocol (RIP),*	
Soporte de enrutamiento estático	
Soporte de servicio DHCP	
SEGURIDAD	
Soporte de ACLs estándar y extendidas en todos los puertos	
Soporte de *SSH*	
ADMINISTRACIÓN	
Administración basada en consola CLI	
Soporte de Telnet,	
Soporte de SNMP v1, v2, y v3	
FUENTE DE PODER	
Debe proveer fuente de poder redundante interna	

Tabla 3.24 Requerimientos equipos de *core*.

3.3.5.5 Número de equipos de conectividad.

Todos los equipos que serán parte del nivel de distribución - acceso para la red, tendrán 24 puertos, para facilitar su reemplazo en caso de falla de alguno de ellos; además se contabilizan los equipos necesarios para cada una de las áreas a brindar cobertura. En la tabla 3.25 se especifican el número de *switches* de acceso a utilizar.

Área	Tipo de *Switch*	Puertos de cobre por *Switch*	Puntos a instalarse	Puntos con 30 % de expansión	Número Total de *Switches*	Puertos disponibles
Administrativo	*Switch Core*	Mínimo 12			2	
Servidores	*Switch* Acceso	24			1	
Administrativo	*Switch* Acceso	24	71	92	4	96
Electrónica	*Switch* Acceso	24	28	36	2	48
Bodegas	*Switch* Acceso	24	19	24	1	24
Inspecciones	*Switch* Acceso	24	17	22	1	24
Bloque de aulas	*Switch* Acceso	24	29	38	2	48
Mecánica Automotriz	*Switch* Acceso	24	21	27	2	48
Mecánica Industrial	*Switch* Acceso	24	14	18	1	24
Electricidad	*Switch* Acceso	24	24	31	2	48
Superior	*Switch* Acceso	24	16	23	1	24
Total	***Switch Acceso*** ***Switch Core***					**17** **2**

Tabla 3.25 Número de equipos de conectividad por área.

En conclusión se utilizarán 16 equipos de conectividad para acceso en las áreas, de 24 puertos, 2 *switches* de *core* con las características antes mencionadas y 1 *switch* para la granja de servidores.

3.3.5.6 Gabinetes.

Los gabinetes que se instalarán en cada uno de los cuartos de telecomunicaciones, deben ser dimensionados para alojar los equipos de comunicaciones activos y pasivos. Se toma en cuenta que a excepción de algunos organizadores que se consideran de dos unidades de rack, todos los

equipos miden 1 UR; además se dimensiona el gabinete para que pueda soportar futuras expansiones. Debido a esto, en la tabla 3.26, se observa el cálculo del rack cerrado de piso del Edificio Administrativo.

ADMINISTRATIVO		
Descripción	**Cantidad**	**Tamaño en UR**
Patch Panel de fibra óptica	1	1
Switch de *core*	2	2
Organizadores horizontales	4 (2 UR) + 3 (1 UR)	11
Switch 24 puertos	5	5
Patch Panel de 24 puertos	7	7
Firewall	1	1
Monitor	1	2
Servidores	4	4
Multitomas Horizontal	2	2
	TOTAL	**35**

Tabla 3.26 Espacio ocupado por los equipos del rack principal en unidades de rack.

Para las Áreas de Electrónica, Bloque de aulas, Electricidad, Mecánica Automotriz, se realiza el siguiente análisis para el cálculo de los gabinetes que albergará los equipos de comunicaciones.

En la tabla 3.27, se observa como ejemplo del rack de electrónica, debido a que para los otros racks mencionados el dimensionamiento será el mismo.

ELECTRÓNICA		
Descripción	**Cantidad**	**Tamaño en UR**
Patch Panel de fibra óptica	1	1
Organizadores horizontales	2	4
Switch 24 puertos	2	2
Patch Panel de 24 puertos	2	2
Multitomas Horizontal	1	1
	TOTAL	**10**

Tabla 3.27 Espacio ocupado por los equipos del rack de electrónica.

Para las áreas de Bodegas, Inspecciones, Superior y Mecánica Industrial, se realiza el siguiente análisis para obtener las medidas de los gabinetes.

En la tabla 3.28, se observa como ejemplo del rack de bodegas, debido a que para los otros racks mencionados el dimensionamiento será el mismo.

BODEGAS		
Descripción	**Cantidad**	**Tamaño en UR**
Patch Panel de fibra óptica	1	1
Organizadores horizontales	1	2
Switch 24 puertos	1	1
Patch Panel de 24 puertos	1	1
Multitomas Horizontal	1	1
	TOTAL	**6**

Tabla 3.28 Espacio ocupado por los equipos del rack de bodegas

Se toma en cuenta que se debe dejar un espacio entre cada uno de los elementos sujetos a los racks, de 1UR por cada tres elementos. En conclusión se utilizarán los siguientes gabinetes abatibles de pared y rack cerrado de piso para los cuartos de telecomunicaciones y sala de equipos respectivamente.

- Se necesita 1 rack cerrado de piso de 42 UR, para la sala de equipos puesto que se sobredimensiona este rack para que permita futura expansiones así como se pueda tener un monitor para la administración de los servicios.
- Se necesita 4 gabinetes abatibles de pared de 18 UR.
  - Electrónica
  - Bloque de aulas
  - Electricidad
  - Mecánica Automotriz
- Se necesita 4 gabinetes abatibles de pared de 12 UR.
  - Bodegas
  - Inspecciones
  - Superior
  - Mecánica Industrial

A continuación en las figura 3.8 se muestra la recomendación de la disposición de los elementos a ser instalados.

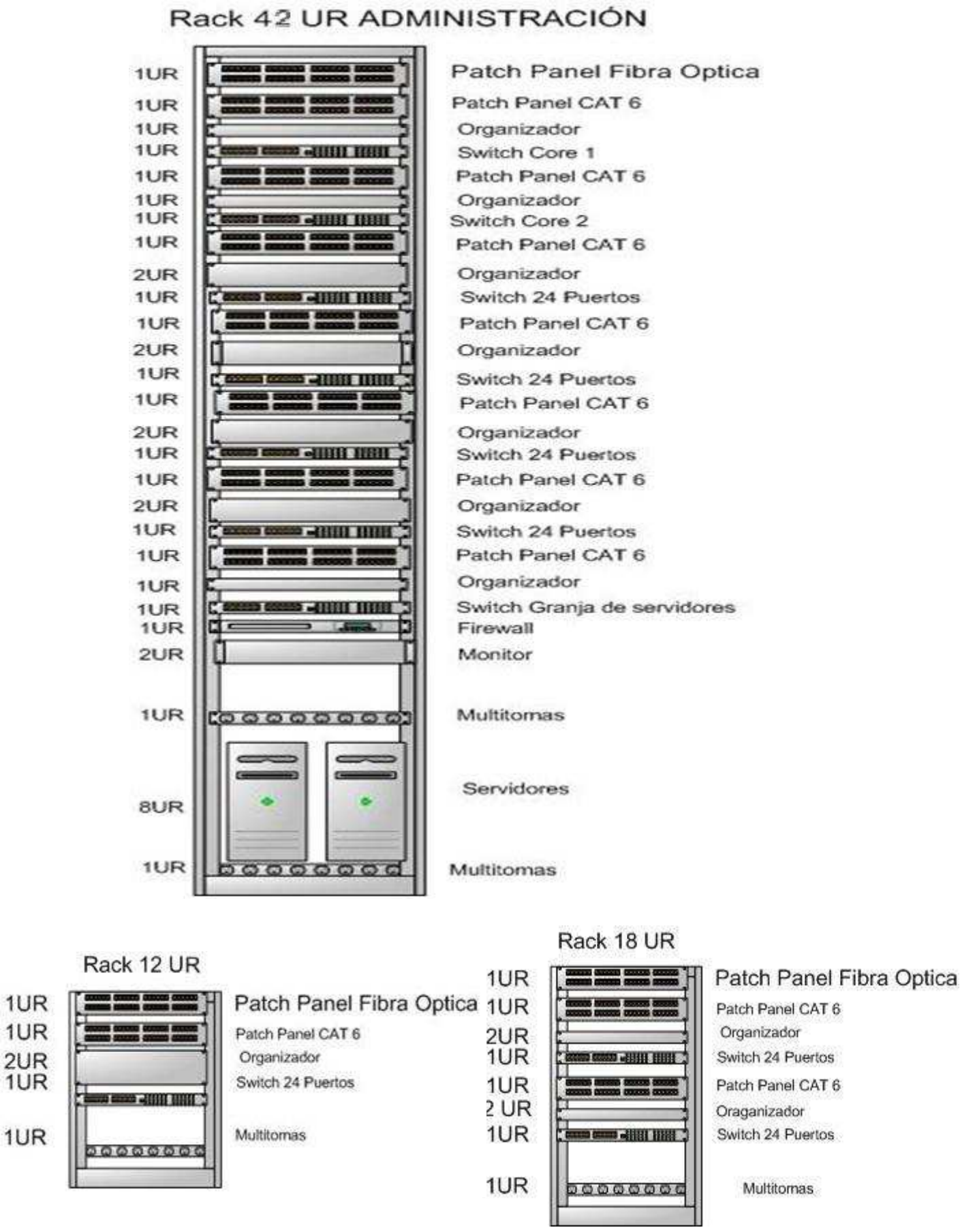


Figura 3.8 Disposición de elementos para los diferentes tipos de rack a utilizarse

3.4 DISEÑO DE LA RED DE ÁREA LOCAL INALÁMBRICA.

Las redes inalámbricas brindan movilidad a los usuarios y sirven como complemento a la red cableada cuando el acceso a esta en ciertos lugares no es posible, además brindan una solución para conexiones que se van a realizar de manera temporal, como por ejemplo invitados.

La red inalámbrica brindará los mismos servicios que la red cableada; razón por la cual se tomarán en cuenta sistemas de seguridad con autenticación de usuarios, cifrado de información, etc. para evitar problemas de seguridad inherentes a los medios de acceso compartido.

El Instituto Tecnológico Superior Central Técnico, dispone de una red cableada más no de una red inalámbrica. Como se ha descrito en el capítulo 2, las instalaciones de la Institución disponen de un cableado estructurado precario para su red.

La posible integración de nuevos usuarios, y las cambiantes necesidades departamentales, que eventualmente modifican la ubicación física de los miembros de la comunidad educativa, podrían generar un gran problema en la creación de nuevos puntos de red, o movimiento de los mismos por lo que se considera necesario brindar servicios de acceso inalámbrico a los usuarios que así lo requieran, especialmente en el área administrativa.

Con el propósito de disponer de un sistema de acceso inalámbrico para los equipos, solucionar los problemas de movilidad de los departamentos, y abaratar los costos de incluir nuevos usuarios a la red, se determina que la mejor opción es la creación de una red inalámbrica que coexista con la red cableada que actualmente se dispone.

Se proveerá servicios de red inalámbrica para sectores como: biblioteca, área de electrónica, área de electricidad, nivel superior, salón de actos, área administrativa y sector de aulas. La justificación para brindar cobertura inalámbrica en estas áreas se detallada a continuación. En la Figura 3.9 se especifica la ubicación de los *Access Points*.

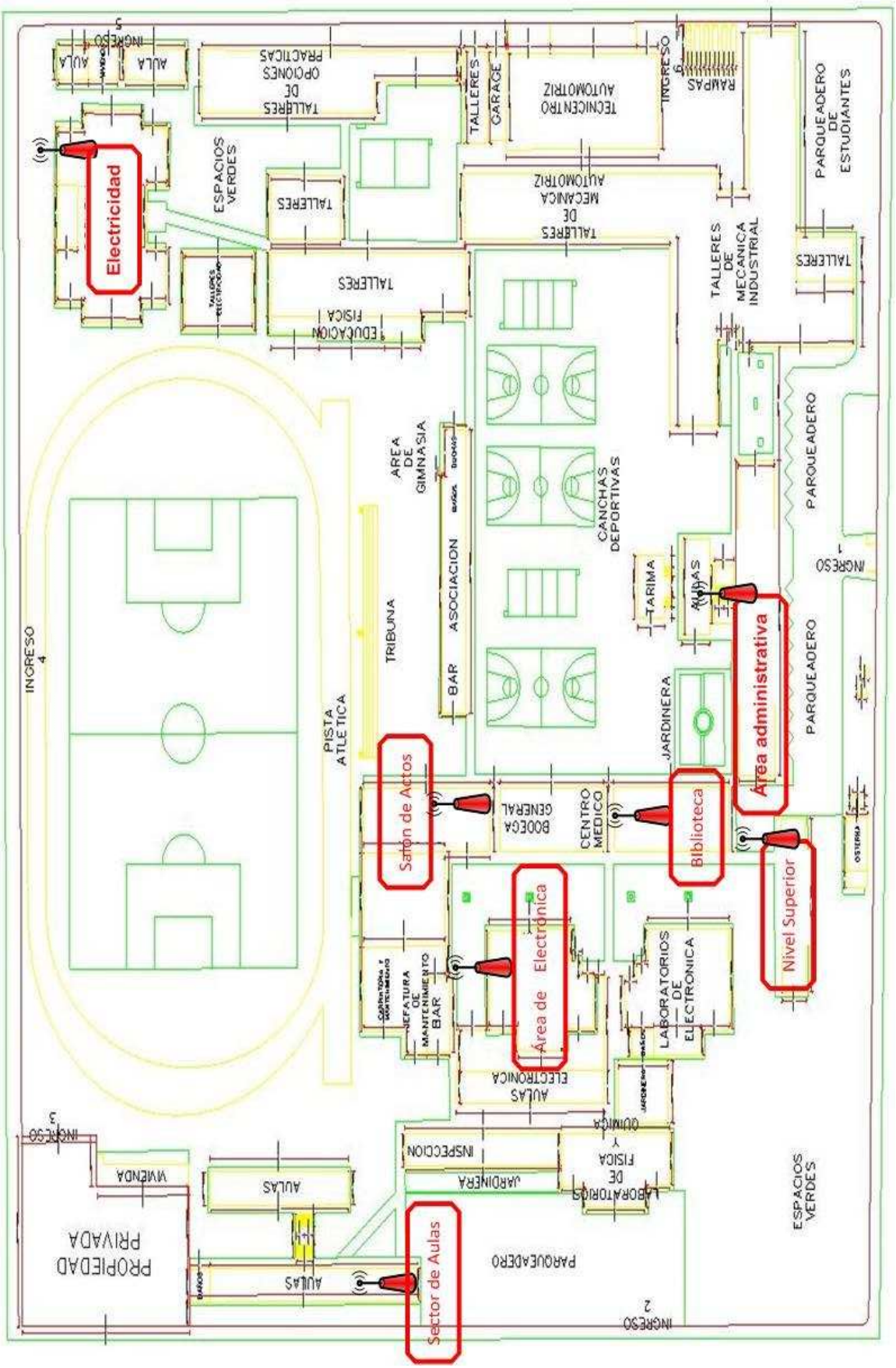


Figura 3.9 Ubicación de los *Access Point* a través del campus de la Institución

En base a las necesidades de los estudiantes y el personal de la Institución, los criterios para la instalación de puntos de acceso inalámbrico, son los siguientes:

• Biblioteca: Necesita del acceso inalámbrico debido a que es un centro de acopio de información; además de tratarse de un lugar en el que los usuarios van a ingresar con computadoras portátiles mediante las cuales van a acceder a la red.

Figura 3.10 Biblioteca

• Área de Electrónica: Al tratarse de un área relacionada con las tecnologías de la información necesita del acceso continuo tanto a Internet como a los demás servicios de red. Además de la red cableada que se va a instalar en esta área, se requiere de acceso inalámbrico, debido a la existencia de los laboratorios de electrónica digital y el centro de cómputo, como se muestra en la figura 3.11.

En estas dependencias los computadores ubicados son utilizados esporádicamente por lo que ubicar puntos de red fijos mediante el cableado sería un desperdicio. Además, en esta área los estudiantes en especial aquellos de los últimos años y los del nivel superior de la Institución acuden con computadores portátiles y necesitan del acceso a la red.

Figura 3.11 Laboratorio de computación en el área de electrónica

• Área de Electricidad: De la misma manera que en el área de electrónica, esta área se requiere el acceso inalámbrico a la red, debido a las aulas en las que los estudiantes acceden a la red por medio de dispositivos portátiles, como por ejemplo en el aula de mecatrónica donde se realizan actividades las cuales requieren de acceso a la red de datos.

• Nivel Superior: El nivel superior de la Institución posee laboratorios y demás dependencias donde ubicar puntos de red exclusivos para el uso de un usuario seria un desperdicio de recursos, además de lo expuesto los usuarios de esta área en su mayoría acceden a la red a través de computadores personales y dispositivos portátiles por lo que se hace imprescindible el uso de una red inalámbrica.

• Salón de actos: El salón de actos es un lugar donde se realizan los eventos formales de la Institución cuenta con un área de 120 metros cuadrados. Con eventos formales se hace referencia a actos protocolarios, seminarios, conferencias, reuniones entre otros. Debido a lo expuesto anteriormente se considera al salón de actos como un punto de acceso temporal, por lo que es necesario el establecer una red inalámbrica para este sitio que sin embargo al no ser un sitio de acceso permanente no estará activa todo el tiempo sino cuando la

situación lo requiera siendo responsabilidad del área de informática la activación de este servicio para este sector.

• Área administrativa: El área administrativa por su carácter de punto de consolidación de información necesita acceso inalámbrico. Esta área se puede dividir en tres partes:

- Zona de servicio social
- Secretarías
- Autoridades
- Laboratorios

En la zona de servicio social el acceso inalámbrico no es estrictamente necesario debido a que esta zona tendrá sus propios puntos de red y las estaciones de trabajo allí instaladas son fijas; sin embargo se encuentra dentro del área de cobertura de esta porción de la red y puede ser necesaria en algún caso excepcional.

En las secretarías el acceso a la red es fundamental, por lo que el acceso inalámbrico, además de proveer acceso a la red directamente, proveerá un nivel de redundancia a la red en caso de existir algún problema con el acceso mediante la red cableada.

La zona de autoridades necesita el acceso inalámbrico por las reuniones que se llevan a cabo en esta zona, además del acceso de invitados a la red e incluso de las mismas autoridades que necesitan de acceso inalámbrico debido a las características de sus equipos personales.

Respecto a los laboratorios tal como se explico en el apartado 3.2.5 los accesos serán esporádicos durante las horas de clase, sin embargo estos serán necesarios cuando los estudiantes o profesores necesiten el acceso a la red caso en el cual serán habilitados equipos de la Institución para este fin, que no estarán permanentemente conectados.

• Sector de aulas: El sector de aulas se proyecta como un punto de acceso inalámbrico para poder integrar el uso de las tecnologías de la información al

proceso de formación diaria de los educandos. Los profesores y estudiantes podrán hacer uso de la red mientras estén en clases, por ejemplo para acceder a los servicios de almacenamiento de la red.

La implementación de la red inalámbrica en esta área de la Institución se implementará como una solución de acceso temporal, por la falta de recursos económicos de la Institución. Para cada una de las aulas, de manera posterior, serán instalados puntos de datos como parte del Sistema de Cableado Estructurado. Estos puntos serán la mayor parte del tiempo para el uso de los profesores por lo que la red inalámbrica será para el servicio de los estudiantes, en la figura 3.12 se muestra una imagen del sector de aulas del Instituto.

Figura 3.12 Aulas del Instituto

3.4.1 TIPO DE APLICACIONES SOPORTADAS

Las aplicaciones que se ejecutarán sobre la red inalámbrica serán las mismas que las indicadas para la red cableada: acceso web, correo electrónico, descarga de archivos, etc. con las consideraciones relativas a una red inalámbrica como por ejemplo que su velocidad de acceso dependerá de la distancia al punto de acceso.

Un punto a ser tomado en cuenta para la red inalámbrica es que el tráfico cursado a través de ella será en su mayoría para el acceso a Internet tanto de los

usuarios permanentes así como de los temporales, estos valores de tráfico y número de usuarios ya fueron analizados en el numeral 3.2.5.

3.4.2 MATERIAL DE CONSTRUCCIÓN DE LAS ZONAS DE COBERTURA DE LA RED INALÁMBRICA

Las diferentes áreas en las que se va a tener el acceso a través de la red de área inalámbrica están construidas de diferentes materiales, sin embargo el material preponderante en estas edificaciones es el ladrillo, por lo que estas edificaciones se consideran como de paredes gruesas. En la zona de aulas y en el nivel superior por el contrario las paredes son de materiales porosos como bloque prensado por lo que por el contrario se podrían establecer estas como paredes finas.

Esta disociación es importante debido a que el interior del área administrativa es un espacio abierto solo separado por divisiones modulares, por lo que un *Access Point* sería suficiente.

En la zona de aulas la interferencia aumenta, debido a que se debe atravesar varias paredes, sin embargo ubicando el *Access Point* en un punto central de esta área se puede tener una cobertura adecuada. Cabe señalar que se recomienda realizar pruebas de *site survey* activo con los equipos a instalarse y de esta manera determinar las áreas de coberturas reales en cada uno de los puntos donde van a ser instalados los dispositivos para el acceso inalámbrico.

En el ANEXO C se especifican las pruebas realizadas con un equipo real donde en los lugares críticos como Aulas, Electrónica y Biblioteca, se observa el nivel de intensidad de señal que llega a las áreas donde se realizaron las pruebas.

Como se puede observar la ubicación de los *Access Points* en los sitios especificados, brindarían la cobertura necesaria sorteando las dificultades como atenuación de la señal debido a la pérdida sufrida al atravesar las paredes.

Se debe tomar en cuenta este factor ya que las ondas electromagnéticas se comportan de diferente manera en relación a los distintos materiales con los que puede estar construido un edificio. A continuación, en la tabla 3.29 se indican los

materiales con los que comúnmente se encuentran construidos los edificios y la atenuación de señal que estos presentan.

Obstáculo	Pérdida de señal
Espacio Abierto	0 %
Ventanas	De 30% a 50%
Paredes Finas	50%
Paredes Gruesas	80%
Suelos y techos	80%
Maderas	70 %

Tabla 3.29 Pérdida de señal por el material de construcción de los materiales[T3]

3.4.3 ÁREAS DE COBERTURA

Cabe anotar que las áreas de cobertura en este caso fueron tomadas solo teóricamente debido a que no se cuenta en este momento con los equipos necesarios para poder determinar las áreas de cobertura reales por medio de un *site survey* activo. Para determinar el área de cobertura del *Access Point* se considera el radio de cobertura *Indoor* del equipo desde el lugar seleccionado para su instalación.

Las distancias a ser cubiertas por los *Access Points* en las diferentes áreas están descritas en la tabla 3.30.

Áreas	Distancia máxima (m)
Biblioteca	15
Área de electrónica	10
Nivel superior	30
Salón de actos	10
Área administrativa	10
Sector de aulas	12

Tabla 3.30 Máxima distancia que debe cubrir el *Access Point* en el área a ser instalado

De la tabla anterior se puede deducir que los rangos de cobertura *indoor* de 30 metros de los equipos estandarizados en 802,11g, como se puede apreciar en la tabla 3.30, se acoplan perfectamente a la cobertura. Como se dijo anteriormente se deben realizar *site surveys* activos para determinar los rangos reales y en caso

de que ser encontrados problemas de cobertura; se recomienda instalar otro *Access Point* en estos puntos, para brindar el servicio al área que lo requiera. De la misma manera se debe seleccionar un lugar estratégico para poder cubrir los sectores de interés.

3.4.4 CONEXIÓN DE LA WLAN CON LA RED CABLEADA

Para la interconexión de los *Access Point* se deben establecer puntos de red exclusivos para la conexión de estos equipos a la red en las áreas requeridas lo cual deberá ser detallado y documentado por el administrador de la red. Se debe tomar en cuenta también tomas eléctricas para la alimentación de estos dispositivos o en su defecto se recomienda el uso de equipos que cumplan con la norma 802.3af (*PoE, Power over Ethernet*) con lo cual el equipo es alimentado de electricidad simplemente con su conexión al equipo de red al que pertenece.

3.4.5 VELOCIDAD DE TRANSMISIÓN Y FRECUENCIA DE OPERACIÓN

Los estándares actuales para la operación de redes inalámbricas con sus respectivos parámetros se presentan en la tabla siguiente:

		801.11b	**802.11ª**	**802.11g**	**802.11n**
Velocidad		11 Mbps	54 Mbps	54 Mbps	450 Mbps
Rango	Interiores	30 - 45 mts	7 – 25 mts	30 - 45 mts	70 – 230 mts
	Exteriores	120 – 390 mts	140 – 460 mts	250 – 820 mts	250 – 820 mts
Frecuencia		2.4 GHz	5 GHz	2.4 GHz	2.4 – 5 GHz
Utilización		Puntos de acceso público al Internet	Común en oficinas y ambientes corporativos	Compatible con las especificaciones técnicas de 802.11b	Compatible con todos los estándares anteriores

Tabla 3.31 Parámetros de funcionamiento de los estándares 802.11[F6][W36]

Actualmente los estándares 802.11a y 802.11b se encuentran en desuso, además sus características son inadecuadas para el proyecto por lo que quedarían desechadas; como alternativa, el estándar 802.11g es el más utilizado actualmente y la mayor parte de equipos inalámbricos lo usan para su conexión.

Sin embargo la tendencia del mercado es utilizar el nuevo estándar 802.11n por lo que se recomienda el uso de equipos compatibles con estos dos últimos, por su penetración en el mercado así como sus mejoras respecto a las características de operación. Además de considerar el funcionamiento a largo plazo de la red por o que este estándar sería el más adecuado.

También se recomienda que posean certificación *Wi-Fi* para asegurar su interoperabilidad con equipos inalámbricos de diferentes fabricantes.

3.4.6 IDENTIFICADORES DE LA RED SSID Y SEGURIDAD DE ACCESO A LA WLAN

Los identificadores de acceso a la red serán dados por el administrador de red; sin embargo se recomienda no utilizar nombres que expresen literalmente la utilidad de red inalámbrica de la Institución, para evitar posibles problemas de accesos no deseados o intrusiones en los datos de la red de la unidad educativa. En la tabla 3.32 se especifica la recomendación para asignar estos identificadores conocidos como *SSID*.

ÁREAS	SSID
Biblioteca	Ct_Biblio
Área de electrónica	Ct_Elec
Área de electricidad	Ct_Elct
Nivel superior	Ct_Tec
Salón de actos	Ct_Act
Área administrativa	Ct_Adm
Sector de aulas	Ct_Gen

Tabla 3.32 Identificadores para la red inalámbrica

3.4.7 RECOMENDACIÓN PARA LA SEGURIDAD DEL PUNTO DE ACCESO INALÁMBRICO

Debido a que el medio inalámbrico es de acceso común este es uno de los puntos más vulnerables en una red, cualquier persona podría interceptar la información que atraviesa a través de este medio poniendo en peligro los datos de la Institución. Por esta razón, es necesario establecer protocolos de seguridad

adecuados que protejan el acceso a través de este medio, tal como se analizó en el apartado 1.6.5.

Se debe utilizar un sistema de cifrado para proteger este medio, en un principio las redes inalámbricas utilizaban sistemas basados en *WEP (Wireless Equivalent Privacy)*, que como lo indica su nombre pretendía el dar un nivel de seguridad equivalente a la red cableada. Sin embargo el algoritmo de cifrado utilizado por *WEP* presentaba varias fallas, en la actualidad este esquema puede ser fácilmente vulnerado por medio de software accesible a cualquier persona. Aunque puede ser utilizado en conexiones donde los datos no sean altamente sensibles.

Para solucionar esta vulnerabilidad se adopto el sistema *WPA (Wi-Fi Protected Access)* que cambia el algoritmo de encripción, utiliza *TKIP (Temporal Key Integrity Protocol)* para volverlo más robusto con el objetivo de adoptar lo establecido por la *WiFi Alliance.*

Existe también la versión WPA2 que utiliza un algoritmo mucho más robusto que *TKIP* que es *CCMP (Counter Mode with Cipher Block Chaining Message),* basado en *AES (Advanced Encription Standar),* por lo que es generalmente denotado de esta manera. WPA2 es; además obligatorio para dispositivos certificados *Wi-Fi* desde 2006.

Para la distribución de las claves de autenticación existen dos métodos:

- *Personal,* diseñado para el hogar y pequeñas oficinas donde la clave es la misma para la autenticación de los usuarios con el punto de acceso.
- *Enterprise,* el cual utiliza un servidor *RADIUS* para la autenticación con lo que se dará restricciones en el acceso a la red.

Estos esquemas pueden ser utilizados tanto con *WPA* como con *WPA2,* por lo que se recomienda el uso de un esquema *WPA2 Enterprise* que presenta las características adecuadas para el proyecto.

3.4.8 RECOMENDACIÓN PARA LA SELECCIÓN DEL PUNTO DE ACCESO INALÁMBRICO

En el mercado existe una variedad de fabricantes de equipos para el acceso a la red de manera inalámbrica. El uso de estos equipos, brinda soluciones en la medida en que el acceso a través de la red cableada resulta complicado o se necesita asegurar la movilidad de los usuarios.

Los equipos a ser utilizados deberán cumplir al menos con los requerimientos mínimos descritos en la tabla 3.33.

Velocidad de transmisión	**54 Mbps**
Protocolo de interconexión	IEEE802.11g, IEEE802.11n
Protocolo de gestión	SNMP, HTTP
Algoritmo de cifrado	SHA, MD5, AES
Encriptación	TLS, PEAP, TTLS, TKIP, WPA, WPA2
Método de autenticación	RADIUS
Interfaces	*Ethernet* RJ45 (10 BaseT/100BaseTX)
Cumplimiento de normas:	*IEEE* 802.11x, 802.11g, 802.11n, 802.3af, 802.3u, 802.1q, 802.1p
Características adicionales	Filtrado de direcciones, *firewall*, *DHCP*
Protecciones contra condiciones ambientales variantes solo para los *access points* a ser ubicados en exteriores	

Tabla 3.33 Características mínimas de los *Access Points*

3.5 TELEFONÍA IP

3.5.1 REQUERIMIENTOS DE VOZ

Los requerimientos de la red de voz serán analizados tanto para los usuarios existentes en la red de voz así como para los usuarios que tendrán una extensión telefónica a partir de la implementación del proyecto.

3.5.1.1 Número y tipo de usuarios de la red de voz actual

El servicio telefónico provisto en la unidad educativa está dirigido al personal que labora en la Institución, con un espacio físico fijo para su trabajo. Actualmente, el personal de la Institución está conformado por 301 personas, distribuidas por grupos de la siguiente manera: 55 administrativos, 246 docencia (profesores,

inspectores, autoridades). Es importante mencionar que no todos poseen una oficina o espacio de trabajo fijo determinado por lo que no todos tendrán un punto de voz.

Del personal citado anteriormente, se tiene que las extensiones existentes abastecen a 22 personas en el grupo de personal administrativo y 13 docentes. Es decir, 35 personas acceden a la red de voz analógica que se encuentra actualmente en funcionamiento, esto implica que el número de extensiones es muy reducido en función de las necesidades del personal de la Institución.

El número de extensiones telefónicas será determinado en función del número de usuarios que van a tener acceso a la red de voz, por medio de la nueva red de datos integrada.

3.5.1.2 Número y tipo de usuarios de voz para la nueva red

Actualmente se cuenta con 35 extensiones telefónicas en la Institución y la proyección es que todos los espacios con oficina fija tengan una línea telefónica. Tal como se especificó el número en el punto 3.1.2, el número de puntos de voz para extensiones telefónicas a ser implementadas será de 52.

Además de los puntos específicos para teléfonos IP existen otras maneras de acceder a la red de voz, un ejemplo claro son los denominados *softphone.* Este software, instalado en computadores con las características adecuadas, proporciona funcionalidades similares a los de los teléfonos en *hardware.* De esta manera, en el computador asignado para uso personal, se puede tener también el dispositivo necesario para la comunicación de voz. Con esto se pretende hacer generalizado el uso de este servicio en la Institución, sin necesidad de incurrir en gastos mayores.

Otro dispositivo que puede ser implementado es un conversor analógico - IP para poder reutilizar los teléfonos analógicos en la red integrada, aunque estos no van a poder beneficiarse de las características adicionales que brinda este sistema, debido a que estos dispositivos la única función que realizan es la conversión de la señal analógica a señal digital para su transmisión a través de la red.

3.5.1.3 Circuitos troncales hacia la red pública telefónica

Los circuitos troncales son las líneas telefónicas que permiten la interconexión hacia la red telefónica pública. Para realizar un adecuado dimensionamiento se deben considerar las llamadas que se realizan y su promedio de duración en un intervalo de tiempo.

Los datos de la central telefónica no pueden ser accedidos debido a un error en el software del dispositivo, lo que hace imposible la extracción directa de estos; por lo que se toma en cuenta la información obtenida de las encuestas realizadas al personal que posee una extensión telefónica en el Instituto, que arroja un máximo de 10 llamadas externas en una hora tal como se ha especificado en el ANEXOD.

Para complementar esta información se coteja estos datos con los proporcionados por la secretaría de la Institución, en la tabla 3.34, se muestran datos de ejemplo, de las mediciones realizadas presentadas en el ANEXO F, correspondientes a los días 16 de Agosto, 14 de Octubre, 17 de Diciembre con el fin de determinar las horas pico y los máximos de ocupación de la central telefónica.

	16 Agosto	14 Octubre	17 Diciembre
7 – 9	2	3	1
9 – 11	14	7	3
11 – 13	12	26	15
13 – 15	15	19	18
15 – 17	9	4	8
17 – 19	4	2	4
19 – 21	0	3	1
21 – 23	0	1	1

Tabla 3.34 Llamadas realizadas y recibidas en intervalos de dos horas durante los días de prueba

De estos datos se puede concluir que las horas pico de utilización del canal están entre las 11 y las 15 horas y que el número máximo de llamadas en estos intervalos es de 26 por lo que tendríamos un máximo de 13 llamadas por hora, este valor se acerca al máximo valor proporcionado en la encuesta que es de 11 llamadas hacia teléfonos exteriores en una hora.

La unidad adimensional *Erlang* se define como un canal utilizado de forma continua, es decir cuyo grado de ocupación es del 100 % por lo que se utiliza la ecuación 3.1 para determinar la intensidad de tráfico representada por A, donde C representa el número de llamadas y T su duración promedio, durante una hora como la intensidad de tráfico que atraviesa por la central telefónica.

$$A = C \times T$$

Ecuación 3.1[L3]

De los valores especificados anteriormente, se estiman los valores máximos de estos parámetros. Estos valores son considerados críticos debido a que se han considerado los valores máximos obtenidos tanto en las encuestas como por los datos de secretaría, especificados en los anexos.

Número máximo de llamadas en una hora = 13

Promedio de duración de las llamadas = 2 minutos

$$A = 13 \frac{llamadas}{hora} \times \frac{1\ hora}{60\ minutos} \times 2\ minutos$$

A = 0,43 *Erlangs*

Se debe tomar en cuenta la proyección de usuarios finales debido a que a partir de la implementación del proyecto el número de usuarios crece en función de los puntos de voz instalados, por lo que se utiliza la ecuación 3.2 para proyectar la intensidad de tráfico conocido el número de usuarios actuales.

$$A_f = \frac{U_f}{U_a} A_o$$

Ecuación 3.2[T4]

Donde Af = Intensidad de tráfico proyectado

Uf = Número de usuarios proyectados

Ua = Número de usuarios actuales

Ao = Intensidad de tráfico actual

$$A_f = \frac{U_f}{U_a} A_o = \frac{58}{35} 0{,}43 = 0{,}718\ Erlangs$$

Lo que da como resultado que el flujo de tráfico telefónico es de aproximadamente 0,72 *Erlangs*. La probabilidad de pérdida de llamadas, se considera debe ser del 1%, propio de sistemas telefónicos. Con estos datos y basados en las tablas de *Erlangs;* el número de troncales necesarias es de 4 tal como se puede observar en la figura 3.13 que representa la fórmula de *Erlang* B. Esta fórmula se aplica bajo la condición de que una llamada no se llega a realizar debido a que la línea está ocupada, no se pone en cola o se vuelve a intentar, se pierde para siempre.

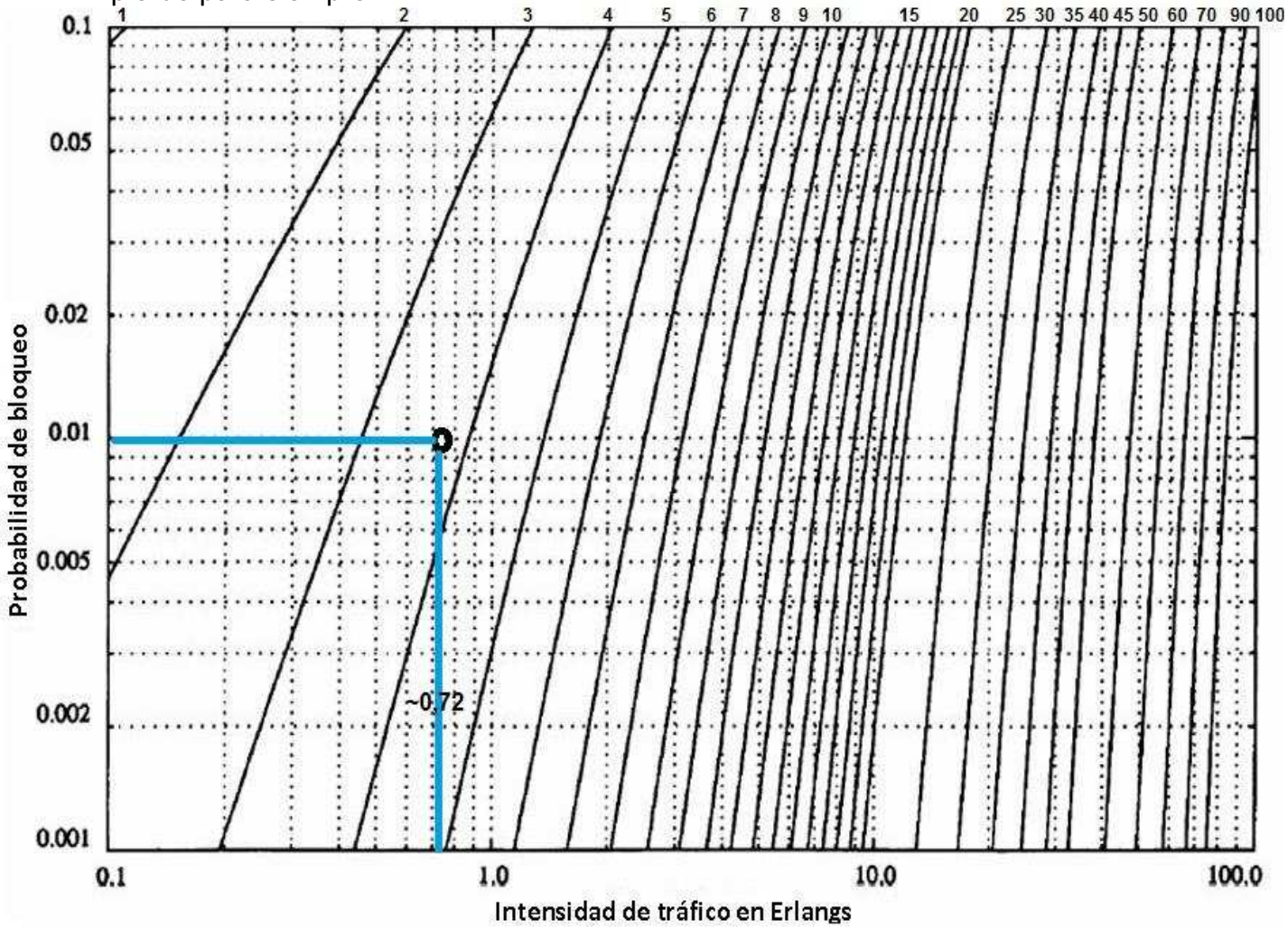


Figura 3.13 Figura que representa la fórmula de *Erlang B*[W39]

En la figura 3.14, se muestran los resultados obtenidos mediante una calculadora de *Erlang B* con la cual se obtiene los mismos resultados.

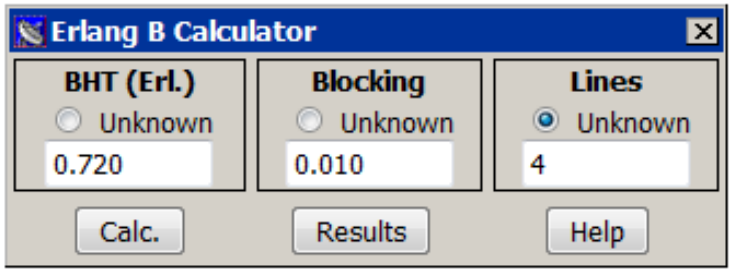


Figura 3.14 Calculadora de *Erlang B* [W40]

Como se analizó anteriormente estos valores son críticos y abastecen completamente a las demandas actuales de la Institución, sin embargo debido a que la red deberá estar en funcionamiento al menos durante 10 años se recomienda realizar un análisis detallado después del primer año de funcionamiento de la red y así establecer si la demanda aumenta debido al uso intensivo de la red por la masificación de la telefonía IP. De los resultados obtenidos se determinará la necesidad o no del aumento del número de troncales.

Nota: Seleccione un criterio de Búqueda para obtener un resultado más rápido.

Por Razón Social: PICHINCHA / INSTITUTO TECNOLOGICO SUPERIOR CENTRAL — Buscar — Limpiar

FORMA DE USO:

- Seleccione la provincia o el criterio de búsqueda
- Si el criterio de búsqueda es por NUMERO TELEFONICO, escoja el código de provincia y digite el NUMERO TELEFONICO
- Si el criterio de búsqueda es por RAZON SOCIAL, escoja la PROVINCIA e ingrese el NOMBRE DE LA EMPRESA
- Si el criterio de búsqueda es por NOMBRE, escoja la PROVINCIA y digite preferiblemente los APELLIDOS y NOMBRES.
- Posterior a esto presione ENTER o clic en BUSCAR

Para nuevas búsquedas puede volver a ingresar los datos o dar clic en el botón LIMPIAR e ingresar nuevamente los datos

:: DATOS TELEFONICOS ::

Número Telefónico	Razón Social / Nombre del Propietario	Dirección	Localidad
22240977	COLEGIO CENTRAL TECNICO / INSTITUTO TECNOLOGICO SUPERIOR CENTRAL TECNICO	AV GASPAR DE VILLARROEL SN	QUITO
22245449	COLEGIO CENTRAL TECNICO / INSTITUTO TECNOLOGICO SUPERIOR CENTRAL TECNICO	GASPAR DE VILLARRUEL 1274 Y AV AMAZONAS	QUITO
22274931	COLEGIO CENTRAL TECNICO / INSTITUTO TECNOLOGICO SUPERIOR CENTRAL TECNICO	AV GASPAR DE VILLARROEL E6-125 ISLA SEYMOUR	QUITO
22430925	COLEGIO CENTRAL TECNICO / INSTITUTO TECNOLOGICO SUPERIOR CENTRAL TECNICO	AV GASPAR DE VILLAROEL 1274 DPTO DE ORIENTACION VOCACIONAL 2DO PISO	QUITO
Número Reservado			
22448155	COLEGIO CENTRAL TECNICO / INSTITUTO TECNOLOGICO SUPERIOR CENTRAL TECNICO	INQ GASPAR DE VILLARROEL 1274	QUITO
22449044	COLEGIO CENTRAL TECNICO / INSTITUTO TECNOLOGICO SUPERIOR CENTRAL TECNICO	INQ GASPAR DE VILLARROEL 1274	QUITO
22275705	COLEGIO CENTRAL TECNICO / INSTITUTO TECNOLOGICO SUPERIOR CENTRAL TECNICO	AV GASPAR DE VILLARROEL E6- 125 Y ISLA SEYMOUR	QUITO
23343777	COLEGIO CENTRAL TECNICO / INSTITUTO TECNOLOGICO SUPERIOR CENTRAL TECNICO	DE LOS MORTIÑOS E14 120 Y DE LAS GROSELLAS SECTOR LOS LAURELES JARDIN DE INFANTES SECTOR LOS-LAURELES-JARDIN DE-INFANTES	QUITO
Número Reservado			
Número Reservado			

Figura 3.15 Especificaciones de líneas de salida a nombre de la Institución registradas en la CNT

Del análisis realizado anteriormente, se puede desprender que 4 troncales hacia la red telefónica pública son suficientes para satisfacer las demandas de los usuarios de la red. Debido a que en la actualidad según la información de la Corporación Nacional de Telecomunicaciones se encuentran 8 líneas telefónicas a nombre de la Institución que actúan como troncales telefónicas como se muestra en la figura 3.15.

3.5.2 CÓDEC DE AUDIO PARA LA TRANSMISIÓN DE VOZ

Con el fin de optimizar los recursos utilizados la transmisión de voz a través de la red de datos es necesario seleccionar un códec adecuado, debido a que de este depende la mayor o menor utilización del ancho de banda debido a la compresión utilizada por este. A continuación en la tabla 3.35 se presenta con las características de los códecs utilizados en telefonía.

Códec	Payload (bytes/paquete)	paquetes / segundo	Consumo de ancho de banda promedio WAN (kbps)		% reducción
			w/o compresión	w compresión	
G.711 (64 Kbps)	160	50	84	68.5	~18%
G.729A (8 Kbps)	20	50	27.5	13	~53%
G.723.1 (5.3 Kbps)	20	33	18	9	~50%
G.723.1 (6.3 Kbps)	24	33	19	10	~47%

Tabla 3.35 Especificaciones de los códecs utilizados en telefonía IP [F5]

De estos valores se puede considerar que el códec más adecuado para el presente proyecto es el G711 debido a su alta calidad, y su aceptable grado de aceptación de acuerdo al parámetro MOS donde G711 es aceptado como "*Toll Quality*"[32]. A pesar de que el ancho de banda requerido es el mayor entre todos los códecs, debido a que será utilizado únicamente en la LAN, este factor no es crítico. Este códec al no tener compresión también reduce el tiempo de procesamiento de los dispositivos, lo que resulta beneficioso para poder disminuir la latencia conservando la calidad de la voz.

[32] "*Toll Quality*" se refiere a una calificación mayor a 4 en una escala de 5 del MOS. G711 posee un MOS de 4.41. [W69]

3.5.3 CÁLCULO DE ANCHO DE BANDA

El sistema de telefonía a ser integrado en la red convergente de voz y datos para la Institución consumirá recursos tanto en procesamiento de los equipos encargados del *networking* así como del ancho de banda total de la red. Para calcular el ancho de banda necesario para el sistema se debe tomar en cuenta las cabeceras de sobrecarga que incrementa la red para el transporte de la información como son las de las tramas *IP, UDP y RTP* de los paquetes de voz además del tipo de enlace, el códec utilizado, las técnicas de compresión de cabecera y compresión de silencios.

En este caso al tratarse de una red local, se usa para la transmisión *Ethernet* utilizado como cabecera de la capa de enlace, es así como la trama completa de voz quedaría de la forma en que lo muestra la figura 3.16.

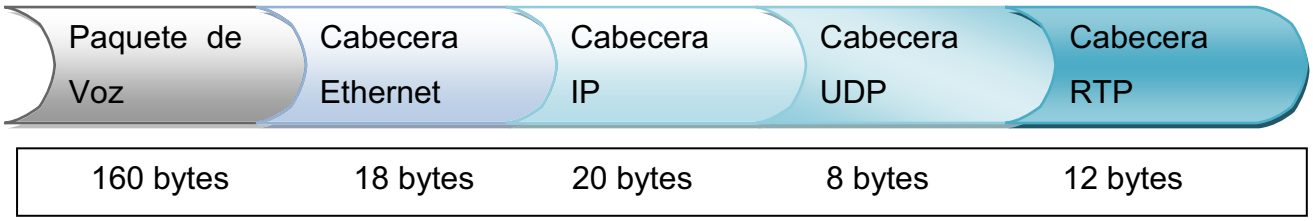


Figura 3.16 Formato del paquete VoIP

La suma del tamaño de las cabeceras de *IP, UDP y RTP* es de 40 bytes, si a este valor, por ser una red *LAN*, se añade el encabezado de 18 bytes de la trama *Ethernet,* se obtiene un *overhead* total de 58 bytes y el ancho de banda requerido se calcula mediante la ecuación 3.3.

$$AB_{requerido} = AB_{códec} \times \frac{Tamaño\ \text{del overhead} + \text{Tamaño del paquete de voz}}{Tamaño\ \text{del paquete de voz}}$$

Ecuación 3.3[T4]

A partir de la cual se calculan el valor de ancho de banda, tomando el valor del ancho de banda del códec G711 de 64 Kbps, tal como se indica en la tabla 3.33.

$$AB_{requerido} = 64\ Kbps \times \frac{58\ \text{bytes} + 160\ \text{bytes}}{160\ bytes} = 87.2\ Kbps$$

Lo que significa que son necesarios 87.2 Kbps por cada canal de comunicaciones, si se toma en cuenta una proyección de 52 usuarios a futuro se tendría un máximo consumo del ancho de banda de 4.5344 Mbps. Este valor

sería válido en si todos los usuarios estarían haciendo uso del servicio al mismo tiempo. Si se toma en cuenta el grado de simultaneidad de uso de la red telefónica, este valor se reduciría alrededor del 70 %, que resulta un valor que puede ser soportado sin problemas por la red con las características a implementarse.

$$AB_{total} = 87.2\ Kbps\ \times 52\ \ usuarios\ = 4.54\ Mbps$$

$$\text{Porcentaje de simultaneidad} = 30\ \%$$

$$AB_{total} = 87.2\ Kbps\ \times (52\ usuarios)0.3\ = 1.36\ Mbps$$

3.5.4 ALTERNATIVAS PARA LA IMPLEMENTACIÓN

Para la implementación del sistema de telefonía existen diferentes alternativas, en función de los requerimientos de la Institución y parámetros como la factibilidad de su implementación y la capacidad del sistema en general, tanto en número de usuarios como de llamadas; se escogerá la más conveniente y que ofrezca el mayor beneficio.

3.5.4.1 Solución IP por hardware

Los diferentes fabricantes de soluciones de *networking,* en el afán de integrar servicios en redes convergentes han fabricado equipos (*routers, switches*, etc) que a través del incremento de módulos implementa las diferentes funcionalidades de una central telefónica. En este caso específico sería una central completamente IP, es decir que integre las funcionalidades propias de un sistema de telefonía IP analizado en el apartado 1.3.2.1 en función de la arquitectura que utilicen (H323, SIP, etc).

Su funcionamiento está controlado por el denominado *Call Server,* el cual realiza funciones de gestión propias de una *PBX* tradicional (admisión, establecimiento, desconexión, tarificación de las llamadas, etc). Este servidor de comunicaciones puede ser único o estar constituido por varios servidores. Cada uno de estos servidores puede realizar las mismas funciones o pueden ser simplemente instalados para funciones auxiliares, como manejo de los archivos de sonido, descarga de archivos de configuración entre otros.

El tener varios servidores, distribuidos a través de la red, interconectados entre sí se denomina como "*clustering*". Esta técnica permite evitar puntos de falla comunes sin perder la operabilidad única del sistema global, es decir el cluster se comporta como un único servidor.

Si se trata de un entorno completamente LAN el servidor de comunicaciones podría trabajar perfectamente; sin embargo para la comunicación con redes externas se necesita del denominado Gateway o Switch de voz. Este dispositivo permite la interconexión con centrales externas o con la red pública telefónica; además permite la conexión con teléfonos analógicos mediante tarjetas FXS y con la red pública telefónica a través de tarjetas FXO. También realiza funciones suplementarias propias de la telefonía tradicional como envío de tonos de llamada, generación de timbrado etc.

Las terminales IP se conectan a puntos de datos provistos por tarjetas de línea instaladas en los switches de acceso de la red por medio de la cual acceden a la red interna o a través de una red pública en caso de acceso de usuarios remotos.

El hecho de implementar una solución de voz mediante elementos de networking, optimiza el uso de la red integrada al tener compatibilidad con la mayoría de protocolos empleados; además de tener un sistema único de administración de los equipos que conforman la red integrada debido a que estos equipos permiten su configuración y mantenimiento remoto.

Un sistema de estas características presenta problemas desde el punto de vista de escalabilidad e interoperabilidad, debido a que se debería comprar equipos de un solo fabricante para aprovechar todas las funcionalidades que ofrecería dicha solución. Este tipo de soluciones está dirigida principalmente a entornos empresariales de gran tamaño, donde es necesaria la interconexión de varias sucursales integradas en un entorno WAN sea privado o a través de la red pública. De lo analizado anteriormente, se deduce que esta solución no sería completamente factible para el presente proyecto.

3.5.4.2 Solución por central telefónica híbrida IP-PBX

Una central telefónica híbrida básicamente es aquella que puede soportar terminales de usuario de diversas naturalezas, sean éstos analógicos, digitales,

inalámbricos o IP, para lo cual necesitan diferentes tarjetas las cuales son adquiridas de acuerdo a las necesidades y la capacidad del sistema. En la mayoría de ocasiones utilizan una tecnología y protocolos propios del fabricante lo que restringe su integración, escalabilidad, funcionamiento y mantenimiento.

Las labores de mantenimiento de sistemas de este tipo se realiza mediante software especializado instalado en un computador personal o en su defecto por dispositivos fabricados específicamente para este fin.

En el caso de la Institución que posee una central Panasonic KXTDA200 esta central telefónica está instalada para manejar teléfonos tanto analógicos como digitales; sin embargo carece del módulo que permite su integración a la red de datos. Esta central soporta las operaciones propias de una *PBX* y mediante el sistema de procesamiento de voz tiene funciones avanzadas de telefonía como buzón de mensajes, llamada en espera entre otros que sin embargo no se encuentran en total funcionamiento.

Posee un módulo principal *MPR* el cual es la tarjeta principal de la central y controla todas las operaciones de la misma, el armario se alimenta a través de una unidad de alimentación (*PSU*)

A través del sistema central de control se puede: configurar los atributos, propiedades y limitaciones de cada elemento del sistema, agrupar extensiones, permitir o no salida de llamadas, horarios de atención, desvíos automáticos de llamada, etc.

Como se indicó en la tabla 2.8 necesita el módulo IP - GW 16 para la conexión hacia la red de datos a través de IP, este dispositivo actúa como *Media Gateway*, es decir no es posible la implementación de una red de VoIP únicamente con el servidor de comunicaciones como en el caso de la implementación por *hardware*.

Este dispositivo realiza funciones de procesamiento de las señales de voz debido a que realiza la integración de voz y datos en la red.

Los terminales telefónicos que funcionan para esta central telefónica deben ser Panasonic, debido a los protocolos que manejan por lo que respecto a la escalabilidad e interoperabilidad la solución representa un problema. Además las

consolas de administración y los módulos para poder integrar son escasos y requieren de personal especializado en este tipo de centrales para su funcionamiento y mantenimiento.

Debido a estas consideraciones esta solución quedaría descartada como opción para el presente proyecto, sin embargo se recomienda mantener el sistema actual para realizar una migración progresiva hacia el sistema IP en tanto los usuarios sean familiarizados y capacitados en el uso de las prestaciones del nuevo sistema.

3.5.4.3 Solución mediante servidores

Esta solución basa su funcionamiento en la arquitectura de un computador personal para el control de las actividades de la *PBX* mediante el uso del *software* adecuado, las funcionalidades son escalables a través de tarjetas *PCI (Peripheral Component Interface),* las cuales tiene funciones similares a las que utilizaría una *IP-PBX*, el número de estas depende de las aplicaciones, número de usuarios y procesador que sea utilizado.

Existen diversas soluciones para la implementación de centrales telefónicas IP a través de *software,* tanto en plataformas *Windows* como *Linux*, de las que se prefieren elegir aquellas que se implementan en plataformas de software libre tanto por la información de soporte así como por la reducción de costos; porque no necesita de la compra de licencias para su funcionamiento.

En el mercado la solución basada en software libre más popular es *Asterisk*, de la cual se derivan otras distribuciones basadas principalmente en esta plataforma como por ejemplo *Elastix* la más común.

Para la conexión hacia la red pública telefónica se utilizan módulos, que son utilizados para conectar con troncales mediante puertos FXO, donde se conectan las líneas telefónicas analógicas contratadas con el proveedor de servicios y las llamadas son enrutadas por la central a través de ellas.

La distancia que puede existir entre la central y el terminal del usuario son relativamente grandes, alrededor de 1 Km, con lo que no existiría problemas en implementar la solución dentro de un campus.

A estas centrales se pueden conectar diversos tipos de terminales IP como por ejemplo teléfonos IP nativos, terminales que se conectan directamente a la red, teléfonos analógicos con adaptadores y *softphones*; también es posible tener terminales analógicos conectados directamente a puertos *FXS* del servidor, el tipo de extensiones soportadas dependerá del *software* utilizado.

Este sistema es el que resulta más conveniente para la Institución debido a que es completamente escalable, simplemente se deberán instalar las tarjetas *PCI* adecuadas para su funcionamiento. Y entre las opciones que puedan surgir en el mercado se recomienda el uso de *Elastix* a las características de funcionamiento, escalabilidad e integración detallado el apartado 3.5.4.4.

3.5.4.4 Características de la distribución utilizada

Se detallan las características principales por las que se escoge a la distribución *Elastix* como la solución para la telefonía IP del Instituto y se realiza una breve descripción del sistema *Asterisk* en la que se encuentra basada la solución.

3.5.4.4.1 *Asterisk* [W41]

Asterisk es un software de comunicaciones libre, desarrollado bajo licencia *GNU General Public License*, que permite crear una central telefónica a partir de un computador ordinario.

Un sistema *Asterisk* puede funcionar como *Gateway* de voz, central *IP- PBX* o incluso para *call center* debido a su escalabilidad y habilidades en el manejo de funciones remotas.

Inicialmente desarrollado para sistemas *GNU/Linux* con arquitectura x86, mantenido por el equipo de trabajo de *Debian*; sin embargo puede funcionar bajo diversas plataformas como *OpenBSD, FreeBSD*[33] y *Mac OS X.* Para su interconexión con redes telefónicas analógicas o digitales los creadores de *Asterisk* recomiendan el uso de tarjetas *Digium;* sin embargo el sistema es capaz de soportar dispositivos de otras marcas.

[33] Sistemas operativos basados en *UNIX* por la universidad de *Berkeley* con funcionalidades que varían de acuerdo a su distribución. Usados para aplicaciones específicas de seguridad o criptografía

3.5.4.4.2 *Elastix* [W42]

Elastix nació como una interfaz para reporte de llamadas de *Asterisk* que cambió hasta convertirse en una distribución de este sistema, basada también en otros sistemas como *Hylafax, Openfire y Postfix*[34] para integrar sistemas de comunicaciones en un ámbito empresarial como se puede observar en la figura 3.17.

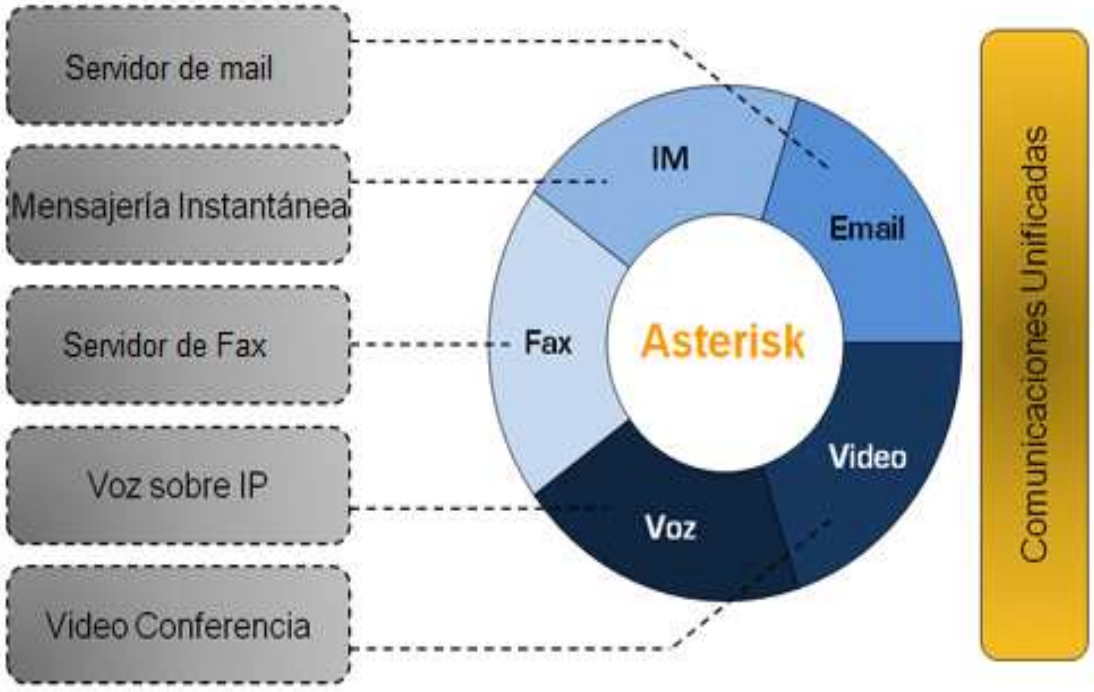


Figura 3.17 Integración de comunicación con *Elastix*[W42]

Elastix fue creado por la compañía *PaloSanto Solutions,* el sistema es distribuido en un disco que posee la instalación del sistema operativo *CentOS* más los paquetes necesarios para la instalación; sin embargo puede ser cargado también en sistemas operativos instalados con anterioridad y basados en *CentOS* ó *RedHat.* La última versión disponible es la 2.0.3 que es una versión estable del 15 de Noviembre de 2010. Al ser de distribución libre existe amplia documentación con respecto al tema además de diversos sitios web y foros de discusión y apoyo en Internet.

[34] *Hylafax* (Servidor de fax), *Openfire* (Servidor de mensajería instantánea) y *Postfix* (Servidor de correo)

Los *códecs* que soporta son G.711, G.722, G.723.1, G.726, G.729, *GSM, iLBC* (opcional) y protocolos como *IAX, SIP, HTTP, RTP, RTCP* entre otros; además de ser posible la conexión de interfaces tanto analógicas (*FXO/FXS*) como digitales. Posee una interfaz para detección de hardware. Posee un sistema de reconocimiento de voz completamente configurable y flexible.

Dentro de las opciones básicas de telefonía se pueden mencionar

- Grabación de Llamadas
- Centro de Conferencias con Salas Virtuales
- Correo de Voz
- Identificación de llamadas (*Caller* ID)
- Cancelador de eco integrado
- Configuración de Rutas entrantes y salientes
- Soporte para teléfonos con soporte para videollamada
- Soporte para grupos de timbrado
- Panel de Operador basado en Web
- Reporte de detalle de llamadas (*CDR*)

Es configurable vía *HTTP* mediante interfaz gráfica por parte del administrador, además de manejar protocolos como *SSH* y *HTTPS* para transacciones de datos seguras. Es completamente escalable respecto del número de usuarios y no necesita de licencias adicionales para añadir servicios. Por estos motivos es que *Elastix* es la opción más conveniente para el sistema telefónico IP del Instituto.

3.5.5 CARACTERÍSTICAS DE LOS EQUIPOS [L5]

El equipo que va a ser utilizado como servidor de telefonía se debe dimensionar adecuadamente para evitar la sobrecarga del sistema y la pérdida de llamadas o fallas en el servicio. El equipo deberá contar de preferencia con las siguientes características:

- Procesador.- Debido a la gran cantidad de operaciones matemáticas que debe realizar el equipo para cumplir las funciones de la central telefónica, este se puede considerar el elemento crítico para el buen funcionamiento del sistema. El tipo de procesador utilizado definirá el número de usuario

que se puede atender, un procesador con una velocidad de procesamiento alta acompañada de una eficiente unidad de punto flotante nos brinda confiabilidad en el sistema.

Un sistema considerado pequeño (hasta 10 teléfonos), se considera un sistema de aprendizaje y puede ser incorporado con un procesador de tipo Celeron de 433 a 700 MHz.

Un sistema mediano (de 10 a 50 teléfonos) como es el caso de la Institución por el contrario, puede ser implementado en uno o dos servidores donde cada uno se encargue de tareas diferentes. Sin embargo cabe tomar en cuenta que con las actuales capacidades de los procesadores, un procesador con varios núcleos puede ser utilizado de tal forma que cada uno de estos se encargue de las diferentes tareas del servidor, sin necesidad hacer más complejo el sistema mediante una solución con servidores independientes.

- *Motherboard*.- Deberá proveer la latencia necesaria para atender a las demandas del sistema, se deberán tomar en cuenta puntos como el tipo de tarjetas PCI que van a ser instaladas, en este caso específico en la Institución, para la interconexión con la red telefónica pública. Dependiendo si la tarjeta que va a ser utilizada es de 3,5 o 5 voltios es sistema deberá soportar el tipo de tarjeta tal como lo muestra la figura 3.18.

- Otra recomendación a ser tomada en cuenta es evitar el uso de *motherboards* con todo incluido por defecto debido a que es caso de falla de uno de sus componentes toda la tarjeta debería ser reemplazada, el proveedor recomienda el uso de tarjetas externa tanto para audio, video así como interfaces de red, sin embargo esto no implica que el uso de ellas no sea posible.

Figura 3.18 Tipos de ranuras para conexión de las tarjetas del sistema[L5]

- Alimentación.- La alimentación debe ser provista de una fuente confiable, de ser posible que se tenga un sistema de redundancia que puede ser una fuente adicional o un banco de baterías, y conectado a un UPS que le provea de energía libre de señales parásitas o sobrevoltajes.
- Tarjetas para conexión con la red pública.- Para la conexión con la red pública existen diferentes opciones como son las tarjetas analógicas, digitales, bancos de canales o *gateways.* En el caso de la Institución son necesarias tarjetas *FXO* analógicas debido al número de enlaces de salida y el tráfico que va a ser dirigido hacia la red telefónica pública, por lo general se pueden encontrar tarjetas que permiten manejar cuatro puertos para la conexión de líneas analógicas.

Finalmente se debe tomar en cuenta las características que se recomiendan por el fabricante para la implementación de un sistema *Elastix*.

Respecto de los teléfonos que pueden ser instalados en la Institución, se debe tomar en cuenta que los teléfonos que posee actualmente son analógicos lo que implica que estos deben ser reemplazados para poder disfrutar de las funcionalidades completas de la telefonía IP.

Los teléfonos analógicos actualmente disponibles, pueden ser integrados a la red mediante el uso de adaptadores telefónicos conocidos como *ATA* (*Analog Terminal Adaptor*). Estos adaptadores transforman las señales analógicas en digitales para que puedan ser transmitidas a través de la red de datos sin prejuicio

del tipo de información que llevan; sin embargo esta solución además de ser una solución temporal podría resultar mucho más costosa que la migración paulatina completa del sistema.

Como alternativa se propone el uso de teléfonos implementado mediante *software* o *softphones.* En el mercado existen diferentes soluciones de este tipo que incluso pueden resultar gratuitas o de bajo costo dependiendo del número de funcionalidades integradas ejemplos de esta solución pueden ser *eyeBeam, Xlite Zoiper* etc*.*

En conclusión, los requerimientos mínimos del servidor que alojará este sistema deben ser:

- Procesador dual core @700Mhz
- Memoria RAM 256 MB
- Doble fuente de alimentación
- Soporte para tarjetas PCI
- Tarjeta PCI FXO con soporte para 8 puertos analógicos

3.6 SERVICIOS DE VIDEO

3.6.1 VIDEOCONFERENCIA

La videoconferencia a ser implementada sobre la red de comunicaciones de la Institución será dimensionada con el fin de proveer servicios de video en tiempo real para la comunicación entre las diferentes áreas académicas de la Institución. Estos servicios serán prestados a través de un servidor en el cual residirá el programa principal de acceso a la videoconferencia, para los diferentes usuarios que así lo necesiten.

Una solución por medio de equipos especializados para el efecto resulta bastante ineficiente en este caso, debido a que el servicio va a ser utilizado esporádicamente, y que los equipos resultarían costosos con respecto a los beneficios a obtenerse. Existen diferentes posibilidades para la implementación de este servicio sin embargo la más adecuada resulta un servidor con interfaz web, donde los usuarios puedan conectarse a través de ella. De ser necesario el

acceso al servicio los usuarios deberían conectarse al programa por medio de una dirección o un enlace desde el navegador *web*.

3.6.1.1 Open Meeting [W43]

Open Meeting es una herramienta que permite realizar videoconferencias que utiliza una plataforma de *software* libre para su utilización, puede ser implementado sobre casi cualquier plataforma basada en Linux, e incluso tiene la posibilidad de ser instalado directamente desde un *live CD* con todos los servicios integrados previamente con un sistema operativo *Ubuntu.*

El uso de Open Meeting permite además el uso de la aplicación a través del Internet mediante un servidor propio instalado en la Institución o accediendo al servidor de la aplicación ubicado en el Internet, sin limitación en el uso o el número de usuarios.

Entre las características integradas de esta aplicación se pueden mencionar:

- Licencia Pública
- Integrado con *Moodle* y *SugarCRM*[35].
- Permite validación integrada con cuentas de *Facebook*.
- Tiene una administración que pasa por usuarios, organizaciones, salas, eventos.
- Se pueden organizar conferencias (en las que todos los invitados pueden participar) o auditorios (en los que el moderador puede hacer de conferenciante único o permitir algunas funciones a los invitados).
- Permite escribir texto, subir ficheros, poner puntero, controlar remotamente a los participantes de la videoconferencia.
- Se puede hacer uso Integrado con micrófono y webcam.
- Cualquiera de los participantes pueden mostrar el escritorio de su computadora, lo cual es muy útil para el uso en cursos a distancia.
- Soporta varios tipos de formatos de archivos para compartirlos durante una conferencia

[35] *Moodle:* Es un sistema de gestión de cursos para un ambiente educativo de distribución libre.
SugarCRM : Es un sistema empresarial para la gestión de clientes.
Facebook: Es un sitio web *de* redes sociales

- Contiene una pizarra donde lo que se escribe el moderador visualizado por los participantes.
- Se puede enviar invitaciones a otros usuarios por correo electrónico para que formen parte de una conferencia.

3.6.2 VIDEO SEGURIDAD

En la Institución se requiere proveer servicios de seguridad a nivel físico, es decir, los bienes materiales que pueden ser objeto de hurto o daño deben estar vigilados verificando y registrando actividades que se puedan convertir en siniestros de mayor o menor magnitud pero que afecten a los componentes de la comunidad educativa.

Con el propósito de proveer este servicio en la red integrada de voz y datos se utilizará la denominada video vigilancia IP, que se basa en el transporte de video a través de la red sea inalámbrica o cableada, sin necesidad de una red aparte para este fin como es el caso de los circuitos cerrados de televisión, CCTV (Circuito cerrado de televisión).

Como fue explicado en el capítulo 1, un sistema de video vigilancia a través de la red está compuesto principalmente de una cámara de red, el codificador de video (que se utiliza para la conexión a cámaras analógicas en caso de ser necesario), la red, el servidor y el equipo necesario para el almacenamiento, así como el *software* de gestión de video. Para la Institución se planea el uso de cámaras IP para los sitos más vulnerables.

3.6.2.1 Ubicación de las cámaras de seguridad

Como se explicó anteriormente, las cámaras serán ubicadas en puntos que sean sensibles con respecto a la seguridad, es decir, donde existan bienes materiales que precautelar.

Tomando en cuenta esta premisa y en base al estudio realizado con respecto a los bienes que se esperan proteger en la Institución se han tomado en cuenta los puntos detallados en la tabla 3.36 como los posibles puntos de instalación de cámaras de video vigilancia.

Número de cámara	Ubicación	Ubicación
1	Oficina autoridades	Interior
2	Secretaría	Interior
3	Cuarto de equipos	Interior
4	Nivel Superior	Exterior
5	Electrónica	Exterior
6	Mecánica Industrial	Exterior
7	Mecánica Automotriz	Exterior
8	Tecnicentro	Exterior
9	Ingreso a aulas	Exterior
10	Inspección	Interior
11	Biblioteca	Interior
12	Electricidad	Interior
13	Bodegas	Interior

Tabla 3.36 Lugares donde serán instaladas las cámaras IP

La ubicación exacta de las cámaras de seguridad se encuentra en el ANEXO B.
Se estima un factor de crecimiento del 40% con lo que se tendría un total de 16 cámaras, para el dimensionamiento total del ancho de banda de la red, por lo que se trata de un sistema de vigilancia relativamente pequeño.

3.6.2.2 Consideraciones para la elección de las cámaras

Existe una diversa cantidad de cámaras de este tipo, es por lo cual que se deben definir ciertos parámetros para la elección de una u otra en función del proyecto a ser implementado.

Definir el objetivo de video vigilancia es importante en la medida de detalle que se desee esperar, es decir si se desea como en el caso de los bancos el detalle de rostros de la personas que ingresan, o en las carreteras para por ejemplo identificar las placas de un automóvil, o como es el caso de la Institución registrar los movimientos generales de la gente.

La zona de cobertura determinará el tipo y el número de cámaras que se utilizarán además de las características específicas de las mismas, dependiendo de la zona a ser cubierta y factores como la distancia, la iluminación del lugar donde van a

ser ubicadas, la distancia entre ellas y con los objetos o áreas a cubrir, seguridad de las mismas y protección física de las mismas.

• **Calidad de imagen y resolución**: La calidad de la imagen dependerá del menor o mayor grado de detalle de la imagen que va a ser capturada esta puede ser baja, media o alta. Según estos parámetros se puede especificar la resolución de la imagen. Para el caso de la Institución una cámara con resolución de 640 x 480 provee la funcionalidad adecuada para las necesidades a cubrir.

• **Compresión:** Los tres estándares de compresión que ofrecen los productos de video en red son H.264, *MPEG-4* y *Motion JPEG*. El estándar H.264 es el que resulta más conveniente debido al alto ahorro de recursos que implica el uso del mismo.

No necesita la compra de licencias para su funcionamiento a diferencia de los otros; además se espera que este formato de compresión sea el más utilizado para implementar tecnologías de resolución de video de mayor capacidad. Este estándar es capaz de soportar cámaras con resoluciones en el orden de los mega píxeles debido a la alta compresión que ofrece, entre el 50 y 80 por ciento, con respecto a los otros.

Se recomienda la utilización de H.264, pero a fin de brindar flexibilidad al sistema, las cámaras a ser utilizadas deben soportar la mayor cantidad de estándares de compresión de video.

• **Audio:** Definir si es necesario el registro de audio para las cámaras, asegurar si éstas tienen audio incorporado o conectores para colocar dispositivos externos para tener audio unidireccional o bidireccional. En el caso de la Institución, el audio no es un punto crítico por lo que no se ha considerado para las cámaras a ser implementadas en el proyecto.

• **Funcionalidades de red:** Las cámaras deben tener características básicas de interacción con la red de datos, como por ejemplo incluir *PoE*, cifrado *HTTPS* para cifrado de secuencias de video.

Además la red deberá tener las características de seguridad necesarias para poder mantener a salvo la información transmitida por las cámaras, como por

ejemplo filtrado de direcciones IP, *VLANS* y permisos que eviten el acceso de personas no autorizadas a las cámaras y a los servidores de video.

• **Interfaz abierta y aplicaciones de software**: Los productos a ser instalados en la implementación del proyecto deberán asegurar la escalabilidad y compatibilidad con diferentes productos del mercado, es decir, deben asegurar que las aplicaciones tanto de grabación como de administración sean de interfaz abierta y permitan su actualización e instalación de una manera sencilla.

Los productos de video en red con interfaz abierta incorporada ofrecen mejores posibilidades de integración con otros sistemas. Asimismo, es importante que el producto esté respaldado por una buena selección de aplicaciones de software y software de gestión que permitan instalarlos y actualizarlos fácilmente, tanto a corto (6 ó 7 meses) como a largo plazo (8 ó 10 años).

Otras características que deben exigirse en una cámara son:

- Determinar que si resulta más adecuado el uso de cámaras fijas ó PTZ[36]. Una cámara PTZ permite cubrir una mayor área de cobertura debido a los movimientos que se pueden hacer con este tipo de cámaras, ofrecen un gran detalle de imágenes sin embargo proporcionan una vista reducida en comparación de una cámara fija la cual ofrece una mayor extensión de la cobertura.

- La vigilancia de las zonas puede cubrirse mediante varias cámaras fijas o pocas cámaras PTZ. Además se debe tomar en cuenta que las cámaras PTZ deben estar intervenidas constantemente por un operador para aprovechar sus capacidades.

- Considerar las condiciones de iluminación del lugar a ser monitoreado, y si el intervalo va a ser diurno o nocturno para así escoger cámaras más o menos sensibles a los estímulos luminosos y así estimar si es necesario o no dispositivos que brinden luz adicional.

[36] *PTZ (Pan:* Giro de 360 grados*, Titl:* Movimiento hacia arriba o hacia abajo*, Zoom:* Acercamiento*)*

- Evaluar el nivel de protección física que necesitaría el dispositivo para su funcionamiento óptimo. El dispositivo según su lugar de ubicación debe estar protegido tanto de condiciones ambientales adversas (humedad, lluvia, polvo, etc.) así como de actos vandálicos (robo, destrucción intencionada etc.). Por lo general para protegerlos de estos factores se escogen cámaras con carcasas o en su defecto aquellas que permitan ser montadas de manera que queden ocultas a simple vista.

En resumen se recomienda la utilización de cámaras con las siguientes características:

- Cámaras PTZ, opcional
- Resolución 640 x 480
- Interface Ethernet 10/100 Base T
- La mayor cantidad de estándares de compresión H.264, MPEG y JPEG.
- Protocolos TCP/IP, HTTP, TELNET, SNMP y DHCP
- Fotogramas mayor a 15 cuadros por segundo
- Protección para exteriores, para las cámaras que lo necesiten.

3.7 DIMENSIONAMIENTO DE LOS SERVIDORES.

En la granja de servidores se instalarán los servicios que toda la comunidad educativa necesita. Los servicios que a partir del estudio realizado en el capítulo 2, son considerados como primordiales para la Institución son:

- WEB: Para la publicación de la página de la Institución
- FTP: Almacenamiento de documentos para las labores de los miembros de la comunidad educativa, al que podrán acceder con permisos de solo lectura para evitar problemas de pérdida o modificació de la información.
- DNS: Resolución de nombres, en especial para el acceso a los servicios de la intranet. Este servicio permite utilizar nombres genéricos que sean fáciles de recordar para los usuarios en vez de las direcciones IP.
- DHCP: Para brindar la facilidad de tener un direccionamiento dinámico de los dispositivos finales de usuario, como por ejemplo los teléfonos IP, o los usuarios de la red inalámbrica.

- Correo Electrónico
- AAA: Permite la autenticación de los usuarios para evitar el acceso no autorizado a través del medio compartido por la red inalámbrica,
- Antivirus: Un servidor único de antivirus permite que las actualizaciones del mismo sean descargadas por el servidor y después distribuidas a los usuarios, disminuyendo el tráfico que supondría que cada usuario lo realice por separado.

Los servidores deben manejar compatibilidad, para el acceso a las prestaciones que brindan. Para lo cual es conveniente seleccionar un sistema operativo en común, este sistema operativo es *CentOs* en la versión 5.4.

Cabe destacar que se seleccionó este sistema operativo puesto que es *software* libre y de código abierto. Además que esta plataforma está basada en *Red Hat Enterprise Linux (RHEL).*

Una de la ventajas para escoger esta plataforma informática se debe a que este software está orientado para servidores, ampliamente probado y que las versiones del software son estables pudiendo ser actualizadas en cualquier momento.

Inclusive esta plataforma permite una fácil administración, y puesto que todos los servidores se instalarán con el mismo sistema operativo el soporte técnico para los servicios tendrá un costo menor, así como también el uso de esta plataforma no exige costo por licencias.

En la tabla 3.37, se listan las características para la instalación de *CentOs* versión 5.4, en parámetros de CPU, memoria RAM instalada y espacio en disco duro necesario para su instalación y funcionamiento.

REQUERIMIENTOS HARDWARE CentOS		
CPU	ARQUITECTURAS	*Intel (Intel Pentium I/II/III/IV/Celeron/Xeon)* *AMD K6/K7/K8,* *AMD Duron, Athlon/XP/MP)*
	VELOCIDADES	Modo texto: 200 MHz o mejor. Modo gráfico 400 MHz o mejor
	COMPATIBILIDAD	Arquitecturas X64: AMD64 Intel EM64T
MEMORIA	ARQUITECTURA X86_32	RAM mínimo para modo texto: 256 MB Mínimo de RAM para gráficos: 384 MB RAM recomendado para gráficos: 512 MB
	ARQUITECTURA X86_64	RAM mínimo para modo texto: 256 MB Mínimo de RAM para gráficos: 384 MB RAM recomendado para gráficos: 512 MB
DISCO DURO	El tamaño en disco dependerá del medio que se utiliza para la instalación, así como de los paquetes que se instalaron. El espacio puede ir de 90 MB hasta 175 MB	

Tabla 3.37 Requerimientos mínimos para la instalación del Sistema Operativo *CentOS*.[W70]

De la tabla de características para la instalación del sistema operativo *CentOS* se decide definir los parámetros para la instalación de los servidores para la Institución utilizando la plataforma antes detallada.

Procesador: 400 MHz o superior.

Memoria: 2 GB

Disco duro: 2 GB recomendado

3.7.1 HARDWARE Y SOFTWARE PARA LOS SERVIDORES

Una vez establecida la plataforma informática sobre la cual se instalarán los servicios es necesario conocer los requerimientos específicos para cada uno de los mismos. Por lo tanto se definirá la aplicación más adecuada para instalarse en cada servidor y características de hardware para un adecuado funcionamiento.

Con el fin de no saturar los servidores, facilitar la administración de los mismos, que se conviertan en problemas de seguridad o que estos equipos se conviertan en cuellos de botella dentro de la red se ha decidido separar los servicios de la siguiente manera:

- Servidor *WEB, FTP y DHCP*
- Servidor *DNS,* correo electrónico *y AAA.*
- Servidos de servicios en tiempo real, telefonía y video.
- Servidor de antivirus

Para los servicios *Web, FTP*, *DHCP, DNS,* correo electrónico *y AAA* se recomienda instalar estos servicios en un solo equipo que actúe como servidor, debido a que estos trabajan conjuntamente y los requerimientos de hardware no son críticos.

Por ejemplo, el servicio WEB además de la publicación de la página web del Instituto, alojará la base de datos de las notas del colegio para el acceso a ellas mediante una dirección pública. Para realizar este tipo de consultas hará uso del servidor *FTP,* a través de una interface segura para evitar ataques.

El servidor de correo electrónico, traducirá nombres como central.tecnico@centraltecnico.edu.ec, a direcciones IP para su comunicación en este caso un *Mail Server Agent*, razón por la cual hace uso del servidor *DNS.*

Sin embargo se recomienda la virtualización de estos servicios en dos sistemas operativos. Cabe recalcar que para esta solución las consideraciones de saturación de memoria, velocidad del procesador, y tamaño en disco son primordiales para que la solución no colapse y no se genere un cuello de botella en la red, debido al grado de simultaneidad de los usuarios. A continuación se presentan las recomendaciones para el software que brindará estos servicios.

3.7.1.1 Servidor *Web*

El servicio Web a utilizar dentro del Instituto Tecnológico Superior Central Técnico servirá para publicar su página web, y evitar el *hosting* que se venía manteniendo, de esta forma el personal de la Institución será el encargado de administrar la página y realizar cambios cuando ellos lo deseen.

El servidor Web tendrá la funcionalidad de aceptar y responder las solicitudes cuando realicen consultas por medio de protocolo *HTTP*. Uno de los beneficios de tener un servidor web en su red interna es el que los administradores pueden modificar y actualizar la información, además que ofrece escalabilidad y flexibilidad al sistema. La seguridad de la información podrá protegerse y se podrán ejecutar copias de seguridad en cualquier instante.

Se recomienda el uso de de software libre, por el hecho de ser los más utilizados además de la documentación y la facilidad de poder ser instalados y configurados sin la necesidad de licencias.

Entre los parámetros a ser tomados en cuenta para la elección del software para el servidor web se pueden mencionar:

La autenticación para negociar credenciales entre el servidor web y el navegador puede ser básica y encriptada. La autenticación encriptada es mucho más segura pues protege la contraseña enviada a través de la red a diferencia de la autenticación básica, que realiza este proceso en texto plano. Esto lo vuelve más vulnerable.

El protocolo *HTTPS,* permite la transmisión de información sensible de una manera segura a través de un canal cifrado.

Respecto del contenido dinámico se recomienda que soporte los siguientes protocolos:

CGI (Common Gateway Interface): Permite a un cliente solicitar datos de un programa ejecutado en el servidor web.

- *FastCGI*: CGI atiende una petición a la vez, con *Fast CGI* se incrementa su escalabilidad y rendimiento atendiendo varias peticiones al mismo tiempo.
- *SSI (Server Side Includes)*: Permite el uso del contenido dinámico, generado durante una petición.
- *PHP (Hypertex Pre-processor):* Permite la generación de páginas web dinámicas.

- *ASP.net:* Es un *framework*[37] comercializado por *Microsoft,* Permite la generación de sitios web dinámicos y servicios web *XML.*

Entre las opciones de software más conocidos para sistemas operativos *Linux* se pueden mencionar: *Apache, Cherokke, Tomcat, lighttpd, thttpd* A continuación, en la tabla 3.38, se presentan algunas de las características de cada uno de ellos.

Tomando en consideración esto se selecciona el software Apache, puesto que de este servidor *web* existe abundante soporte técnico en Internet; además de tener una arquitectura modular que permite añadir funciones adicionales si así es requerido por los usuarios.

Servidor	Última versión estable	Autenticación para el acceso	HTTPS	Consola de administración	Plataformas	Contenido dinámico
Apache HTTP Server	2.2.19 / Mayo 2011	Básica / encriptada	Sí	Sí	Windows / Linux	CGI, Fast CGI, SSI, PHP, ASP.net
Cherokee HTTP Server	1.2.98 / Mayo 2011	Básica / encriptada	Sí	Sí	Windows / Linux	CGI, Fast CGI, SSI, PHP
Apache Tomcat	7.0.14 / Mayo 2011	Básica / encriptada	Sí	Sí	Windows / Linux	CGI,SSI, PHP
Lighttpd	1.4.28/ Agosto 2010	Básica / encriptada	Sí	No	Windows / Linux	CGI, Fast CGI, SSI
Thttpd	2.25b / Diciembre 2003	Básica	No	No	Cygwin[38] / Linux	CGI

Tabla 3.38 Características de los servidores web considerados para la intranet.[P15]

[37] *Framework,* es un conjunto de pr[acticas (bibliotecas, procedimientos, etc.)en base a la cual otro proyecto de software puede ser organizado y desarrollado

[38] Cygwin es una colección de herramientas que permiten a Linux tener un ambiente de trabajo Windows.

Otra ventaja para utilizar este software es su robustez frente a las versiones ligeras como *lighttpd o thttpd.* Con respecto a la seguridad este servidor admite el uso de autenticación básica y cifrada, además del protocolo *HTTPS*. Finalmente su portabilidad permite su operación en cualquier plataforma sea *Linux o Windows*.

3.7.1.1.1 *Apache Server*[W71]

Apache server es un servidor *web HTTP* de código abierto implementado en *HTTP 1.1*. Entre otras, funciona bajo plataformas Linux, Windows y Macintosh. En la actualidad es el servidor web más utilizado en gran parte por sus características de configuración, bases de datos para autenticación y negociación de contenido.

Este servidor es principalmente usado para la publicación de páginas web tanto estáticas como dinámicas. Junto con *MySQL* (Servidor de base de datos) y los lenguajes de programación PHP/Perl/Python forman los sistemas *XAMP*, donde la primera letra indica el sistema operativo en el que funciona.

Además de las características mencionadas anteriormente, se pueden citar las siguientes:

- Modular: Puede ser adaptado a diferentes entornos y necesidades, con los diferentes módulos de apoyo que proporciona, e incluso se pueden desarrollar módulos específicos.
- Basado en hilos de procesos, que permiten obtener respuestas en menor tiempo
- Al ser altamente popularizado se pueden obtener informes de fallos y parches para la solución de los mismos.
- Se desarrolla de forma abierta
- Los módulos pueden actuar como filtros de contenido
- Soporte para IPv6
- Directivas simplificadas
- Respuesta a errores en diversos idiomas

3.7.1.2 Servidor *FTP*.

El servidor *FTP* es uno de los servicios básicos para la Institución, este permite que usuarios externos, colaboradores, miembros de la comunidad educativa, proveedores de servicios, puedan descargar información relevante como documentos, material bibliográfico, material educativo, catálogos, publicaciones, certificados, etc.

Los servidores *FTP* son usados incluso por otros servidores, como por ejemplo los servidores web para actualizar su contenido. Razón por la cual uno de los factores más importantes en la elección de uno debe ser la seguridad.

En este tipo de servidores es igualmente importante el asignar permisos a los diferentes usuarios, como se explicó anteriormente, para evitar la modificación o el acceso no autorizado a documentos sensibles.

Entre los servidores *FTP* para Linux se tienen: *vsFTPd, ProFTPd, PureFTPd*, en la tabla 3.39 se presentan las características de cada una de estas opciones.

Servidor	Características
vsFTPd,	Flexible Permite la utilización de usuarios virtuales Control de ancho de banda Limite de conexiones IP por usuario Encripción por medio de SSL Certificados digitales
ProFTPd	Autenticación por medio de LDAP Control de seguridad con TLS y SSL
PureFTPd	Encripción TLS Limitador de tráfico Integración con MySQL y LDAP

Tabla 3.39 Características de los servidores *FTP* considerados para la intranet.[P16]

Todas estas opciones de *software* permiten brindar el servicio que la Institución requiere, pero se selecciona la opción del servidor *vsftpd*. Se recomienda su uso debido a que es más seguro que los otros mencionados, sus versiones son

estables y su configuración es sencilla, tal como se menciona en diversas publicaciones web con respecto a estos aspectos.

Como por ejemplo que es el más utilizado en servidores con alta demanda de usuarios y que sus vulnerabilidades son mínimas.

Así también *vsFTPd* brinda una seguridad que resulta una ventaja frente a las otras opciones, además de utilizar mecanismos de autenticación por medio de protocolos *SSL* y el uso de certificados digitales.

3.7.1.3 Servidor DNS y DHCP

Un Servidor *DNS* tendrá la funcionalidad de traducir el nombre de un dominio a una IP, en el caso de la Institución el dominio para asignarse será:

@centraltecnico.edu.ec.

Al implementar este dominio los usuarios podrán acceder al sitio web como a correo electrónico institucional.

Para implementar este servicio es recomendable la utilización del servidor *BIND*, el cual viene por defecto los servidores con sistema operativo *Linux*. Este servicio permite eliminar la carga excesiva en la red además de ser de distribución gratuita.

Este servidor es el más utilizado, en general, por lo que puede llegar a ser considerado como un estándar de facto, lo que es muy importante pues funciona como una base de datos distribuida que mantiene información sobre las direcciones textuales de las redes.

Además de ser multiplataforma provee soporte en español. Su última versión es la 9.6.1b1 de marzo de 2009, la cual tiene solucionados problemas de seguridad encontrados en las versiones anteriores.

El servidor *DHCP* viene por defecto en todo las la distribuciones para servidores en *Centos,* por lo cual simplemente se debe configurar para asignar que las máquinas conectadas a la red reciban una IP dinámicamente, se recomienda esta alternativa debido al número de equipos finales del Instituto, pero será decisión de

los administradores asignar las direcciones IP dinámicamente o de manera estática.

3.7.1.4 Servidor de Correo Electrónico.

Entre las alternativas de *software* especializados para correo electrónico se han escogido aquellos que tienen características de ser los más comunes; además de ser de libre desarrollo.

Se han tomado en cuenta características como:

- *SMTP (Simple Mail Trasfer Protocol),* que es el estándar de Internet para la transmisión de correo electrónico. Puede ser transmitido de manera plana o por seguridad encriptado por ejemplo sobre *SSL (Secure Socket Layer*) o *TLS (Transport Layer Security).*
- IPv6 para asegurar funcionamiento con tecnología futura.
- El almacenamiento puede ser a través de una base de datos como por ejemplo *SQL, MySQL* o en un sistema de archivos donde los archivos son organizados en directorios dentro del sistema operativo
- Filtros *anitspam*,
  - *DNSSBL (DNS-based Block List),* es uno de los filtros antispam más utilizadosse basa en una lista de sitios bloqueados a través del servicio *DNS.*
  - *Gray Listing,* es un método de defensa donde un agente de correo bloquea aquellos mensajes enviados por remitentes no reconocidos hasta que puedan ser letigimados.
  - Las expresiones regulares hacen referencia a secuencias de caracteres que coincidan con palabras comunes. En un filtro antispam, por ejemplo pueden ser utilizados para rechazar correos con contenido relacionado a publicidad, contenido sexual entre otros.
  - Algunos servidores incluyen antivirus y *antispam* embebidos lo que protege a los usuarios de este tipo de mensajes.

Entre los servidores de correo más usuales se tiene *Postfix* (*Unix*), *Sendmail* (*Unix*), *Exim* (*Unix*), *Qmail* (*Unix*). En la tabla 3.40 se presentan las características de estas opciones.

Servidor	Plataformas	Características	Almacenamiento	Filtros Antispam
Postfix	Linux, Unix	SMTP, SMTP sobre TLS, IPv6, SSL,	Base de datos, Sistema de archivos	DNSSBL, *Gray Listing*, SPF, Expresiones regulares, antivirus y antispam incluidos
Sendmail	Linux, Unix	SMTP, SMTP sobre TLS, SSL	Sistema de archivos	*Gray Listing*
Exim	Linux, Unix, Cygwin	SMTP, SMTP sobre TLS, IPv6, SSL,	Base de datos, Sistema de archivos	DNSSBL, *Gray Listing*, SPF, Expresiones regulares, antivirus y antispam incluidos
Qmail	Linux	SMTP, POP3	Sistema de archivos	*Gray Listing*

Tabla 3.40 Características de los *mail servers* considerados para la intranet.[P17]

3.7.1.4.1 *Postfix*

Se selecciona el *software Postfix* como una alternativa efectiva para este servicio. Posee métodos de autenticación para *SMTP,* lo que hace que el envío y recepción de mails pueda realizarse a través de un canal seguro de comunicaciones. Puede ser configurado para utilizar almacenamiento tanto en una base de datos como en un sistema de archivos lo cual le brinda flexibilidad en el caso de que desee incrementar la capacidad o migrar hacia otro servidor.

Otras características de este servidor son:

- Diseño modular, que permite al administrador activar o desactivar diversas características según su utilidad; además de determinar los errores sus soluciones en caso de fallo del servicio.
- Seguridad además de los protocolos que maneja para la transmisión de los mensajes, posee filtros y restricciones de acceso para evitar tanto el correo no deseado como para proteger al servicio ante un ataque.
- Facilidad de configuración frente a otros servidores como sendmail o exim lo que permite a los administradores tanto brindar servicios de una manera más sencilla, asi como resolver problemas en un menor tiempo.

Pero para que *Postfix* pueda funcionar correctamente se necesita además instalar, *Dovecot* que incorpora protocolos *IMAP, POP3* para el funcionamiento del servidor. Sin embargo, es necesario anotar que por facilidad de administración del servicio se requiere de una interfaz gráfica para la revisión y envío de correos por parte de los usuarios. Para ello debe ser instalado paralelamente *Squirrelmail* que es una aplicación web, compatible con protocolos *IMAP, POP3* y basada en *PHP.*

3.7.1.5 Servidor AAA[P18]

Para los servicios a ser implementados en la Institución en especial el acceso a la red por medio de la red inalámbrica, se debe tener un servidor AAA que ofrezca características de autenticación, autorización, y registro. Debido a esto se considera los siguientes servidores: *freeRADIUS, OpenRADIUS,* por ser los que se encuentran con una mayor incidencia en el mercado, adem[as que se encuentran bajo licencia *GPL.*

El servidor a elegirse es el *freeRadius* debido a que permite interactuar con sistemas operativos *Linux*, es un *software* que no es licenciado y de distribución gratuita, además que soporta brindar el servicio para muchos usuarios en redes empresariales.

Incluye tanto el cliente como el servidor *RADIUS,* que incluyen una variedad de utilidades que pueden funcionar en diferentes plataformas. También permite responder de manera dinámica las peticiones almacenando las autorizaciones a estas en una base de datos lo que permite una respuesta más rápida.

Cumple completamente con los RFC 2865 y 2866, que son los estándares de Internet para el servicio *RADIUS,* soporta varios protocolos de autenticación y encripción (*EAP, LEAP, MD5, TLS, TTLS*) lo que hace que sea compatible con diferentes proveedores de equipos como *CISCO, JUNIPER, HP, MICROSOFT etc.*

Como se mencionó anteriormente, este servicio permite diversos tipos de autenticación, que asegura el correcto funcionamiento de toda la red, además que este servicio utiliza una base de datos que almacenará toda la información, esta

base de datos será *PostgreSQL*, para tener todo sobre la misma plataforma informática.

Se debe tener en cuenta que al realizar peticiones a este servidor la concurrencia será alta debido a la autenticación que deberá soportar para dar permisos a los usuarios de la Red del Instituto Tecnológico Superior Central Técnico.

3.7.1.6 Servidor de Antivirus.

Este servidor ayudará a mantener la seguridad de la red frente a ataques maliciosos. El mismo protegerá la información de virus, gusanos, etc. que puedan causar un potencial riesgo de seguridad. Además se tiene la facilidad de tener instalado este servicio en un equipo diferente, esto reduce la carga del servidor de correo que también necesita de éste. El servidor de antivirus provee fiabilidad y eficacia así como su administración deberá ser centralizada para los equipos conectados a la red.

Entre los servidores de antivirus más conocidos se tienen, *Kaspersky, ESET NOD 32, Symantec Norton Antivirus*. Todos estos productos comerciales necesitan de una licencia para poder ser actualizados y que brinden facilidad a los usuarios.

Para la elección del servidor antivirus se deben tomar en cuenta las siguientes características:

- Velocidad de escaneo
- Capacidad de actualización
- Capacidad de detección y remoción de virus
- Herramientas y facilidades disponibles

A continuación en la tabla 3.41 se presenta una tabla comparativa con algunas de las características de estos antivirus basados en referencias y mediciones realizadas por varios sitios de Internet.

Antivirus	Escaneo			Actualización		Detección			
	Rapidez	Tiempo real	Bajo demanda	Archivo de virus	Programa	Adware	Spyware	Falsos positivos	Detalle de detecciones
Kaspersky	HDD 80 GB 8 minutos	✓	✓	Horaria	Manual	✓	✓	3 – 4	Sí
ESET NOD 32	HDD 80 GB 25 minutos	✓	✓	Al encender el equipo	Manual	✓	✓	No	No
Symantec Norton Antivirus	HDD 80 GB 60 minutos	✓	✓	Semanal	Manual	✓	✓	No	Sí

Tabla 3.41 Características de los antivirus considerados para la intranet.[W72]

Si bien es imposible determinar cuál es el mejor antivirus, debido a que cada uno presenta diferentes funcionalidades y beneficios con respecto a una u otra característica, la mayor parte de las referencias consultadas sitúan a *Kaspersky* como el antivirus con un mejor rendimiento tanto en facilidad de uso, como en rapidez así como en detección de software malicioso.

Kaspersky Anti-Virus 2011 escanea la navegación web y los correos electrónicos. Monitoriza los programas en ejecución detectando la ejecución de procesos que puedan poner en riesgo al equipo. También posee herramientas de restauración del sistema para regresar a un estado anterior en caso de ser afectado de alguna manera.

Esta solución permite la protección de sistemas operativos *Windows o Linux*, lo que permite proteger tanto a los equipos de usuario como a los servidores.

Para la utilización de este servicio a través de la red se necesitan de dos entidades, la consola de administración y los agentes de red. La consola de administración define varias reglas y parámetros para la seguridad para

estaciones de trabajo y servidores; además de descargar las actualizaciones de Internet para distribuirla en las máquinas de la red. Los agentes de red trabajan directamente sobre los equipos realizando las funciones de escaneo, detección y eliminación.

3.7.1.7 Características de hardware para los servidores

Una vez definidas las características del software a ser utilizado en cada uno de los servidores de la intranet, se debe definir el hardware adecuado para que estos brinden la funcionalidad adecuado para el funcionamiento óptimo de la red.

Estos dispositivos deben asegurar ciertas características obligatorias para un servidor como:

- Robustez: Debe ser tolerante a fallas, debe asegurar su disponibilidad y de ser posible debe asegurar redundancia. Se considera que los servidores deben poseer una fuente de poder redundante.
- Rendimiento: Debe asegurar múltiples conexiones simultáneas por lo que debe ser multitarea, además que de preferencia se utilizará servidores con múltiples procesadores. Algo que se debe tomar en cuenta es que los servidores posean diferentes interfaces de red para poder tanto tener redundancia de comunicaciones como poder escalar los servicios de ser necesario.
- Debe tener la capacidad de ser escalable, para soportar el futuro crecimiento tanto de la red como de la Institución en general.

Para la implementación de la granja de servidores se considera dividirlos en tres equipos que alojarán los servicios:

3.7.1.7.1 *Servidor 1: WEB*, FTP, DHCP, DNS, *correo electrónico* y AAA.

Como se mencionó anteriormente, estos servicios serán alojadas por un solo equipo, sin embargo se dividirán en dos grupos para su administración.

El servidor WEB a ser instalado, como se explicó en el numeral 3.7.1.1, es el Apache Server 2.2.19, la última versión estable y que pude ser descargada del sitio web de *Apache HTTP Server Project.* El único requerimiento de hardware que recomienda el desarrollador es un espacio en disco de 50 *MB*, sin embargo

en otras fuentes, se pueden encontrar características más específicas como son la memoria RAM necesaria (entre 192 y 256 MB), la velocidad del procesador (superior a 250 MHz), y un disco duro de entre 4.5 y 8 GB, para el almacenamiento del contenido a ser publicado.

El servidor *vsFTPd,* de la misma manera no presenta características mínimas para su funcionamiento sin embargo en referencias se recomiendan las siguientes características: “Servidor a 250 Mhz, 256 MB RAM, 8 GB disco duro”.

Debido a que el servidor *FTP,* debe almacenar un número de archivos se debe considerar el espacio en disco duro disponible para el servicio en función de éstos, con el propósito de tener el suficiente espacio para aquello.

El servicio *FTP,* será utilizado por los usuarios administrativos y los profesores lo que completa un total de 300 usuarios, como se observa en la tabla 2.11. Se debe tomar en cuenta que no todos los usuarios van a hacer uso de este servicio por lo que se considera que este es el número máximo de la carga para el servidor, por lo que este servidor estaría sobredimensionado para preveer la expansión del servicio.

Si se considera que en los servidores *FTP,* que prestan estos servicios en Internet ofrecen en general es de 100 MB, se considera este valor aceptable para las necesidades de la Institución. Con lo que el espacio requerido para este servidor sería de 30 GB.

Para el diseño del servidor de correo electrónico, se considera a los usuarios potenciales de la red, 4866, detallados en el apartado 2.3, como valor máximo de ocupación. Se dimensiona el servidor proyectando que atenderá a un total de 5.000 cuentas para usuarios entre personal administrativo, profesores y estudiantes.

Las características de almacenamiento, se calculan en base al espacio asignado para el buzón que es de 50 Mbytes, que resulta un valor razonable si se toman en cuenta que un correo en texto plano, sin imágenes, archivos adjuntos, pesa alrededor de 5 Kbytes y el máximo permitido para envío es de 10 Mbytes por los correos tradicionales (Hotmail, Yahoo,).

Multiplicando estos valores se tiene un total de espacio requerido en disco de 250 GB. Este valor al igual que el servidor FTP, se encuentra sobredimensionado debido a que los usuarios no harán uso del total de la capacidad del servicio. Y en base al nivel de utilización se puede asignar un valor menor o mayor de almacenamiento sin reducir el rendimiento del servidor.

Con respecto a las características de hardware adicionales como memoria RAM, velocidad del procesador u otras no se requieren de características adicionales por lo que se toma como referencia las mismas de las otros servidores. Servidor a 250 Mhz, 256 MB RAM

Este servidor fortalecerá la comunicación entre las diferentes áreas del Instituto ayudando así a tener permanente información entre todos los usuarios de la red. Mediante este servicio toda comunicación será enviada y registrada en el servidor de correo.

El servidor AAA, no tiene requerimientos de hardware más que los del mismo sistema operativo, además de en función del número de usuarios un espacio de almacenamiento capaz de almacenar la información (alrededor de 1GB para 3000 usuarios).

Servidor	**Requerimientos mínimos**		
	Disco Duro	**Memoria RAM**	**Velocidad el procesador**
WEB	*8* MB	256 MB	250 MHz
FTP	30 GB	256 MB	250 MHz
DHCP	1 GB	256 MB	250 MHz
DNS	1 GB	256 MB	250 MHz
E mail	250 GB	256 MB	250 MHz
AAA	1 GB	256 MB	250 MHz
Sistema Operativo	2 GB x 2	2 GB x 2	400 MHz
Servidor 1	**287 GB**	**5.57 GB**	**400 MHz**

Tabla 3.42 Resumen de los requerimientos de servicios para el servidor 1.

En la tabla 3.42, se mencionan las características del servidor que alojará este servicio. Debido a que el servidor será virtualizado los valores del sistema operativo deben ser multiplicados por dos para lograr un adecuado dimensionamiento.

Cabe tomar en cuenta que a pesar de que la capacidad de la memoria RAM resulta bastante alta, un equipo servidor puede poseer varios

3.7.1.7.2 *Servidor 2: Servicios en tiempo real (Voz y video)*

Las características para el servidor de telefonía se encuentran detallas en el apartado 3.5.5 estas son:

- Procesador dual core @700Mhz
- Memoria RAM 256 MB
- Doble fuente de alimentación
- Soporte para tarjetas PCI
- Tarjeta *PCI FXO* con soporte para 8 puertos analógicos

Para el servicio de videoconferencia se consideró el uso de *Open Meeting* que requiere de estas características como mínimo para su instalación.

- Procesador Intel® Pentium® 2.2 GHz o equivalente.
- Memoria RAM 128 MB
- Tarjeta de sonido.
- Micrófono y parlantes.

Finalmente para el servidor de video vigilancia, los requerimientos son similares a los de video conferencia, debido a que el requerimientos de procesamiento de imágenes son los mismos. Sin embargo para este servidor se debe tomar en cuenta el almacenamiento del video que se va a hacer. Para la grabación de las imágenes se considera hacerlo en el formato más ligero posible de acuerdo a la tabla 3.43. Una vez obtenido este valor se multiplica por el número de imágenes que se procesan en un segundo y por el número de segundos a ser grabados de la siguiente manera.

$$\frac{0{,}292\ \text{Mb}}{1\ \text{segundo}} \times \frac{3600\ \text{segundos}}{1\ \text{hora}} \times \frac{24\ \text{horas}}{1\ \text{día}} = 25{,}228\ \text{GB}$$

Este valor se considera tomando en cuenta que el sistema va a estar continuamente grabando las imágenes; sin embargo no va a ser así, debido a que esta se realizará simplemente los fines de semana y en horas nocturnas, conforme a los requerimientos del usuario.

Si se consideran, que se instalarán las 11 cámaras recomendadas, esto implica que el espacio en el disco necesario sería de 277, 52 GB.

Tamaño en pixeles	Profundidad de pixel	Tamaño del archivo		Formatos
		Bits	Mbytes	
640 x 480	x 1 bit	307.200	0,036	 GIF, BMP
640 x 480	x 8 bits	2´457.600	0,292	 GIF, BMP
640 x 480	x 24 bits	7´372.800	0,878	 BMP, TGA, TIF, PSD, PICT
640 x 480	x 32 bits	9´830.400	1,171	 BMP, TGA TIF, PSD, PICT, JPG

Tabla 3.43 Tamaño de las imágenes en función de su tamaño y el tipo de archivo.[W73]

En la tabla 3.44 se presentan las características mínimas para este servidor

Servidor	Requrimientos mínimos		
	Disco Duro	**Memoria RAM**	**Velocidad el procesador**
VoIP	*8* GB	256 MB	700 MHz
Videoconferencia	30 GB	128 MB	2.2 GHz
Cámaras IP	278 GB	256 MB	250 MHz
Sistema Operativo	2 GB	2 GB	400 MHz
Servidor 2	**318 GB**	**256 MB**	**2.2 GHz**

Tabla 3.44 Resumen de los requerimientos de servicios para el servidor 2

3.7.1.7.3 *Servidor3: Antivirus*

El servidor de antivirus, *Karspersky*, como se mencionó anteriormente requiere de una servidor de administración que se encarga de la actualización, y administración de políticas de cada uno de los agentes ubicados en cada una de las máquinas a través de la red. Los requerimientos de hardware y software para este servidor son:

Servidor de administración[39]

Sistema operativo: *Microsoft Windows Server* 2008

Requisitos hardware:

Procesador: Intel Pentium III 800 MHz o superior.

Memoria: Por lo menos 128 MB de memoria RAM disponible

Disco Duro: Por lo menos 400 MB de espacio libre en el disco duro

3.7.1.7.4 *Requisitos mínimos para el funcionamiento de los servidores de la intranet*

A continuación en la tabla 3.45 se presenta un resumen de las características mínimas que deben poseer los diferentes servidores para la implementación de los servicios de la intranet del Instituto.

[39] Kit de administración Kaspersky [www.karspersky.com]

Servidor	Requrimientos mínimos		
	Disco Duro	**Memoria RAM**	**Velocidad el procesador**
Servidor 1	287 GB	5.57 GB	400 MHz
Servidor 2	318 GB	256 MB	2.2 GHz
Servidor Antivirus	400 MB	128 MB	800 MHz

Tabla 3.45 Resumen de los requerimientos para los servidores

3.8 SEGURIDAD DE LA RED

La implementación de una nueva red de datos para la Institución, además de aportar una amplia gama de servicios de los que se beneficie la Institución, trae también responsabilidades inherentes tanto a los usuarios de la red como al personal encargado del área de redes de la Institución. Para el correcto funcionamiento de la red y para garantizar su uso a largo plazo, es necesario establecer una serie de políticas que permitan el uso responsable de la misma.

Estas políticas deben ajustarse a la realidad institucional para garantizar su funcionalidad. Son basadas en el control de la seguridad de la información así como su adecuada gestión siempre guardando concordancia con los objetivos institucionales. Para esto se debe generar un documento de seguridad el cual debe ser comunicado a todos los empleados, y debe tener continuidad además de establecer ciclos para su evaluación y posibles modificaciones derivadas de ésta.

Los roles deben ser claramente especificados así como las responsabilidades de los diferentes usuarios de la red. Debe ser controlada cada acción referente a la seguridad de información, es decir se deben crear procesos de autorización, acuerdos de confidencialidad, identificación de participantes externos en caso de requerir algún soporte, por último se debe asegurar la información antes de que esta sea entregada a los diferentes usuarios.

Se deben crear normas referentes a la gestión de activos, documentar la información disponible y qué papel ocupa cada activo dentro de la Institución con la finalidad de ser clasificada de acuerdo a su importancia. Se debe clasificar y etiquetar esta información de acuerdo a ciertos términos como lo son: jurídicos, sensibilidad y criticidad. La seguridad de la información como se analizó en el

apartado 1.4.2.2, se puede agrupar en tres módulos como personal, tecnología y operación, a partir del cual se realiza el estudio de amenazas y vulnerabilidades y la generación de las políticas de administración de la red, así como la tecnología más adecuada para lograr tal cometido.

Las amenazas son los posibles ataques de los que puede ser presa la red mientras que las vulnerabilidades son los puntos donde la red puede ser atacada.

3.8.1 IDENTIFICACIÓN DE ACTIVOS

Un activo se refiere al dispositivo, documento o personal que genera, transporta o hacen uso de la información según el caso.

Tipo de información	Lugar	Descripción de la información de los documentos
Contable	Contabilidad	Pagos por servicios básicos, facturas de compras, asignaciones presupuestarias, pagos.
Académica	Biblioteca	Proyectos de titulación de los estudiantes
	Áreas académicas	Oficinas de profesores donde se almacena información respecto a las materias impartidas
	Sala de Internet	Software
Administrativa	Oficinas de autoridades	Convenios, actas, estatutos, reformas, mallas curriculares
	Inspecciones	Hojas guías, reportes de asistencia, calificaciones
	Secretarías	Actas, oficios, comunicaciones.
	DOBE	Convenios para pasantías, información psicológica de los estudiantes.
Externa	Servidor de Notas	Calificaciones, registros de asistencia.

Tabla 3.46 Clasificación de los documentos de la Institución

Respecto a la identificación de los activos físicos, es decir equipos, estaciones de trabajo e instalaciones de la Institución se puede encontrar una explicación detallada en el capítulo 2 referente a la situación actual de la red de datos así como su ubicación a lo largo del campus.

Como activos de información, se pueden citar los diferentes documentos que se encuentran en la Institución para el desenvolvimiento de las actividades diarias de la misma. Se puede mencionar que la mayor parte de esta documentación se encuentra impresa, es decir son papeles que se encuentran almacenados en los archivadores de la Institución. Estos documentos pueden ser divididos en diferentes grupos de acuerdo al tipo como se muestra en la tabla 3.46.

Existe poca información que se encuentra en medios digitales (discos, dispositivos USB de almacenamiento, etc.), la única información que se encuentra digitalizada es la referente a proyectos de los estudiantes almacenada en la biblioteca y las áreas académicas. Razón por la cual se recomienda la migración de este actual sistema a uno digital, lo que permitirá tener un respaldo de la información de manera digital además de optimizar ciertos procesos como por ejemplo el envío de comunicados, memorandos, oficios etc.

Finalmente dentro de los activos se puede considerar la seguridad de las personas relacionadas al manejo de la información debido a que estos pueden ser presas de ataques tales como los denominados de ingeniería social, además que son los encargados de la generación y el manejo de la información.

3.8.2 SEGURIDAD FÍSICA DE LA RED

Se refiere a las protecciones del entorno, tanto del Cuarto de Equipos, los racks de telecomunicaciones, y los terminales finales de usuario, como por ejemplo cubrir los Cuartos de Telecomunicaciones con pintura piroretardante con el propósito de retardar la acción del fuego en caso de un incendio.

- Control de ubicación de equipos, lo que fue definido en el diseño de cableado estructurado es decir tener los dispositivos de comunicaciones en áreas seguras donde el acceso a los usuarios en general sea restringido,

por ejemplo en las bodegas donde una sola persona es la responsable del sistema.

- Análisis de la topografía de la red para poder definir puntos más vulnerables de ser atacados directamente por intrusos o usuarios mal intencionados.

Es de suma importancia realizar medidas para mantener dentro del rango permisible tanto la temperatura como la humedad del cuarto de telecomunicaciones, para lo que se recomienda implementar un sistema de aire acondicionado en el sitio.

Se recomienda el implementar un sistema de ingreso, que puede contener un dispositivo de acceso biométrico para el Cuarto de Equipos que es el sitio más sensible dentro del diseño de la red. Un sistema biométrico es aquel al cual solo se pueda ingresar mediante autenticación por medio de la medición y análisis de características humanas como por ejemplo la huella digital.

A su vez, o en lugar de este, puede ser instalado un dispositivo de acceso que permita el ingreso de un código ó la identificación por medio de una tarjeta. Este sistema finalmente debería estar conectado a una cerradura magnética que se activa mediante señales recibidas por el sistema de ingreso ó la tarjeta controladora de ingreso al validar la tarjeta, el parámetro o contraseña de ingreso.

La seguridad de la información en el área de trabajo estará a cargo del usuario aginado a ella, el usuario se hará responsable de los documentos así como de los dispositivos y pertenencias, por lo que será responsable directo de las mismas.

La persona encargada de bodega, será custodio de los dispositivos ubicados en cada una de las áreas donde se ubican los racks secundarios y debe mantener documentada la adquisición, salida y traspaso de los equipos y accesorios y será el responsable dentro de la Institución.

3.8.3 CONTROL DE ACCESO LÓGICO

Dentro de la seguridad lógica se deben analizar las medidas necesarias para asegurar la información en formato digital de la Institución, que se encontrará

almacenada en los servidores de la intranet o que se transmita a través de la red de datos.

Se deben implementar mecanismos adecuados de autenticación para los usuarios y los equipos, métodos de conexiones seguras. Rechazar las conexiones remotas no seguras, siempre autenticar a los usuarios que se conecten hacia el servidor desde Internet, además de considerar el enmascaramiento de las direcciones IP internas al exterior mediante la implementación de un servidor *Proxy* y el servicio de NAT, así como control de software malicioso por medio de *antivirus, antispyware*, *firewall*s, etc.

Los equipos de interconectividad deben estar protegidos por medio de una adecuada configuración de los mismos a fin de evitar ataques que provoquen la pérdida de información. Esta configuración debe tener esquemas de claves robustas, que no sean basadas en diccionario para que no sean fáciles de romper, establecidos por el administrador.

En caso de que estos ataques sean realizados esta configuración deberá precautelar que el daño sea mínimo La creación de *VLAN's*, como se analizó en el diseño de la red es una estrategia conveniente para este propósito. La segmentación de la red (subredes y *VLANS*) permite tener control sobre pequeños segmentos con similares características de generación de tráfico.

En los *switches*, se deben crear de listas de control de acceso, que permitan restringir a ciertas direcciones IP el flujo entrante o saliente de información en la Intranet. Además de protección basada en puertos en los *switch*s de acceso, ya que con esta medida de seguridad el atacante tiene menores opciones para lograr su cometido.

Otros puntos con respecto a la seguridad lógica de la red son:

- Controles de Prevención y Detección, es decir poseer un *IPS -IDS* que permita el monitoreo del tráfico considerado como acceso no autorizado a la red y permita tomar las acciones pertinentes al respecto.
- Manejo de algoritmos de cifrado variados como por ejemplo DES, Triple DES, AES que brindan un nivel adicional de seguridad.

- Filtrado de contenido al ser una Institución educativa restringir contenidos que no estén de acuerdo a las actividades inherentes a la misma.

3.8.4 POLÍTICAS PARA LOS USUARIOS DE LA RED

Las políticas de administración serán documentadas para luego ser aprobadas por las autoridades de la Institución e informadas a todos los integrantes de la comunidad educativa. Las políticas de seguridad deben estar planificadas conforme a la estructura institucional nombrar representantes de las diferentes áreas de la Institución que cumplan con los objetivos, metas y responsabilidades del plan de seguridad de la información que la comunidad educativa crea adecuado para su entorno.

A continuación se presentan las recomendaciones acerca de los aspectos a que conviene tomar en cuenta para la generación de estas políticas en función de los aspectos mencionados anteriormente.

3.8.4.1 Administración de los equipos de red

El ó los responsables de los equipos de la red, serán los únicos encargados de la administración, supervisión y mantenimiento tanto preventivo como correctivo de los equipos de comunicaciones. Para lo cual se debe establecer cronogramas de mantenimiento periódico, de acuerdo a la recomendación del fabricante, con el fin de mantener los equipos en óptimo estado.

Se deberá poseer un software adecuado para la administración de la red que permita la detección de posibles problemas que se puedan presentar tanto en los equipos de comunicación así como en las terminales de usuario. Este software deberá ser completamente compatible con los equipos de red y debería tener las licencias completas y actualizadas. El procedimiento para detección de errores y su posterior corrección debe ser establecido por el área técnica de la Institución.

Este software de administración debe generar alarmas y reportes tanto a petición del administrador así como, generar automáticamente reportes de *logs* de errores ocurridos en la red, para tener el adecuado control y seguimiento de los mismos.

Las claves de acceso y de control de los dispositivos son de completa responsabilidad de él o los administradores de red y deberá mantenerse en completa reserva.

3.8.4.2 Políticas sobre uso de hardware y software.

El equipo informático se refiere a todos los computadores personales, *scanner*, copiadoras, proyectores, plotters e impresoras conectadas a la red de la Institución, el mismo que debe ser utilizado en labores relacionadas con el trabajo en ella.

El cuidado y limpieza externa de los equipos informáticos son responsabilidad exclusiva del custodio del bien, se prohíbe tener cerca de los equipos alimentos o bebidas para evitar daños a los equipos.

El usuario será responsable de precautelar su contraseña de inicio de sesión, con el fin de evitar accesos no autorizados a su equipo. Todo lo que devenga del mal uso del equipo será de responsabilidad del custodio. En caso de la detección de daños o anomalías en el equipo computacional deberán reportarlos de forma inmediata al administrador de red para su inspección informática.

La instalación de software así como el cambio o salida de equipo informático deberá ser aprobada por el administrador de red, ya que éste puede ocasionar daño al equipo computacional.

3.8.4.3 Políticas de uso de la red.

El uso de los servicios de la red será exclusivamente con fines laborales, de investigación o a nivel educativo, lo que excluye cualquier uso comercial de la red o cualquier otra actividad que de una u otra manera afecte con el desenvolvimiento o resulte dañino para los demás usuarios o la red en sí misma.

Los daños provocados por el inadecuado uso de los equipos conectados a la red interna o a redes externas serán exclusiva responsabilidad del usuario al que son asignados.

La red no puede ser utilizada además para distribuir programas maliciosos, *spywares*, virus o demás software que afecte a los equipos de otros usuarios o congestionen los enlaces de la red. Los usuarios tampoco están autorizados a

hacer uso de la red para interferir o modificar archivos para los cuales no tengan los permisos de manejo necesarios.

Bajo esta misma línea se considera como uso inadecuado de la red intentar acceder sin autorización a la red, a cuentas de propiedad de otros usuarios o a los dispositivos de interconectividad, en especial si se trata de hacerlo mediante programas como reveladores automáticos de contraseñas.

3.8.4.4 Gestión de Incidentes

Dentro de las políticas de seguridad también es adecuado, generar planes de acción para la operación de la red.

El usuario deberá revisar diariamente las notificaciones con respecto a los servicios de la Institución, que deben ser enviadas a través del correo electrónico institucional por el administrador de la red,

Para esta notificación los administradores deberán definir las acciones a ser tomadas en caso de incidente, cambio, o mantenimiento de los servicios o dispositivos de la red.

En caso de incidente esta gestión se refiere los pasos a seguir luego de ocurrido éste, como por ejemplo proceder a la evaluación de daños por medio del personal de la Institución, hacer válido el servicio de mantenimiento o garantía provisto por el fabricante o proveedor de servicios etc.

El administrador además deberá establecer mecanismos para la recuperación de la red después del incidente, es decir, cómo mantener operativa la red luego de superar el problema ocurrido, por ejemplo mediante el cambio del equipo, el reinicio del servicio según sea el incidente y la magnitud del mismo.

Finalmente capacitar adecuadamente al personal y a los usuarios en general con respecto al uso adecuado de la red. Crear una cultura de buen manejo de los equipos informáticos a fin de concientizar a los usuarios con respecto de sus responsabilidades en base a las políticas de seguridad. Establecer las sanciones necesarias para asegurar este fin enmarcadas dentro de las consideraciones legales (leyes, reglamentos y estatutos de la Institución).

3.8.5 TECNOLOGÍA

Luego de definir las políticas o reglas a ser implementadas para el uso de la red de la Institución se define la arquitectura de seguridad que debe ser empleada para asegurar el cumplimiento de estas políticas tomando en cuenta los diferentes aspectos que cubren las políticas, asegurando la confidencialidad, la disponibilidad y la auditoría del sistema. La seguridad, como se explicó en el diseño de la red, será provista en diferentes niveles. Se debe considerar seguridad tanto a nivel de configuración de equipos como de restricción de acceso.

El esquema de seguridad a implementarse está basado en el modelo restrictivo que brinda un nivel de seguridad medio con un firewall conectado en trípode como se especificó en el literal 3.3.5.

Este tipo de configuración permitirá tener control y administración a través de éste, con las características mínimas expresadas en la tabla 3.47. En esta tabla se detallan las características principales así como los componentes adicionales que brindarían la funcionalidad completa a la red.

Interfaces	Puertos WAN Ethernet 10/100 Mbps Ethernet (Enlaces hacia Internet) Puerto DMZ Ethernet 10/100 Mbps Ethernet (Enlace para ingreso a las aplicaciones de usuarios sin poner en riesgo la red) Puertos LAN Ethernet 10/100 Mbps Ethernet (Conexión de servidores)
Soporte *firewall*	*Network Address Translation (NAT)* Configuración de políticas programables para el acceso Sistemas de detección y prevención de intrusos Manejo de *VLANS*
Algoritmos de cifrado	*DES/3DES/AES*
Filtrado de contenido	Bloqueo de páginas mediante filtros *web* basados en *URL*

Tabla 3.47 Características mínimas del firewall

En algunos casos, los componentes vienen incorporados o podrían estar sujetos a licencias de funcionamiento de acuerdo al fabricante. Estos componentes pueden ser implementados después de acuerdo a los diferentes requerimientos de la Institución y de los usuarios, cuando ya la red entre en funcionamiento y puedan ser detectados los problemas, o posibles vulnerabilidades. En la tabla 3.47, se especifican las características mínimas del firewall que debería funcionar en la Institución.

CAPÍTULO 4.

ALTERNATIVAS TECNOLÓGICAS Y ANÁLISIS DE COSTOS PARA EL REDISEÑO DE LA RED.

Una vez realizado el análisis de la situación actual de la red de la Institución, y definido las características para la implementación y funcionamiento de la red multiservicios, en el presente capítulo, se realiza el análisis de las diferentes alternativas. Para un análisis más sencillo se ha dividido éste en dos partes, que se detallan a continuación:

- Costo de la red pasiva
- Costo de la red activa
- Costos de operación mantenimiento

4.1 COSTOS DE LA RED PASIVA.

Dentro de los costos de la red pasiva se analizarán, principalmente, los costos referentes a la implementación del Sistema de Cableado Estructurado que soporte la red multiservicios. Estos costos incluyen los cables (tanto de cobre como de fibra óptica), *patch cords*, conectores, canaletas, escalerillas, racks, gabinetes y sistemas de protección tanto física como eléctrica que debe incluir la nueva red del Instituto Tecnológico Superior Central Técnico.

4.1.1 MATERIALES A UTILIZARSE

A continuación se presenta el detalle de los materiales a utilizarse, dividido por cada una de las áreas, en la que se ha dividido el proyecto de esta manera se permite escoger a la Institución las áreas que considere críticas y donde la implementación de la red sea inmediata.

4.1.1.1 Número de rollos de cable

Para la instalación de los puntos de voz y datos se considera que se instalarán en un total de 239 puntos de red. Para el cálculo de los rollos de cable, se basa en la recomendación del norma EIA/TIA 568C.2. Entre los aspectos más importantes a

tomar en cuenta es obtener la distancia mínima y la distancia máxima que recorrerá desde el cuarto de telecomunicaciones correspondiente hasta el área de trabajo, luego de lo cual se obtendrá el promedio.

Se contempla que la longitud de rollo de cable tiene 305 metros esto es una medida estándar. El mínimo de puntos de red a instalarse para el cálculo de rollos de cable están descritos en las tablas del numeral 3.1.2. Se establece dejar un factor de holgura de 10 % para contemplar el respectivo enrutamiento de subida y bajada hacia la salida de telecomunicaciones así como al gabinete.

Es decir para el cálculo de la longitud promedio por punto, la fórmula a utilizarse sería:

$$L_{prom} = \frac{d_{mín} + d_{max}}{2} + 10\ \%\ holgura$$

Ecuación 4.1[F2]

A continuación se presenta el cálculo de las distancias promedio de acuerdo a los planos del anexo B.

Área	Distancia Máxima [m]	Distancia Mínima [m]	Distancia Promedio [m]	Distancia Promedio + 10 % holgura [m]
Administrativo Planta Baja	69.3	10.5	39,9	43,89
Administrativo Primer Piso	64.6	7.7	36,15	39,77
Electrónica	64.16	10	37,08	40,79
Bodegas	43.32	3.1	23,21	25,53
Inspecciones	68.5	3.2	35,85	39,44
Bloque de Aulas	51.3	7.1	29,2	32,12
Superior	31.61	2.26	16,935	18,63
Industrial	33.3	3.1	18,2	20,02
Electricidad	50	3.2	26,6	29,26
Automotriz	81.44	4.36	42,9	47,19

Tabla 4.1 Cálculo de las distancias promedio en cada una de las áreas.

Determinadas las distancias promedio de las diferentes áreas se calcula el número de corridas de cable que se van a tener por cada rollo, mediante la siguiente ecuación. Se tomará como ejemplo para el cálculo los valores del área administrativa en la planta baja.

$$\#\ Corridas = \frac{longitud\ del\ cable\ por\ rollo}{Distancia\ promedio} = \frac{305\ [m]}{43{,}89\ [m]} = 6{,}94$$

El valor calculado de la ecuación anterior se aproxima por debajo puesto que existe un segmento del rollo de cable que no se utiliza, este segmento es el sobrante. Con este valor, finalmente, se calcula el número de rollos a ser utilizadas en cada área.

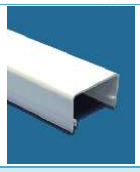
$$\#\ Rollos = \frac{\#\ Número\ de\ puntos\ a\ instalar}{\#\ de\ corridas\ por\ rollo} = \frac{44}{6} = 7{,}33 = \mathbf{8\ rollos\ Admin.Planta\ Baja}$$

El valor que da como resultado esta ecuación se aproxima por arriba puesto que se desea obtener un número de rollos de valor entero. Los resultados del número de corridas por rollo, el número de puntos a instalarse (cámaras, voz y datos); además el número de rollos necesarios, se los puede observar en la tabla 4.2.

Área	Distancia Promedio + 10 % holgura [m]	Número de corridas por rollo	Número de puntos a instalarse	Número de Rollos.
Administrativo Planta Baja	43,89	6	44	8
Administrativo Primer Piso	39,77	7	27	4
Electrónica	40,79	7	28	4
Bodegas	25,53	11	19	2
Inspecciones	39,44	7	17	3
Bloque de Aulas	32,12	9	29	3
Superior	18,63	16	16	1
Industrial	20,02	15	14	1
Electricidad	29,26	10	24	3
Automotriz	47,19	6	21	4

Tabla 4.2 Cálculo de las corridas de cable, número de puntos y los rollos a ser utilizados por cada área.

Para la instalación del sistema de cableado estructurado además se hace imprescindible el uso de accesorios tal como se detallan en la tabla 4.3.

Accesorios	Medidas	Descripción
Caja sobrepuesta de plástico		
Canaleta Plástica Decorativa	100 x 45 [2m] 60 x 40 [2m] 40x25 [2m]	
Angulo Interno	100 x 45 60 x 40 40 x 25	
Sección T para canaleta	100 x 45 60 x 40 40 x 25	
Jack CAT 6 Salida de telecomunicaciones		
Patch Panel CAT 6	24 puertos	
Face plate Doble		
Face plate Simple		
Patch Cord UTP CAT 6	3 ft 6 ft	

Accesorios	Medidas	Descripción
Organizadores horizontals		
Tubo Conduit EMT	12,7 mm (1") x 3m 25.4 mm (2") x 3m	
Bandeja de cables		
Rack cerrado de Piso	42	
Gabinetes abatibles de pared	12 18	
Bandeja de Fibra Óptica SC		
Patch Cord Fibra óptica LC-SC		

Tabla 4.3 Accesorios necesarios para la instalación del Sistema de Cableado Estructurado

En las siguientes tablas se pueden observar el costo de la red pasiva por cada Área del Instituto Tecnológico Central Técnico, se pueden ver desglosados las cantidades y precios que se utilizarán para implementar el cableado estructurado cada una de las Áreas, el detalle de precios de los elementos a describirse se encuentran en las cotizaciones del ANEXO E.

Administrativo			
Descripción	**Cantidad**	**Precio [USD]**	
		Unitario	**Total**
Cable UTP CAT 6 23 AWG 4 pares (1 Rollo)	12	179,95	2159,4
Caja sobrepuesta de 40 mm de plástico	41	1,75	71,75
Canaleta Plástica Decorativa 100x45 2m	10	16,94	169,4
Canaleta Plástica Decorativa 60x40 2m	18	7,92	142,56
Canaleta Plástica Decorativa 40x25 2m	85	5,41	459,85
Angulo Interno 100x45	5	4,10	20,5
Angulo Interno 60x40	4	2,19	8,76
Angulo Interno 40x25	80	0,87	69,6
Sección T para canaleta 100x45	4	4,10	16,4
Sección T para canaleta 60x40	7	0,87	6,09
Sección T para canaleta 40x25	40	0,87	34,8
Jack CAT 6 Salida de Telecomunicaciones	71	6,76	479,96
Jack CAT 6 Patch Panel	71	6,76	479,96
Face plate Doble	30	1,58	47,4
Face plate Simple	11	1,58	17,38
Patch Panel Modular de 24 puertos	7	25,43	178,01
Patch Cord UTP 3 ft CAT 6	71	7,93	563,03
Patch Cord UTP 7 ft CAT 6	71	9,23	655,33
Organizadores horizontals	7	11,61	81,27
Tubo Conduit EMT de (3/4") x 3m	30	4,13	123,9
Bandeja Portacables x 2.4m	22	18,45	405,9
Rack cerrado de Piso 42 UR	1	967,75	967,75
Cable Fibra óptica Multimodo 50/125 um 6 HILOS (1 mt)	910	3,30	3003
Bandeja de Fibra Óptica SC	1	105,57	105,57
Patch Cord Fibra óptica LC-SC	8	10,44	83,52
TOTAL			**10351,09**

Tabla 4.4 Resumen de costos de la red pasiva Administrativo

Electrónica			
Descripción	**Cantidad**	**Precio USD**	
		Unitario	**Total**
Cable UTP CAT 6 23 AWG 4 pares (1 Rollo)	4	179,95	719,8
Caja sobrepuesta de 40 mm de plástico	24	1,75	42
Canaleta Plástica Decorativa 100x45 2m	10	16,94	169,4
Canaleta Plástica Decorativa 60x40 2m	3	7,92	23,76
Canaleta Plástica Decorativa 40x25 2m	75	5,41	405,75
Angulo Interno 100x45	2	4,10	8,2
Angulo Interno 60x40	2	2,19	4,38
Angulo Interno 40x25	40	0,87	34,8
Sección T para canaleta 100x45	2	4,10	8,2
Sección T para canaleta 60x40	2	0,87	1,74
Sección T para canaleta 40x25	15	0,87	13,05
Jack CAT 6 Salida de telecomunicaciones	28	6,76	189,28
Jack CAT 6 Patch Panel	28	6,76	189,28
Face plate Doble	4	1,58	6,32
Face plate Simple	20	1,58	31,6
Patch Panel Modular de 24 puertos	2	25,43	50,86
Patch Cord UTP 3 ft CAT 6	28	7,93	222,04
Patch Cord UTP 7 ft CAT 6	28	9,23	258,44
Organizadores horizontals	2	11,61	23,22
Tubo Conduit EMT de (1 1/4") x 3m	13	8,88	115,44
Tubo Conduit EMT de (1") x 3m	9	5,93	41,51
Tubo Conduit EMT de (3/4") x 3m	13	4,13	53,69
Gabinete Abatible de 18 UR	1	353,25	352,25
Cable Fibra óptica Multimodo 50/125 um 6 HILOS (1 metro)	75	3,30	247,5
Bandeja de Fibra Óptica SC	1	105,57	105,57
Patch Cord Fibra óptica LC-SC	3	10,44	31,32
TOTAL			**3362,26**

Tabla 4.5 Resumen de costos de la red pasiva Electrónica

Bodegas			
Descripción	**Cantidad**	**Precio USD**	
		Unitario	**Total**
Cable UTP CAT 6 23 AWG 4 pares (1 Rollo)	2	179,95	359,9
Caja sobrepuesta de 40 mm de plástico	11	1,75	19,25
Canaleta Plástica Decorativa 40x25 2m	50	5,41	270,5
Angulo Interno 40x25	16	0,87	13,92
Sección T parta canaleta 40x25	8	0,87	6,96
Jack CAT 6 Salida de telecomunicaciones	18	6,76	121,68
Jack CAT 6 Patch Panel	18	6,76	121,68
Face plate Doble	7	1,58	11,06
Face plate Simple	4	1,58	6,32
Patch Panel Modular de 24 puertos	1	25,43	25,43
Patch Cord UTP 3 ft CAT 6	18	7,93	142,74
Patch Cord UTP 7 ft CAT 6	18	9,23	166,14
Organizadores horizontales	1	11,61	11,61
Tubo Conduit EMT de (3/4") x 3m	6	4,13	24,78
Gabinete Abatible de 12 UR	1	276	276
Bandeja de Fibra Óptica SC	1	105,57	105,57
Patch Cord Fibra óptica LC-SC	1	10,44	10,44
TOTAL			**1693,98**

Tabla 4.6 Resumen de costos de la red pasiva Bodegas

Inspecciones			
Descripción	**Cantidad**	**Precio USD**	
		Unitario	**Total**
Cable UTP CAT 6 23 AWG 4 pares (1 Rollo)	3	179,95	539,85
Caja sobrepuesta de 40 mm de plástico	13	1,75	22,75
Canaleta Plástica Decorativa 40x25 2m	30	5,41	162,3
Angulo Interno 40x25	12	0,87	10,44
Sección T parta canaleta 40x25	8	0,87	6,96
Jack CAT 6 Salida de telecomunicaciones	17	6,76	114,92
Jack CAT 6 Patch Panel	17	6,76	114,92
Face plate Doble	4	1,58	6,32

Face plate Simple	9	1,58	14,22
Patch Panel Modular de 24 puertos	1	25,43	25,43
Patch Cord UTP 3 ft CAT 6	17	7,93	134,81
Patch Cord UTP 7 ft CAT 6	17	9,23	156,91
Organizadores horizontals	1	11,61	11,61
Tubo Conduit EMT de (1 1/4") x 3m	15	8,88	133,2
Gabinete Abatible de 12 UR	1	276	276
Cable Fibra óptica Multimodo 50/125 um 6 HILOS (1 metro)	45	3,30	148,5
Bandeja de Fibra Óptica SC	1	105,57	105,57
Patch Cord Fibra óptica LC-SC	2	10,44	20,88
TOTAL			**2005,59**

Tabla 4.7 Resumen de costos de la red pasiva Inspecciones

Bloque de aulas			
Descripción	**Cantidad**	**Precio USD**	
		Unitario	**Total**
Cable UTP CAT 6 23 AWG 4 pares (1 Rollo)	3	179,95	539,85
Caja sobrepuesta de 40 mm de plástico	28	1,75	49
Canaleta Plástica Decorativa 40x25 2m	30	5,41	162,3
Angulo Interno 40x25	24	0,87	20,88
Jack CAT 6 Salida de telecomunicaciones	29	6,76	196,04
Jack CAT 6 Patch Panel	29	6,76	196,04
Face plate Doble	1	1,58	1,58
Face plate Simple	27	1,58	42,66
Patch Panel Modular de 24 puertos	2	25,43	50,86
Patch Cord UTP 3 ft CAT 6	29	7,93	229,97
Patch Cord UTP 7 ft CAT 6	29	9,23	267,67
Organizadores horizontales	2	11,61	23,22
Tubo Conduit EMT de (1 1/4") x 3m	9	8,88	79,92
Tubo Conduit EMT de (3/4") x 3m	27	4,13	111,51
Gabinete Abatible de 18 UR	1	353,25	353,25
Bandeja de Fibra Óptica SC	1	105,57	105,57
Patch Cord Fibra óptica LC-SC	1	10,44	10,44
TOTAL			**2440,76**

Tabla 4.8 Resumen de costos de la red pasiva Bloque de aulas

Superior			
Descripción	**Cantidad**	**Precio USD**	
		Unitario	**Total**
Cable UTP CAT 6 23 AWG 4 pares (1 Rollo)	1	179,95	179,95
Caja sobrepuesta de 40 mm de plástico	11	1,75	19,25
Canaleta Plástica Decorativa 40x25 2m	45	5,41	243,45
Angulo Interno 40x25	14	0,87	12,18
Jack CAT 6 Salida de telecomunicaciones	16	6,76	108,16
Jack CAT 6 Patch Panel	16	6,76	108,16
Face plate Doble	5	1,58	7,9
Face plate Simple	6	1,58	9,48
Patch Panel Modular de 24 puertos	1	25,43	25,43
Patch Cord UTP 3 ft CAT 6	16	7,93	126,88
Patch Cord UTP 7 ft CAT 6	16	9,23	147,68
Organizadores horizontales	1	11,61	11,61
Gabinete Abatible de 12 UR	1	276	276
Bandeja de Fibra Óptica SC	1	105,57	105,57
Patch Cord Fibra óptica LC-SC	1	10,44	10,44
TOTAL			**1392,14**

Tabla 4.9 Resumen de costos de la red pasiva Superior

Electricidad			
Descripción	**Cantidad**	**Precio USD**	
		Unitario	**Total**
Cable UTP CAT 6 23 AWG 4 pares (1 Rollo)	3	179,95	539,85
Caja sobrepuesta de 40 mm de plástico	23	1,75	40,25
Canaleta Plástica Decorativa 40x25 2m	100	5,41	541
Angulo Interno 40x25	30	0,87	26,1
Sección T 40x25	16	0,87	13,92
Jack CAT 6 Salida de telecomunicaciones	24	6,76	167,24
Jack CAT 6 Patch Panel	24	6,76	167,24
Face plate Doble	1	1,58	1,58
Face plate Simple	22	1,58	34,76
Patch Panel Modular de 24 puertos	2	25,43	50,86

Patch Cord UTP 3 ft CAT 6	24	7,93	190,32
Patch Cord UTP 7 ft CAT 6	24	9,23	221,52
Organizadores horizontales	2	11,61	23,22
Tubo Conduit EMT de (3/4") x 3m	20	4,13	82,6
Gabinete Abatible de 18 UR	1	276	276
Bandeja de Fibra Óptica SC	1	105,57	105,57
Patch Cord Fibra óptica LC-SC	1	10,44	10,44
TOTAL			**2482,47**

Tabla 4.10 Resumen de costos de la red pasiva Electricidad

Industrial			
Descripción	**Cantidad**	**Precio USD**	
		Unitario	**Total**
Cable UTP CAT 6 23 AWG 4 pares (1 Rollo)	1	179,95	179,95
Caja sobrepuesta de 40 mm de plástico	11	1,75	19,25
Canaleta Plástica Decorativa 40x25 2m	30	5,41	162,3
Angulo Interno 40x25	18	0,87	15,66
Sección T 40x25	6	0,87	5,22
Jack CAT 6 Salida de telecomunicaciones	13	6,76	87,88
Jack CAT 6 Patch Panel	13	6,76	87,88
Face plate Doble	2	1,58	3,16
Face plate Simple	9	1,58	14,22
Patch Panel Modular de 24 puertos	1	25,43	25,43
Patch Cord UTP 3 ft CAT 6	13	7,93	103,09
Patch Cord UTP 7 ft CAT 6	13	9,23	119,99
Organizadores horizontales	1	11,61	11,61
Gabinete Abatible de 12 UR	1	276	276
Bandeja de Fibra Óptica SC	1	105,57	105,57
Patch Cord Fibra óptica LC-SC	1	10,44	10,44
TOTAL			**1227,65**

Tabla 4.11 Resumen de costos de la red pasiva Industrial

Automotriz			
Descripción	**Cantidad**	**Precio USD**	
		Unitario	**Total**
Cable UTP CAT 6 23 AWG 4 pares (1 Rollo)	4	179,95	791,8
Caja sobrepuesta de 40 mm de plástico	20	1,75	35
Canaleta Plástica Decorativa 40x25 2m	23	5,41	124,43
Canaleta Plástica Decorativa 60x40 2m	50	0,87	43,5
Angulo Interno 40x25	16	0,87	13,92
Angulo Interno 60x40	7	2,19	15,33
Sección T 40x25	7	0,87	6,09
Sección T 60x40	7	0,87	6,09
Jack CAT 6 Salida de telecomunicaciones	21	6,76	141,96
Jack CAT 6 Patch Panel	21	6,76	141,96
Face plate Doble	1	1,58	1,58
Face plate Simple	19	1,58	30,02
Patch Panel Modular de 24 puertos	2	25,43	50,86
Patch Cord UTP 3 ft CAT 6	21	7,93	166,53
Patch Cord UTP 7 ft CAT 6	21	9,23	193,83
Organizadores horizontals	2	11,61	23,22
Tubo Conduit EMT de (1") x 3m	15	5,93	88,95
Gabinete Abatible de 18 UR	1	353,25	353,25
Cable Fibra óptica Multimodo 50/125 um 6 HILOS (1 metro)	120	3,30	396
Bandeja de Fibra Óptica SC	1	105,57	105,57
Patch Cord Fibra óptica LC-SC	1	10,44	10,44
TOTAL			**2668,63**

Tabla 4.12 Resumen de costos de la red pasiva Automotriz

Área	Costo [USD]	Área	Costo [USD]	Área	Costo [USD]
Administrativo	**10351,09**	Bloque de aulas	**2440,76**	Automotriz	**2668,63**
Electrónica	**3362,26**	Industrial	**1227,65**	**COSTO TOTAL**	
Bodegas	**1693,98**	Electricidad	**2482,47**	**27624,57**	
Inspecciones	**2005,59**	Superior	**1392,14**		

Tabla 4.13 Resumen de costos de la red pasiva del Instituto

4.2 COSTOS DE LA RED ACTIVA.

4.2.1 EQUIPOS DE CONECTIVIDAD

Los equipos de conectividad considerados para la implementación del proyecto son de las marcas más comunes en el mercado, Cisco, HP y D-Link, debido a su confiabilidad además de la facilidad de conseguirlos.

A continuación se presentan las principales características de los *switches* considerados para la red.

4.2.1.1 Cisco

4.2.1.1.1 *Cisco Catalyst 2960 24 TS – L*

Figura 4.1 Cisco Catalyst 2960 24 TS – L

Características:

Switch 24 puertos administrable

Puertos: 24 x 10/100/1000 + 4 x SFP

Capacidad de conmutación: 176 Gbps

Rendimiento: 41.7 Mpps

Protocolo de gestión remota: *SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH*

Características y cumplimiento de normas: Conmutación Layer 2, auto-sensor por dispositivo, asignación dirección dinámica IP, negociación automática, soporte BOOTP, soporte ARP, equilibrio de carga, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP, soporte para Syslog, soporte DiffServ, Broadcast Storm Control, soporte IPv6, Multicast Storm Control, Unicast Storm Control, admite Rapid Spanning Tree Protocol (RSTP),

admite Multiple Spanning Tree Protocol (MSTP), snooping DHCP, soporte de Dynamic Trunking Protocol (DTP), soporte de Port Aggregation Protocol (PAgP), soporte de Access Control List (ACL), Quality of Service (QoS), Protocolo de control de adición de enlaces (LACP), Port Security, MAC Address Notification, Remote Switch Port Analyzer (RSPAN)

IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP)

Garantía del fabricante: Garantía limitada de por vida.

MTBF[40]: 349,824 horas

Costo: **3026,93 USD**

4.2.1.1.2 *Cisco WS Catalyst 3560 G24 TS- S*

Figura 4.2 4.2.1.1.2 Cisco WS Catalyst 3560 G24 TS- S

Características:

Switch 24 puertos Capa 3 administrable

Puertos: 24 x 10/100/1000 + 4 x Gigabit SFP

Rendimiento: 38.7 mpps

Protocolo de direccionamiento: RIP-1, RIP-2, HSRP, direccionamiento IP estático, RIPng

Protocolo de gestión remota: SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, SSH-2

[40] *MTBF (Mean Time Between Failures),* promedio del tiempo entre fallos de un sistema.

Características y cumplimiento de normas: Capacidad duplex, conmutación Layer 3, conmutación Layer 2, auto-sensor por dispositivo, Encaminamiento IP, soporte de DHCP, negociación automática, soporte ARP, concentración de enlaces, soporte de MPLS, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP, limitación de tráfico, activable, admite Spanning Tree Protocol (STP), admite Rapid Spanning Tree Protocol (RSTP), admite Multiple Spanning Tree Protocol (MSTP), snooping DHCP, soporte de Dynamic Trunking Protocol (DTP), soporte de Port Aggregation Protocol (PAgP), soporte de Trivial File Transfer Protocol (TFTP), soporte de Access Control List (ACL), Quality of Service (QoS), Servidor DHCP, Virtual Route Forwarding-Lite (VRF-Lite), rastreador MLD, Dynamic ARP Inspection (DAI), Time Domain Reflectometry (TDR), Per-VLAN Spanning Tree Plus (PVST+), tecnología Cisco EnergyWise, Uni-Directional Link Detection (UDLD), Protocolo de control de adición de enlaces (LACP)

IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s

Garantía del fabricante: Garantía limitada de por vida

MTBF: 230,000 horas

Costo: **4785,54 USD**

4.2.1.2 HP

4.2.1.2.1 *HP 4210 G 24 puertos*

Figura 4.3 HP 4210 G 24 puertos

Características:

Puertos 20 puertos RJ-45 autosensing 10/100/1000

Capacidad de conmutación: 128 Gbps

Rendimiento: Hasta 95.2 mpps

Características y cumplimiento de normas:

Puertos 10 Gigabit Ethernet opcionales, (IEEE 802.3 tipo 10BASE-T, IEEE 802.3u tipo 100BASE-TX, IEEE 802.3ab tipo 1000BASE-T), Auto-MDIX, Duplex: 10BASE-T/100BASE-TX: half o full duplex; 1000BASE-T, full duplex. 4 Puertos duales 10/100/1000 (IEEE 802.3 tipo 10BASE-T, IEEE 802.3u tipo 100BASE-TX, IEEE 802.3ab tipo 1000BASE-T); 802.3 z, 1 puerto para consola RJ-45; Soporta un máximo de 4 puertos 10-GbEthernet.

IEEE 802.1ag, IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1s (MSTP), IEEE 802.1s, IEEE 802.1v, IEEE 802.1w, IEEE 802.1X, IEEE 802.3ad, IEEE 802.3ad, IEEE 802.3ae, IEEE 802.3i, IEEE 802.3x, IEEE 802.3z, UDP, ICMP, TCP, ARP, TELNET, TFTP Protocol (revisión 2), CIDR, DHCP, RADIUS, SNMP, RMON, IEEE 802.1X Control de acceso a la red basado en puertos.

Garantía del fabricante: Garantía limitada de por vida.

MTBF: 350,000 horas

Costo: **2487,01 USD**

4.2.1.2.2 *HP E4510 24 G 24 puertos*

Figura 4.4 HP E4510 24 G 24 puertos

Características:

Puertos: 20 RJ-45 auto-negotiating 10/100/1000

Capacidad de conmutación: 170 Gbps

Rendimiento: Hasta 93.2 mpps

Características y cumplimiento de normas:

Puertos (IEEE 802.3 tipo10Base-T, IEEE 802.3u tipo 100Base-TX, IEEE 802.3ab tipo 1000Base-T), 4 puertos SFP 10/100/1000 auto negociables (IEEE 802.3 tipo 10Base-T, IEEE 802.3u tipo 100Base-TX, IEEE 802.3ab tipo 1000Base-T), 802.3 z.

IEEE 802.1ag, IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q (GVRP), IEEE 802.1s, , IEEE 802.1v VLAN, IEEE 802.1w, IEEE 802.1X, IEEE 802.3ad, IEEE 802.3ae, EEE 802.3x, UDP, ICMP, TCP, ARP, TELNET, RIPv1 y v2, TFTP Protocol (revisión 2), CIDR, DHCP, RADIUS VLAN & Priority ,IPv6, OSPFv3 para IPv6, SNMPv1/v2c/v3, IEEE 802.1X Control de acceso a la red basado en puertos.

Garantía del fabricante: Garantía limitada de por vida.

MTBF: 198,720 horas

Costo: **3520,29 USD**

4.2.1.3 D-LINK

4.2.1.3.1 *DGS-1210-24*

Figura 4.5 DGS-1210-24

Características:

Puertos Switch con 20 puertos Gigabit y 4 puertas SFP

Capacidad de conmutación: 48 Gbps

Rendimiento: 35,7 mpps

Características y cumplimiento de normas:

IEEE 802.3, IEEE 802.3u, IEEE802.3ab, IEEE 802.3z, Soporta operación Half/Full-Duplex, Auto-negociación, Soporta Auto MDI-X/MDI-II, Soporta control de flujo de IEEE 802.3x,

Soporta IGMP v1,v2, Spanning Tree, 802.3ad, Port Mirroring, Estándar 802.1Q, 256 grupos de VLAN en total, Max 256 Grupos VLAN estático, soporta 01 VLAN de administración, ACL (*Access Control List*), QoS, soporta 802.1p, soporta control ancho de banda basado en puerto, DSCP, 802.1X Control de acceso basado en puerto, motor de seguridad D-Link, control de tormentas broadcast, enmascaramiento DHCP, administración web, CLI, ping, Telnet, TFTP, Configurable Auto MDI/MDIX,

Soporta SNMP v1/v2c/v3, STP, DHCP, UDP, IP, ICMP, TCP, ARP.

Garantía del fabricante: Garantía limitada de por vida.

MTBF: 410,948 horas

Costo: **392 USD**

4.2.1.3.2 *DGS 3612*

Figura 4.6 DGS 3612

Características:

Puertos 12 puertos 10/100/1000BASE-T

4 Combo SFP

Capacidad de conmutación: 24 Gbps

Rendimiento: 17,86 mpps

Características y cumplimiento de normas:

IEEE 802.3, IEEE 802.3u, IEEE 802.ab, IEEE 802.3z, soporta operaciones Half/Full-Duplex, IEEE 802.3x, soporta 802.1D, 802.1w, 802.1s, 802.3ad, soporta 802.1AX, Port Mirroring, GVRP, Cisco CDP, VLAN, 802.1Q, 802.1v, Q in Q basado en puerto, soporta IGMP v1, v2 y v3, IGMP Snooping, VLAN Trunking, soporta 802.1p, ARP Proxy, ACL.

Soporta RIP v1/v2, OSPF , BGP, Ruta estática, control de ancho de banda, SSH, SSL, motor de seguridad D-Link, enmascaramiento DHCP, RADIUS, 802.1X, autenticación WEB y basada en MAC. Soporta RMON, SNMP, administración web y por consola mediante Puerto RS 232.

Garantía del fabricante: Garantía limitada de por vida.

MTBF: 402,111 horas

Costo: **2688 USD**

4.2.1.4 Cumplimiento de requerimientos

Una vez identificados los equipos que pueden ser utilizados para la implementación de la red para la Institución, se procede a hacer la comparación entre las características de los equipos conforme al detalle de especificaciones que se realizó en el apartado 3.3.5.2, para determinar si cumplen o no con los requerimientos de la Institución.

Como se especificó en el numeral 3.3.5.2, no todos los *switches* utilizarán los 4 módulos de fibra; sin embargo se ha solicitado que todos los *switches* cumplan con este requerimiento con el propósito de brindar las características de escalabilidad a la red en caso de una futura expansión.

En el caso de los equipos D-Link y HP, el requerimiento de 24 puertos está condicionado a la instalación o no de los módulos de fibra, debido a la dualidad del uso de los puertos. Sin embargo, de acuerdo al dimensionamiento realizado

en el capítulo 3, estos equipos pueden entrar en funcionamiento en la red sin que esto implique algún tipo de complicaciones actuales o futuras.

DETALLES DE HARDWARE		**CISCO Catalyst 2960 24 TS – L**	**HP HP 4210 G**	**D-Link DGS-1210-24**
Capacidad de *backplane* mínima	54 Gbps	✓	✓	No
CARACTERISTICAS CAPA 2		✓	✓	✓
Puertos Ethernet 10/100/1000 Mbps	24	✓	✓	✓
Adicional Puertos de fibra *Gigabit Ethernet* 10/100/1000 Mbps	2,3,4 (según el requerimiento)	✓	✓	✓
SPF conector LC		✓	✓	✓
Protocolos de Red Soportados		✓	✓	✓
Protocolo IEEE 802.3 u		✓	✓	✓
Protocolo IEEE 802.3 z		✓	✓	✓
Protocolo IEEE 802.3 x		✓	✓	✓
Protocolo IEEE 802.1 p		✓	✓	✓
Protocolo IEEE 802.1 q		✓	✓	✓
Protocolo IEEE 802.1 d		✓	✓	✓
Protocolo IEEE 802.1 w		✓	✓	✓
Protocolo IEEE 802.1 x		✓	✓	✓
Capacidad para troncalización en puertos		✓	✓	✓
ADMINISTRACIÓN		✓	✓	✓
Soporte de administración basada en *Web*		✓	✓	✓
Administración basada en consola CLI		✓	✓	✓
Soporte de *Telnet*		✓	✓	✓
Soporte de *SNMP* v1, v2, y v3		✓	✓	✓
COSTO [USD]		**3026,93**	**2487,01**	**392**

Tabla 4.14 Cumplimiento de las características mínimas para los *switches* de acceso

A continuación en la tabla 4.15 se presenta el cumplimiento de características para los *switches* de *core.*

DETALLES DE HARDWARE		CISCO WS Catalyst 3560 G24 TS- S	HP E4510 24 G	D-Link DGS 3612
Capacidad de *backplane* mínima	32 Gbps o superior	✓	✓	✓
CARACTERÍSTICAS CAPA 2		✓	✓	✓
Puertos Ethernet 10/100/1000 Mbps	**Mínino 12**	✓	✓	✓
Adicional Puertos Gigabit Ethernet 10/100/1000 Mbps	**4**	✓	✓	✓
SPF conector LC		✓	✓	✓
Protocolos de Red Soportados		✓	✓	✓
Protocolo IEEE 802.3 u		✓	✓	✓
Protocolo IEEE 802.3 z		✓	✓	✓
Protocolo IEEE 802.3 x		✓	✓	✓
Protocolo IEEE 802.1 p		✓	✓	✓
Protocolo IEEE 802.1 q		✓	✓	✓
Protocolo IEEE 802.1 w		✓	✓	✓
Protocolo IEEE 802.1 d		✓	✓	✓
CARACTERISTICAS CAPA 3		✓	✓	✓
Soporte *de Routing Information Protocol (RIP),*		✓	✓	✓
Soporte de enrutamiento estático		✓	✓	✓
Soporte de servicio DHCP		✓	✓	✓
SEGURIDAD		✓	✓	✓
Soporte de ACLs estándar y extendidas en todos los puertos		✓	✓	✓
Soporte de *SSH*		✓	✓	✓
ADMINISTRACIÓN		✓	✓	✓
Administración basada en consola CLI		✓	✓	✓
Soporte de Telnet,		✓	✓	✓
Soporte de SNMP v1, v2, y v3		✓	✓	✓
FUENTE DE PODER		✓	✓	✓
Debe proveer fuente de poder redundante interna		✓	✓	✓
COSTO [USD]		**4785,54**	**3520,29**	**2688**

Tabla 4.15 Cumplimiento de las características mínimas para los *switches* de *core*

Luego del análisis realizado de la documentación referente a cada uno de los equipos, se escoge como alternativa más viable para el proyecto a los *switches* HP tanto para acceso como para *core*.

La decisión de escoger estos *switches* brinda a la red una estandarización de criterios frente a los equipos Cisco, los equipos Cisco en su mayor parte utilizan protocolos propietarios que a pesar de cumplir con las características mencionadas, limitan el uso de ciertas funcionalidades de la red multiservicios.

La serie de switches *Cisco Catalyst* ofertados; además, está orientada a la implementación de redes en *Data Centers,* donde los volúmenes de información y necesidades son muy diferentes a los que se han proyectado en la red de la Institución.

Finalmente se recomienda la utilización de equipos *HP* debido a su menor costo frente a los equipos *Cisco*, sin que esta disminución del precio sea porque no soporte las mismas funcionalidades de éstos.

Algunas características como por ejemplo el uso de *ACL´s,* el manejo de prioridades en lo relacionado a calidad de servicio y autenticación 802.1x, utilizan reglas propias del fabricante lo que limitaría la interconexión a dispositivos finales o hacia otros sistemas además de dificultar la migración o escalabilidad de servicios.

Los equipos *D-Link* ofertados con el cumplimiento de las características mencionadas, son del tipo *smart*. Esta característica implica que son medianamente administrables. Los equipos del tipo *smart* soportan configuración de algunas de sus características; sin embargo otras quedan configuradas por defecto y no pueden ser cambiadas. Esta sería una limitante en caso de integración de funcionalidades adicionales o administración por medio de scripts de configuración, que faciliten la administración de la red.

Los equipos HP por el contrario son completamente administrables lo que es una ventaja tremendamente importante para poder regular y administrar de una manera eficiente la red.

4.2.1.5 Costos de los equipos de interconectividad

Función	Equipo	Número	Precio Unitario [USD]	Precio Total [USD]
Acceso Distribución	HP E4210-24G (JF844A)	3	1514,492	4543,48
Acceso Distribución	HP E4210-24G (JF844A) + 1 HP X124 1G SFP LC SX	4	1757,622	7030,49
Acceso Distribución	HP E4210-24G (JF844A) + 2 HP X124 1G SFP LC SX	6	1786,385	12004,51
Acceso Distribución	HP E4210-24G (JF844A) + 3 HP X124 1G SFP LC SX	2	2243,875	4487,75
Acceso Distribución	HP E4210-24G (JF844A) + 4 HP X124 1G SFP LC SX	2	2487,01	4974,01
Core	HP E4510-24G Switch (JF847A) + 4 HP X124 1G SFP LC SX	2	3520,294	7040,58
Total		**19**	**-**	**40080,82**

Tabla 4.16 Costos de los *switches* de la red

En la tabla 4.16 se presenta el resumen de los costos de los equipos de interconectividad a ser utilizados. En el ANEXO E se presenta las cotizaciones de los diferentes equipos analizados. Estos precios incluyen el IVA.

4.2.2 FIREWALL

De igual forma que para los *switches* se han considerado las mismas marcas para la elección de un equipo para la protección de la red. A continuación se presentan las principales caracterísiticas de los equipos analizados.

4.2.2.1 ASA 5505 Appliance with S/W-10 Users 8 Port DES

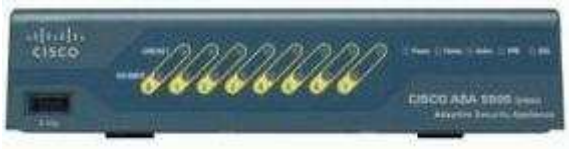


Figura 4.7 ASA 5505 Appliance with S/W-10 Users 8 Port DES

Características:

Dispositivo VPN, crear hasta diez conexiones mediante IPSec y SSL

8 Puertos RJ-45 10/100Base-TX, dos incluyen *PoE*

1 Puerto RJ-45 para administración por consola, 3 puertos USB 2.0

4000 conexiones por Segundo y 10000 Concurrent Connection

Soporte para 802.1Q VLAN

ASA 5500 Nivel base de encripción (DES)

Costo: 634,37 USD

4.2.2.2 HP S200-S UTM Appliance

Figura 4.8 HP S200-S UTM Appliance

Puertos: 5 puertos *Ethernet, Fast Ethernet, Gigabit Ethernet*

Red / Protocolo de transporte: L2TP, ICMP/IP, IPSec, PPPoE

Protocolo de gestión remota: SNMP 1, SNMP 3, SNMP 2c, HTTP, HTTPS, FTP, SSH, Telnet

Conexiones concurrentes: 60000

500 Túneles IPSec VPN simultáneos, 512 Túneles L2TP VPN simultáneos

Características: Protección firewall, Encaminamiento IP, soporte de NAT, asistencia técnica VPN, soporte ARP, soporte VLAN, limitación de tráfico, prevención contra ataque de DoS (denegación de servicio), soporte IPv6, análisis de antivirus, Sistema de prevención de intrusiones (IPS), filtrado de URL,

prevención de ataque DDos, protección anti-spam, Quality of Service (QoS), Servidor DHCP, DNS proxy.

Algoritmo de encripción: 3DES, AES, DES, MD5, SHA-1

MTBF 315,000 Horas

Costo: 4116 USD

4.2.2.3 DFL-860 ENetDefend UTM Firewall

Figura 4.9 DFL-860 ENetDefend UTM Firewall

Puertos: DB9, RS-232 para administración, 2 Puertos WAN Ethernet 10/100 Mbps Ethernet, 1 Puerto DMZ Ethernet 10/100 Mbps Ethernet, 7 Puertos LAN Ethernet 10/100 Mbps Ethernet

VPN (3DES/AES)

Sesiones Concurrentes: 20.000

Sesiones por segundo: 4.000

Características:

Ruteo, *Network Address Translation (NAT), Port Address Translation (PAT), OSPF Dynamic Routing, Port Forwarding,* Configuración de políticas programables en el tiempo, *DHCP*, Rutas estáticas

Soporta IEEE 802.1q VLAN: hasta 8 VLANs, IP Multicast: IGMP v3 ruteo y reenvío (compatible con v1 y v2), HTTP, FTP, H.323, POP3, SMTP, SIP, TFTP, TLS 1.0 (RFC 2246), Sistema de Detección y Prevención de Intrusos (IDS/IPS), balanceo de carga.

Protocolo IPSec, *DES/3DES/AES/Twofish/Blowfish/CAST-128/NULL*

Algoritmo de autenticación: MD5, SHA-1

Antivirus, Filtro del Email remitente/destinatario y Lista Negra/exentas (para el protocolo SMTP solamente)

Comprobación del encabezado MIME para filtrar extensiones de de archivos

Protección de tasa del correo electrónico (por el protocolo SMTP solamente)

Lista negra de DNS basada en Peso

MTBF 140.532 Horas

Costo: 1932 USD

4.2.2.4 Cumplimiento de características del firewall

A continuación en la tabla 4.16 se presenta el cumplimiento de las características requeridas para la red por los equipos analizados.

		CISCO ASA 5505	HP HP S200-S	D-Link DFL-860
Interfaces	Puertos WAN Ethernet 10/100 Mbps	✓	✓	✓
	Puerto DMZ Ethernet 10/100 Mbps	✓	✓	✓
	Puertos LAN Ethernet 10/100 Mbps	✓	✓	✓
Soporte *firewall*	*Network Address Translation (NAT)*	*No*	✓	✓
	Configuración de políticas programables para el acceso	*No*	✓	✓
	Sistemas de detección y prevención de intrusos	*No*	✓	✓
	Manejo de *VLANS*	✓	✓	✓
Algoritmos de cifrado	*DES/3DES/AES*	*DES*	✓	✓
Filtrado de contenido	Bloqueo de páginas mediante filtros *web* basados en *URL*	No	✓	✓
COSTO [USD]		**634,37**	**4116**	**1932**

Tabla 4.17 Cumplimiento de características mínimas del firewall

Como se puede observar en la tabla 4.17, los equipos HP y D-link presentan las mejores características de seguridad para el firewall respecto al equipo Cisco analizado. Se recomienda la utilización de firewalls HP para asegurar homogeneidad en la red de datos sin embargo se deja a elección de los administradores de red la implementación con uno u otro proveedor.

4.2.2.5 Costo del firewall

A continuación, en la tabla 4.18, se presentan los costos del firewall seleccionado, se debe anotar que algunas funcionalidades como IDS/IPS, además de características adicionales como la protección antivirus y el filtrado de correo electrónico están ligadas a la compra de licencias anuales por lo que estos costos deberían ser pagados por la Institución para mantener la defensa completa, durante todo el tiempo.

Se deja a criterio de los administradores de la red, el trabajo con las características en el equipo o configurar estos servicios mediante otros métodos.

Descripción	Costo (USD)
HP S200-S UTM Appliance	1.235,00
HP SecPath U200-S 1 Year Anti-Spam Serv	890,00
HP SecPath U200-S 1 Year AV Updates	660,00
HP SecPath U200-S 1Year Web Content Filt	890,00
TOTAL	**3675,00**
TOTAL incluido el IVA	**4116,00**

Tabla 4.18 Costos del firewall

4.2.3 SERVIDORES

Como se analizó en el apartado 3.7.1.7, las características para los servidores, en cuanto a memoria RAM, disco duro y velocidad de trabajo de los procesadores como se resume en la tabla 4.19.

Luego del análisis realizado con el personal de la Institución y demás personas vinculadas al medio, se llegó a la conclusión que para estos servidores se recomienda el uso de los servidores *HP Proliant ML350G6.* Estos servidores

brindan robustez, fiabilidad, además de compatibilidad con los equipos de interconectividad a ser instalados en la red.

	Disco Duro	Memoria RAM	Velocidad del procesador
Servidor 1	287 GB	5.57 GB	400 MHz
Servidor 2	318 GB	256 MB	2.2 GHz
Servidor Antivirus	400 MB	128 MB	800 MHz

Tabla 4.19 Características mínimas para los servidores

Otra facilidad que brindan estos equipos es que pueden ser armados de acuerdo a las necesidades del usuario. Permite la capacidad de ampliarlos su confiabilidad ante fallos mediante una fuente de alimentación redundante, ventiladores, memoria y discos que pueden ser adquiridos por separado.

Se pueden ampliar para procesador adicional, y puede llegar hasta 192 GB de memoria; además posee integración con tarjetas *Gigabit Ethernet.* Una de las características más importantes en lo referente a la implementación del proyecto recae en la capacidad de virtualización, importante para brindar la adecuada plataforma para cumplir con las especificaciones definidas en el capítulo tres.

Se recomienda que para los servidores 1 (WEB, FTP, DHCP, DNS, correo electrónico y AAA) y servidor 2 (Voz y video), se consideren dos servidores *HP Proliant ML350G6* para tener características de redundancia en caso de falla de alguno de ellos. Además se sobredimensionan porque estos soportarán la mayor carga de trabajo en la red. En el servidor 2 se considera además una mayor capacidad de memoria debido al procesamiento de voz y video que debe realizar.

El servidor de antivirus, debido a los requerimientos puede ser implementado en el equipo que funcionan actualmente como servidor 1, numeral 2.5.2.1.

A continuación en la tabla 4.20 se presentan las características y costos de los servidores que se recomiendan para la Institución.

Servidor	Características			Complementos		Costo unitario (USD)
	Procesador	Memoria RAM	Tarjeta de red	Disco duro	Fuente de poder redundante	
Servidor 1 y 2	ProcesadorQUAD-CORE (1) Intel® Xeon® Processor E5620 (2.40 GHz, 12MB L3 Cache	2 DDR3-1066, HT, (3GB) + HP PC3-10600 (2GB)	Red Gigabit NC326i PCI-e doble puerto	2 HP 300GB SAS DP HDD	HP 460W HE 12V Hot Fuente de poder para servidor ML350G6	3.285,00
Servidor 3	*Intel Core 2 Quad @ 2.4 Ghz*	4 GB	Realtek RTL 8168/8111 PCI-E Gigabit	Disco duro Samsung Samsung HD322HJ	No posee	0

Tabla 4.20 Características mínimas para los servidores

4.2.4 TELEFONÍA IP

El servicio de telefonía IP se planea a ser implementado por software, por lo que el servidor 2, será utilizado para este propósito. El único complemento que va a ser instalado en este, es la tarjeta para soportar los puertos analógicos que van a servir para conectar a la red para llamadas hacia la red telefónica pública.

Los costos de estas tarjetas se especifican en la tabla 4.21. Se realizó la cotización para los teléfonos IP, sin embargo estos no han sido considerados para el análisis de costos debido a que el precio de estos harían que el costo de la red se incremente volviendo el proyecto inviable económicamente. Debido a esta razón se deja a criterio de la Institución la adquisición o no de éstos equipos.

Se ha escogido a las tarjetas *Openvox* frente a las *Diguim* debido a la recomendación de los proveedores y a que estas presentan mejores

características de confiabilidad cuando están en funcionamiento. Además las tarjetas

Las tarjetas soportan 8 troncales analógicas, que cumplirían los requerimientos de 4 que se especificaron en el capítulo 3, más las líneas que funcionarán como teléfonos directos. Se recomienda además la compra de dos de ellas para el reemplazo en caso de falla.

Equipo	Cantidad	Costo unitario [USD]	Costo Total [USD]
Tarjeta Openvox A800P 8 puertos FXO	2	480,00	960,00
Telefono Grandstream GXP1450	52	138,00	7176,00
Total			8136,00
Total incluido el IVA			**9112,32**

Tabla 4.21 Costos para la Telefonía IP

4.2.5 CÁMARAS IP

Para las camáras IP se recomiendan las Panasonic BLC-111 para interiores y las Panasonic IP BL-C140CE para exteriores. A continuación se presentan las características de las mismas, debido a que cumplen con las características adecuadas para el proyecto y su precio resulta conveniente.

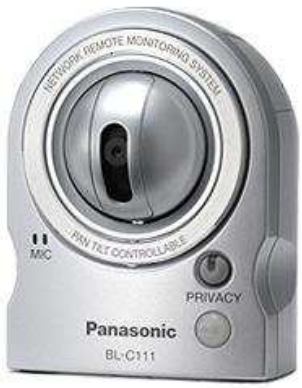


Figura 4.10 Cámara Panasonic BLC - 111

Características

Cámara PTZ

Compresión JPEG (Motion JPEG), MPEG-4

Resolución 640 x 480, 320 x 240 (default), 192 x 144

Máxima tasa de fotogramas 30 cuadros por segundo

Protoclos: TCP, UDP, IP, HTTP, FTP, SMTP, DHCP, DNS, ARP, ICMP, POP3, NTP, UPnPTM, SMTP Autenticacin, RTP, RTSP, RTCP

Zoom 10x zoom digital

Ethernet (10Base-T/100Base-TX)

Figura 4.11 Cámara Panasonic IP BL-C140CE

Compresión: JPEG (Motion JPEG), MPEG-4

Resolución: 640 x 480, 320 x 240 (default), 192 x 144

Calidad de imágen: JPEG, MPEG-4

Máximo cuadros por segundo

IPv4: TCP, UDP, IP, HTTP, FTP, SMTP, DHCP, DNS, ARP, ICMP, POP3, NTP, UPnPTM, SMTP Autenticación, RTP, RTSP*5, RTCP, SSL, HTTPS, TLS

Zoom 10x zoom digital

Ángulo de visión 58 ° horizontal, 45 ° vertical

Intensidad luminosa: 5 a 10,000 lux

Equipo	Número de cámaras	Costo unitario [USD]	Costo total [USD]
Cámara Panasonic BLC - 111	7	174,10	1218,70
Cámara Panasonic IP BL-C140CE	6	270,17	1621,02
TOTAL	13	-	2839,72
Total incluido el IVA			**3180,49**

Tabla 4.22 Costos para las cámaras IP

4.2.6 RED INALÁMBRICA

Para la red inalámbrica se han considerado los equipos HP y los equipos D-link que son los que cumplen con las características especificadas en la tabla 4.32. Se escoge la opción D-link debido a su facilidad de manejo y configuración. Además que el soporte de esta solución es amplio en contraste con los equipos HP, que no se encuentra detallado por los proveedores HP de los cuales su información es sumamente escasa. A continuación se presentan las características de los equipos considerados.

4.2.6.1 D-LINK RANGEBOOSTER N 650 WIRELESS ACCESS POINT DAP-1353

Figura 4.12 Access Point DAP 1353

Puerto de 10/100/1000BASE-TX: IEEE 802.3, IEEE 802.3u, IEEE 802.3ab

Estándar: IEEE 802.11b, IEEE 802.11g, IEEE 802.11n

Modulación: 802.11b: DQPSK, DBPSK, DSSS, y CCK

802.11g y n: BPSK, QPSK, 16QAM, 64QAM, OFDM

Modos de Operación: Access Point, WDS with AP, WDS

Seguridad: WPA, WPA2, 4 SSID Para segmentación de Red, Filtro de dirección MAC, Función de deshabilitar SSID *broadcast*, 802.1Q VLAN, Quality Of Service (QoS)**,** Soporte 802.11x RADIUS, 802.3 af, 802.3

Administración del dispositivo: HTTP, SNMP, Telnet, Soporta protocolo SSL/SSH

4.2.6.2 HP 3Com Airconnect 9550

Figura 4.13 HP 3Com Airconnect 9550

IEEE 802.11n: 2.4-2.484 GHz & 5.15-5.85 GHz; IEEE 802.11a: 5.15-5.85 GHz, IEEE 802.11b/g: 2.4-2.484 GHz

Conectividad: RJ-45 10BASE-T 10/100/1000

Algoritmo de seguridad: WPA2- Enterprise, WPA2- Personal, WPA - Personal, WPA- Enterprise, AES/TKIP; WEP 64/128-bit

Cumplimiento de estándares del mercado: IEEE 802.3i, 802.3u, 802.3ab, 802.3af, 802.11d, 802.1X; IEEE 802.11a, 802.11b, 802.11g, 802.11n draft 2.0; WMM, WPA2/WPA Wi-Fi

Protocolo de Gestión: SNMP v1 & v2c

En la tabla 4.23 se presentan los costos de la solución.

Equipo	Número de equipos	Costo unitario [USD]	Costo Total [USD]
D-LINK RANGEBOOSTER N 650 ACCESS POINT DAP-1353	7	183,79	1286,53
Total incluido el IVA			**1440,92**

Tabla 4.23 Costos de los Access Points

4.3 COSTOS DE OPERACIÓN

Para el adecuado mantenimiento de la red se deben tomar en cuenta además los costos de operación y mantenimiento que se estiman en la tabla 4.24.

Servicio	Descripción	Costo USD
Internet	3072 Kbps Empresa Claro (Convenio con la Institución)	151,20
Antivirus	Valor de las licencias para 100 equipos (2100 anual)	175 mensual
Administrador	Sueldo estimado de administrador de red trabajando 8 horas incluido beneficios de ley	850
TOTAL mensual		**1176,20**

Tabla 4.24 Costos de operación

4.4 COSTO TOTAL.

A continuación se presenta el costo total[41] de la red tanto en la parte activa como pasiva.

Item	Costo USD
Sistema de Cableado Estructurado	27624,57
Equipos de Conectividad	40080,82
Firewall	4116
Servidores	7358,40
Telefonía IP (módulo FXO + 57 teléfonos)	9112,32
Cámaras IP	3180,49
Red Inalámbrica	1440,92
TOTAL	**92913,52**

Tabla 4.25 Costos total de la red multiservicio

[41] Estos precios incluyen el IVA

CAPÍTULO 5.

CONCLUSIONES Y RECOMENDACIONES.

5.1 CONCLUSIONES.

• El análisis de la situación actual de la red del Instituto Tecnológico Superior Central Técnico, permitió encontrar las debilidades en ella. Fue posible evaluar el desempeño de utilización de la red, con el objetivo de optimizar los servicios y recursos que esta provee.

Este análisis constituye el punto de partida para brindar una nueva perspectiva para el sistema tecnológico de la Institución y que facilite realizar el rediseño pasivo como activo de la red, dimensionamiento de servidores y proveer la escalabilidad de estos sistemas.

• Se estableció el rediseño de la red de datos en función de un esquema modular en capas jerárquico centralizado con topología en estrella, estableciendo dos niveles: la capa de acceso – distribución y la capa de núcleo. Las principales ventajas de este esquema es brindar escalabilidad, seguridad, y que sea adaptable a las necesidades de los usuarios, contemplando de este modo, que si existe la necesidad de generar nuevos puntos de red los mismos no alterarán el diseño y utilizarán el esquema de conexión ya existente.

• El diseño establecido provee redundancia a nivel de equipos conectividad, y enlaces de comunicación (fibra óptica), este mecanismo evitará que los recursos existentes de la red se vean afectados simultáneamente, lo que provocará que siempre exista un equipo o medio de transmisión de respaldo.

• La migración hacia la telefonía IP trae beneficios, por ejemplo desde el punto de vista económico, disminuye el gasto en líneas telefónicas utilizadas; además brinda flexibilidad para la instalación de nuevas extensiones

telefónicas. Esta situación no se puede dar al momento con la red telefónica analógica en funcionamiento, a la que ni siquiera se le puede dar el mantenimiento adecuado debido a que la persona que realizó la instalación se encuentra fuera de la ciudad. Además en caso de ser necesario se pueden instalar otros dispositivos adicionales como por ejemplos teléfonos por software o añadir equipos analógicos a la red mediante adaptadores. Tanto la infraestructura como la central telefónica tienen la suficiente capacidad para esta expansión.

- Acceder a la red de la Institución a través de la red inalámbrica permitirá a los diferentes usuarios tener la posibilidad de utilizar sus equipos personales para poder desempeñar sus actividades, además que permite el acceso en sitios donde implementar la red cableada resulta complicado o simplemente la implementación de esta signifique un desperdicio de recursos. Además se puede brindar los servicios de red a los usuarios temporales como invitados o a los estudiantes que utilicen los laboratorios de la Institución

- Brindar una adecuada calidad de los servicios que la Intranet proporcionará, es uno de los objetivos de este proyecto. Para esto fue necesario dimensionar los servidores para que la red sea completamente escalable y versátil. La plataforma informática así como el software seleccionado se recomendó para obtener una estandarización en todos los servicios, y operar con un solo tipo de soporte para los servidores.

- Implementar los servicios básicos de la intranet tales como correo, DNS, DHCP y demás, permiten brindar la plataforma adecuada para implementaciones de servicios integrados futuros. En el caso de una Institución educativa estos servicios pueden ser de educación virtual, repositorio digital entre otros, brindando a la Institución la oportunidad de aprovechar el desarrollo tecnológico en el proceso educativo.

- Asegurar la compatibilidad en los equipos de conmutación, que utilicen una tecnología estándar sustentará el diseño y rendimiento de la red. La selección de los equipos se basó en función de la escalabilidad, confiabilidad, cumplimiento de las características técnicas, y la disponibilidad de los productos en el mercado.

La alternativa tecnológica seleccionada fue la propuesta por HP (antes conocida como 3COM) la cual constituye la más viable desde el aspecto económico como técnico ya que esta no trabaja con protocolos propietarios y las funcionalidades de los equipos son estándares para trabajar con cualquier tecnología. Esta alternativa permite reutilizar algunos equipos activos 3COM por ejemplo para los laboratorios.

- El diseño provee escalabilidad tanto a nivel de hardware y de software. Luego del levantamiento de la información de la Institución y de conversaciones con los diferentes integrantes de la comunidad educativa, se llegaron a los valores mencionados en el diseño en base a la estimación de crecimiento del uso de los servicios de la red a partir de la implementación del proyecto.

El Sistema de Cableado Estructurado es capaz de soportar un número de servicios mayor a los que se encuentran actualmente en funcionamiento por lo que no sería un impedimento para el aumento de aplicaciones a futuro. Los equipos de conectividad tienen puertos adicionales a los que serán instalados para proveer estos servicios a los nuevos usuarios sin necesidad de compras necesarias, se ha estimado un valor de 30% de crecimiento, y pueden funcionar a 1 Gbps, para cuando las tarjetas de red de los equipos posean estas características.

Los servidores han sido dimensionados de tal manera que se puedan instalar diferentes aplicaciones a futuro, como por ejemplo aulas virtuales, sin que esto comprometa los recursos de las aplicaciones ya previstas en el proyecto. Las plataformas sobre los que se implementarán los servicios son escalables en su totalidad para soportar una mayor carga de tráfico

- La mayoría de equipos de conectividad presentes actualmente en la Institución no presentan las características necesarias para poder integrarlos en la nueva red; sin embargo algunos como por ejemplo los switches 3Com especificados en el capítulo 2, pueden ser utilizados para acceso en sitios donde se encuentra únicamente un punto de red como es el caso de los laboratorios, debido a que son completamente compatibles con los nuevos equipos. El servidor 1, es reutilizado para brindar el servicio de antivirus en la nueva red debido a que posee las características adecuadas para este fin.

5.2 RECOMENDACIONES.

• Se recomienda que para realizar el diseño, análisis e implementación de una red, es necesario que la planificación este sustentada en estándares y normativas internacionales que conlleve en una ambiente real a la optimización de los recursos, y que los resultados sean satisfactorios, de tal manera se evita sobredimensionar de una manera exagerada los enlaces, los equipos de interconectividad y las interfaces para su conexión.

• Se sugiere que la fibra óptica sea instalada de manera subterránea; sin embargo, esta puede ser canalizada vía aérea en los sitios donde sea necesario, respetando las normas establecidas y cuidando la integridad del medio de transmisión. Esto con el fin de evitar el corte accidental o provocado de los enlaces de comunicaciones, a lo que se puede añadir un nivel de redundancia tal como se especificó en el diseño.

• Para la red inalámbrica, se recomienda la realización de pruebas con los equipos activos en funcionamiento con el fin de determinar puntos que no posean cobertura, incluso la ubicación más adecuada de los equipos con el propósito de brindar total conectividad en los sitios establecidos para el efecto.

• Como parte de la administración de la red, es fundamental tener la documentación y memoria técnica de la red pasiva y activa. La documentación debe contener las políticas de administración, seguridad, claves de acceso, configuraciones de los equipos, contratos con proveedores, SLAs, y manuales de usuarios de los diferentes programas computacionales.

Será responsabilidad del administrador de la red tener esta información disponible, para poder realizar cambios en la infraestructura rápidamente así como detectar fallas o errores en la misma.

• Se recomienda como una alternativa proponer un sistema de administración para el monitoreo de los equipos, debido a que los equipos seleccionados soportan el protocolo de administración SNMP. Este software de

administración facilitará y reducirá el tiempo para encontrar errores, suministrando una comunicación fiable en la red.

Inclusive se debería tener un sistema de monitoreo de tráfico de red para poder generar reportes y observar si la Intranet y el enlace de Internet no se están saturando, y determinar si no se están desperdiciando los recursos.

- Es necesario que las políticas tanto de seguridad como de uso de la red, sean difundidas masivamente entre los usuarios de la red, con el fin de crear una cultura de manejo y ambientación en el uso de la misma. Estas deberán tomar en cuenta todos y cada uno de los aspectos organizativos inherentes a las actividades que cumple en Instituto.

- Se recomienda la contratación de personal calificado para atender las diferentes necesidades de operación y mantenimiento de la red. O en su defecto capacitar adecuadamente a las personas que en el momento se encuentran a cargo del funcionamiento de la misma. En la actualidad no existe una sistematización en el manejo de incidentes por lo que se realiza de una manera precaria y disminuye la productividad de la Institución en general.

- Respecto a los sistemas de protección eléctrica, se recomienda en especial la protección de los Cuartos de Telecomunicaciones y de la Sala de equipo, debido a que poseen los equipos más sensibles de la red. Para el efecto se sugiere el uso de tomas eléctricas polarizadas en cada uno de los racks; conectadas a su vez a un sistema de puesta a tierra; además de la protección de los equipos mediante un UPS en caso de suspensión del servicio eléctrico. Para los equipos de los usuarios como método de contingencia frente a problemas eléctricos se puede disponer de reguladores de voltaje.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS

[L1] **STALLINGS**, Williams, *"Comunicaciones y Redes de Computadores"*, Sexta edición. Prentice Hall. 2003.

[L2] **TANEMBAUM**, Andrew, *"Comunicaciones y Redes de Computadoras"*, Tercera edición. Prentice Hall. 1998.

[L3] **FREEMAN**, Roger, *"Telecommunication System Engineering"*. Tercera Edición, Wiley-Interscience. 2004.

[L4] **COMER**, Douglas E; **STEVENS**, David L, *"Interconectividad de Redes con TCP/IP"*. Volumen I. Tercera edición. Prentice Hall. 2000.

[L5] **MEGGELEN**, Jim Van; **SMITH**, Jared, *"Asterisk, The future of telephony"*. O'Reilly. 2005.

[L6] **ZIEGLER**, Robert, *"Firewalls LINUX", Primera edición*. Prentice Hall. 2003.

PUBLICACIONES (REVISTAS, PAPERS, ETC)

[P1] ANSI/TIA/EIA STANDARD Commercial Building Telecommunications Cabling Standard, RNDS, Buenos Aires Argentina, n 59, febrero marzo 2011.

[P2] DTC Conectividad, Dlink, D-Link Technology Institute, Estados Unidos, abril 2009.

[P3] Networking Essentials, Cisco Academy, Estados Unidos, 1998.

[P4] Videoseguridad IP Revista negocios de seguridad, RNDS, Buenos Aires Argentina, n 59, febrero marzo 2011.

[P5] DI Training - NetDefend Update , Dlink, D-Link Technology Institute, Estados Unidos, abril 2007.

[P6] SISTEMA HÍBRIDO IP KX-TDA15, KX-TDA30, KX-TDA100, KX-TDA200, Panasonic, Barcelona - España, 2005.

[P7] REGLAMENTO DE USO DE LAS HERRAMIENTAS INFORMÁTICAS Y EQUIPOS DE CÓMPUTO DEL GOBIERNO PROVINCIAL DEL AZUAY, Gobierno Provincial del Azuay, Cuenca - Ecuador, octubre 2007.

[P8] ANSI/TIA/EIA STANDARD Commercial Building Telecommunications Cabling Standard, RNDS, Buenos Aires Argentina, n 59, febrero marzo 2011.

[P9] Instalación y configuración de APACHE un servidor Web Gratis, Universidad del Norte, Colombia, n 01, 2002.

[P10] Instalación y configuración del Servidor *ftp PureFTP*, Universidad de León,León, España, n 01, 2006.

[P11] Modelo realista para la función de coordinación distribuida del estándar IEEE 802.11b, Universidad de Tarapacá, Arica, Chile, n 01, marzo agosto 2005.

[P12] Estándar IEEE 802.1 X de las WLAN, Universidad Tecnológica Nacional, Tucumán, Argentina, n 01, 2009.

[P13] Evaluación del Desempeño de la Tecnología ADSL en la Red de Internet banda Ancha, Universidad Rafael Belloso Chacín, No 1,Maracaibo, Venezuela, 2005.

[P14] Tyco Electronics, ANSI/TIA 568 C

[P15] Comparación de servidores web, Comparison of web server software Source: http://en.wikipedia.org/w/index.php?oldid=435430555, 2011

[P16] Comparación de servidores ftp, Creative Commons, Comparison of FTP server software at the Open Directory Project, 2011

[P17] Comparación de servidores mail, Creative Commons, Comparison of mail servers Source: http://en.wikipedia.org/w/index.php?oldid=437623084, 2011

[P18] Comparación de servidores radius, Creative Commons, List of RADIUS servers Source: http://en.wikipedia.org/w/index.php?oldid=424417556, 2011

TESIS

[T1] **BRAVO**, Sergio, *"Estudio y puesta en servicio de una central telefónica – IP Híbrida para la Central Hidroeléctrica Pullinque – subsidiaria de ENEL"*, Cid, Valdivia - Chile 2006

[T2] **QUELAL,** Josue, *"Rediseño de de red de comunicaciones de la Empresa Metropolitana de Obras Públicas (EMOP-Q) para soportar aplicaciones de voz sobre IP (VoIP)",* EPN, Quito – Ecuador, marzo 2010

[T3] **TRELLES**, César; **VALLEJO**, **Ricardo,** *"Diseño de la Intranet de la empresa MEGAREDES Cía. Ltda"*, EPN, Quito – Ecuador, marzo 2009

[T4] **CARRASCO,** Soraya; **PARRA,** Esther, *"Reingeniería de una red de datos corporativa para la Univesidad de las Américas, sede Quito, Análisis, lineamiento y aplicación",* EPN, Quito – Ecuador, junio 2007.

[T5] **MATANZO** Arturo *"Implementación del Protocolo CHAP en un Sistema de Seguridad para Redes WLAN "*.Universidad de las Américas Puebla, México 2006.

[T6] **MONTES** Eduardo, *"Estudio de la Migración del Estándar 802.11 al estándar 802.16 en zonas rurales"*. Pontificia Universidad Católica del Perú. Lima Perú 2008.

[T7] **RODRÍGUEZ** José, *"Gestión de Recursos para Servicios de Tiempo Real sobre Redes WLAN"*. Universidad de Granada. Granada España 2009.

[T8] **CONDE** José, **LANDETA** Cristian, *"Diseño de una Red Convergente de Servicios de voz, datos y video para las diferentes dependencias de la Industria Textil INDUTEXMA aplicando tecnología IP"*. EPN. Quito Ecuador 2010.

[T9] **PALACIOS** Erick, *"Redes Inalámbricas de 2G, 2,5G y 3G"*.Universidad de las Américas Puebla, México 2006.

[T10] **VILLACÍS** Andrés, *"Diseño de un Centro de Provisión de Servicio de Internet con acceso de última milla Inalámbrico utilizando el Estándar IEEE 802.11 para el parque Industrial de Ambato"*. EPN. Quito Ecuador 2007.

[T11] **ROMAN** Francisco, *"Reingeniería de la INTRANET de la Empresa TECNOMEGA C.A".* EPN. Quito Ecuador 2008

[T12] **CEDEÑO** Simón, **ROBALINO** Jorge, *"Rediseño de la infraestructura del proveedor de servicios de internet OnNet S.A. para la optimización del servicio en el Distrito Metropolitano de Quito"*, EPN, Quito, 2008

[T13] **ULLARI** Omar, **SIGUENZA** Hernán, "*Normas 802.11a, 802.1b, 802.1g*". UPS, Cuenca Ecuador 2006.

[T14] **VÁSQUEZ,** Juan Pablo, "*Seguridad en Redes Inalámbricas de Área Local WLAN*". Universidad de Costa Rica, San José Costa Rica 2005.

[T15] **VÁSQUEZ,** Juan Pablo, "*Diseño de una Red Local Inalámbrica utilizando un Sistema de Seguridad basado en los protocolos WPA y 802.1x para un Complejo Hotelero*". Pontificia Universidad Católica del Perú, Lima Perú 2007.

FOLLETOS

[F1] **JIMÉNEZ**, María Soledad, Escuela Politécnica Nacional, *"Teoría de Comunicaciones",* 2009.

[F2] **GONZÁLEZ**, Fabio, Escuela Politécnica Nacional, "Sistemas de Cableado Estructurado", 2009.

[F3] **HIDALGO**, Pablo, Escuela Politécnica Nacional, *"Redes TCP/IP",* 2009.

[F4] **HIDALGO**, Pablo, Escuela Politécnica Nacional, *"Redes de Área Local (LAN)",* 2009.

[F5] **ÁVILA**, Nelson, Escuela Politécnica Nacional, *"Telefonía IP",* mayo 2009.

[F6] **SINCHE**, Soraya, Escuela Politécnica Nacional, *"Redes de Área Local Inalámbricas",* mayo 2009.

[F7] **BERNAL** Iván, Escuela Politécnica Nacional, *"Comunicaciones Inalámbricas",2009.*

REFERENCIAS DE INTERNET

[W1] *"Cable STP: Montar una red, elementos necesarios"*
URL: http://www.configurarequipos.com/doc858.html

[W2] **MARTÍNEZ**, Josuet, *"Cableado para redes: Cable Coaxial"*
URL: http://cableadopararedes.blogspot.com/2011/05/cable-coaxial.html

[W3] *"Fibra Óptica"*
URL: http://www.monografias.com/trabajos16/fibras-opticas/fibras-opticas.shtml

[W4] *"Fibra óptica... la luz al servicio de las telecomunicaciones"*
URL: http://telecomjournalelsalvador.blogspot.com/2010/05/fibra-optica-la-luz-al-servicio-de-las.html

[W5] **SYSCOM Tcnologías**, *"VoIP"*
URL: http://www.syscom.com.mx/tecnologias_voip.htm

[W6] *"Medios de transmisión: La fibra óptica"*
URL: http://www.opcionweb.com/index.php/2007/04/30/medios-de-transmision-la-fibra-optica

[W7] **DELL** , *"Documentation"*
URL:http://support.dell.com/support/edocs/network/pc6024/sp/ug/cables_p.htm

[W8] *"Instercom & Cia. Ltda"*
URL: http://www.instercom.com/tienda/index.php?cPath=40_21_73

[W9] *"Sistemas telecomunicaciones, Concepto IP nuevas redes Integradas"*
URL: http://www.plusformacion.com/Recursos/r/Sistemas-telecomunicaciones-Concepto-IP-nuevas-redes-Integradas

[W10] *"SolutionBase: Strengthen network defenses by using a DMZ"*
URL: http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/5756029

[W11] *"Request for comments"*
URL: http://es.wikipedia.org/wiki/Request_for_Comments

[W12] *"Modem motorola"*
URL: http://articulo.mercadolibre.com.ec/MEC-8209310-vendo-barato-motorola-cable-modem-sbv5121-usado-_JM

[W13] *"Cisco 2600"*
URL: http://www.depaginas.com.mx/fotosde_Cisco_2600.htm

[W14] *"DLink DES 1008"*
URL: http://anuncios.ebay.es/compraventa/switch-d-link-10-100-fast-ethernet-modelo-des-1008d/5458746

[W15] *"Cnet"*
URL:http://www.fixya.com/support/t4765717cnet_power_switch_cnsh_1600power_light

[W16] *"3com baseline"*
URL:http://www.synaptech.com/catalog/index.php?main_page=index_&cPath=49_52

[W17] *"3com"*
URL: http://www.zdtronic.com/NETWORKING/3COM-NETWORKING/3COM-3CR17661-91-3CR17661-91-US-4200G-24-PORT-LAYER-3-SWITCH.html

[W18] *"DLink DWL 2100ap"*
URL: http://seidicalsac.com/productos.php?id=10

[W19] *"Lexmark e260"*
URL:http://www.lexmark.com/lexmark/product/home/156/0,6970,245102346_653293751_1290303644_es,00.html?tabId=1

[W20] *"HP LaserJet MI522nf"*
URL:http://www.tiendatinta.com/default.asp?maquina=HP_LaserJet_MFP_M1522nf

[W21] *"HP Laserjet 1320n"*
URL: http://opiniones.terra.es/impresoras/opiniones_hp-laserjet-1320_18320_rendimiento.htm

[W22] *"HP Laserjet 1300"*
URL: http://printers.bizrate.com/hp-laserjet-1300-laser-printer--pid7434054/

[W23] *"HP Color LaserJet CP3525dn"*
URL: http://www.lacasadelasimpresoras.com/index.php?cPath=42_156

[W24] *"Epson LX-300+"*
URL: http://guayaquil.olx.com.ec/impresora-matricial-epson-lx-300-210-iid-103451987

[W25] *"KXTDA 200"*
URL: http://chile.lapapa.cl/lista_historicas/262463

[W26] *"TVM50"*
URL: http://www.dasia.com.my/Communication/Voicemail/tvm50.aspx

[W27] *"Panasonic KX TS500MXW"*
URL:
http://www.doubleacatalogue.com/product_detail07.aspx?gid=7140

[W28] *"Panasonic_KX_T7730RU"*
URL:http://www.bestoffice.ru/part/sta/STA_PANASONIC/Panasonic_KX_T7730RU.html

[W29] *"Panasonic KX – T7436"*
URL: http://www.voicesonic.com/customer/Panasonic_phone_system-905-Digital_Phones.html

[W30] *"Panasonic KY –FHD351"*
URL: http://www.kxtda.com.ve/fax-papel-bond-termico/fax-panasonic-papel-bond-termico.html

[W31] *"Rack"*
URL:http://www.cein.ec/web/index.php?option=com_content&task=view&id=18&Itemid=42

[W32] *"Gabinete"*
URL:http://www.martel.com.ec/productos_detalle.php?id=313&idiom=1&categ=4&subcateg=13

[W33] *"Modelo Jerárquico"*
URL: http://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/

[W34] *"DMZ"*
URL: http://cojala.blogspot.com/2009/09/zona-desmilitarizadas-dmz.html

[W35] *"DMZ"*
URL: http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/5756029

[W36] *"Wi-Fi Alliance: Discover and Learn"*
URL: http://www.wi-fi.org/discover_and_learn.php

[W37] *"Panasonic KY –FHD351"*
URL: http://www.kxtda.com.ve/fax-papel-bond-termico/fax-panasonic-papel-bond-termico.html

[W38] Facomallas URL :
URL:http://www.facomallas.com/arppa.html

[W39] **BERNAL**, Iván , *"Prueba V"*
URL:http://clusterfie.epn.edu.ec/ibernal/html/CURSOS/AbrilAgosto06/Trafico/Pruebas/prueba_5.htm

[W40] *"Erlang B Calculator"*
URL: http://www.erlang.com/calculator/erlb/

[W41] *"Asterisk"*
URL: http://www.asterisk.org

[W42] *"Elastix"*
URL: http://www.elastix.org

[W43] *"Open Meeting"*
URL:http://groups.google.com/group/zonanorte_lug/browse_thread/thread/e4f442241bc633df?pli=1

[W44] "*El estándar IEEE 802.11 Wireless LAN."*
URL: http://dis.eafit.edu.co/cursos/st0059/material/08-802.11-Francisco-Lopez-Ortiz-res.pdf

[W45] ESCUDERO Alberto, *"Estándares en tecnologías inalámbricas".*
URL:http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/11_es_resolucion-de-problemas_guia_instrucciones_v02.pdf

[W46] *"IEEE 802.11".*
URL: http://gsyc.es/~mortuno/rom/02-802.11.pdf

[W47] BARAJAS Saulo, *"Protocolos de seguridad en redes inalámbricas".*
URL: http://www.saulo.net/pub/inv/SegWiFi-art.htm

[W48] *"Redes en Educación 2 Redes WAN"*.
URL: http://hera.cnice.mec.es/redes2/contenido/Pdf/mod1_3.pdf

[W49] *"Instalación de un servidor DNS con Bind".*
URL: *http://www.liberaliatempus.com/dns-bind.html.*

[W50] "Servidor de de Nombres de Dominio (DNS) en CentOS."
URL:http://www2.linuxparatodos.net/web/comunidad/base-de-conocimiento/-/wiki/Base+de+Conocimiento/Servidor+de+Nombres+de+Dominio+%28DNS%29+en+CentOS

[W51] *"DNS"*
URL:http://eisc.univalle.edu.co/materias/Administracion_De_Redes_Y_Servidores/material/07_ARS_DNS.pdf

[W 52] Henning Brauer, Trad. Iván Juanes Prieto , *"MI vida con djbdns"*.
URL:http://lifewithdjbdns.org/es/#Los%20componentes%20de%20djbdns:%20c%C3%B3mo%20interact%C3%BAan

[W53] *"PowerDNS"*.
URL: http://en.wikipedia.org/wiki/PowerDNS

[W 54] *"MYDNS".*
URL:
http://www.linuxparty.com/modules.php?name=News&file=article&sid=4442

[W55] CentralTECH, *"Linux original Courseware LX4".*
URL: http://es.scribd.com/doc/7417942/74/Exim

[W56] EMAGISTER, "*Wikilearning*".
URL:
http://www.wikilearning.com/articulo/servicio_de_correo_basado_en_qmail_smtp-entendiendo_qmail/7085-2

[W57] Wikipedia, *"Qmail"*.
URL: http://es.wikipedia.org/wiki/Qmail

[W58] Wikipedia, "*Lighttpd".*
URL: http://es.wikipedia.org/wiki/Lighttpd

[W59] Wikipedia, "*Thttpd".*
URL: http://es.wikipedia.org/wiki/Thttpd

[W60]Zelu Jose Luis, "*VSFTPD"*
URL: http://usuarios.multimania.es/zelu/descargas/vsftpd.pdf

[W61] ECURED, "*ProFTPD"*
URL: http://www.ecured.cu/index.php/Proftpd
[W62] Linux para Todos, *"Servidor DHCP."*
URL:
http://www.linuxparatodos.net/geeklog/staticpages/index.php?page=servidor-dhcp
[W 63] "Servicios de Videoconferencia en Redes IP."
URL: http://es.scribd.com/doc/14971169/Servicios-de-VideoConferencia-en-Redes-IP

[W64] "Rack de piso"
URL: http://sinfotecnia.com/prestashop/product.php?id_product=11

[W65] *"Modelo Jerárquico de red"*
URL: http://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/

[W66] "Zona desmilitarizada"
URL: http://ticdeveloper.blogspot.com/2008/10/implemente-una-zona-desmilitarizada-dmz.html

[W67] "*Diseño de redes con fibra óptica."*
URL: http://www.alsurtecnologias.com.ar/fibra-optica.php

[W68] "*Estudio de códecs de compresión MPEG4 para su aplicación a la videovigilancia ."*
URL: http://personales.gan.upv.es/jlloret/pdf/ursi2005-mpeg4.pdf
[W69] "*Toll Quality."*
URL: http://bandwidth.com/wiki/article/MOS_score
[W 70]"*Red Hat Inc, Notas de lanzamiento Fedora 13."*
URL:
Http://docs.fedoraproject.org/esES/Fedora/13/html/Release_Notes/index.html#sect-Release_Notes-Hardware_Requirements
[W 71] *"Apache"*
URL: Http://www.apache.org
[W 72] *"Comparación antivirus 2011"*
URL: Http://www.pacasalvo.com
[W 73]"*Disco video conferencia y profundidad de bits"*
URL:http://www.jaguar.edu.co/z_aprendizaje/tutoriales/imagenDigital/profundidad.php